

Security Annual

2020 EDITION

OUTLOOK FOR 50 CYBER CONTROLS

PUBLISHED BY TAG CYBER

Interviews with
Cyber Luminaries

Handbook
& Reference Guide

LEAD AUTHOR

Ed Amoroso

RESEARCHERS

Matt Amoroso
Felix Andersen
Liam Baglivo
Pete Cornell
Shawn Hopkins
Andy McCool
Kelly McCool
Miles McDonald
Stan Quintana
Katherine Teitler

MEDIA

Matt Amoroso
Laura Fanelli
Miles McDonald

DESIGN

Wkshps
Alicia Amoroso
Miles McDonald
Rich Powell

FACILITIES

WeWork, NYC

TAG CYBER LLC

P.O. Box 260
Sparta, NJ 07871

Copyright ©2020 TAG Cyber LLC.
All rights reserved.

This publication may be freely reproduced, freely quoted, freely distributed, or freely transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or any information storage and retrieval system without need to request permission from the publisher, so long as the content is neither changed nor attributed to a different source.

Security experts and practitioners must recognize that best practices, technologies, and information about the cyber security industry and its participants will always be changing. Such experts and practitioners must therefore rely on their experience, expertise, and knowledge with respect to interpretation and application of the opinions, information, advice, and recommendations contained and described herein.

Neither the author of this document nor TAG Cyber LLC assume any liability for any injury and/or damage to persons or organizations as a matter of products liability, negligence or otherwise, or from any use or operation of any products, vendors, methods, instructions, recommendations, or ideas contained in any aspect of the 2020 TAG Cyber Security Annual volumes.

The opinions, information, advice, and recommendations expressed in this publication are not representations of fact, and are subject to change without notice. TAG Cyber LLC reserves the right to change its policies or explanations of its policies at any time without notice.

To the Reader:

Welcome to the new 2020 Edition of the Security Annual from TAG Cyber. As you've no doubt already noticed, this year's work looks different from what we've done in the past – and hopefully, you'll agree it's so much better! Liam Baglivo and I decided last year that we wanted to improve the shape and feel of our work, commensurate with our goal of always exceeding your expectations (and our own too). After a bit of searching, we discovered the fantastic design team at WKSHPs in Manhattan. And after a couple of meetings in their cool office (polished plywood floor and rows of gorgeous books in their conference room), we agreed to work together on this book. And that's how the new 2020 work you have in front of you was born.

As always, our goal is to democratize world class cyber security industry research and advisory material to the masses (that's you, by the way). We thus provide the narratives, articles, and interviews of this book as an aggregate collection of cyber security industry market reporting. Each section is intended to be crazily useful and insanely free and open source. Every business advisor I've engaged during the past three years has begged me to sell our reporting. Yet we remain convinced that the information should be free. Recall the observation from Stewart Brand of Whole Earth Catalogue fame: "Information wants to be free, because the cost of getting it out is getting lower and lower all the time." He was right.

The themes of our 2020 work remain consistent with observations from past years: Cloud services continue to improve and become more secure (Capital One notwithstanding); mobility is more embedded in day-to-day computing habits; perimeters are being dissolved under the new flag of Zero Trust Security (ahem, coined at Forrester); automation continues to drive more streamlined processes, especially in the hallowed Security Operations Center (SOC); and the use of artificial intelligence – deep learning, in particular – is coming into its own as a legitimate means for detecting previously observed malware and attacks based on learned patterns. Yes – 2020 is likely to shape up as another truly exciting year in cyber security.

And yet – there remains much that is sadly depressing about our industry. One issue is that new security start-ups are being spawned at an unsustainable pace and with bad mission statements. Here’s a common refrain: “I learned cyber while running an elite military group,” claims the founder of ACME Cyber, “so I founded ACME to cash in big time. Uh, did I really say that last thing out loud? Can we cut that out?” OK – so perhaps this is a bit of an exaggeration, but you get the idea. My advice to new companies: Figure out what you honestly believe in. Then decide if a cyber security company is consistent with your beliefs. What you do is less important than why you do it. Making money is no reason to start a company. Take it from me.

Unlike in past years, we did not make any changes to the TAG Cyber Fifty Controls. The control categories still worked for our analysis, albeit with different emphases in our commentary. (We try not to invent new categories each year for marketing purposes, like Gartner). And most of our Trend Charts are also largely consistent with previously published graphs – again, with some adjustments commensurate with observations made in 2019. Our goal is for these chapters to become a useful roadmap for your strategy and tactics in building a cyber defense. Throughout 2020, we’ll be issuing these chapters as individual Market Reports. So, watch for weekly reissuance on social media and the TAG Cyber website – which we redesigned this past year.

And on this topic of websites, we decided this year to embed and maintain our massive list of cyber security vendors in a database accessible on-line. The TAG Cyber website thus includes a link for users to gain access to the database and to run basic queries to find companies of interest. Each of the fifty control discussions in this volume include lists of companies that cross-reference with the topic of that chapter – so this will provide an initial guide. Security engineers and other interested parties can thus easily figure out which vendors are providing GRC support, or which happen to mention Wisconsin in their title, and so on. We are building more advanced query capability now. I hope it helps you. Oh – and it’s free, of course.

To close, I will offer my annual pep talk: I wish I could just say to keep up the good work, and many of you are maintaining excellent security protection for your organization (or at least yourself). But many of you are not, especially in the United States Government, where the level of cyber security support is openly acknowledged to lag. If you are in this category, then please do whatever is necessary to step up your game. This volume provides a basis for action by cyber defenders to significantly improve their protections. I know that most security schemes are weak for other reasons – politics, budget, personality, bad bosses, and on and on. But this is no time for excuses: Use the work provided here to take things to the next level. Start today.

Dr. Edward G. Amoroso, September 2019
Chief Executive Officer, TAG Cyber LLC
Fulton Street Station on Broadway

ENTERPRISE CONTROLS

- 18** IDPS/Deception
 - 29** DLP and UEBA
 - 37** Firewall Platforms
 - 49** Network Access Control
 - 52** Unified Threat Management
 - 56** Web Application Firewall
 - 59** Web Fraud Prevention
 - 70** Web Security Gateway
-

NETWORK CONTROLS

- 73** CA/PKI Solutions
 - 77** Cloud Security/CASB
 - 84** DDOS Security
 - 91** DMARCsec Email/DMARC Security
 - 99** SDNsec BGP/DNS/SDN Security
 - 102** Network Monitoring
 - 106** Secure File Sharing
 - 114** VPN/Secure Access
-

ENDPOINT CONTROLS

- 117** Anti-Malware Tools
 - 125** Endpoint Security
 - 132** HW/Embedded Security
 - 140** ICT/IoT Security
 - 147** Mainframe Security
 - 151** Mobile Security
 - 154** Password/Privilege Management
 - 165** Multi-factor Authentication
 - 173** Voice Security
-

GOVERNANCE CONTROLS

- 176** Digital Risk Management
 - 180** Bug Bounty Support
 - 183** Cyber Insurance
 - 190** GRC and Risk Management
 - 193** Incident Response
 - 200** Penetration Test/Simulation
 - 211** Security Analytics/SOC Hunt Tools
 - 223** SIEM Platform
 - 229** Threat Intelligence
-

DATA CONTROLS

- 240** Application Security
 - 250** Content Protection
 - 254** Data Destruction
 - 265** Data Encryption
 - 279** Digital Forensics
 - 285** IAM and Identity Platforms
 - 293** Compliance Support
 - 305** Vulnerability Management
-

INDUSTRY CONTROLS

- 312** Industry Analysis
 - 315** Information Assurance
 - 319** Managed Security Services
 - 326** Security Consulting
 - 333** Security Career Support
 - 337** Security R&D
 - 344** Security Training/Awareness
 - 351** Security VAR Solutions
-

ENTERPRISE CONTROLS

- 21** Deep Instinct
 - 25** Capsule8
 - 33** Attivo Networks
 - 42** Garrison
 - 45** Corsa Security
 - 62** XTN Cognitive Security
 - 65** Tala Security
-

NETWORK CONTROLS

- 80** CloudPassage
 - 87** Valimail
 - 95** Mimecast
 - 109** Egress
-

ENDPOINT CONTROLS

- 121** Bitdefender
 - 128** Cybereason
 - 136** Bayshore Networks
 - 143** Mocana
 - 157** CyberArk
 - 161** Remediant
 - 169** HYPR
-

GOVERNANCE CONTROLS

- 187** Willis Towers Watson
 - 197** XM Cyber
 - 203** ExactData
 - 207** SafeBreach
 - 215** InQuest
 - 219** Respond Software
 - 226** Jazz Networks
-

DATA CONTROLS

- 233** IronNet Cybersecurity
 - 237** HYAS
 - 243** Vicarius
 - 247** TrueFort
 - 257** ObserveIT
 - 261** Sertainty
 - 268** Cord3
 - 272** InfoSec Global
 - 275** Varonis
 - 282** BlackRidge Technology
 - 289** QOMPLX
 - 296** AttackIQ
 - 301** ControlCase
 - 308** CYR3CON
-

INDUSTRY CONTROLS

- 322** Edgewise
 - 329** Digital Defense, Inc.
 - 340** Symantec
 - 347** Cybrary
 - 355** TenFour
 - 359** White Ops
 - 363** Onapsis
-

SUMMARY OF CONTROLS

- 367** TAG Cyber Security Controls
-

2020 TAG CYBER SECURITY ANNUAL

OUTLOOK FOR FIFTY CYBER SECURITY CONTROLS

**PREPARED BY THE TAG CYBER SECURITY ANALYSTS
TEAM LEAD: DR. EDWARD G. AMOROSO**

The underlying basis for our expert industry research and advisory work at TAG Cyber is our periodic table of cyber security controls. The table includes fifty different aspects of enterprise cyber security management that we deem to be essential to any modern information risk reduction program. The table is organized into six categories, which were created to highlight the purpose of each control in the context of an enterprise cyber security protection program.

The original fifty controls were first introduced and explained in Volume 1 of the 2017, 2018, and 2019 TAG Cyber Security Annuals, along with cross-referenced listings of world-class cyber security vendors supporting each control. Readers are advised to take time to review those previous volumes to build familiarity with the TAG Cyber research approach. These previous reports are available as free PDF downloads at tag-cyber.com.

For this year's work, we've placed emphasis on redesigning the look, feel, and format of our material. While strict emphasis on technical substance has always been our obsession at TAG Cyber, we understand the importance of form and design. To that end, you can see, via the report in front of you now, that we've made dramatic stylistic changes. We hope this right-brain emphasis enhances your use and enjoyment of the material.

As has been our approach in previous years, the sections below follow directly from the periodic table of controls. Each section briefly introduces the associated control, and offers a summary outlook based on our current views of the industry. This guide can be read stand-alone, or can be used as a companion document to the original TAG Cyber Security Annuals from previous years. We hope our work is useful for you.

In addition, we have now embedded our massive list of cyber security vendors into an on-line database with a simple search and query front-end available on the TAG Cyber website. It is our sincere hope that this improved ability to search, find, analyze, research, and query commercial cyber security vendors will make source selection and procurement easier. Let us know what you think of the new automated capability.

Furthermore, as part of the vendor support function on our site, we've also pre-analyzed search for certain popular concepts in our industry. Specifically, we've created metadata tags for companies that support the following research, advisory, analysis, and marketing categories that have become part of the day-to-day parlance in the enterprise cyber security space:

- Zero Trust Security
- Security Orchestration, Automation, and Response (SOAR)
- Endpoint Detection and Response (EDR)
- Cloud Access Security Broker (CASB)
- Deception
- Enterprise Mobility Management (EMM)

Obviously, users of our vendor support function can try their own phrases for analysis on the stored data. If you'd like to find companies with presence in Connecticut, for example, then give it a go. We are doing our best on the back-end to maintain accuracy and currency of this vendor data. Recognize that we do not scrape sites, but rather do all the writing and updates by hand. This is a tedious approach with pros and cons, but it's how we've chosen to do it. Watch for launch of this capability in early October 2019 on the TAG Cyber website.

2020 TAG CYBER DISTINGUISHED VENDORS

Each year, we manually research about 1700 security vendors that we can positively confirm to be actively in business, selling some sort of product or solution that reduces cyber risk. We cull this massive list from every possible source we can get our hands on, including security conference floor plans (thank you, RSA), lists of cyber security companies on investor sites, personal interactions with security professionals on a day-to-day basis, knowledge gained from our consulting and coaching business, and old-fashioned word-of-mouth. It's not a perfect process, but it sure does generate a damn long list.

From this list, the TAG Cyber team then carefully selects a subset of companies that we deem to be worthy of additional investigation. This is an admittedly subjective process, one which – unlike Gartner and Forrester – does not involve us mailing ridiculous spam surveys out to unknown participants. Rather, we use our decades of experience and insight to decide which companies are worthy of the additional attention. Period. That is how we down-select companies from 1700 to about 500 for deeper analysis. We admit to our bias, but it's not a financially driven one. We are looking for value and unique capability.

As we identify these 500 or so vendors – and this is done on a rolling basis throughout the year – appointments are set up to meet with the principals in order to learn more about their offering. We are proud to say that 100% of our vendor outreach has been successful in setting up these technical reviews. We've never encountered one vendor – not one – that was unwilling to take our call and provide a technical and marketing briefing. Some of the briefings are face-to-face in New York City, some are face-to-face in non-descript conference rooms

around the world, and many are done over a video conference bridge.

From these discussions, where we try hard to offer great (and 100% free) advice to the principals, we generally down-select once more to about 150 or so companies whose offering seems so incredibly important as to warrant an article. Usually, an 800-1000 word article is then created and posted to social media, suitable blog sites, and many syndication sources (such as our friends at HMG Strategy). This work is done gratis, and we are happy when it brings new business to the company being reviewed. We believe these articles, which you might see on LinkedIn or Twitter, are part of our vocation as the un-Gartner.

Like clockwork – and this is TAG Cyber's fourth year in business – roughly 50 or so of the 150 worthy vendors we write about, establish a deeper, more intimate connection with our work, and vice versa. These 50 vendors, and it's generally a different list each year, become collectively our TAG Cyber Distinguished Vendors. We ask them for a modest (and we mean modest) fee to help with our rent and business costs, and in return, they help us distribute this PDF to the community, as well as receiving some ancillary services such as support for videos and webinars. That's how we monetize TAG Cyber.

But more importantly, it's how we arrive at our list each year. The list of vendors below was thus produced from the original 1700, down-selected to the 500 interviews, down-selected to the 150 written about, and then down-selected finally to the 50 or so sponsors. This is a long, tedious process that does not include pay-for-play, and we routinely refuse sponsorship dollars from vendors who have not gone

through the steps with our team. We acknowledge that such approach might not build to a billion in revenue, but it maintains sufficient integrity that I am proud to write of it here.

And so – below, please find our list of 2020 TAG Cyber Security Distinguished Vendors who were kind enough to work with us this past year and to sponsor the work in front of you. Each of these companies survived a rigorous review, down-selection, and year of nagging by me and my team for more and more and more information. They are all fine companies and you would be doing yourself a favor to be in touch. I know some companies that contact the entire TAG Cyber Distinguished Vendor list each year (and no, I do not send them a reimbursement check).

ATTACKIQ

AttackIQ was a delight to work with this past year. One highlight of the year was our work together to develop a set of recommendations on breach and attack simulation which we will send to NIST to include in their future standards. The entire TAG Cyber team learned much from AttackIQ this year, and we are so grateful for their kind sponsorship of our program.



Attivo Networks has helped our entire team at TAG Cyber come to appreciate the power of well-designed deception in the reduction of enterprise risk. Tushar Kothari and his team, including Carolyn Crandall, are truly world-class, and have spent more time sharing their insights than we could ever repay. Thanks to the Attivo Networks team for their support!



Bayshore Networks has been one of the pioneers in the field of IoT and industrial control security. Toby Weir-Jones and Kevin Senator have been great supporters of our work, and we are so grateful to have their fine team as part of this year's TAG Cyber program.



Bitdefender introduced us to some incredibly forward-looking work protecting cloud infrastructure. A highlight of our year was work we did together to survey CISOs about their strategies for shifting right or left. The results of that study reinforced the balanced protection philosophy of Bitdefender and helped us appreciate their world-class insights.



BlackRidge is one of the most consequential and inventive companies you've probably not heard of in your day-to-day work. They offer a creative solution for TCP-based authentication that we believe will enhance almost any security architecture. Mike Miracle and the team at BlackRidge have been wonderful supporters of our work, and we value the interactions.

CAPSULE8

Capsule8 provides an essential Linux security function from one of the most capable teams in our industry. John Viega is an old friend (and NYU colleague) of ours, and he was patient to help us understand the basics of modern data center attack detection and prevention. It seems impossible today to imagine anyone running Linux not also running Capsule8 for security.



CloudPassage, led by our friend and industry icon, Carson Sweet, remains at the forefront in helping enterprise teams navigate the risks of putting their workloads in the cloud. Carson has helped the TAG Cyber team understand best practices for distributed workload protection, and our entire industry benefits from CloudPassage's fine support for so many engagements.



Control Case offers a cloud-based security compliance solution for small and medium sized businesses that seems perfectly designed to handle the growing burden of managing risk. When our longtime friend Norm Laudermilch notified us about this company, we quickly jumped at the chance, and have been impressed with their amazing range of capabilities.



Cord3 provides an encryption capability that we immediately found exciting. After some deliberation and discussion with their team, we jointly coined the phrase "cloud encryption security broker" (as a take-off on CASB) and we were so pleased with the community response. Our team is so grateful to the Cord3 team for their support and willingness to share.



Corsa is a wonderfully creative company that has managed to make load balancers cool again. Through the innovative use of virtualization and the service chaining that comes with it, Corsa has managed to capitalize on the amazing vantage point of load balancers to build what looks to us like an SDN firewall. Very cool stuff from Corsa!



CyberArk is one of the truly iconic brands that has become synonymous with the security technology they support. Their team has served as our collective guru when it comes to privileged access management and we are so appreciative of their patience in explaining the basic practical nuances of making this control work in an enterprise environment.



Cybereason helped us learn so much about modern next-generation anti-malware defense, especially in the context of endpoint detection and response. We held a wonderful group technical and marketing session in Boston, and we are so appreciative of their support this past year and willingness to share their creative insights.



Cybrary is a creative start-up in the area of cyber security learning and career development. Ed had the wonderful privilege to serve as an instructor for two of their courses this past year, and we have all been impressed with the quality of support and engagement they share with their students. Our thanks to Cybrary for being part of the TAG Cyber program this year.



CYR3CON is a start-up conceived from excellent research done by a team at Arizona State University led by former Army Officer, Dr. Paulo Shakarian. After reading some of his fine books describing their technical approach to interpreting hacker conversations for intelligence purposes, we were immediately hooked. Thanks to CYR3Con for their support.



Cytegenic provides an Automated Cyber Risk Officer (ACRO) solution that we've admired at TAG Cyber for some time. Elon Kaplan has been generous with his time, helping us understand the practical nuances of enterprise cyber risk management. We are so appreciative of the sharing, insights, friendship, and support from Elon and his entire team.



Deep Instinct has been our tour guide at TAG Cyber into deep learning technology. Guy Caspi and Eli David, in particular, have provided such excellent support to our team in understanding the possibilities of this amazing technology for cyber security. Our sincere appreciation goes out to this fine company for their participation in our program.



Digital Defense is a premier provider of vulnerability management, and this comes after the company spent many years supporting the cyber security professional service needs of businesses, large and small. Larry Hurtado is one of the most successful CEOs in our industry, and his support has been consistent and appreciated by the entire TAG Cyber team!



Edgewise provides a platform that supports zero trust security. They are run by an engaged, capable, and enthusiastic leader named Peter Smith, who sure looks like someone I would want to work for. I love the Edgewise platform for building an SDP, and I am so appreciative of their support for TAG Cyber in 2019 and beyond.



Egress is run by my friend Tony Pepper. I had a wonderful meal with practically their entire leadership team in New York City, and enjoyed the time immensely. We worked together on several projects this year, including a research survey and analysis that remains on-going as I type these words. Thanks to the Egress team for participating in our program.



Exact Data makes synthetic data and does it well. I've spent quite a bit of time with the Rochester-based start-up, because while they came to TAG Cyber as supremely capable data experts with great algorithms, they'd not started the company to focus on cyber security. So, it has been our pleasure to help with that - and they've been super successful in 2019!



Fortinet offers a world-class portfolio of security solutions that collectively form a powerful fabric of protection for enterprise. Ken Xie and his team are so amazing - and have been great supporters of TAG Cyber since our inception. We appreciate their partnership.



Garrison offers one of the most unique solutions in cyber security with its hardware-based isolation technology. The TAG Cyber team has enjoyed the kind support of the entire Garrison team this year and appreciates its contributions to the industry. Much of the resurgence in interest in high assurance platforms using flexible hardware can be attributed to this fine company!



HYAS provides a unique solution to cyber attribution and we are so appreciative of the time they spent helping us understanding this vital task. Jeff Spenser has been particularly helpful, and we expect this platform will become a vital aspect of the toolbox for all security analysts, including in law enforcement. Thanks to the HYAS team for this fine support.



HYPR has been a leader in decentralized authentication toward passwordless experience for some time now, and their fine team, under George Avetisov, has been supportive of our program now for the past two years. The capability and enthusiasm of the HYPR team is infectious, and everyone at TAG Cyber is so appreciative of their participation in our work.



InfoSec Global provides a cryptographic lifecycle capability that our team at TAG Cyber believes wins the award for most important control that is most ignored in enterprise – especially with the threat of quantum computing looming on the horizon. So, it was such a pleasure to include the company in our program and we hope to increase awareness of their fine offering!



InQuest offers a wonderful platform that ingests data and subjects it to world-class analytics. We have enjoyed a great year of support with the company's visionary CTO, Pedram Amini – who has been willing to share great insights with our team about this important area of cyber security. Our thanks to InQuest for their support!



IronNet has been serving customers with its world-class network security and analytic platform for several years now. A highlight of our work together was a multi-part series authored with IronNet CEO and industry icon, General Keith Alexander, retired former head of NSA. Thanks are offered from the TAG Cyber team for the support we've received from IronNet.



Jazz Networks has successfully connected the endpoint detection and response (EDR) solution set with the challenge of supporting the SOC analyst. A highlight of our work together this year was a fun hands-on training session we ran together in NYC for several analysts. We learned a lot during the session and are so appreciative to Jazz Networks for their support.



KoreLogic is a mature company with years of incredibly valuable experience supporting enterprise teams with a variety of security services – including a unique password recovery service. We've enjoyed our interactions with Bob Austin and his fine team, and we are so appreciative of their support for the TAG Cyber program!



McAfee is obviously one of the great iconic firms in our industry and TAG Cyber values the time McAfee spends with us, helping to provide insights into the industry, threats, and security technology trends. We appreciate their support for the TAG Cyber program and look forward to many years of continued interaction.

mimecast®

Mimecast focuses on email security with a solution that addresses the problems so many enterprise teams face with transition to Office 365 and need for cloud architectures. The Mimecast team has been so helpful in explaining this vital control, including phishing risk reduction, and we are so appreciative of their continued support for our team.

MOCANA

Mocana is a premier providers of cyber security for IoT devices and infrastructure. Bill Diotte and his fine team were generous in helping us gain insights into this important area of protection. Thanks to the Mocana team for their support.

netskope

Netskope provides an amazing platform for addressing hybrid cloud infrastructure threats through provision of a world-class cloud access security broker (CASB). Jason Clark and Sanjay Beri have been so helpful and supportive of TAG Cyber for several years, and we cannot express our thanks enough to the entire Netskope team for their partnership.

observe **it**

ObserveIT provides a world-class platform for user and behavior analytic-based security to deal with the insider threat. Mike McKee is one of the finest CEOs in the business and has become one of TAG Cyber's most enthusiastic supporters. We enjoy our visits in Boston with the amazing ObserveIT team and are so appreciative of their kind support.

onapsis

Onapsis offers a world-class security solution for SAP and other critical business applications. A highlight of our work this year included support for their awesome all-hands meeting in Boston, where they showed considerable warmth and willingness to share. The TAG Cyber team is so appreciative of the support from Mariano Nunez and his fine Onapsis team.



Palo Alto Networks is one of the iconic brands in the cyber security industry. The company has been an enthusiastic supporter of our program for years, and their capable marketing lead, Janet Masuda, has helped us understand next-generation security. Thanks to Palo Alto Networks for everything they do to support our cyber security community!

Pulse Secure®

Pulse Secure focuses on one of the most important challenges in modern security architecture – namely, secure access solutions for zero trust networks. Scott Gordon has been a longtime friend and supporter of TAG Cyber and his continued willingness to help us learn is both appreciated and admired. Kudos to Pulse Secure for their great contributions.

QOMPLX:

QOMPLX – which was formerly known as Fractal Industries, helped us better understand the possibilities for decision engines in cyber security analysis. Their unique focus on Kerberos telemetry was inspiring to learn, and we are so appreciative and enthusiastic to continue our work with Jason Crabtree and his amazing team.



Remediant's just-in-time solutions for privileged access management seem a perfect match for the modern enterprise trying to move to cloud and to implement zero trust security. JD Sherry and the entire Remediant team have been so helpful in sharing insights in this important area and we are so appreciative of their great support for our program.



Respond Software believes in automation as much as TAG Cyber does, and their application of robotic decision making to cyber security analysis will add productivity, cost-efficiency, and detection accuracy to the modern SOC. We offer our great thanks to industry veteran Mike Armistead and his team for their willingness to support our work this year.



RiskSense is headed by a super smart young man named Srinivas Mukkamala who continues to impress our team with his insights, knowledge, and never-ending supply of enthusiasm for identifying and prioritizing cyber risk in the enterprise. Our thanks to the RiskSense team for their continued support of the TAG Cyber program.



SafeBreach is a leader in the emerging field of breach and attack simulation, and they were always willing to answer questions, share insights, provide demos, and serve as a fountain of knowledge in this area. We are impressed with their fine solution for enterprise and are proud to include Guy Berjerano and his team in our TAG Cyber program.



Sertainty is headed up by our great friend and supporter Greg Taylor. The wonderful Sertainty team has been as enthusiastic a supporter of our program as any company, and they are always amazing hosts during visits to Nashville. Their solution for empowering data is unique and clever, and continues to provide enterprise teams with an amazingly effective control.



Symantec has been a supporter of the TAG Cyber program since our inception in 2016. With exciting changes in corporate control, we are certain that Symantec customers will continue to enjoy the usual progression of fine enhancements to their world-class products and services. Our congratulations to Symantec as they embark on the next leg of their journey.



Tala Security helped us understand the power of client-side security in addressing the growing threat of web application fraud. Aanand Krishnan and his team worked hard with us on a technical report in this area, and we are appreciative and encouraged to have Tala Security as part of our program. (And kudos to Paul McGowan for bringing us together!)



TenFour provides such a wonderful network service for its business customers that we expect to see the company as a household name shortly. It is important as analysts that we try to keep an unbiased view, but it's really tough not to root enthusiastically for our great friends, neighbors, and supporters at TenFour under the capable leadership of Bruce Flitcroft.



Trail of Bits is one of the premier professional service teams in cyber security, led by industry icon Dan Guido. Dan has been so generous to come by our office in New York and provide us with so much amazing advice. We value his leadership in cyber security, and are so grateful for his team's support.



Varonis provides advanced analytics to protect data in an enterprise, and the team was generous in sharing how this is accomplished in practice. A highlight this year involved participating in multiple of their technical events in Boston and New York – and we are so thankful to David Gibson and his fine team for their support of our work.



TrueFort – which was formerly known as CIX Software, offers visibility and control into applications, and has been doing so now for several years under the direction of our great friend Sameer Malhotra. The TrueFort team works as hard as any we see in our analysis, and we know they have great plans for continued expansion and growth. Thanks to Sameer and the team!



Vicarius impressed us from the start with their creative solution for securing applications, including proprietary ones that do not receive regular patches. Roi Cohen has been particularly helpful sharing his ideas and knowledge. We extend our great thanks to the entire Vicarius team for this support and participation in our program this year.



vArmour, under the leadership of the iconic industry expert Tim Eades, has been helping enterprise teams deal with cloud threats for many years. Tim and his fine team, including Marc Woolward, have been generous with their time, and we've done some great technical papers together! Thanks to vArmour for their continued belief in TAG Cyber!



White Ops focuses on protecting enterprises from sophisticated bot attacks by verifying the humanity of more than one trillion interactions per week. Tamer Hasan and his capable team – including the great Dan Kaminski, were a delight to work with and exemplify the best of our industry. We're so proud to have White Ops as part of our TAG Cyber program.



Valimail provides a range of email security solutions including support for DMARC and BIMBI. Alexander Garcia-Tobar is a great leader, and everyone at TAG Cyber would almost certainly vote Valimail one of the most well-run and capable companies we've ever dealt with – and their technology is amazing too! We appreciate having this fine company in our program.



Willis Towers Watson is one of the world's leading organizations in the provision of insurance for business, so their willingness to help us learn and share information about cyber insurance was so invaluable. We enjoyed our webinar series with the company and are so grateful that they would spend so much time with the TAG Cyber team this year.



XM Cyber provides an impressive solution for simulating attacks and validating the effectiveness of deployed controls. Their team shared many valuable insights over the past year, and we enjoyed developing great technical content with the XM Cyber team. We are grateful for their assistance and support.



XTN Cognitive was a delight to work with this past year – and we would like to extend our special thanks to Guido Ronchetti for being such a wonderful partner. We learned much from XTN Cognitive Security about dealing with on-line fraud, and we look forward to continued work together (along with a future trip to Italy – we hope).

1

IDPS, DECEP- TION

The design of intrusion detection/prevention systems (IDPS) was originally focused on simple devices that used signatures to detect indicators on networks and hosts. Soon-to-emerge network-based IDS (NIDS) and host-based IDS (HIDS) were part of a subsequent decade of uneven protections starting in the late 1990's. The challenge during this period was two-fold: Signatures were easy to evade, and coverage of relevant activity was difficult, if not impossible.

The progression from detection to prevention – that is, from IDS to IPS – was also uneven during this period and since. Many enterprise security teams were originally driven to the notion of actively shunning offending sources during an attack. But these same teams grew wary of the side effects of such powerful automatic blocking. Most teams thus ran in a combined mode, where the baseline was to remain passive, hence the IDPS moniker.

An important recent component to this control area involves deception-based security solutions, which use probes, lures, and fake content to detect evidence of cyber attacks. Deception was originally based on simple honey content, but more recently has evolved to effective commercial products that offer realistic means for security teams to catch bad actors in the process of live exploitation. This is now necessary functionality in the enterprise.

Generation of realistic synthetic data is an interesting new dimension for emerging deception systems. The objective is that by creating truly believable databases of users, credentials, and other information, intruders will be more likely to be lured into environments where forensics and response activity can be initiated. Readers should expect continued innovation in these areas of enterprise cyber security.

2020 Trends for IDPS

The use of IDPS, including deception, has evolved from a less-effective control initially to a much more effective control today (see Figure 1-1). Progress was achieved based on three factors: First, introduction of behavioral security analytics in the early 2000's reduced the dependence of enterprise security teams on pure signature processing. Security teams could compare observed behavior with profiles to detect anomalies more accurately.

Second, the introduction of deception as a component of the overall detection and prevention process created a new live means for dealing with clever adversaries. Deception was a clumsy technology in the 1990's, often relying on poorly-conceived honey pots that were easy to spot. But deception technology improved considerably in the 2000's and 2010's with more effective commercial offerings emerging from vendors during that period.

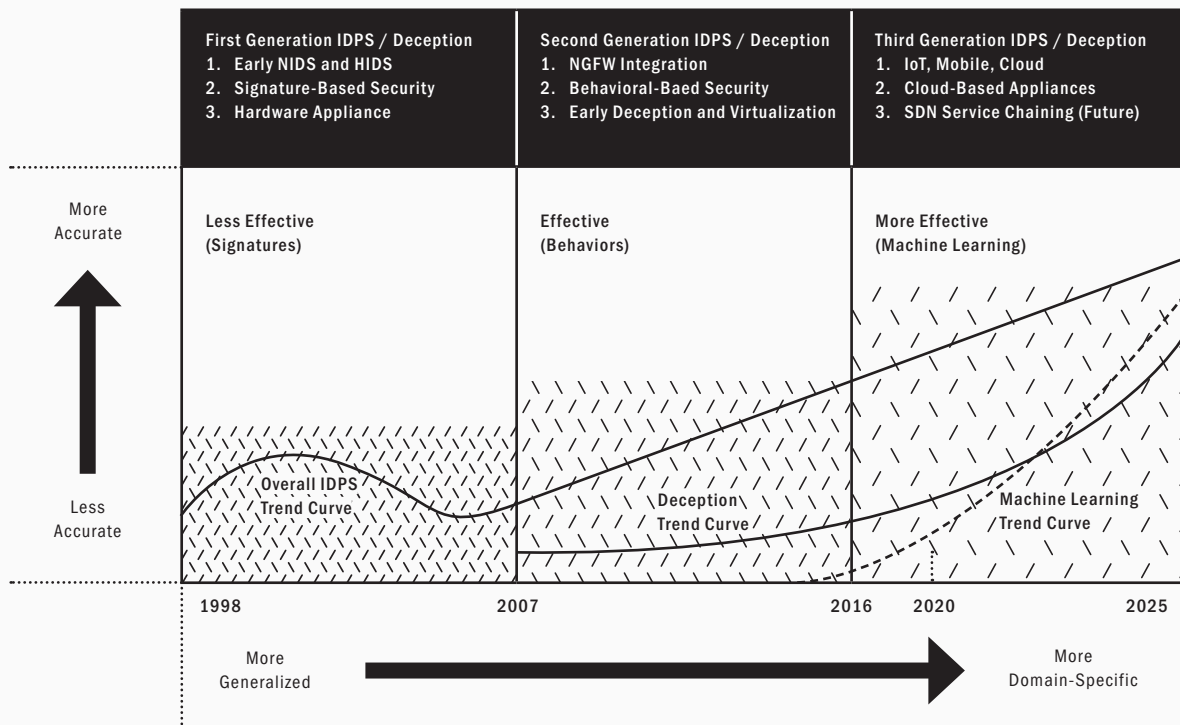
And third, introduction of machine learning (ML) as an underlying algorithmic enhancement to the detection and prevention process improved the accuracy of attack and indicator detection. The moniker 'artificial intelligence' produces a range of visceral reactions among experts, and is often avoided by marketing teams to sidestep customer friction.

Nevertheless, the effective use of supervised or unsupervised ML and deep learning has moved cyber security forward. It is interesting to note that the effectiveness of IDPS took a dip after its earliest promise – and this stemmed directly from the realization that keeping signatures current was not going to be feasible. Furthermore, the best hackers viewed IDPS signatures as little more than a speed bump. Luckily, improved signature deployment methods, behavioral algorithms, virtual detonation, machine learning, and advanced deception have improved matters considerably.

The future of intrusion detection, prevention, and deception is bright, and will likely include continued advances in behavioral detonation of attacks in virtual environments, more accurate deception algorithms, and more extensive use of powerful ML technologies. All these advances will continue to use cloud assistance, but software defined networking (SDN) usage will grow in the latter portion of the 2010’s as service providers embed these tools into SDN deployments.

Amidst this progression to more effective intrusion detection, prevention, and deception, two trends can be observed: The first is that the technology has moved from more generalized processing at its inception to more domain-specific processing now and into the future. In addition, the overall accuracy of detecting relevant indicators has improved over the three generations of products. Both trends are welcome and make this a desirable security control.

Figure 1-1. IDPS/Deception Trend Chart





AN INTERVIEW WITH GUY CASPI
CEO & CO-FOUNDER, DEEP INSTINCT

APPLYING DEEP LEARN- ING TO CYBER SECURITY

FOR MANY years, it seemed unlikely that artificial intelligence would provide a meaningful impact on how cyber security was implemented in practice. But with recent advances in computing power for neural processing and in the algorithms that support on-the-fly learning from live data, deep learning has emerged as one of the most exciting and promising aspects of our industry. And this is good news for defenders who just seem to lose ground to hackers every day.


Deep Instinct has pioneered the use of deep learning technology to detect threats. Its technology offers risk reduction for both known and unknown threats and can be applied to a variety of practical cyber security applications. We connected recently with Guy Caspi, CEO and Co-Founder of Deep Instinct, to learn more about how this technology is likely to evolve – as well as how their platform works and is expected to evolve.

EA Guy, can we start with your views on the current and future cyber security challenges of the CISO?

GC Yes – it is clear that CISOs have many challenges, and here are just a few that we see in our work at Deep Instinct. First of all, we see an increase in the number and capability of new machine-generated malware attacks that are proving to be successful at compromising enterprises. The sophistication of these new cyber attacks is accelerating. That is, they are becoming multi-stage integrated attacks across platforms and domains. The challenge for CISOs is that most solutions today are not well-suited to deal with the complexity of these advanced attacks. Furthermore, the shortage of cyber security experts is expected to grow, and this gap is becoming more difficult to manage as security tools continue to necessitate human involvement.

EA How does the Deep Instinct platform work and why is it different from other enterprise protection solutions?

GC Deep Instinct's platform is based on an end-to-end deep learning (DL) framework that was purpose-built for cyber security. Most other enterprise solutions use traditional machine learning (ML). The advantage of DL over ML is that it achieves greater results of predictive accuracy by analyzing all the raw data in a file or process and by picking up on non-linear patterns and correlations. In contrast, ML requires feature engineering, where a human expert effectively guides the machine through the learning process by extracting the features that need to be learnt. This results in the ability to identify only linear patterns and correlations. The DL analysis means that the platform is able to better predict and prevent new first-seen attacks like APTs and zero days. It can also achieve a better detection rate and get a broader coverage of attack vectors, while reducing false positives and false alarms significantly. Deep Instinct's DL platform can protect any type of endpoint, including mobile devices and servers. It can also be applied across different operating systems in any kind of environment (e.g., cloud, premise, VDI, online, offline). Unlike detection-



Unlike detection and response-based solutions, which wait for the attack before reacting, Deep Instinct's solution works preemptively.

and response-based solutions, which wait for the attack before reacting, Deep Instinct's solution works preemptively. By taking a preventative approach, files and vectors are automatically analyzed prior to execution, keeping customers protected in zero time. This is critical in a threat landscape, where real time is too late.

EA What are the true prospects of artificial intelligence for offense? Do you see a future where AI-based attacks are mitigated by an automated, AI-based defense?

GC Currently the use of AI in offensive attacks is pursued at an academic level, but as information disseminates, we do foresee attacks using AI to more efficiently achieve their objectives. We anticipate three types of AI attacks: First, we expect to see AI-based cyber attacks will involve malware operating AI algorithms as an integral part of its business logic. An example of this is DeepLocker, demonstrated by IBM Security, which encrypted ransomware to autonomously decide which computer to attack based on a face recognition algorithm. Second, we will see AI-facilitated cyber attacks, where the malicious code and malware running on the victim's machine do not include AI algorithms, but the AI is used elsewhere in the attacker's environment. An example of this is Info-stealer malware, which uploads personal information to command and control (C&C) server, which then runs a natural language processing (NLP) algorithm to cluster and classify sensitive information as interesting (e.g. credit card numbers). Finally, we expect to see AI-adversarial attacks, where malicious AI algorithms are used to subvert the functionality of benign AI algorithms. This will be done using the algorithms and techniques that are built into a traditional ML algorithm and breaking it by reverse engineering.

EA Do you see any shifting trends either from prevention to detection and response (right shift) or from response to detection and prevention (left shift)?

GC Yes, with the availability of DL-based security solutions, we anticipate a wholesale left shift

to prediction and prevention. During the period just after traditional anti-virus (AV) showed its weaknesses, the cyber security market moved away from a preventive approach as their experience taught them that it is impossible to prevent an attack. This was mostly due to the limitations of the technology available, which couldn't adequately protect against emerging sophisticated and complex attacks. The current approach of detection and response is also losing confidence as the attack landscape is escalating in its sophistication – with APTs and complex threats easily evading most security solutions. The new availability of DL-based platforms means the entire cycle to analyze whether a file is benign or malicious can take place pre-execution, in just milliseconds. This enables the prevention of an attack pre-emptively.

EA Deep Instinct has done some interesting partnership deals recently, including with HP. Can you share the details?

GC Yes, Deep Instinct recently partnered with HP to develop HP Sure Sense, which enables zero-time threat prevention against the most advanced cyber threats. HP Sure Sense is a standalone, self-managed solution offering a streamlined user-experience on the millions of endpoints on which it is to be implemented. It will be available on the new HP EliteBook 800 G6 series, HP ZBook 14u and HP ZBook 15u. By leveraging Deep Instinct's DL-based threat prevention engine, HP Sure Sense provides zero-time detection and prevention – coupled with anti-ransomware, behavioral protection. The AI pre-execution solution can scan any file type while predicting and preventing known or unknown threats before damage occurs. By the way, other recent deals at Deep Instinct include a partnership with Tech Data, and an agreement that the Deep Instinct agent will be supported on all Point of Sale (POS) systems at Kings Supermarkets. We're excited about these awesome deals.



AN INTERVIEW WITH JOHN VIEGA
CEO & CO-FOUNDER, CAPSULE8

ADVANCED SECURITY FOR PRODUCTION LINUX

WHETHER anyone ever really questioned the operating system of choice for the data center seems irrelevant now: Linux is the clear choice. We could justify this situation by listing here the many advantages of Linux from a maintenance, administration, and deployment perspective. But our focus is less on why the open source operating system dominates the data center, and more on how cyber security controls for Linux can be practically deployed.

John Viega is one of the finest cyber security experts in our industry, with skills that roam equally between cyber defender and professional hacker. His company, Capsule8, provides a powerful suite of security tools for Linux that are derived from this dual defensive and offensive focus. We caught up with Viega in Brooklyn recently and asked him to share his insights into how his team's platform is transforming security for production servers in the data center.

EA We all know that Linux has basically won the battle for the data center. Why do you suppose there hasn't been more emphasis on providing better security for production Linux?

JV Often people come to us because they recently had a breach in their Linux production infrastructure. They never have any idea how the attacker got in. In fact, most of the time, they never would have known they got breached, except that their AWS bill shot up, and when they investigated, they found crypto-mining. These organizations know they're flying blind, without the visibility they would have if it were any other environment. When we ask them why they were willing to deploy without detection or even basic visibility, the answer is invariably that operations is too concerned about stability and performance to allow any of the products the security team has considered for deeper visibility. The business needs to run. In the pre-cloud world, security appliances could sit off to the side and provide value (even if the fidelity of data could have been better). Today, the only sensible place to be is on the workload, but ops teams are worried that a bug in a security vendor's kernel module can take down a workload. Or they are worried that a workload handling 1000's of connections a second will end up falling over because the security processing takes up too much CPU. Or they are worried that an EDR solution will generate a massive amount of telemetry that will flood their network and increase cost. Capsule8 was designed to address those big concerns that an operations team would address, while still providing world class security.

EA Tell us about your technology and how it works.

JV You can think of us, first and foremost, as a fully-featured, container-aware EDR system for Linux infrastructure. We detect attacks in real time and we make incidents easy to investigate. Each node has an agent that runs in user space, and has intelligent rate limiting to make sure we are good citizens when it comes to stability and performance. These controls and our focus on performance make us good enough that a major



We detect attacks in real time and we make incidents easy to investigate.

public CDN (Content Distribution Network) deploys us on all of their edge-nodes, which are incredibly performance-sensitive. The analytics are all done in real time, in the agent wherever possible. The only detection data that will stream out is alerts. Being real time allows us to shut down attacks as they're happening if the customer chooses. The analytic models are very expert-driven. We build models that collect the minimum possible data and have minimal performance impact. We pair exploit writers and a data science capability to help minimize the amount of data we need to collect to be highly effective. Then we test our 0-day detection capabilities by testing against exploits for important new CVEs when they come out. For our investigations data, we start by collecting only the data a customer wants to keep and making it as compact and valuable for investigations as possible. For example, instead of keeping a record of every single `exec()` a system makes, we do an analysis to determine when commands are interactive, and only record the interactive commands. Otherwise, you'd collect way too much data and could risk performance problems. The investigations data can be cached locally and flushed to any data sink. Many of our customers are using cloud storage such as S3 buckets. We keep the data in the Parquet format, making it easy to run SQL queries in near-real time straight from Amazon Athena (and similar offerings from other cloud providers). We even can provide an OSQuery plug-in that allows you to backend queries to S3, so that you can run nearly-live queries of production data. We've found that one of the biggest impediments to making OSQuery useful for investigations is that Ops teams won't allow the risk of letting anyone do live queries against production, so they only allow scheduled queries. Our architecture sidesteps the problem. Locally on the agent, we can also keep to fixed storage and memory. Again, we need to provide our customers with confidence that we won't fall over in production.

EA How well do you integrate with SecOps and how important is it that you operate at high speed and scale?

JV The scale issue is critical for many enterprises. It's harder to scale on a single incredibly busy workload than it is to take our model to a large cluster (because the system is so distributed and so much of the work is done in completely independent agents). Beyond that, it's critical that we don't require anyone to use our console. You've already got a dozen single panes of glass, so you don't need another. We make it easy to integrate with your operational investments, whatever they look like, across configuration management, orchestration, data storage, and so on. For instance, there's a really simple webhook capability that allows you to filter and reformat alerts, sending a single alert to Slack, S3, and Demisto if you like.

EA You said you're an EDR solution, but you have policy capabilities as well, correct?

JV Yes. For instance, we have a much better way to do File Integrity Monitoring (FIM) than any other solution we've seen. We've heard from many customers that, while they need to run FIM solutions for compliance reasons, the existing solutions are too spammy. In particular, they need to have policies that say: "no system binaries should ever change," but inevitably system updates run and tons of system updates change at once, spamming the SOC. Some companies do after-the-fact analytics to weed out the wave of spammy alerts. But a smart attacker knows that system update time is the time to make any changes to the file system. Our agent does something unique, in that it has enough context to know what processes are changing files. So, we can correlate that with all the standard ways to update software and allow our customers to have much more accurate policies like: "System executables shouldn't change, unless they happen through the correct Puppet instance." This is hugely important for making policy products useful.

EA Your team must see some interesting attacks in live settings. Any ones that you can share?

JV By far the most common incidents we see are actually not attacks in the traditional sense,

but legitimate users egregiously violating their organization's policies around what's acceptable in production. More and more development teams are deploying and maintaining their production applications. They tend to do things they shouldn't be, like debugging in live production or downloading things from the open Internet. This kind of stuff happens all the time, and we can not only detect it, but give a full audit of everything that happened during the offending interactive session (both the input and output). For actual attacks, command injection using known vulnerabilities in open source definitely is the most common thing we're seeing. The most common thing to do post-exploitation is to do as much bitcoin mining as you can get away with. Some attackers, however, will try to escalate privileges, so they can be stealthier and have much more flexibility.

EA Any near- or long-term predictions about Linux security for production systems?

JV We believe over the next couple of years, the assumption that Linux and cloud are more secure will quickly melt away. We hear all sorts of rationales, including these: Smaller attack surface, containers providing isolation and controls like SELinux enforcing tight policies. While all those can raise the bar, the attacker can often jump right over them. For instance, if the attacker has a kernel exploit that allows for running arbitrary code within the kernel, then it's not too hard to escape from a container (unless you're running only one container per VM, in which case the container is a machine anyway), and even totally disable SELinux. Production is typically full of high-value data flowing through Linux systems, and Linux is becoming a valuable enough target to be worthy of more resource expenditure by attackers. People will need to start paying attention to the risks, because they are very real.

DLP & UEBA

The design of data leakage prevention (DLP) systems was originally centered on detecting whether files with certain keywords were being transferred externally by insiders. This emphasis had the advantage of being easy to implement at gateways, but had the challenge that most of the structured and unstructured files in a typical enterprise are poorly marked. The result was a mixed initial attempt to keep corporate data inside the enterprise.

DLP systems – because they focus on insider leakage – were quickly extended to reside anywhere users might allow data to slip away. The endpoint is an obvious target, so most DLP systems include support for controlling how data is shared, copied, downloaded, and even backed-up to memory sticks. This one feature – restricted use of external storage media – brings both great security benefit and enormous inconvenience to enterprise users.

An issue with early DLP that remains relevant in all environments today is that sidestepping DLP systems through unsanctioned shadow IT or off-network tools is easier than it should be. Employees who would like to exfiltrate a document can easily snap images on their personal iPhone, or they can create and maintain the document using external systems such as from Google or Box. Shadow IT is the scourge of DLP and must not be ignored by security teams.

For these reasons, most existing DLP installations have been correctly advertised to senior leadership as effective controls against inadvertent, non-malicious transfer of data outside the enterprise. But even this requires that corporate data be properly marked to detect such leakage, either across a network or from an endpoint onto a separate storage device such as a portable memory stick. Unfortunately, proper marking is not commonly enforced.

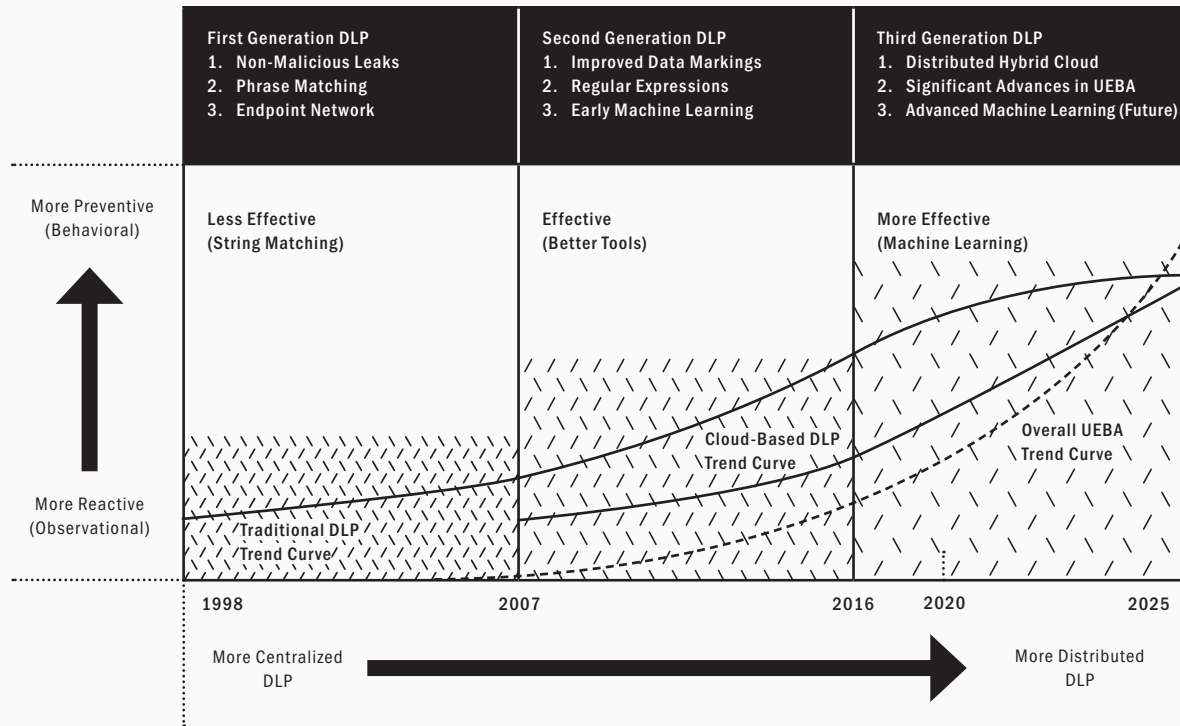
The transition from static matching of strings and markings toward more behavior approaches suggests a great opportunity for integration of user entity behavioral analytics (UEBA) technology. Focused more broadly than DLP, UEBA solutions encompass both insider data leakage and more general suspicious insider behavior on endpoints, applications, and systems. While UEBA and DLP are separate functions, they are well-suited to integrated cooperation.

It is not an exaggeration to view UEBA (also referred to as user behavioral analytics or UBA) as a bright spot in enterprise cyber security toward 2020. Especially for environments that include the reasonable expectation by employees that some monitoring is on-going (such as in a call or contact center), UEBA is a strong control. White collar and technical staff might still need some convincing, however, before they will be fully comfortable with such monitoring.

2020 Trends for DLP

Despite its challenges, DLP technology has progressed from a less effective method at its inception to an effective cyber security control (see Figure 1-2). This progress has been achieved through the following initiatives: First, companies have done a (somewhat) better job marking assets – especially

Figure 1-2. DLP & UEBA Trend Chart



structured, sensitive data. Such marking allows DLP systems to more accurately detect potential leakages from a gateway, endpoint, or system.

And second, algorithms for DLP from the best security vendors have progressed from phrase-matching toward better use of regular expressions and machine learning. With this comes a greater ability to address malicious, intentional data exfiltration from compromised insiders. This coverage now extends to virtual computing on distributed hybrid cloud systems, which is important as most organizations depend less than ever on their perimeter.

It is worth mentioning that indirect methods for DLP have also been included in UEBA tools that focus on insider threats. That is, by observing the behaviors of insiders, effective determination can be made about whether that target might be inclined to cause a problem.

In the better UEBA tools, direct observation can be made about suspicious activity that might lead to an information leak. UEBA is now a necessary function in enterprise.

The inclusion of DLP capability in present and future cloud-based systems and services, including SDN, represents a growth area in cyber security. Stated simply – your as-a-service provider will soon, if not already, begin to offer customers DLP-like functionality. It remains to be seen how much UEBA they can add, because cloud has less of an “insider threat” focus. Nevertheless, expect to see considerable adoption growth in these cloud-based DLP offerings.

The future of DLP – and its adjacent UEBA functionality – lies in advanced, embedded algorithmic controls that will recognize the indicators of potential future leakage in advance of an actual exfiltration. This will require management planning to minimize the temptation for employees

to evade such detection via shadow IT services. A well-orchestrated balance between security and the freedom to use the best DLP and UEBA tools will emerge.

In addition, UEBA vendors must convince white collar and technical staff that monitoring controls are designed to protect them from attacks rather than to snoop on behavior. While companies have a right to such behavioral observation, most employees who are not already in highly monitored environments will tend to hate these controls. This can have a negative effect on the workplace. User messaging is thus an important requirement for UEBA vendors in 2020.



AN INTERVIEW WITH TUSHAR KOTHARI
CEO, ATTIVO NETWORKS

THE POWER OF DECEP- TION FOR CYBER SECURITY

THE use of deception in computing has reached the point where its absence as a security control is no longer acceptable in most environments. The power of deception ranges from the introduction of uncertainty for an intruder to the establishment of an accurate means for detecting both well-known and zero-day attacks. Deception also provides a fertile ground for performing forensics on attacks to learn tactics.

Attivo Networks has been at the forefront of this innovation, and organizations of all sizes and industries are deploying deception. Their platform has evolved to include those features and capabilities that are deemed optimal from a security and compliance perspective. We recently connected with Attivo's CEO Tushar Kothari, to learn more about how deception is being used by enterprise teams today to reduce their security risk.

EA Tushar, it's great to see how far deception has come in the context of cyber security. Do you still see enterprise teams who need to be convinced of the importance of this control?

TK We are seeing a remarkable change in the market as the enterprise teams are now focusing on detection. While prevention is important, it is clear that in today's environment the attackers are going to find a way to get in if they are already not inside the network. Within detection tools, deception rises above all other methods due to its efficiency, efficacy and no false positive. Analysts like Gartner are promoting this very same message and Attivo ranked highest in 13 out of the 14 categories. So today we are seeing great global progress in the market as far as deception as one of the key controls in the security stack, but we still have some more work to do.

EA Tell us about your platform – how would an enterprise team deploy your software into their network?

TK The ThreatDefend platform is made up of several components that together create a full deception fabric, offering network, endpoint, applications, and data deception for comprehensive detection and visibility. The platform is designed to scale to the needs of the organization and can be deployed to meet the needs of a regular enterprise seeking no-nonsense detection, to mature enterprises with a small/virtual SOC, to lean forward enterprises with a large SOC, teams, and desire for counterintelligence and hunting programs. Organizations will start with the BOTsink server, which is a hardware, virtual, or cloud appliance that manages the deception environment, projecting decoys to any part of the network. It installs quickly and learns the environment to customize the deception campaigns which deploy in as little as an hour. The BOTsink is often paired with the ThreatDirect solution, that provides easy scalability to remote or branch offices, cloud infrastructure, or micro-segmented environments. It is available as a VM, container application, or endpoint-installed service. For multi-appliance deployments, there is also a



The ThreatDefend platform is made up of several components that together create a full deception fabric.

central manager server for enterprise deception management from a single pane of glass. The dashboard and UI provide simple management and easy operations, with minimal resources to operate. Cloud-specific deceptions can also be created for decoy storage buckets, containerized applications, cloud-based applications, and serverless functions to detect attacker activity targeting these objects. The ThreatStrike endpoint suite is an agentless component that installs on production systems to detect credential theft, Active Directory data gathering, ransomware spread, and mapped share access. It can also redirect port and services-based attacks into the deception environment for virtually locking down the endpoint from lateral movement. The ThreatPath solution can be deployed for endpoint visibility to credential exposures and misconfigurations that attackers can use to move laterally across the network and is available as an add-on component or as a standalone service offering. Remediation can be automated within the solution or through native 3rd party integrations. Deploying the ADSecure solution protects production Active Directory by intercepting unauthorized queries, hiding real results, and inserting deceptive data. This is also available as an add-on component or a standalone solution. Overall, the breadth and depth of the solution can provide deception in virtually any network environment, both IT and OT. Organizations can also activate automated incident response and ThreatOps' playbooks to accelerate incident handling and response. Over 30 native integrations are available to automate blocking, isolation, and threat hunting with major firewall, SIEM, EDR, and NAC products.

EA What are some of the more interesting types of attacks you've seen customers find using your deception platform?

TK We have seen the full spectrum of attacks as you would expect. Our technology has detected not only infected machines and attackers attempting lateral movement, but we have also detected rogue employees/malicious insiders. One of the most interesting detection alerts was when a healthcare customer detected malware spreading from a

brand new IoT medical device that had just come from the factory. Luckily, with the early alert on this activity, the customer was able to quickly trace the infected system and remediate before it spread to other systems.

EA I know you are asked this all the time, but can deception extend into cloud infrastructure?

TK Good you asked the question. In fact, while many of today's traditional controls don't easily migrate to the cloud environment, our deception technology is easily deployed and is ideal for today's serverless application environments. The Attivo solution is available for AWS, Microsoft Azure, GCP as well as Oracle cloud. More and more of our customers are deploying the platform in their cloud infrastructure for visibility and many are even starting in the cloud and then extending into on-premises environments.

EA How are the compliance organization treating deception? Is it now an established control?

TK We are seeing a positive trend here. We map extremely well to MITRE's attack vector and most recently deception technology was included in the updated draft NIST framework. Additionally, in India the central bank of the country has put out a framework for banks in India which includes deception. So, I would say we are making a lot of progress and expect to see deception technology mentioned as an integral part of these compliance frameworks in the near future.

FIREWALL PLAT- FORMS

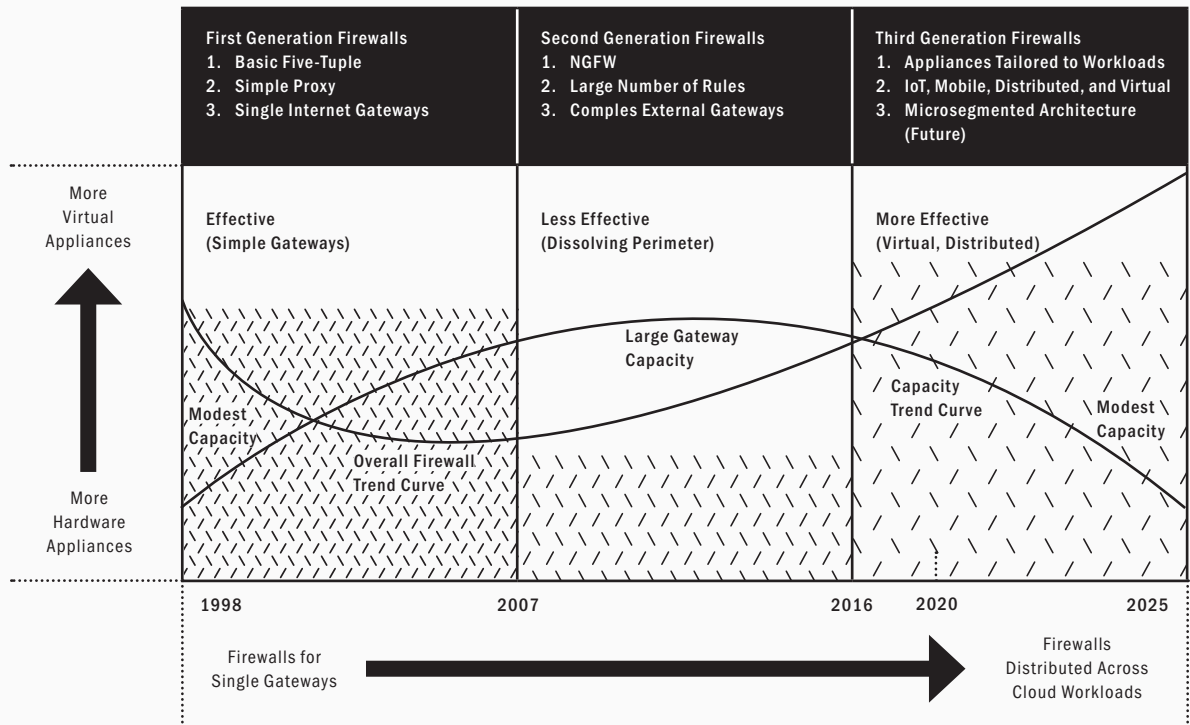
The future of firewall technology and architecture can be summed up in one word: Virtual. Every sign points to increased software-based implementation with orchestration across distributed systems based on software-defined controls.



The original purpose of a firewall was to protect enterprise networks from the lurking dangers of the emerging Internet. This evolved toward the more general notion of protecting one network from another, but the idea that this would be accomplished at a well-defined chokepoint remained central to the proper placement and operation of a firewall. This basic notion served as the basis for network security for nearly two decades.

The bad news is that the latter portion of that two-decade era of firewall usage was not a period of exemplary cyber security. Rather, with the accelerating dissolution of the perimeter in the mid-2000s, organizations began to realize that their overall network security architecture was ill-suited to how companies operated. Most of the major breaches that occurred during this era were not prevented by firewalls. In short, the firewalls were often almost useless.

Figure 1-3. Firewall Platforms Trend Chart



The good news, however, is that commercially available firewall solutions have become progressively better since their initial inception. So-called next generation firewalls (NGFW) from the best security vendors are now incredibly powerful, feature-rich devices that provide the most advanced cyber security available today. The capabilities embedded in a modern NGFW are essential for proper assurance and security protection of a network.

All of this highlights the challenge for enterprise security teams regarding firewalls. That is, they must work with commercial vendors to ensure that the power and capability of NGFW technology continues to evolve, but in a way that is consistent with the mobility-enabled, cloud-based architectures that are emerging. This includes the migration of PCs and servers on a local area network (LAN) to a device-to-cloud scheme for accessing business apps.

An obvious advance with wonderful promise involves the use of distributed firewalls to create so-called software-defined perimeters (SDP). This architectural approach requires coordination and orchestration of multiple policy engines deployed virtually to ensure a common enterprise policy enforcement approach. This is not easy – but it is not hyperbole to call this method the future of enterprise security. Virtual firewalls will be the drivers of this welcome shift.

And a new term has emerged in the context of SDPs – namely, zero trust security. Coined by Forrester, the term references secure access to resources using authentication, authorization, and access control that require no inherent trust in the local processing environment. So, if implemented properly, no need remains for a perimeter to protect data. Expect 2020 to be a year in which considerable emphasis is placed by the security community on zero trust security.

2020 Trends for Firewalls

Firewall technology has progressed from reasonably effective packet filters to feature-rich gateways that can implement complex security policies and goals

(see Figure 1-3). The obvious good news here is that existing users of firewalls should enjoy continued increases in capability, features, and effectiveness in the coming years. Trends toward virtual, distributed processing in zero trust environments will complement improvements in firewall technology.

A key observation with respect to firewalls in the enterprise is that traditional firewall hardware appliances are being gradually replaced with virtual appliances embedded in software-based infrastructure. In addition, firewalls originally designed for single gateways are being gradually replaced with distributed appliances scattered across cloud workloads to support emerging SDP methods. Most companies work in a tentative hybrid arrangement today, but this will change.



Expect 2020 to be a year in which considerable emphasis is placed by the security community on zero trust security.



Andrew Coelho, Unsplash

The capacity for an individual firewall was originally smaller, given the thin connections most companies had to the Internet at its inception. This capacity expanded dramatically during the second generation of NGFW solutions, with gateways growing to support large wide-area connections. Interestingly, this capacity trend is reversing itself now for individual appliances with segmented workload protection, even though aggregate capacity is larger.

The future of firewall technology and architecture can be summed up in one word: Virtual. Every sign points to increased software-based implementation with orchestration across distributed systems based on software-defined controls. SDP virtualization creates flexibility and support for on-demand provisioning. Organizations of the future will automatically provision new firewalls based on situational awareness, and this will be a welcome advance.

SDN-based firewalls are also likely to provide an exciting new opportunity for firewall vendors to explore new means for cyber defense. With the power of dynamic service-chaining in SDN, enterprise security teams can begin to deploy firewalls that can automatically, and even autonomously, extend their capability based on live circumstances. New capabilities such as IPS or packet analysis will be deployed virtually in the future and orchestrated by SDN firewalls.

Finally, as suggested above, the emphasis on zero trust security will reduce the need for firewall platforms to provide Fort Knox-style bunkers between an enterprise and Internet. Instead, firewalls will provide dynamic, flexible security for workloads scattered across zero trust networks, but that still must respect the policies, rules, and goals of the sponsoring organization. Virtual, distributed firewalls will be the best means for implementing such capability.



AN INTERVIEW WITH HENRY HARRISON
CTO, GARRISON

ISOLATION AS A POW- ERFUL WEB CONTROL

ISOLATION is one of the most powerful primitives in cyber security. That is, by separating assets from threats, the likelihood of an attack successfully occurring is greatly diminished. Assurance is another powerful concept in cyber. It is driven by the observation that trust in the implementation of a control is directly related to how well it protects assets. As one would expect, combining isolation with assurance creates a desirable environment for reducing cyber risk.

Garrison is a UK-based cyber security company that builds an isolation platform with high levels of trust and assurance. Specifically, the platform sits between the content stream from browser to website, making certain that any dangerous malware is detonated away from live assets. By implementing this in high assurance hardware, Garrison offers a valuable and trustworthy platform. We met with Henry Harrison of Garrison to better understand this architecture and how it can be used in enterprise.

EA Henry, can you explain how isolation provides risk reduction for the enterprise? What specific threats are mitigated by secure remote browsing?

HH Isolation is a core principle of computing, recognizing that within a single endpoint, the user will work with both extremely sensitive data and with extremely risky data, and that these need to be kept apart. With secure remote browsing, our team at Garrison focuses on the World Wide Web, which is the number one source of extremely risky data – and how to keep that isolated from the sensitive work that people do on their endpoints. We aim to make it possible for people to click on dangerous links without the risk of introducing malware onto their endpoints.

EA What is the role of hardware in the provision of your security solution?

HH Isolation is already a key feature of the user's operating system and of their browser, and for many people that's enough. But, for some customers, the risk is still too high, and that means they need a level of isolation that is over and above that level. We don't believe that step-up can be achieved using the same software approaches that are already used in the OS and browser. Instead, we believe the isolation needs to be delivered at the hardware layer.

EA How is it possible that users would experience the same behavior with Garrison providing security-in-the-middle versus a direct connection to the Internet?

HH Our hardware turns risky content from the Web into pixels, and delivers just those pixels to the user's endpoint. In the reverse direction, the user can click and type just like they normally do to support a regular web browsing experience. The hardware isolation technologies that we use – namely, our own Garrison SAVI technology, and the hardsec approach described at www.hardsec.org – mean that customers can have a very high degree of confidence that it's just safe pixels that reach the user's endpoint. The result is that the endpoint is protected against sophisticated attacks.

EA Do you see secure remote browsing becoming a greater regulatory and compliance requirement for enterprise?

HG For some parts of some countries' governments, the requirement for isolation and secure remote browsing is already a regulatory and compliance requirement. So, the good news is that compliance governing bodies do recognize the benefit of this control. As ever, these requirements tend to end up flowing down into the Critical Infrastructure and Financial Services sectors.

EA Any near- or long-term predictions about isolation and secure remote browsing?

HH Leading financial services firms in particular are beginning to recognize two things: First, they have come to see that secure remote browsing can make a massive difference to their risk exposure. And second, they've learned that regardless of the isolation vendor they choose, it's not going to be a trivial project. That means that there's an increased focus on ensuring they really get an attractive return on investment (ROI) to justify the effort they're going to expend deploying it. This is done by providing significant risk reduction in the areas that really matter.



AN INTERVIEW WITH EDUARDO CERVANTES
CEO, CORSA SECURITY

SCALING NETWORK SECURITY WITH VIRTU- ALIZATION

NETWORK traffic inspection has evolved from simple firewall appliances blocking bad IP addresses to more sophisticated next generation firewalls (NGFW). And this worked well enough until a new killer app has arrived on the scene: SSL/TLS encrypted traffic. And now the reality is inspection is not keeping up. The combination of SSL/TLS adoption and huge bandwidth demands is resulting in decreased inspection capability for high capacity links. We find ourselves with a model that is broken where the traditional approaches to inspection aren't working.

Corsa Security has its roots in SDN and sees network security through that lens. It is enabling the transformation to scaling traffic inspection and security services by using two of their oldest tricks: horizontal scaling and virtualization. We recently chatted with Eduardo Cervantes, CEO of Corsa Security, to learn more about how his company is addressing network security virtualization, something we have often referred to as software-defined network security.

EA Your team has been well-known for scaling SSL traffic inspection and load balancing. Before we get into your newer capabilities, tell us about how these functions are supported at Corsa.

EC With the exponential increases in traffic volumes, and with most traffic now being encrypted – by some estimates, over 72%, even the largest security devices suffer from an unacceptable performance degradation when trying to decrypt SSL traffic. The result is an SSL inspection gap, which reflects the point where an enterprise can no longer decrypt incoming traffic and also maintain sufficient levels of network performance. To address this problem, our team at Corsa has developed a security services load balancer that provides a simple way to scale SSL/TLS inspection capabilities horizontally. It redirects traffic into multiple virtual security appliances, so that operators of high-throughput networks can gain full visibility into their SSL/TLS traffic.

EA You've embraced the concept of security service chaining in the context of virtualizing network security. Help us understand how this provides Corsa with such powerful capability.

EC Service chaining is an important component of our software-defined network security vision. It supports dynamic scaling of network security services, and this goes beyond just traffic inspection. Service chaining also supports dynamic creation of per-tenant security. On the road to the development of chaining, we started with a fully turnkey network security virtualization platform that economically scales up virtualized firewall instances, on-demand, to maintain 100% traffic inspection, under all conditions. In other words, we essentially created a virtual NGFW that elastically expands and contracts inspection capacity to meet demand. It's the tight integration of the elements of the platform – namely, the load balancer, commodity server, virtual firewall instances from leading vendors, and the Corsa virtualized infrastructure manager – which produces a solution that is instantly usable by the customer. This packaged approach to virtualizing network security is compelling, because network and security engineers can focus on policy and performance



Even the largest security devices suffer from an unacceptable performance degradation when trying to decrypt SSL traffic.

while the platform takes care of inspection capacity. Then, as networks establish the use of virtualization for traffic inspection, the Corsa platform can support the evolution to multiple security services and chaining those services into per-tenant security service chains.

EA Is it possible, given the vantage point of your Corsa platform in a typical architecture, for firewall functions to become embedded into the platform itself?

EC Firewall functions are crucial for the Corsa platform, which is tuned specifically for the demands of dynamic firewalling. Our integrated virtualization solution uses load balancing to redirect traffic into virtual firewall instances, and builds up an entire security stack using commodity compute and a VM manager. The firewall functions are more overlays than embedded, in the same way that a mobile application becomes an overlay to a handset's operating system. Beyond firewalls, we are also evolving the same platform to support any type of virtual security service, like IDS or IPS. Our platform can thus be viewed as the operating system and compute function for a network security system. When new inspection capacity or security posture is required, a virtual NGFW or any other virtual security service can be added just as one would add applications to any OS. It is a simple matter of software-defining the new security position, which no longer requires any form of hard wiring or physical appliances and offers far better TCO.

EA You've done some interesting partnerships recently. Tell us about these integrations and how your customers benefit.

EC As a turnkey virtualization platform, we are the optimized infrastructure integration that economically scales network security. It's our technology alliance partners who bring decades of security inspection intelligence. We have integrations with firewall, IDS, and IPS vendors. By running the virtual network security functions from this partner ecosystem on general purpose x86 servers, we deliver unlimited scale to any network security function, including such killer apps as SSL visibility. For our customers, this

means being able to inspect all their traffic, all the time, without impacting network performance. Since we provide the necessary network, server, load balancing, and management components in a turnkey hyperconverged infrastructure (HCI) package, customers can focus on security policy and no longer have to spend time struggling to predict network traffic needs to scope required hardware. With the virtualization platform, when more capacity is needed, it's just a matter of licensing more virtual machines from the security vendor, and the platform scales accordingly. Because Corsa is offering the virtualization platform on a subscription basis, customers can disassociate themselves from all forms of hardware refresh-cycles for network security.

EA Any near- or long-term predictions about modern network security?

EC Transition to 5G, IoT, and cloud is forcing network and security engineers to look at network security differently. Security in layers is something that will need to be applied at multiple points in the network. The only way to do this in a timely and effective manner will be to automate, so that responses are dynamic and proactive. At network gateways, this means having virtual security services that auto-scale to meet traffic volume changes, traffic mix changes, and changing threats – all at a per-tenant level. We are well on our way to becoming an integral part of that evolution.

NETWORK ACCESS CONTROL

The original goal of network access control (NAC) was to ensure some degree of policy and integrity enforcement before a device could join a local area network (LAN). Standards such as IEEE 802.1X were created to govern such functionality, and network technology vendors created generations of solutions that enterprise buyers tried for years to make work on their perimeter-protected environment. Some were successful; others not so much.

So, most early generation enterprise NAC implementations experienced uneven results with their customers. Certainly, the goal of NAC is clear, and the objective of ensuring high integrity for devices joining a network remains entirely rational. But so many complicating factors have made typical NAC a tough proposition for larger companies. Mid-sized and homogeneous firms have reported better results, often because their networks are simpler.

The current situation in NAC is that many organizations continue to rely on this control for their existing, legacy networks. This situation will gradually change, but for the foreseeable future, NAC vendors will continue to do considerable business, and enterprise teams will continue to install the control, with its associated quarantines and other functional measures designed to protect the LAN and minimize annoyance for visitors.

The primary business question for NAC vendors is whether they can easily transition their traditional LAN-hosted capabilities toward a more virtual, SDP-based architecture. There is no reason why they cannot make this shift, but it will introduce a new set of competitors. Cloud access security broker (CASB) or virtual private network (VPN) vendors, for example, might introduce NAC-like controls for SDPs. The NAC vendors will have to navigate this new terrain.

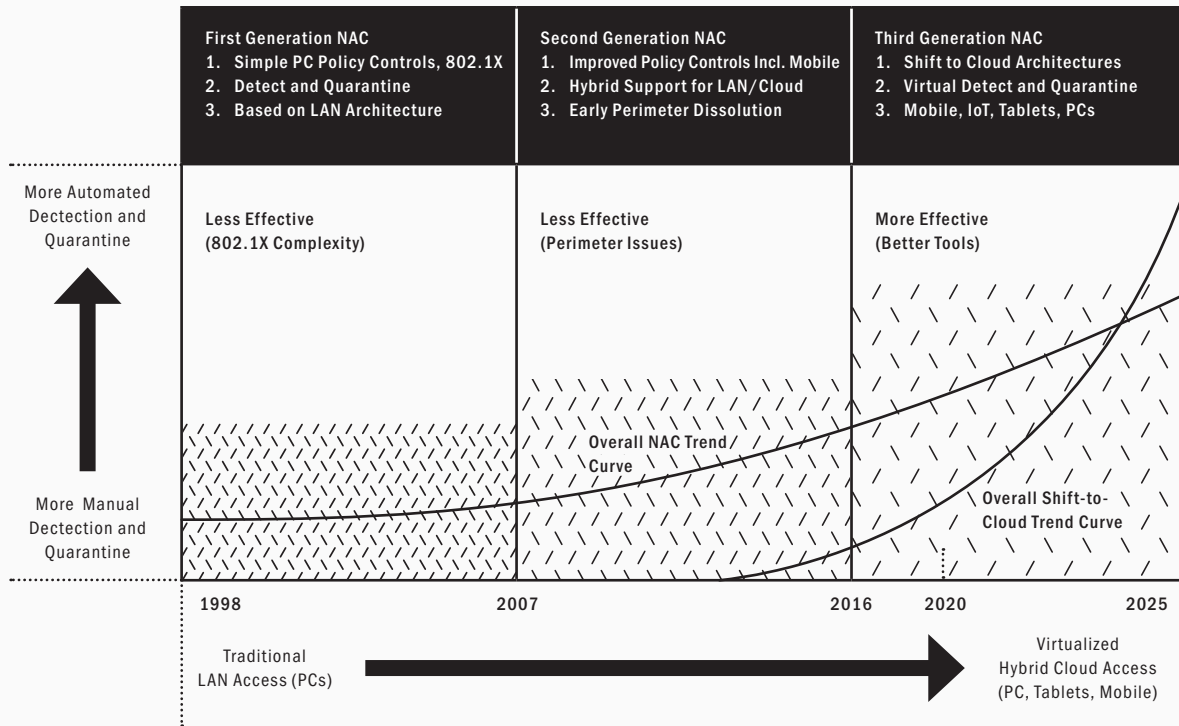
Zero trust security is also an issue that must be successfully traversed by NAC vendors. Secure remote access solutions that involve policy decisions made by security-as-a-service capabilities in the cloud represent an alternative to NAC that will be attractive to any perimeter-free enterprise. The advantage of NAC solutions remains, however, the clarity with which NAC requirements can be defined, recognized, and understood with respect to device admission.

2020 Trends for NAC

Network Access Control (NAC) has progressed from solutions with high promise and well-known standards (e.g., 802.1X) toward a more cloud-based and virtual present and future (see Figure 1-4). This progression to virtual follows the shift in LANs toward device-to-cloud enterprise computing solutions. Such shift does create new opportunities for NAC vendors to provide admission control and quarantine capabilities for these new network approaches.

One clear trend in the delivery of commercial NAC solutions involves the evolution of early detection and quarantine solutions that previously relied on manual configuration, static administration, and clumsy operation, toward smoother, more automated NAC delivery. In addition, NAC is experiencing

Figure 1-4. Network Access Control Trend Chart



a shift from its traditional role protecting LAN infrastructure toward a more integrated delivery across virtualized hybrid cloud, including mobility.

An interesting observation worth noting is that international enterprise security teams, especially in the Middle East, Asia, and Africa, continue to center their protection solutions around LAN-based NAC. One would expect this to provide additional runway for traditional NAC vendors targeting IEEE 802.1x needs to experience revenue growth while cloud-based SDPs begin to shift the functional requirements for NAC toward virtualization.

The overall shift to cloud in the enterprise is accelerating in the current timeframe, and is having a clear impact on emerging SDP architectures for network access and security control. An inflection point is being approached where the effectiveness of new, virtualized NAC will exceed that of more traditional LAN-based solution offerings. This is good news for NAC vendors, as it creates excellent

new business and revenue opportunities. The reality remains, however, that enterprise perimeters define and delimit the networks that NAC solutions have been designed to protect. It stands to reason that if such perimeters are dissolving that NAC solutions must evolve accordingly. Any enterprise team currently dependent on NAC, and any vendor focused on NAC for its revenue, must therefore take note of this change and build suitable strategies for the coming years.

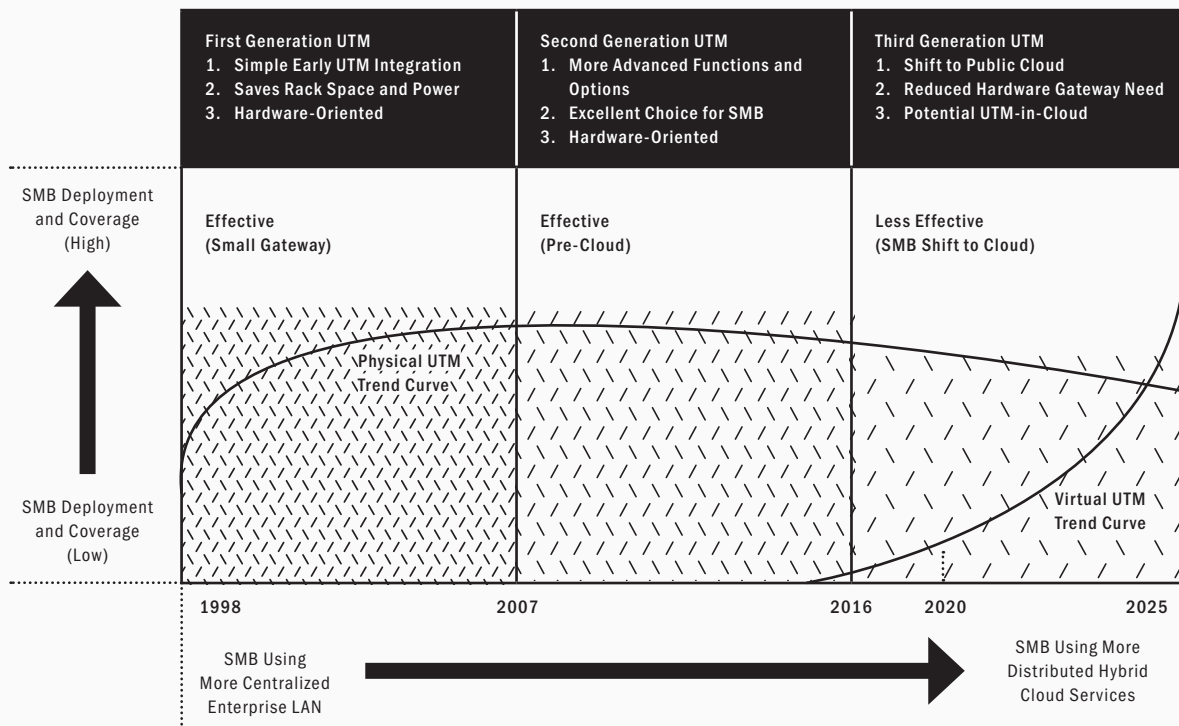
**UNIFIED
THREAT
MANAGEMENT**

The idea in UTM is that a smaller enterprise would like its various cyber security-related functions to be integrated into a single, common appliance with a simple, consistent interface for managing and administering these various capabilities.

A creative cyber security solution that emerged over the past decade for small and medium-sized businesses is known as unified threat management (UTM). The idea in UTM is that a smaller enterprise would like its various cyber security-related functions to be integrated into a single, common appliance with a simple, consistent interface for managing and administering these various capabilities. The resulting UTM devices included such familiar capabilities as firewall functionality, simple intrusion detection, VPN termination, and other commonly found security gateway functions. The simplicity of design and ease of operation made UTM solutions especially popular with these smaller entities, and allowed them to enjoy the advantage of next-generation features without having to go select and procure new products from a range of vendors.

The challenge with UTM is that smaller businesses are moving quickly to public cloud services, which dramatically reduces their local area network (LAN) footprint. Without a LAN gateway to the Internet, the role of a UTM solution becomes less clear.

Figure 1-5. Unified Threat Management Trend Chart



Nevertheless, the specific functions embedded in a UTM are still demanded, so the challenge for UTM vendors involves how to extend these capabilities to newer, more virtual architectures.

An additional challenge with UTM solutions is that they have tended to be implemented as hardware products. A clear trend in our industry involves some pause (or even a total halt, in some cases) by supply chain and procurement teams when hardware is being selected for purchase. The shift to software-defined-everything will find its way to UTM, and this represents both a challenge and a massive opportunity for UTM providers.

It is worth adding that named categorization of security solutions such as UTM will come and go based on marketing decisions by vendors as well as the whims of research and advisory firms who often create these names. Observers should be flexible when a given solution meets or does not meet the specifics of a category. For UTM this is important, because the included functions will remain vital, even if the hardware packaging changes.

2020 Trends for UTM

Traditional, gateway-based UTM has progressed from effective devices that met a specific need for small businesses toward more uncertain effectiveness in today's hybrid cloud systems (see Figure 1-5). The justification for the 'less effective' view shown in the trend chart is reduced need for hardware-based UTM appliances at the dissolving perimeter. Such chokepoints are diminishing in frequency of use – hence the reduced need for hardware UTM appliances. The good news, however, is the dramatically increased need to support the same basic gateway functions such as firewall and intrusion detection/prevention in the emerging, virtual small business enterprise. This need will drive a renaissance for UTM providers and will create demand for commonly provisioned, configured, and administered security along the same lines as traditional UTM, but rather for hybrid, and eventually complete public cloud usage.

The coverage of small and medium-sized business (SMB) with UTM has progressed from a small initial footprint toward a greater deployment, and then toward a gradual trending downward for traditional hardware deployments. The trending for virtualized UTM is expected to increase dramatically in the coming years. Readers should note that this involves some prediction on the part of the analysts here, since virtualized UTM is not a big business today.

The future of UTM is bright, so long as vendors recognize that SMB users will desire all the benefits of common UTM management, but in the context of a virtual infrastructure. This evolution will cause some competition with cloud access security brokers (CASBs) and microsegmented security solutions, but the UTM vendors will have the advantage of having served the SMB market for many years.

SMB users have also driven the leading edge of cloud usage in the enterprise. Unlike previous generations, where large business had the resources to drive modern solutions, smaller companies have had the freedom, flexibility, and non-capitally intense environments to make use of virtualized, cloud-based services. As a result, larger companies have tended to watch and learn from smaller companies regarding cloud effectiveness.

**WEB
APPLICATION-
TION
FIREWALL**

Web application firewalls (WAFs) originated as a means for tailoring policy controls to a particular application hosted on a website. This contrasts with the more general nature of intrusion detection and prevention systems, as well as conventional firewalls, which must include broad sets of rules that must address the policy needs for all the applications, systems, networks, and users that are being protected by that device. WAFs can be more specific.

The way a WAF works is that it sits in-line with the HTTP conversation that occurs between a client browser and a web server. Its main purpose is to reduce the risk of attacks on the server, and this includes prevention of commonly found web application exploits such as cross site scripting (XSS) attacks and SQL injection. Surprisingly, these two well-known exploits continue to occur, despite their stubborn existence in the offensive arsenal for so many years.

Security architects often differentiate client and server protections in the context of a so-called proxy. That is, if some entity desires interaction with a resource, then a proxy can reside in-line and play the role of that targeted resource to ensure proper security. When this is done for clients, the proxy is maintained by the administrator of that client group. When this is done for servers, the function is called a reverse proxy, and WAFs generally fall into that category.

A challenge in deploying and maintaining any WAF is that as the HTTP application being protected is modified, the corresponding reverse proxy functionality must be adjusted accordingly. This complicates services such as managed WAF, because the policy and rules adjustments for a given application might occur frequently. One might view such adjustment as an acceptable burden for the tailored protection, but it certainly does

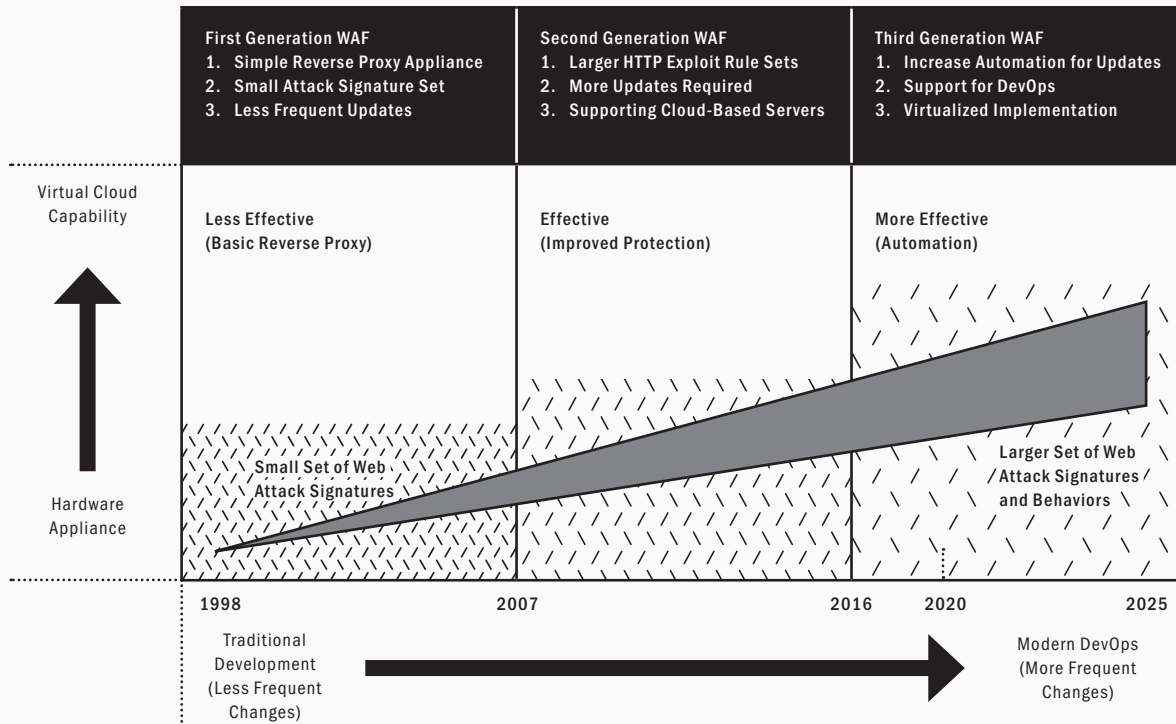
increase workloads. An interesting future cyber security capability for WAFs would utilize advanced algorithms, perhaps using artificial intelligence, to deal with, or even predict, the changing nature of applications. Integration with DevOps lifecycles would be a good place to deploy such functionality, because it supports the potential to identify changes in development before the production application receives any new features. The WAF could then be updated.

2020 Trends for WAFs

WAFs have progressed from reverse proxy devices toward more full-featured HTTP security devices, to more automated solutions for protecting web applications in DevOps environments in the current generation (see Figure 1-6). An obvious progression through this evolution is that the initial small attack exploit signature set has grown to include many more types of attacks that can be detected by more advanced means.

As one would expect, it has been a challenge to keep up with the shift from less frequent changes in a typical web application toward the present day (and future), where application changes are frequent and the norm. In a typical DevOps environment, for example, application changes might occur daily, which implies that any corresponding

Figure 1-6. Web Application Firewall Trend Chart



WAF must be integrated with this maintenance lifecycle, preferably using automation. One would also expect to see application hosting providers offering WAF-like capabilities to their customers as an embedded service. This will be best done in partnership with the WAF provider marketplace, because most application hosting teams will likely underestimate the challenges of maintaining WAF accuracy with ever-changing app functionality. Nevertheless, this will be a growth area for the WAF ecosystem – and hence an opportunity for vendors.

The future for WAFs lies in several trending areas: First, WAFs must continue to improve the accuracy and coverage of the exploit detection for HTTP applications. This must continue to shift from simple detection of XSS attacks and SQL injection toward behavioral-based detection, perhaps using advanced heuristics, that can learn from observed client-server communications to recognize attacks that might be brewing.

Second, WAFs must continue to integrate into the DevOps lifecycle, so that as HTTP application owners making rapid, frequent changes to a given software application can rely on the WAF to keep up. This is only possible in the context of automated controls that are integrated directly into the DevOps lifecycle. This constraint is consistent with other cyber security tools, but is particularly important for WAF evolution.

Finally, WAFs would appear to be excellent platforms for advanced learning algorithms that can identify functionality as either benign or malicious. The observational nature of a WAF with an application provides an excellent operational vantage point for such learning. We should expect to see this trend in the emerging functionality for WAFs, especially ones that are implemented in virtualized environments.

**WEB
FRAUD
PREVEN-
TION**

Web fraud prevention tools emerged in direct response to an increase in malicious fraudulent activity aimed at websites, usually targeting eCommerce or financial applications, in the early 2000's. The goal of such fraudulent attacks almost always involves financial gain. The tactics used range from easily identified steps that can be codified into signatures, to more subtle tactics that exploit specific weaknesses in the targeted site.

Readers might be tempted to interpret “web fraud prevention” tools in the broadest sense, perhaps including the range of detection, response, and notification services offered by banks, credit card companies, and other large entities. A more acceptable interpretation for the work presented here involves an automated cyber security tool placed adjacent to, or in-line with, a given website to perform an intrusion detection-like function.

That said, the technologies offered to prevent fraud in a web context are often easily generalized to other areas. Many vendors thus reference their capabilities in the context of fraud prevention, inclusive of identity theft, electronic crimes, and other areas considered outside the scope of traditional enterprise cyber security. Readers should keep this in mind as they try to understand and characterize commercial anti-fraud offerings.

A typical heuristic involves watching a web session to determine if the initiating user is exhibiting behavior indicative of fraud. For example, if an eCommerce website includes a wizard that allows for some sort of account sign-up, then normal users might be expected to patiently click through the wizard steps. A fraudster, expecting to deal with many wizards, will more likely find a way to skip the interim clicks; web fraud prevention tools would watch for this.

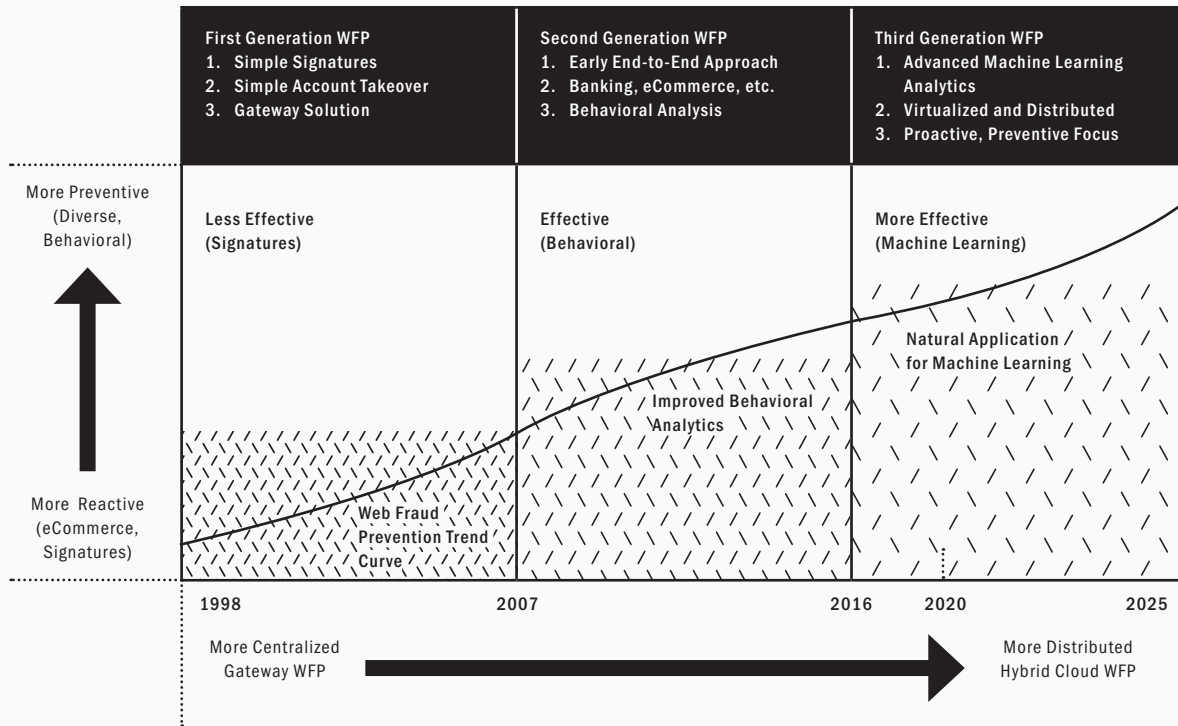
A more recent adjunct to the web fraud prevention capability addressed here involves emerging tools to address the increasingly high potential for abuse of cryptocurrencies. These tools tend to rely on threat intelligence, behavioral analytics, and cryptography in a manner that is highly consistent with the controls found in web-based fraud settings. Cryptocurrency ecosystem security is a fast growing area in 2020.

2020 Trends for Web Fraud Prevention

Web fraud prevention has progressed from these early use of signatures to more effective use of behavioral analytics. The present generation promises to be a welcome era for web fraud prevention, including application to new computing ecosystems such as cryptocurrency, as emerging machine learning and artificial intelligence-based processing appear to be well-suited to this type of cyber security challenge (see Figure 1-7).

The general strategy in all type of fraud prevention has evolved from a reactive control that watches for evidence that the fraudulent behavior has already begun, toward a more proactive control that focuses on detecting evidence that fraud might later occur. The architecture for addressing fraud risk has thus shifted from centralized gateway solutions to more distributed, virtualized functions capable of

Figure 1-7. Web Fraud Prevention Trend Chart



becoming embedded in a software-defined network. Perhaps a more fundamental question for fraud prevention tools is how important any web-based technologies will be to business activity in the future. The introduction of mobile apps, social networks, and new ecosystems for cryptocurrency represent challenges to the status quo in eCommerce. One thing is for certain, however, and that is the inevitable attempts at fraud that will follow whatever means for commerce is in use in coming decades.

The future of fraud prevention appears to be centered on the use of truly advanced predictive heuristics, which points, in turn, to machine learning and artificial intelligence. Since the nature of this control involves determining characteristics of the user (or automation) at the other end of a session, Turing tests and other forms of advanced processing are also well-suited to this security control to reduce fraud risk.

It seems reasonable to expect convergence of all aspects of fraud risk mitigation for individuals and businesses in the coming years. This is likely to include reducing risk of fraud for credit cards, individual identities, Internet domains, and many other personal, business, and technology-based attributes. Such convergence will allow for reduced reference to web-based fraud prevention in lieu of a more general reduction of fraud in society and business.



**AN INTERVIEW WITH GUIDO RONCHETTI
CTO, XTN COGNITIVE SECURITY**

STOPPING ONLINE FRAUD

STOPPING FRAUD is a mature issue in online payment applications and services, and is based on well-conceived concepts such as profile-based analytics. But extending these techniques to web-based eCommerce has not been as straightforward, simply because attribution, network protocols, application credentials, and account management are so different from legacy approaches. Cyber security solutions for addressing web fraud have thus required creative algorithms and novel methods for detection, mitigation, and response.

XTN Cognitive Security is an Italian firm that specializes in addressing fraud-related issues. Their platform is well-known in local Italian markets because of its integrated approach to fraud protection, smart authentication, and behavioral monitoring. We spent time with Guido Ronchetti of XTN Cognitive Security to learn more about their plans to extend their solution to an international market and how he sees the web-based fraud ecosystem evolving.


EA How do traditional fraud methods translate to online services? What is the goal of the fraudster?

GR Online services suffer from a wide variety of frauds. One of the more common patterns is related to account or sensitive information takeover. Takeovers range from taking control of the bank account of the victim, to stealing their credit card information. The result is that, most of the time, an undesired transfer to a temporary account is accomplished by the fraudster. There are also more technologically-advanced fraud scenarios, where the attacker takes control of the application used to perform fraudulent transactions directly. With the rising of online onboarding procedures in next-generation payment services, there is also a rising trend related to rogue identities and BOT driven account creation. The fraudster's goal is to monetize the attack as quickly as possible, and to find an easy to scale and maintain fraud flow (cost reduction is an issue for everybody).

EA How does the XTN Cognitive Security Platform work? What problems are you solving?

GR XTN Cognitive Security Platform is a comprehensive fraud prevention platform. Our vision is to correlate different layers of analysis to obtain a holistic approach to detect fraudulent events. The platform considers the posture of the endpoint used to access a critical service, the digital identity of the user, and the risk profiling related to business content of events. Our unique technology relies on cutting edge artificial intelligence to provide for accuracy. Our technology combines different needs that are mandatory in the fraud analysis space: Behavioral perspective, the intelligibility of the risk causes, flexibility, and real-time response. We address the challenge of providing visibility about fraud attempts coming from consumer-facing or internal critical services. The banking sector is one of our reference markets, where limiting payment related fraud is especially important. But other markets also need this kind of protection. We are working, for example, in the automotive environment to protect connected vehicles' services.

EA You've had great success in the Italian market. What is your strategy for extending your offer globally?



Our vision is to correlate different layers of analysis to obtain a holistic approach to detect fraudulent events.

GR We are excited to be approaching the global market, knowing full well that our technology offers a unique set of features and differentiators. From a go-to-market point of view, we are selecting some strategic partners with specific skills in fraud and logical security fields. Moreover, we are engaging in marketing initiatives (online channels, exhibitions, market events) in order to spread the know-how about our solutions. Finally, we activate partnerships with other synergistic vendors or partners.

EA How does your solution enhance authentication for mobile and web applications?

GR Authentication to us implies use of multiple proof factors. In the XTN Cognitive Security Platform, digital identity validation relies on different layers: Behavioral biometrics features, endpoint trust, and cryptographic quantities. These layers let us modulate the authentication factors considering the endpoint trust or risk, and including continuous behavioral analysis to recognize anomalies. Our goal is to provide the smoothest user experience possible, while keeping the highest security level. To do that, we consider the endpoint, and in particular, mobile devices, as the central actor in identity proofing.

EA Any near- or long-term predictions about online fraud or about mobile and web application security in general?

GR We see high pressure globally on mobile online services. Security awareness is increasing, and users demand secure services, both considering privacy and money. On the other hand, service providers are struggling to address growing security threats, while also maintaining ease of use in their apps. We are now very focused on getting everyone to understand the importance of In-App Protection. We strongly believe that protecting the app goes beyond the app assets in the end-point. We think that modern protection requires implementing a probe-evaluate-react pattern, including the app's technological threats detection together with behavioral and identity-related features. Our technology is taking all relevant information from the app to our clients without any user experience impact, and building risk-driven reaction flows that originate at server-side, where the trust should be.



AN INTERVIEW WITH AANAND KRISHNAN
CEO, TALA SECURITY

REDUCING WEB FRAUD USING TALA SECURITY

THE HACKING group Magecart emerged several years ago with a card-skimming attack that easily bypassed conventional server security controls. Addressing Magecart required a clever application of client and server protections, generally based on policy control methods that helped reduce the risk of credential compromise from website-embedded malware. The good news is that websites are now being upgraded to deal with this insidious privacy-impacting attack.

Tala Security has served at the forefront in the fight against Magecart with their advanced commercial security platform. The Tala Security team provides a software solution that detects web fraud in ways that conventional controls such as Web application firewalls cannot. We spent time with Aanand Krishnan of Tala Security recently to learn more about how their solution addresses web fraud and how commercial clients can integrate the platform controls into their eCommerce ecosystem.

EA Let's start with Magecart. Who are they and what do they do?

AK The term Magecart is a name given to group of attackers that target vulnerabilities in websites. The group has been around for a few years and has changed its methods somewhat as the attack has become more well known. Their main attack vector, however, remains use of malicious JavaScript that is designed to skim credit card information. The attack works as follows: If a user visits the payment page of an eCommerce site infected by Magecart, then malicious JavaScript code will silently collect and send user-entered credit card data and other personally identifying information (PII) data to a drop server. The attack generally causes little notice, since the eCommerce vendor gets paid normally, and the user receives the goods or services requested.

EA Does this attack generally target first-party code on a website?

AK This vulnerability is certainly inherent in first-party code, but it also targets third-party code. In fact, it can expand more, since many advertising vehicles routinely chain in fourth, fifth, and higher parties into a website experience. These multiple unmanaged connections between the client-side browser and external third-party servers provide Magecart attackers with an attractive and expansive attack surface. Recent research confirms this, quantifying that nearly 5000 websites are successfully attacked per month using this method, and that 20% of victimized websites are re-infected within days.

EA This sounds like a serious problem, since most modern eCommerce websites include lots of software from many other vendors.

AK Yes, that's correct. The evolution of the modern website integrates code and tools from a myriad of first-party as well as third-party vendors. These tools enrich the customer experience, provide compelling content, and support critical analytics. They also offer capabilities that assist in customer engagement, customer conversion, and support



Tala is unique in this regard: We provide security capability across the full spectrum of client-side vulnerabilities.

for online eCommerce. These tools are, however, attractive targets of Magecart attackers, because they provide unmanaged access and visibility to the entire webpage, including any financial or other PII data entered by website users. Instead of directly targeting the defenses of the highly secured website owner, threat actors thus follow a path of least resistance. That is, they target the website supply chain's weakest link – namely, the highly privileged and vulnerable code that, in aggregate, represents a customer's website experience.

EA Why can't most existing cyber security tools deal with attacks such as Magecart?

AK Existing website security tools aren't designed to interrogate, monitor, or prevent client-side website attacks like those utilized by Magecart attackers. A web application firewall (WAF), for example, is designed to protect a website server resident within the confines of the website vendor's security infrastructure. A visibility problem emerges for WAFs, however, because the user of website operates outside that controllable security perimeter. If you think of any attack, there is point of incursion, a point of data capture, and a point of data exfiltration. The point of incursion of a Magecart attack is not the server hosting the website, but one of the third-party services integrated into the website's supply chain. These could be marketing automation services, content distribution networks (CDNs), chat agents, advertising libraries, and so on. A product like a WAF has no visibility into third-party services and code and therefore completely misses this point of incursion. The point of capture and exfiltration for Magecart resides with the client, because JavaScript code is sent to the browser, and that is where the code executes. The data capture and exfiltration happen via the browser, invisible to server-oriented controls like WAFs. This is one of the reasons why Magecart attacks have not only been successful, but have gone undetected for months, in some cases over a year.

EA Can you share with us how the Tala Security solution works, and how it deals with this attack?

AK Of course. Tala offers a comprehensive client-

side prevention solution that includes a dynamic AI-driven engine that works in conjunction with the automation of standards-based security capabilities, like CSP, SRI, and HSTS to protect against Magecart attacks. Our platform also addresses a wide range of other app-layer attacks like cross-site scripting, clickjacking, iframe injection, client-side malware, and so on. Tala is unique in this regard: We provide security capability across the full spectrum of client-side vulnerabilities. Our platform detects attacks by continuously monitoring and detecting anomalous activity, whether it is something malicious happening within your server, your website supply chain, or malicious code executing at the user's browser. Our protection engine works by activating and precisely configuring browser-native, standards-based security controls, which offer prevention, detection, blocking, and alerting against a wide range of attacks. By leveraging automation to activate native, standards-based controls, Tala is able to deliver comprehensive security without compromising site performance. Our solution is installed at the web server or the application middleware in a matter of minutes and begins leveraging AI to evaluate and learn the policies optimally suited to prevent client-side attacks from impacting the unique website experience of website owners.

EA Your team often references use of content security policies. What are they and how do they influence the design of your solution?

AK One of the most exciting developments in web security in the last few years has been done at Google. Their team pioneered use of client-heavy web apps on Chrome, and they slowly started embedding powerful security controls into their Chrome browser to protect apps. These security controls include Content Security Policies (CSP), Subresource Integrity (SRI), and Certificate Stapling, as well as iFrame sandboxing rules and referrer policies. These security controls are W3C standards and adopted across all major PC and mobile browsers. For Tala, it was clear to us from the outset that these security controls were the best approach, because they offered incredibly powerful, fine-grained security without slowing down the site. Tala's core IP is in its ability to completely automate

the entire process of determining, configuring, and managing these security controls to detect and block a wide range of attacks. These security controls are powerful, but can be complex, leading to security teams struggling. Our breakthrough is that – with Tala – any website can be up and running with these incredibly powerful security controls in a matter of minutes.

EA That's exciting to hear. Congratulations on such a successful platform. Let's close our discussion with any near- or long-term predictions you might have about web fraud and related attacks.

AK Thanks for the compliment on our platform. We're proud of our work and excited to help new customers every day. Regarding our near or long term predictions, we expect that website attacks will unfortunately continue to grow. There are a couple of reasons for this view. The first challenge is a lack of awareness. Many website owners are still not aware of the scope of this problem, and often hold the client-side-attack-is-not-my-problem type of view. This is changing with high profile breaches and recent news about companies such as British Airways being assessed a \$230 million dollar GDPR fine. We, as an industry, must do a better job of educating website owners about the vulnerabilities inherent in the modern website. An additional challenge relates to economics. For example, the price of online credit card information, often called CVV, has gone up significantly in the last few months in the dark web. Basically, it has become more lucrative for hackers to steal online credit card data than physical card data. Weaponization is also a challenge. Late last year, we started to see Magecart type skimmers going on sale in the dark web. Skimmers are currently for sale for as little as \$200. In addition, we are seeing attack automation. Attackers have a lot more powerful tools at their disposal and, frankly, the overwhelming majority of websites do not.

EA Do these types of attacks easily scale to large numbers of victims across the Internet?

AK Yes, attackers are capable of massive scale, because compromising a single third-party tool enables them to victimize every website served by

the compromised vendor. This allows threat actors like Magecart to attack hundreds or thousands of websites via a single compromise. A final challenge is our industry, and this one that really concerns me. So far, we have seen Magecart type groups go after eCommerce sites with the purpose of stealing credit card info. But the reality is that the same attack vector – malicious JavaScript used as part of a supply chain attack – could be used to steal user banking credentials, PII data, healthcare data, and just about any information that users might enter into a browser. We are starting to see signs of this happening. At Tala Security, we do risk analysis for our customers all the time. And in most cases, we are shocked by how exposed a website is to these kinds of attacks. We have much work to do as an industry, and we are just in the early stages of a long battle to tackle this problem across the web.

WEB SECURITY GATEWAY

Web security gateways (WSG) emerged as critical cyber protections once enterprise teams recognized that any entity inside a perimeter might initiate outbound sessions with both known and unknown websites on the Internet. This included both appropriate and inappropriate sites (e.g., gambling), as well as benign and malicious sites. The malicious websites were ones preconfigured to accept information beaconing from an infected internal entity.

The resulting WSG proxy device soon became an essential filter for enterprise egress traffic, generally fed by a live threat intelligence feed from vendors with research teams watching for suspicious website URLs. Since this gateway filter was typically installed in-line with all Internet traffic, the performance was a key differentiator, and companies specializing in web acceleration were well-suited to developing early products in this area.

Most organizations today view their WSG as an essential safety net for endpoints and users – one that serves as a last resort against policy violations and data exfiltration. That is, for an infected endpoint to beacon out sensitive data, it must have already been compromised and gone undetected. The WSG proxy will hopefully detect and block the exfiltration as a point of last protection. For this reason, the function will remain an essential one for all organizations.

It is worth mentioning that a complementary gateway – one that is intimately adjacent to endpoint security control - involves isolation technology designed to separate potentially malicious traffic from the end user device. The result is a secure remote browsing solution, through a man-in-the-middle gateway, that provides an additional level of defense-in-depth protection for the endpoint (discussed in more detail in our section on Endpoint Security).

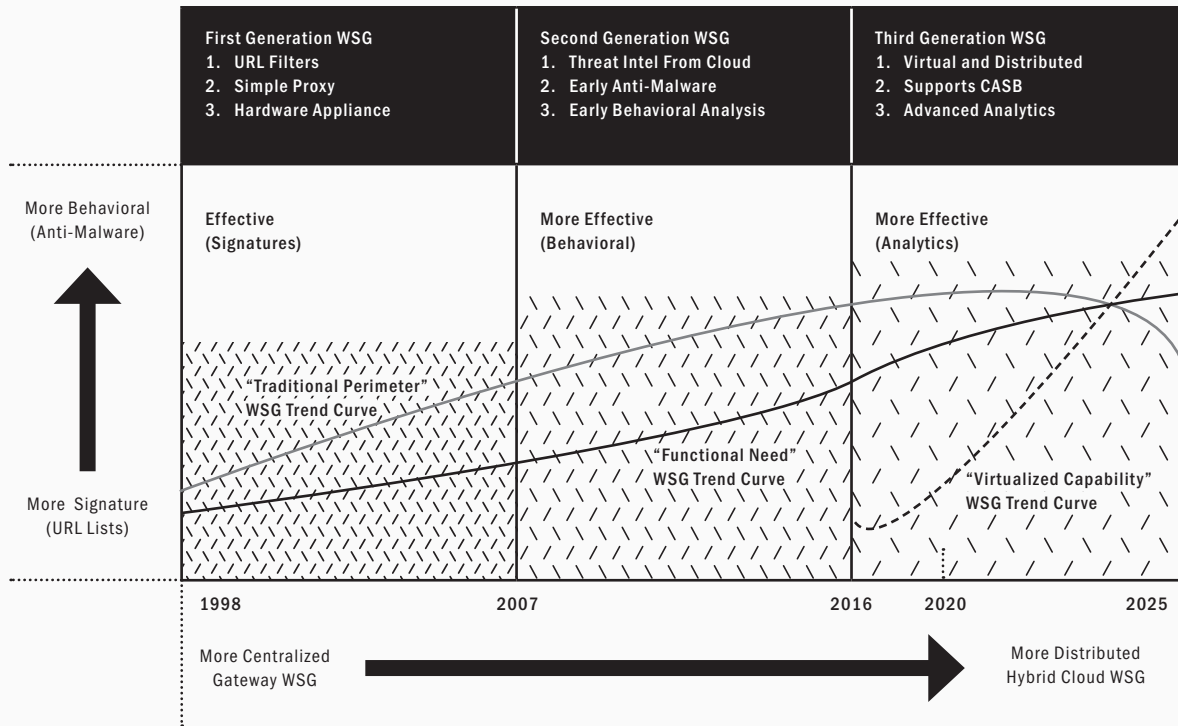
2020 Trends for Web Security Gateway

Web security gateways began as proxy devices that were put in place to support acceptable use policies for web access, and have since evolved to much more effective functions in the present generation as algorithms and threat feeds continue to improve (see Figure 1-8). This trend is good news for enterprise security teams who rely on this important functionality to reduce their data exfiltration risk.

Additional trending involves WSG detection and prevention approaches moving from lists of URLs to more advanced behavioral capabilities designed to detect malware and other exploits. The architecture of the WSG will also shift considerably, as the perimeter dissolves and more organizations adopt a zero trust security methodology. While the functional need for WSG continues to grow, the traditional perimeter set-up has already begun to wane.

The result of all this architectural evolution in the enterprise is that virtualized WSG capability will become an important functional component of emerging cloud-based software defined perimeter (SDP) enterprise set-ups. Expect to see such functional ability to provide both forward and reverse proxy-based protections for cloud workloads, virtual perimeters, application containers, and other virtual constructs.

Figure 1-8. Web Security Gateway Trend Chart



WSG for enterprise cyber security has been one of the most successful functions over the past two decades, but massive de-perimeterization will prompt changes in this solution area. With fewer companies each day relying on a physical Internet perimeter, the web security gateway becomes more a functional requirement than a tangible device. The best vendors will recognize this and will adjust, but security teams should keep watch on how this transition is handled.

Integration of WSG capability with other adjacent controls, such as secure remote browsing via isolation techniques or behavioral analysis for anti-fraud, will likely result in a set of functional requirements for the emerging software defined perimeter (SDP). This is good news, because while many teams talk about SDP for zero trust, it's often been unclear what this actually means. Integrated functional controls for emerging SDP will solve this problem.

9

CA/PKI SOLUTIONS

Public Key Infrastructure (PKI)/Certification Authority (CA) solutions originated with great advances in cryptography half a decade ago, and have continued to be refined and improved by talented computer scientists, many of whom serve in academia. PKI-based technology might be the most elegant, but also the most complex, technology employed in the enterprise security arsenal, and for this reason, has experienced varying levels of proper application and attention.

Surprisingly, few technology companies have found ways in the past few decades to make decent money selling pure PKI solutions. Instead, the capability has emerged as an essential embedded component of many other software and computing functions. It underlies all encryption support, all secure networking, and many other aspects of cyber security including software integrity checking, secure file transfer, and secure messaging.

One area where enterprise users and service providers should be more attentive, and likely will be more attentive in the future, involves the proper security protection of keys and certificates. Like privileges and passwords, these important elements of an underlying enterprise security architecture are often handled either manually or via ad hoc procedures. This is getting better, but deserves more attention in the marketplace.

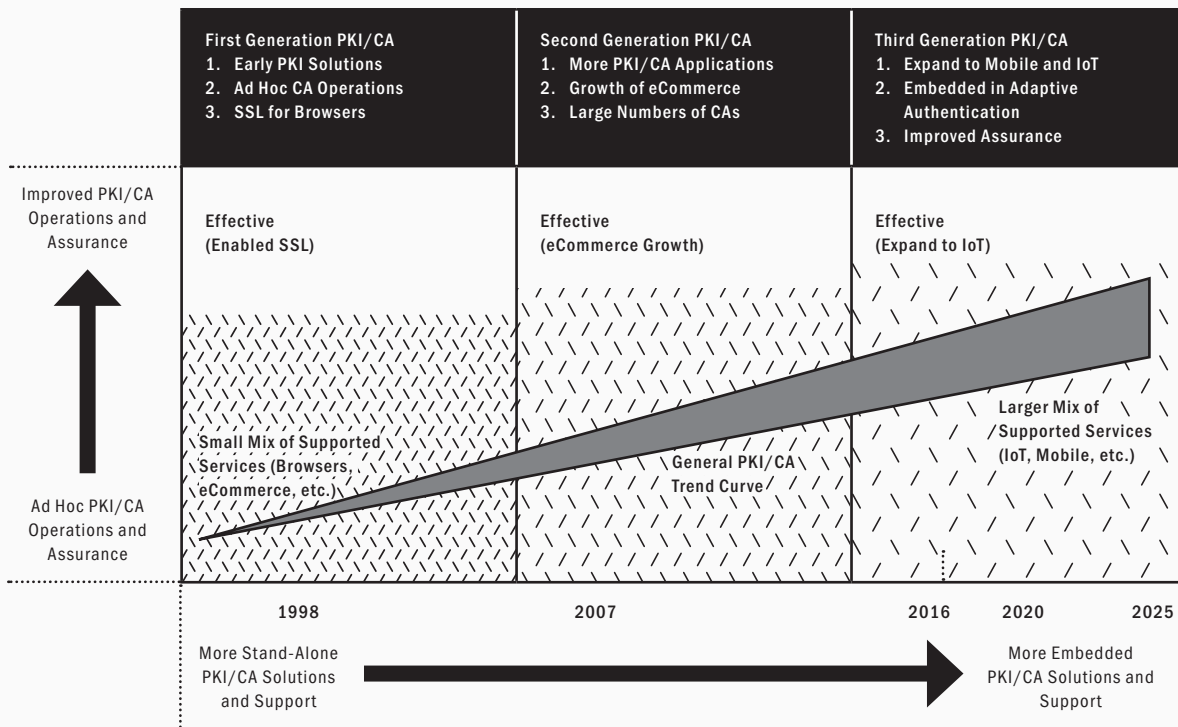
2020 Trends for PKI/CA

PKI/CA solutions have evolved from effective PKI/CA embedded in browsers for SSL (thus enabling early e-Commerce business) toward much improved and more effective operations (see Figure 1-9). The number of global CAs in business remains high, but their business success has been mixed, with perhaps a Pareto chart of financial returns having a long tail of small CAs of dubious quality.

The trend from more ad hoc, manual operations began in the first generation of PKI/CA solutions with the admirable goal that multiple assurance levels would provide users with the ability to determine the proper fit for their application. CAs published statements of their certificate policies and assurance processes, and it was assumed that this would be viewed as valuable information for users.

What happened instead was that few users bothered to review the multiple assurance levels for certificate handling (not unlike users reading user licensing agreements for software), and instead, the process converged on assumed basic assurance levels. This has led to more uniform handling of PKI/CA at the service provider and enterprise levels. Most larger organizations have had their PKI operations audited in the past few years.

Figure 1-9. Public Key Infrastructure Trend Chart





James Eades, Unsplash

The trend from a smaller mix of supported services by PKI/CA solutions to a much larger mix of supported services follows the trend toward more devices needing cryptographic support. The explosive growth of Internet of Things (IoT) and operational technology (OT)-based devices and systems will require comprehensive PKI support for embedded secure communications, authentication, and other operations.

The future of PKI/CA solutions is bright from a technology perspective, in that the underlying algorithms, tools, and protocols will serve as the basis for many emerging innovations. Autonomous machines, for example, will require embedded cryptography for their communications. The business prospects, however, will remain muted, as PKI/CA solutions will continue to serve as embedded, rather than highlighted components of a security architecture.

It remains important, however, to recognize the business challenges in providing generic PKI/CA solutions to the market. Vendors will see much more financial success in the marketplace by integrating their PKI/CA solution support into specific domain areas. IoT/ICS, for example, is one area where PKI-based technology will be essential to ensure high assurance communications between machines. Commercial PKI/CA vendors will make more money being domain-specific.

**CLOUD
SECURITY
/CASB**

Cloud security has emerged as one of the most important areas of cyber security protection, both as a stand-alone category, and as a broad solution descriptor for a mix of sub-categories focused on cloud protection. Perhaps the most prominent offering of these categories, cloud access security brokers (CASBs) and cloud workload visibility software, have truly grown in recent years into components found in virtually all hybrid cloud architectures.

The massive push to hybrid use of public cloud has been the driver of these solutions. The great irony is that some more progressive security experts have come to recognize that cloud might be more in the solution column than the problem column for overall cyber security. Consider, for example, that by scattering app workloads across public cloud as-a-service systems, the frightening lateral traversal risk for advanced persistent threats wanes considerably.

Every enterprise security team today includes some measure of cloud security, if only as a set of protection and data handling requirements for any third-party public cloud services in use. Managing and coalescing the plethora of scattered cloud accounts among individual employees using their work email address into one master account is also popular to better control cloud access, as well as to ensure proper licensing support for enterprise use of cloud service.

It is worth mentioning that the compliance-oriented approach of early enterprise teams to cloud services has now shifted toward functional cyber security. This is good news, because it implies a more active role for CISO-led teams in determining how data and systems are secured in the cloud. The early checklist approach that just passively requested security data from cloud providers has thus been improved dramatically in most enterprise environments.

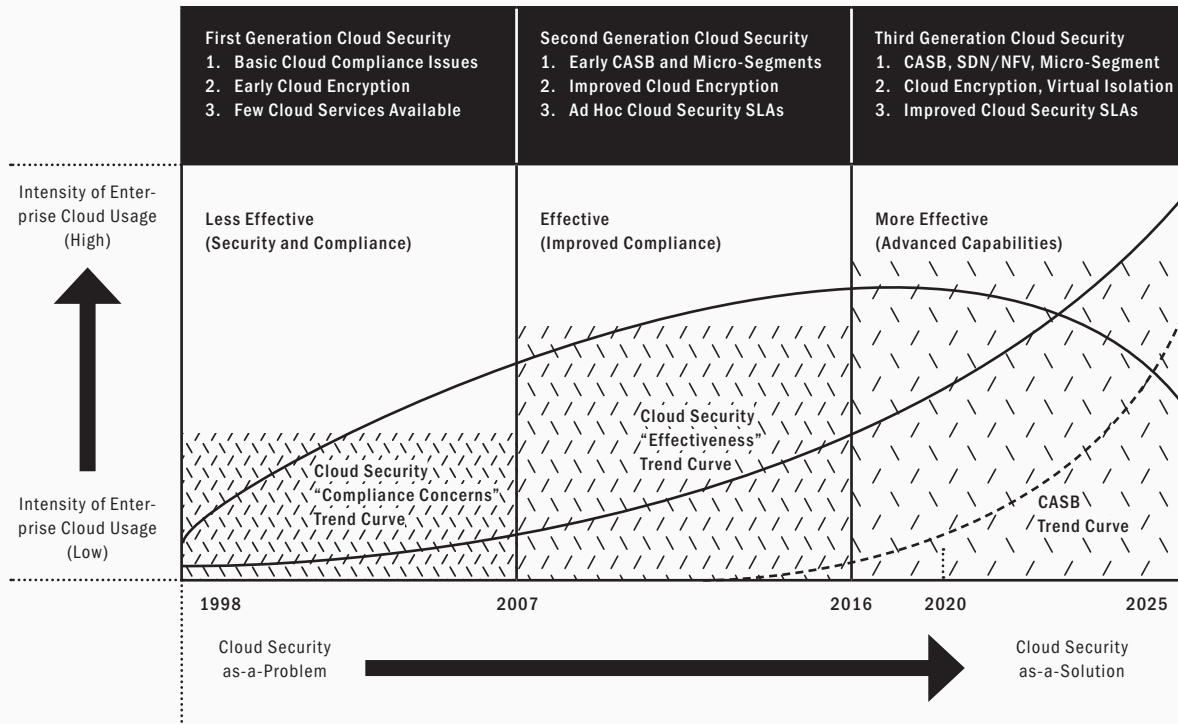
We decided to highlight CASB functionality last year in our report, simply because the solution is so well-suited (and continues to be well-suited today) to the transition to hybrid cloud services in enterprise. The vantage point for CASB devices to monitor cloud usage is attractive, and offers visibility and mitigation options that just seem to match most enterprise architectures – hence, our enthusiasm and highlighting of the approach in our advisory work.

Let's summarize: Cloud security is a big topic in 2020; moving workloads to the cloud is more a security solution than a security problem; vendors offer a massive assortment of cloud security-related offerings (in fact, almost all security solutions are now called cloud security solutions); and the drive to cloud and use of CASB is consistent with most design paradigms including Zero Trust Security and Software Defined Perimeters. That's a lot to digest, but it's all good.

2020 Trends for Cloud Security

Cloud security solutions evolved from less effective initial offerings in the first generation of cloud usage, toward effective solutions in the form of CASB and micro-segmentation products in the second generation, toward a present and future generation of more effective solutions with heavy growth in the use of CASBs for cloud visibility and potentially

Figure 1-10. Cloud Security Trend Chart



software-defined perimeter support (see Figure 1-10). The intensity of cloud usage for enterprise during this generational evolution has gone from low to high, and the attitudes of security and IT staff have shifted from security as-a-problem to cloud security as-a-solution. The importance and magnitude of this shift, especially on the part of senior managers, board members, and compliance auditors, cannot be under-estimated, because it has unlocked one of the most consequential shifts in the history of enterprise IT.

As a result, expect a continued shift downward in compliance concerns across enterprise for cloud systems supporting critical services. Compliance concerns peaked a few years ago, but this will weaken in 2020 as managers and security teams become more comfortable with public cloud services, and as providers continue to innovate. Commercial tools from the best cloud security vendors will also contribute toward this improved comfort zone.

The future of cloud security is about as bright as one will find in the cyber security industry. The need for world-class commercial tools will continue to increase across all segments of the enterprise, and vendors will see significant growth – so long as they continue to provide good solutions. CASBs will play an especially important role in redefining the corporate enterprise as they transition from passive visibility tools to more active mitigation components.

Expect to see SDN-powered solutions play a larger role for cloud security, including in the adjacent area of software-defined data centers (SDDCs). In addition, virtual management and orchestration of policies across distributed workloads will be a massive growth area for cloud and SDDC installations. Vendors who can successfully support orchestration in cloud will see considerable business success and growth in the coming years.



**AN INTERVIEW WITH CARSON SWEET
CO-FOUNDER & CEO, CLOUDPASSAGE**

PROTECTING CLOUD-BASED WORKLOADS

PROTECTION of cloud workloads is a massive undertaking as enterprise teams shift application workloads from traditional data-center architectures to dynamic cloud infrastructure. Proper security for cloud-based workloads requires a combination of functional controls, starting with comprehensive visibility into security and compliance concerns. Delivering this security requires workload protection platforms that are capable of high-scale sensor deployment, data collection, and analysis. These capabilities must extend across public, private, and hybrid deployment models; they must also address a number of workload form-factors including servers, cloud instances, containers, and serverless.

CloudPassage is a recognized industry leader in cloud workload security and compliance. Their emphasis is risk visibility and protection of servers, containers, and serverless workloads. Their approach to visibility and compliance for distributed workloads is consistent with the direction of most modern, technology-driven organizations. We spent time with industry veteran Carson Sweet, founder and CEO of CloudPassage, to gain his unique insights into progress being made in cloud security and compliance.

EA What is the current state of cloud-based architectures for enterprise? Have all teams made the leap, at least to hybrid cloud?

CS Today it's virtually impossible to find an enterprise, big or small, that is not taking advantage of cloud-based infrastructure. With the exception of startups that were "born in the cloud", all of these enterprises are migrating from traditional to cloud-based infrastructure. That doesn't happen all at once, which means by definition they have a hybrid infrastructure security need. This maximizes options and flexibility for an organization to match a workload computing requirement to the right underlying platform, service, or infrastructure. But it also increases the complexity of successful security and compliance. Taming this complexity for the security and compliance stakeholders is where CloudPassage focuses its efforts for customers.

EA Tell us about the CloudPassage solution and how it addresses cloud security in general.

CS All CloudPassage solutions are delivered from a single SaaS-based platform named Halo. This platform was designed and purpose-built to provide security and compliance visibility into cloud infrastructure assets. These assets could be cloud server instances, S3 buckets, database-as-a-service deployments, Kubernetes clusters – really any server-based, containerized or serverless component that could be considered an asset worthy of protection. We do this in a continuous and automated manner, which allows for the consistency and operational efficiency that's critical in these fast-moving environments. The platform can be deployed to protect any workload, but is optimized for workloads hosted in public cloud infrastructure like AWS or Azure. Automation is obviously a critical aspect of the solution, because manual efforts simply fail at the speed and scale of cloud environments.



With the advent of cloud infrastructure, visibility requires instrumenting many different collection points.

EA What are the implications for an enterprise team of having access to the visibility offered by your platform for cloud workloads?

CS Having full visibility is a requirement because cloud-hosted applications have an attack surface that's larger and much more dynamic. In the early days of security, the ubiquitous perimeter paradigm meant security practitioners could focus their attention on a far fewer number of controls – sometimes even a single gateway or firewall – and there was total access to every layer of the stack. But now, with the advent of cloud infrastructure, visibility requires instrumenting many different collection points that must ingest, normalize, and evaluate data in real-time, factoring in all relevant context. This is not an easy task and can only be accomplished with an automated platform such as Halo. And the scale of this kind of platform is not to be underestimated. Halo processes around 325 terabytes of customer data per day and around 150,000 Kafka messages per minute. This isn't the kind of capability that's a snap to build in-house, so Halo users have access to scale and speed that they just can't get elsewhere.

EA Any near- or long-term predictions about cloud security?

CS I think cloud migration will accelerate industry-wide. The “mainstream middle” of the market is onboard now, and that's a tipping point. There will be pain for both large enterprises and mid-sized enterprises. The large enterprise teams will struggle with changing an entrenched mindset – moving application workloads to cloud requires more than just an architecture shift. It also requires a change in how the business operates, performs compliance, installs controls, creates new products, and on and on. The mid-enterprise organizations will struggle to handle the sheer volume of work required, unless they have great automation. Interestingly, we don't see the mid-enterprises spending time trying to

build their own solutions in-house, baking off half a dozen vendors, and other large-enterprise behaviors. They know they just have to get it done. For enterprises of any size, dealing with public cloud migration will demand significant change. My prediction is that the organizations who can do this most effectively will be able to achieve faster overall technology innovation. We all know that buyers expect continuous innovation – I think I have mentioned my “Apple Effect” theory to you – and speed of innovation will equate to competitive advantage. The ultimate value that CloudPassage seeks to deliver is enabling enterprises to do more of what they do best and gain competitive edge, without having to worry about becoming a headline. The first step is visibility – if you can’t see it, you can’t manage it.

DDOS SECURITY

Distributed denial of service (DDOS) Security solutions emerged in response to the growth of brute-force denial of service as a legitimate attack weapon against businesses with real potential consequence. In the earliest days of DOS and DDOS, these attacks were mostly for play and for show, and it was rare for a serious attack to cause much more than a bit of buzz and stir around the networking community (e.g., the early DDOS attacks of 2000 against eBay).

As the attacks grew from small single-digit Mbps capacities to the eye-popping Tbps sizes of today, the DDOS solution space grew into an important consideration for every commercial and government sector. DDOS vendors in this space grew from niche technologists to significant and highly recognized brands in cyber security. This fact underscores how important it is for modern enterprise to ensure that their data can flow into and out of Internet-facing sites.

It is worth mentioning that many teams point to the use of content distribution network (CDN) as providing important protection against DDOS attacks. One cannot dispute that distribution of access points for websites and other on-line resources are great ways to reduce the exposure to a targeted, volume-based flood. Good load balancers can help too! It seems prudent and imperative, however, that procedures be established to deal with unexpected traffic waves.

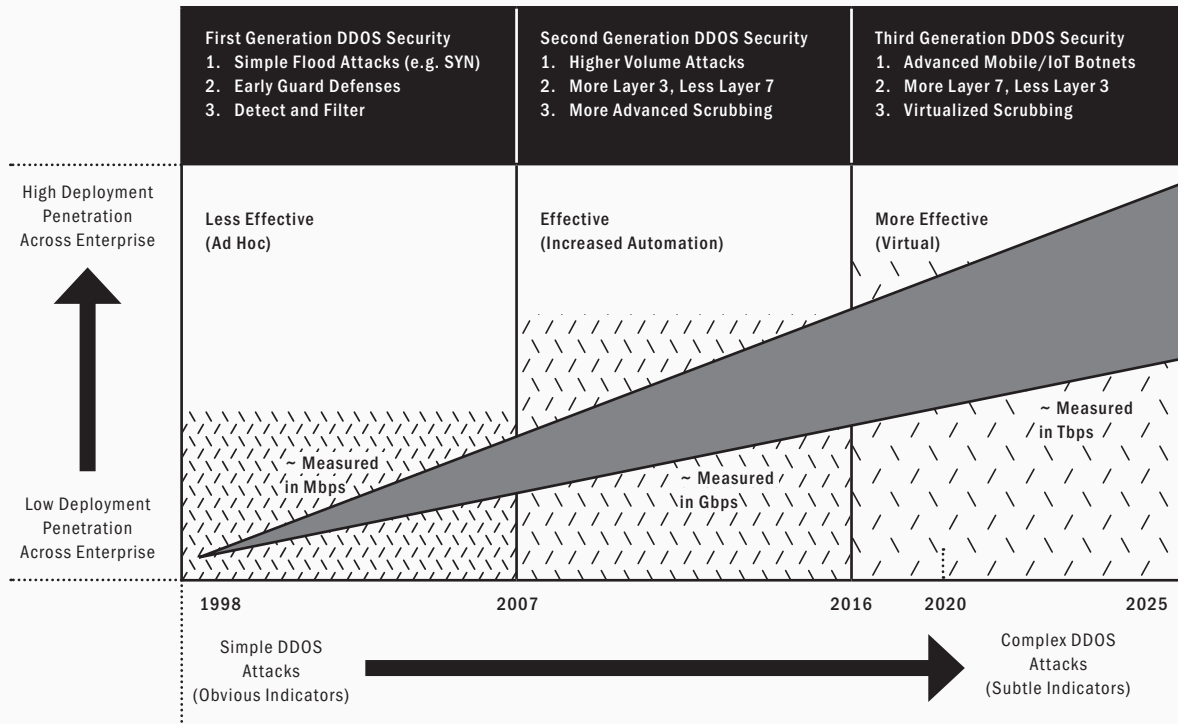
Ultimately, the best DDOS security for enterprise will start with excellent scrubbing capability, including virtualized support, to protect the most important systems and services from significant, targeted attacks. But this capability will be enhanced by well-designed architectures using both CDN and distributed cloud workload approaches to ensure a high level of resilience against DDOS attacks, usually from botnets.

2020 Trends for DDOS Security

Distributed denial of service solutions evolved from less effective, ad hoc filters in the first generation, to effective solutions using automation in the second generation, toward more effective solutions including virtualization support in the present and future third generation (see Figure 1-11). Each of these solutions include designated scrubbers in special data centers, but future DDOS security will introduce virtual scrubbing, which reduces the need for hardware. During this evolution, trending has moved from low deployment across the typical enterprise – perhaps even including little or no DDOS security for many Internet-facing services, to high deployment across all enterprise networks connected to public or external infrastructure (which implies all enterprise networks). Larger enterprise teams complement their DDOS security with a CDN to distribute ingress traffic to multiple gateways.

The algorithmic processing of DDOS security solutions has also progressed from simple Layer 3 procedures that rely on basic signatures of attack, including detection of increases volumes or packet rates, to more advanced means for dealing with complex, application Layer 7 attacks by searching for subtle evidence of a brewing attack. Application-level DDOS solutions are an essential modern control in our industry today.

Figure 1-11. Distributed Denial of Service Trend Chart



The future of DDOS security lies in the introduction of advanced new controls for cloud infrastructure, mobility systems, and dynamic on-demand virtualized services such as software defined networks (SDNs). Virtualization allows for targeted infrastructure to expand (like a balloon) to absorb inbound attacks, and to contract when the volumes wane. This capability is especially exciting, because it can help address the almost limitless size of future attacks.

It is worth mentioning that Internet of Things (IoT) and industrial control system (ICS) devices connected to the Internet will offer a significant base for offensive actors to create massive botnets with great ability to perform DDOS attacks. One would expect DDOS solutions to include some attention to the unique challenges of IoT and ICS endpoints, including their use of often-proprietary protocols and technologies.

Despite these advances, the biggest challenge and greatest annoyance for DDOS vendors is that business is better when the attacks are big and prominent. Sadly, our community is all too reactive, and when a period of relative calm seems to emerge where DDOS attacks get less attention, many enterprise teams tend to view the risk as being lower or even solved. If you work in enterprise, do not fall in this trap. DDOS is a risk: Make sure you have controls.



**AN INTERVIEW WITH ALEXANDER GARCIA-TOBAR
CEO & CO-FOUNDER, VALIMAIL**

MITIGATING EMAIL SECURITY THREATS

EVERY security expert agrees that when all else fails for the intruder in a cyber offensive campaign, phishing always provides a safe means for gaining unauthorized access, even to the most well-protected systems. As such, organizations have learned that ignorance of email security can lead to serious breaches and unnecessarily high levels of information risk. When this happens, it's a shame because excellent controls have emerged for providing high assurance trust in email and collaboration tools.

Valimail is an industry leader in the protection of email from cyber threats. With deep capability in supporting standards such as DMARC, for example, the company supports high assurance for email, collaboration, and workflow activity. We recently caught up with Alexander Garcia-Tobar of Valimail to gain insights into the email security ecosystem and how the company continues to develop and innovate platform capabilities to better support enterprise customers.

EA Is it an exaggeration to say that phishing has become the number one attack approach in the world?

AGT It's no exaggeration. There's a preponderance of research reports that all agree that phishing accounts for more than 90% of all cyberattacks and breaches. These include Verizon's Data Breach Investigations Report, as well as research reports from Barracuda, Proofpoint, Cofense (formerly PhishMe), and others. While zero-days, Trojans, and sneaky network-based intrusions get most of the media coverage, most attacks are initiated by phishing emails. Even ransomware, which spreads through organizations using vulnerabilities in local area network protocols, relies on phishing to gain its first foothold. If you can eliminate phishing, then you cut off the initial vector of infection for the vast majority of attacks, thus forcing attackers to use more difficult methods.

EA How does the Valimail platform reduce email risk?

AGT Modern phishing attacks have moved beyond the obvious vectors, such as malicious attachments and links to malicious websites, and are now exploiting a fundamental weakness in the way email works by deploying sophisticated impersonation campaigns. These fake emails appear to the recipient as someone you'd trust such as your boss or your bank. And in most cases, they don't contain any obvious malware that existing security solutions are looking for. According to a recent study from Barracuda, 83% of all spear phishing emails are impersonations, which means that sender identity is the choke point for stopping the vast majority of phishes. The lack of a comprehensive identity-based solution is why there's been such an explosion in business email compromise (BEC) over the past few years. In fact, the FBI now asserts that BEC is responsible for the vast majority of cybercrime losses — over \$3.6 billion in 2018 alone. Valimail eliminates this vector by validating senders' identities through open standards and a variety of other techniques, so that untrusted and unauthenticated senders simply



Phishers and spammers can use your brand identity — and even your domain name — in their emails.

do not get into the inbox. Our unique focus on “who” sent the email versus “what” is in the email stops attacks that existing security solutions miss, which reduces the risk of BEC and other types of impersonation-driven email fraud.

EA What are the brand protection implications of email security threats?

AGT Apart from the obvious brand damage that occurs when a major breach becomes public, there’s another more insidious brand threat: Phishers and spammers can use your brand identity — and even your domain name — in their emails. These emails aren’t sent to you or your employees, so you may not even be aware of their existence. But customers, partners, and others receive them, and in most cases, the messages are indistinguishable from messages your organization sends. In fact, through social engineering, the email may be an exact copy of the company’s official communication, such as offers or invoices, with only minor changes to redirect funds, passwords, or private data to the criminal. Needless to say, this kind of phishing attack causes tremendous damage to your brand and erodes people’s confidence in the messages you send. In the worst cases, it can drastically hurt your deliverability, as email receivers start to downgrade messages that appear to come from you, because your domain has become associated with spamming and phishing. The solution to this threat is to lock down your domain using publicly available email authentication standards, starting with SPF, DKIM, and DMARC, thus ensuring that only senders you authorize can send messages as you. Implementing DMARC at enforcement usually produces a noticeable 10-20% improvement in deliverability, and it can rise as high as 80% or more in cases where a domain has suffered from a lot of this kind of brand abuse.

EA Your team has been involved in the development of a new standard called BIML. Can you tell us how it works?

AGT Brand Indicators for Message Identification (BIMI) is a draft standard supported by Google,

Verizon Media, ReturnPath, Agari, and LinkedIn, as well as Valimail. We helped start this standard and currently chair the working group that created it. The idea is simple: For messages that have been authenticated with DMARC, BIMI provides a way for mailboxes to display the sender's logo or any other image specified by the domain owner. BIMI solves two problems: One, it gives brands control over how their email messages appear in customer inboxes. And two, it provides a big incentive for companies to implement DMARC at enforcement, because that's the prerequisite to using BIMI. With BIMI, you get millions of new brand impressions, and pilot tests indicate that it will improve open rates for emails by 10% or more. For more information, check out the official website at <https://bimigroup.org>.

EA Any near- or long-term predictions about email security? Are enterprise teams making progress?

AGT Enterprises are making progress in email security. We've seen a dramatic uptick in the rates of companies deploying open standards such as SPF, DKIM, DMARC, and BIMI. They've also implemented training. That's a good first step, but the growing awareness about the role of identity in modern phishing attacks needs to translate into broad anti-impersonation solutions. This is a two-fold approach: First, DMARC must not just be deployed, but it needs to be turned on for enforcement. Only 17% of the domains that deploy DMARC ever get to enforcement, so they're not seeing any benefit from DMARC's anti-spoofing protections. Second, solutions to other types of impersonations that DMARC doesn't address need to be implemented. For example, one of the primary attack vectors our clients are trying to address is "open-sign-up" attacks, where the criminal uses Gmail, Hotmail, or other anonymous email services to create throwaway accounts with the intent to impersonate a trusted sender via a deceptive "friendly-from" name. Another insidious vector involves registering a domain name that resembles a known brand but with subtle differences such as "1bm.com" or "microsoft-alerts.com," and then using that domain to send emails with the aim of

capturing user credentials, deploying ransomware, and so on. Too often the answer to the phishing crisis is "train users better." Training has its place as part of a layered email security strategy, but if that's the only layer, then your email security cake is going to be pretty flat. We look forward to the day when enterprises have a triple-layer email security stack: Content-based secure email gateways, training, and a layer that provides sender identity validation and authentication.

DMARC EMAIL & SECURITY

A photograph of a dense forest with tall, thin, vertical tree trunks. A person wearing a red jacket and dark pants is standing on a wooden platform or walkway built among the trees. The lighting is natural, suggesting daylight filtering through the canopy. The overall mood is serene and natural.

Future email security solutions will need to expand their coverage from pure email usage toward combined use of various over-the-top means of communication.

Email security is arguably the most important and essential control in the modern enterprise – if only because phishing has emerged as the most common and successful attack strategy amongst every type of offensive approach. This suggests that an extensive and coherent email security deployment would be the norm across enterprise, but the reality is that few enterprise teams have an optimal or even rational architecture for email security.

Many modern security teams rely almost solely on awareness programs to deal with the phishing threat. Such education is certainly a reasonable complementary element to any protection program, but functional controls are more desirable to reduce risk. It is reasonable to expect that normal users would not have to carefully police their activities to ensure a primary control. This can only be accomplished through automated functional protections.

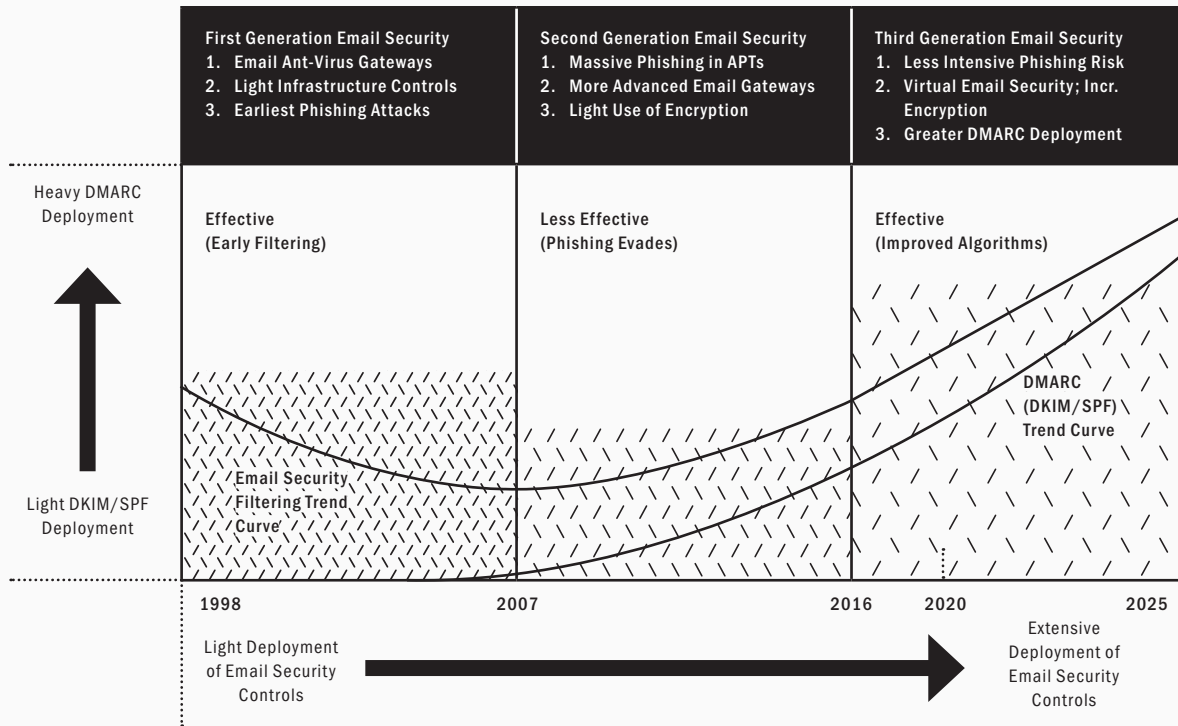
Excellent fraud protection in this regard comes from use of the Domain Message Authentication Reporting and Conformance (DMARC), which binds reported sender identities to infrastructure records that define real sources of email. In addition, email filtering and remote attachment detonation can be included in gateway functionality to identify potentially malicious content and take appropriate steps toward proper removal.

Email encryption has been a nagging issue for personal and enterprise users. One would think that encryption of messages today would be both routine and default, but the industry has not progressed in this manner. Rather, it is true into 2020 that business partners continue to struggle with the desirable practice of encrypting sensitive messages. Progress might come in 2020, but it will likely come slower than most would have expected – or desired.

2020 Trends for Email Security

Email security solutions were initially deployed to catch malware attachments, but slipped in effectiveness as phishing became a more intense threat. Email security platforms are now evolving

Figure 1-12. Email Security Trend Chart



toward effective and required controls in every enterprise. Improved algorithms and more accurate detection of malware, often using machine learning, are major contributors in this shift toward better solutions for protecting email. DMARC deployment is rising quickly from its modest roots in DomainKeys Identified Email (DKIM) and Sender Policy Framework (SPF) in the early 2000’s. The Brand Indicators for Message Identification (BIMI) standard is another good addition for security. This progression is welcome, because fraudulent use of domains, especially in financial services, continues to be a significant attack vector. DMARC usage is an excellent means for reducing this threat.

Additional good news is that email encryption, as suggested above, is gradually becoming more mainstream in modern business, although ease of set-up remains somewhat uneven. It is not uncommon for two business partners in 2019 to have to get their IT teams together to agree on a reasonable means for sending secure email. Creative

solutions for securely sending a document are also beginning to emerge in the industry. Future email security solutions will need to expand their coverage from pure email usage toward combined use of various over-the-top means of communication. Texting has already become a mainstay of modern business, but applications typically include some means for individuals or groups to communicate. Security solutions for these new forms of connecting and communicating will be required – and email security vendors are best positioned for this.

The intensity of threat to email is also tough to predict. One might have expected, for example, that the successful phishing attacks highlighted during the 2016 US Presidential election would have caused an upsurge in the protection of enterprise users from phishing attacks. While things are certainly moving in a more secure direction, the pace of change seems disturbingly slow. One can only hope that email security vendors see business acceleration in 2020.



**AN INTERVIEW WITH MATTHEW GARDINER
DIRECTOR OF SECURITY MARKETING, MIMECAST**

SECURITY SOLUTIONS FOR EMAIL

DESPITE many predictions over the years to the contrary, email has remained – and is likely to remain – the most important source of sharing and collaboration for businesses around the world. In many cases, email literally provides the lifeblood of an organization, serving as the communication means with customers, partners, and other entities. As such, security issues in email are no longer optional to address, but rather become among the most essential considerations for any organization.

Mimecast has been a leader in protecting email from advanced cyber threats for many years. Their portfolio of solution offerings provides advanced protection for the entire email ecosystem, including against the most intense threats. We spent time with Matthew Gardiner of Mimecast, to gain insights into the direction of email security for business and consumers, and to better understand how threats to email are likely to evolve.

EA What are the primary reasons normal email has become unsafe for enterprise and consumers?

MG Email has become the preferred attack delivery system for both sophisticated and unsophisticated attackers. This should come as no surprise, because email is so easy to use, inexpensive, is ubiquitously connected to potential victims, and takes advantage of busy users who don't closely scrutinize their email. In addition, from a technical perspective, email provides useful capabilities to attackers, such as the ability to carry a personalized message with both images and text, hyperlinks and file attachments, has global distribution, and provides relative anonymity. From the intended victim's point of view, email is a key business communications service and often serves as the work queue for busy and transaction-oriented people. But most users do not (and probably cannot) spend enough time determining if an email is from the claimed sender, or whether the email is risky. Furthermore, few users have sufficient insight into email domains, display names, cousin domains, malicious file attachments, social engineering, and obfuscated links to discern the risk of an email.

EA How does the Mimecast solution provide for a more secure email ecosystem?

MG A key principle behind the Mimecast email security solution is zero trust. Applied to email traffic, particularly inbound traffic, this means that every email and everything that goes along with it (links, attachments, content, and sender information) must be thoroughly inspected to verify that it isn't malicious and is wanted. Mimecast does this by inspecting every email using what we call the Mimecast inspection funnel. As an email traverses the Mimecast inspection funnel, many different analytic methods – such as antivirus engines, static file analysis, behavioral sandboxing, sender reputation, URL reputation, web site inspection, and threat intelligence information – are applied to discern if the email should be blocked, quarantined, flagged as risky, or delivered as clean. This system is curated by a global team of security researchers that are monitoring and reacting to new attack tools, tactics, and techniques that appear daily.



Most users do not (and probably cannot) spend enough time determining if an email is from the claimed sender, or whether the email is risky.

This email inspection is run globally across a dozen data centers, which process billions of emails a month for more than thirty-five thousand customer organizations. If an email is malicious or spam, it's highly likely it will cross a Mimecast gateway, usually early in its life.

EA What is the role of threat intelligence in protecting email? And does the use of cloud infrastructure influence the way email is secured?

MG Threat intelligence, both externally and internally sourced, plays a very important role in the fast and efficient detection of malicious and unwanted email. A key value of externally-sourced threat intelligence is that it provides an efficient way for the good guys to share discoveries quickly and efficiently. Without threat intelligence sharing it is every-organization-for-themselves, in effect sentencing every organization or security service provider to go it alone, while attackers share intelligence for their mutual gain. Some examples of external threat intelligence are spammer domain and sender lists, blacklisted file hashes, newly registered domains, and information about phishing kits. Internally sourced threat intelligence helps speed the detection of malicious emails using indicators of compromise that were previously detected or developed by Mimecast's security researchers. An example of this is file hashing of malware that previously required behavioral sandboxing to detect. Once a file is analyzed and discerned to be malicious via the sandbox, that file no longer needs to be sandboxed as it can, going forward, be more efficiently detected using its file hash at an earlier stage of the inspection funnel. Cloud-based deployments of email security systems are critical to its efficiency and efficacy. Cloud-based deployments not only enable the application of effectively unlimited computing resources to the analysis of emails, but also provides a real-time system of community defense which leverages the cloud services' network effect to accelerate detection. The more organizations that use the service and thus the more and more diverse set of email that passes through the system, the faster that the system will detect and apply the best defenses for everyone using the service. The more members

of the community, the more valuable the collective defense. For example, changes to settings, content, detection signatures, or analytics can be applied and be active in the Mimecast global system across a dozen global data centers within minutes. And given how early and often email is used in attacks, cloud-based email security systems provide an excellent early warning system for attacks that can only be effectively created via a global cloud-based deployment. Email security systems that are not truly multi-tenant, cloud-based but are based on an architecture that has a single tenancy per client cannot efficiently leverage this same network effect.

EA You've recently introduced some creative security awareness offerings through your Ataata acquisition. Can you tell us about this?

MG The complement to technical preventive controls is to have strong user security understanding and awareness, as employees can act as the last line of security defense for an organization. This applies to much more than email, but email is a great example of an area where improved security awareness training is needed. Since there is, and never will be, a technical preventive control or even a series of technical controls that are 100% effective, it is very important that organizations maximize their everyday employees and make them part of the solution as opposed to a source of the problem. Mimecast chose to purchase a security awareness platform with content that is particularly well tuned to the learning needs of regular employees, as this is a key point of vulnerability for organizations. In addition, there is a natural relationship between user actions and their demonstrated understanding and the organization's technical security controls and vice versa. For example, stronger security controls can be applied to riskier and more targeted employees and conversely actual phishing attacks can be defanged and be used in user training and phish testing. This integrated approach was a key driver for the acquisition as well as a driver for the planned integration between the Mimecast security controls and our awareness training service.

EA Any near- or long-term predictions about email security?

MG Email is a popular attack vector that is only getting more popular. In fact, approximately sixty percent of all inbound email is unwanted or malicious, according to Mimecast data. As attackers' tactics have become more targeted, sometimes selecting organizations and individuals to go after, detecting and stopping these attacks has become increasingly challenging. Increasingly, attackers are leveraging generally trusted web sites and services to bypass email security systems (and other security systems for that matter), while simultaneously fooling users that they are someone or some organization that they trust. Examples of this involves using cloud-based file sharing services such as Dropbox or Google to deliver malware, impersonating well-known Internet brands to steal users' credentials, registering and using similar looking domains to trusted domains, and using stolen credentials from business partners or the organization itself to enter and spread their email-borne attacks. There is no foreseeable reduction of email as an attack vector.

SDNSEC & BGP/DNS

The category of infrastructure security has always been challenging, because on the one hand, it includes the most intense threat vectors on the Internet today: Routing and naming. On the other hand, the category includes issues that are likely non-actionable by most enterprise security teams, especially ones with smaller teams or fewer experts involved in defining standards or providing cyber security thought-leadership.

The routing issue revolves around the challenges associated with the Border Gateway Protocol (BGP), which can be considered the protocol and supporting infrastructure by which the administrators (and owners) of larger networks can direct and manage traffic flows. When this process is manipulated, and it often is, traffic can be rerouted to unusual mid-points, perhaps to collect intelligence or even sniff traffic content.

The naming issue revolves around the challenges associated with the Domain Name Service (DNS), which can be considered the protocol and infrastructure by which many different individuals and groups around the world can connect names with Internet Protocol (IP) addresses. The types of attacks, tricks, exploits, floods, and other manipulations of DNS have become so voluminous as to be beyond the scope of this document.

The bottom line is that security teams must focus on three activities to reduce BGP and DNS risk: First, they must put pressure on infrastructure and telecommunications providers to manage BGP and DNS infrastructure securely. Second, they must follow best security practices for their own DNS usage and application. Third, they should be vocal wherever possible, such as in industry groups (e.g. Cloud Security Alliance) to keep awareness of these risks high.

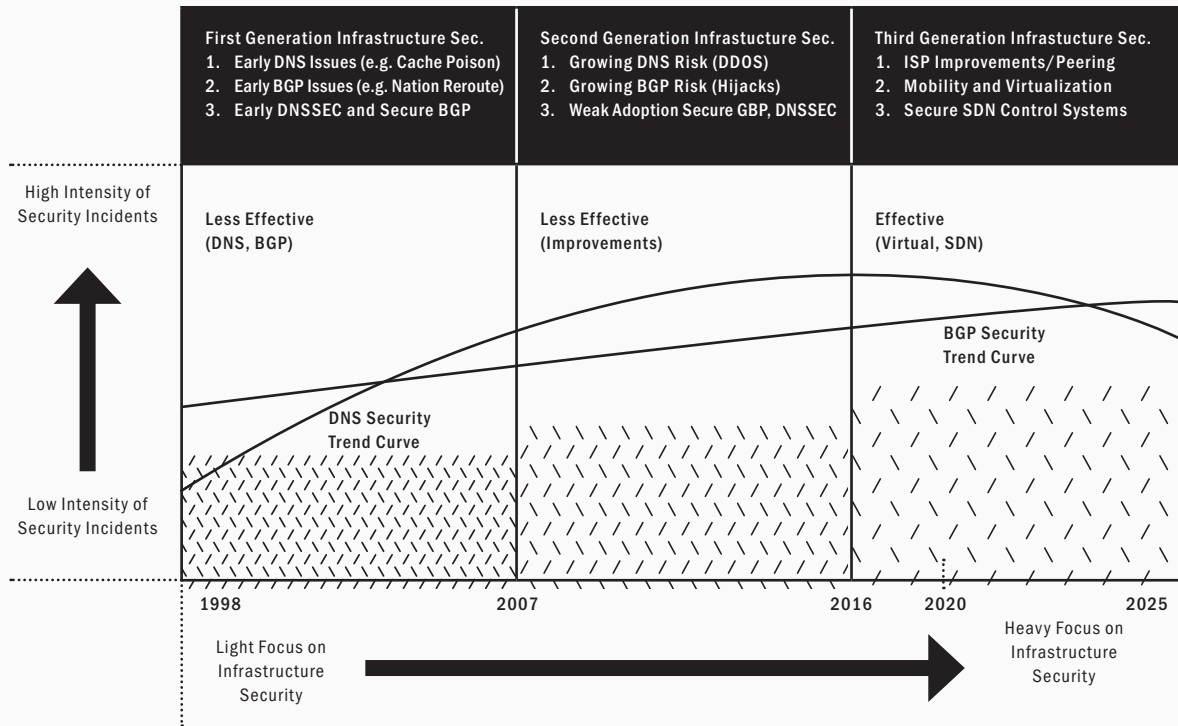
A third significant infrastructure security issue arises with the introduction of software-defined networks (SDNs) to the global network ecosystem. SDN has already pervaded the data center, resulting in software-defined infrastructure that requires proper protection; but its introduction to network fabric, including in emerging standards such as 5G for mobility, raises important obligations for providers to ensure sufficient virtual security protections.

2020 Trends for Infrastructure Security

BGP and DNS infrastructure security was less effective in the first generation as the risks to routing and naming were poorly understood and infrastructure providers had few solutions. The second generation produced slightly increased risk for BGP, but dramatically increased challenges for DNS, especially in supporting DDOS attack. The third generation has improved DNS security, given the enhanced procedural DNS controls across industry (see Figure 1-13).

Security incidents, especially for DNS, have trended generally upwards, but virtualized SDN infrastructure at the carrier and data center levels should have a beneficial impact on infrastructure threats, if done properly. Virtual security improvements should also be present for DNS, due

Figure 1-13. BGP/DNS/SDN Security Trend Chart



to the architectural shifts that occur with SDN. Data center workloads, for example, will rely on SDN controllers for east-west traffic management.

In general, the security community has come to gradually increase its collective emphasis on infrastructure security concerns across the three generations of usage. This is a welcome trend, but has also been characterized by mostly disappointing controls for both BGP and DNS. Adding PKI-based technology to both protocols has done little to reduce risk; in fact, PKI-enablement for DNSSEC could be viewed as increasing DDOS risk due to larger payloads.

Sadly, future infrastructure security solutions for BGP and DNS are likely to continue to play a more negative than positive role in overall global cyber risk. Organizations with research and development (R&D) responsibility such as in academia and government are encouraged to continue their investigations into making both types

of infrastructure security controls more effective in future applications. One big challenge here is that enterprise security teams do not directly control the management and mitigation of this infrastructure risk. Instead, they are mostly dependent on carriers and major service companies including cloud vendors to ensure sufficient risk management. The best approach for CISOs and their teams is to maintain pressure and to demand that security – especially for BGP and DNS – be attended to carefully and diligently.

An additional challenge related to modern infrastructure security – including 5G wireless networks – involves issues related to international supply chain, especially between super-power nations such as the US and China. Where concern is justified that embedded Trojans might allow for infrastructure attacks such as rerouting, one should include the direct manipulation of BGP, DNS, and other infrastructure systems as simpler means toward this goal.

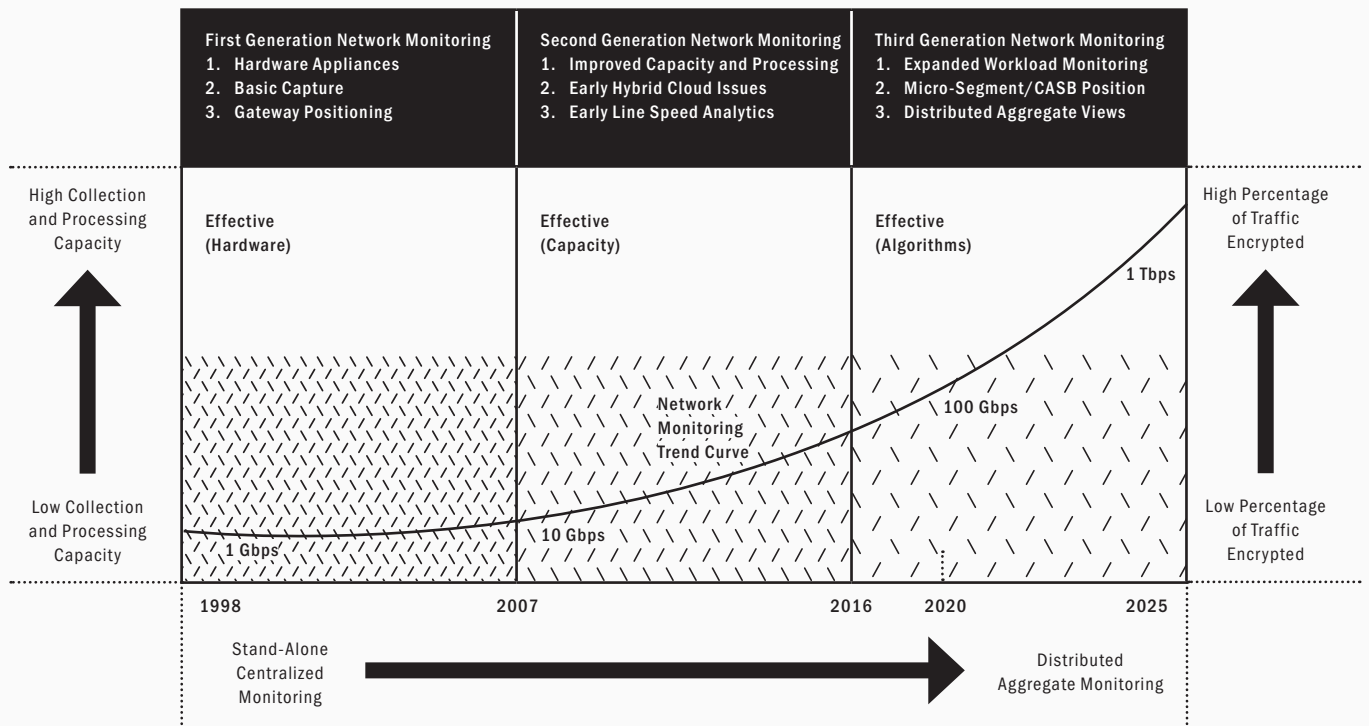
NETWORK MONITOR- ING

Network monitoring evolved from effective hardware platform solutions in the first generation, to continued effective, higher capacity platforms in the second generation, to continued effective solutions with more advanced algorithmic processing in the third generation.

Network monitoring has always been an important component of cyber security architectures, but the specific methods for collecting and processing data have evolved as network systems in enterprise and carrier infrastructure have also evolved. Larger networks have been the prime focus of most network monitoring solutions to date, but with virtualization has come the ability to introduce network visibility in a software-based environment.

The primary functional requirements for network monitoring in cyber security have centered on the capability to (1) collect data at large capacities in the 10 Gbps to 100 Gbps range, and (2) process this collected data at line speed using analytic tools and algorithms designed to detect evidence of the desired properties of interest. For cyber security, this means indicators of compromise. Other areas of focus include law enforcement and network management.

Figure 1-14. Network Monitoring Trend Chart



Privacy has always been an important consideration in network monitoring from two different perspectives: First, citizens in many nations are unhappy with the idea of their personal data being collected and processed, even if algorithms are used to filter unwanted information. Second, with privacy concerns driving increased encryption of network traffic, many monitoring solutions become challenged to detect the desired properties.

Nevertheless, world-class tools and supporting infrastructure for collecting data from a network, making sense of that data – including dealing with any encryption of relevant indicators, and then taking mitigation action based on the network analysis – will remain a staple of large-scale cyber security protection. This cadence also provides a foundation for much of the day-to-day work that occurs in a typical security operations center (SOC).

It is worth noting that many cyber security vendors supporting cloud micro-segmentation have noticed in recent years that their tools have been deployed and relied upon for network visibility more often than active mitigation. This underscores the importance of the monitoring function, not only for visibility, but also as a step toward more aggressive mitigation with reduced risk due to increased understanding of normal network behavior.

2020 Trends for Network Monitoring

Network monitoring evolved from effective hardware platform solutions in the first generation, to continued effective, higher capacity platforms in the second generation, to continued effective solutions with more advanced algorithmic processing in the third generation (see Figure 1-14). The trend curve for capacity has evolved from collection in the Mbps range, with maximums in the low single-digit Gbps range, up to modern solutions in the Tbps range.

This evolution has been characterized by hardware appliances being used exclusively toward a more eclectic mix of offerings, although the highest capacity collection and processing continue to

require specialized hardware. Algorithms have also gone from simple pattern matches and searches for obvious signatures and indicators to more subtle methods that are beginning to rely on advanced heuristics and even machine learning.

One would expect that with the advance of software defined networks (SDNs) in the provision of network infrastructure that network collection techniques would quickly gravitate toward control by SDN applications. Thus, the northbound SDN controller interface would connect to apps that would manage and orchestrate collection from devices across the southbound interface of the SDN controller.

The future of network monitoring will include two basic tracks: As network capacity continues to increase, network monitoring solutions will continue to drive to the maximum size and speed of the infrastructure of interest – often from carriers and larger organizations such as military groups and banks. But in addition, AI-based methods will begin to take hold in network monitoring platforms, offering significant new opportunities to detect indicators quickly.

An additional innovation in recent years is the ability to dynamically service chain network devices using virtual operating systems. This allows for fast, hardware-based network monitoring devices, including active load balancers, to expand their capability – often to introduce new capabilities such as next generation firewall and SSL bump-in-the-wire support. Readers should keep an eye on virtual service chaining as an important capability in 2020.

SECURE FILE SHARING

Secure file sharing is a common name used in the industry to support general collaborative data interactions between consumers, business partners, colleagues, customers, suppliers, and on and on. One subtle issue, however, is that more direct operations such as secure file sending and secure file receiving, are separate from the more general secure file sharing category. The security issues that result from the various cases will in fact be different.

A common goal, however, for both secure file sharing and sending is to support the desired interaction without introducing vulnerabilities or exposures. This generally requires attention to three basic functional requirements: First, the interaction must be authenticated – preferably in a mutual manner. Second, the interaction must include encryption of any transmitted data. Third, the data transfer should include evidence that integrity has been preserved.

Surprisingly, the secure file sharing community has included a plethora of confusing, complicated, and often tough-to-use tools that have been poorly integrated into familiar enterprise tools such as the Microsoft Exchange and Office suites. This is beginning to change, as vendors, including large providers such as Microsoft, have come to realize how important support for secure file sharing and sending has become.

In addition, excellent and easy-to-use utilities have emerged that allow for fast, convenient, and secure file sending and receiving between participants who might not have interacted previously. This is a welcome advance, because it supports business practices that go back many centuries or longer – namely, the routine back-and-forth cadence between buyers and sellers who have not previously interacted. This is the basis for most commerce. The good news is that secure file sharing, sending, receiving, and collaboration have become table-

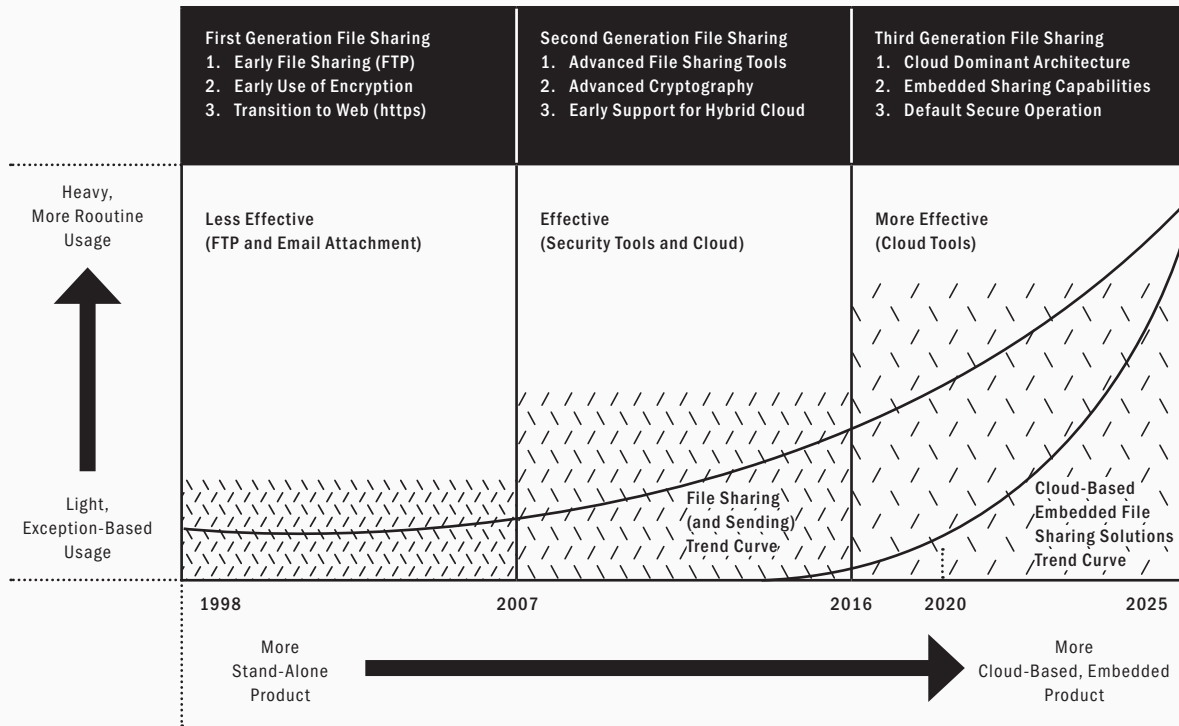
stakes in most organizations to work with third-parties or to serve their customers. This is good news, because solutions and platforms to support these requirements securely are being introduced not because the capability is possible, but rather because the capability is perceived as a necessary function. This is a welcome situation for vendors.

2020 Trends for Secure File Sharing/Sending

Secure file sharing and sending have evolved from less effective first generation solutions based on File Transfer Protocol (FTP) and email, to effective second generation solutions that were more securely designed (although not as widely deployed as they should have been). Third generation secure file sharing and sending solutions are now more effective from both a security and wide deployment perspective (see Figure 1-15).

One of the key aspects of this evolution has been the shift in emphasis from light, exception-based use of encryption or other security enhancements for file transfer and collaboration, to more routine use of security capabilities. Today, it is no longer considered an unusual request for a business partner to demand or expect that files be transferred in a manner that avoids cyber risk. This is a welcome change.

Figure 1-15. Secure File Sharing Trend Chart



Additionally, cloud-based shared services have lent well to more secure remote collaboration, interaction, sharing, and sending of files and other data in a manner that respects security considerations. The concept of a secure cloud-based service involves protections that do not rely on network locality or trust to ensure controls. Instead, cloud services treat all requests as untrusted, which is consistent with secure file handling solutions.

It is worth highlighting that embedded support for secure file sharing, transfer, and sending within popular public cloud-based services is not only inevitable, but has already begun to occur at scale. The industry should expect to see exponential growth in security features for users of public clouds, especially ones that already support data storage, handling, and collaboration by different untrusted entities. The future of secure file sharing and sending lies in the cloud. It seems inconceivable in the coming years that major public cloud providers will not aggressively pursue this business

area. They'll certainly need to work with (or acquire) specialized firms that offer best-in-class tools, including secure sending capabilities. But in the end, one should expect that most consumer and business secure file interactions and handling will be done in the context of cloud services.

This cloud-based focus will lead to many wonderful security innovations, including better support for compliance and reporting, geo-storage support for privacy constraints in certain countries, different levels of data security for differing levels of application criticality, and even better security monitoring support, perhaps using advanced behavioral or machine learning algorithms to detect anomalies.



AN INTERVIEW WITH TONY PEPPER
CEO, EGRESS

SECURING EMAIL AND UNSTRUC- TURED DATA

THE essence of modern business involves data and resource sharing, usually via email, between different entities, often located remotely, and sometimes engaged for a temporary interaction. This suggests that modern data security must be rooted in the process of email collaboration, with control emphasis on auditing, compliance, and leakage protection. But emphasis must also be placed on productivity, on-line experience, and meeting corporate goals through collaboration.

Egress provides a security solution, including desktop and mobile apps, that focuses precisely on this goal of optimizing data protection. Its AI-powered platform protects sensitive information and helps drive productivity for common suites such as Office 365. We recently connected with Tony Pepper, CEO of Egress, to learn more about how the company is serving its enterprise customers, as well as the types of trends the company sees in the protection of modern enterprise data.

EA Why do you suppose so many companies today continue to struggle with the goal of securely sharing unstructured data, usually via email?

TP That's a great question. We have some new facts on the problem that shine a spotlight precisely on why companies struggle with sharing sensitive unstructured data via email, even with investments in the cloud like Office365 and traditional DLP and encryption systems. It's one thing to have fundamentally important technologies like basic email encryption, but it's another challenge entirely to make it frictionless for users on both sides and to solve the insider risk problem. It's rare to hear CISOs say they love traditional email encryption. Users often hate it, as the user experience is a hoop-jumping exercise that's usually painful. Encryption is both friend and foe too, without a modern people-centric approach – providing it can create a new leakage vector that's more invisible than before. Earlier this year, we asked a well-established independent consulting firm to review over 4000 employees and 500 CISOs and IT leaders split across the US and Europe about insider risks in their organization around email. The goal was to see what perception versus truth was in information risk handling. Of course, as the de-facto standard for business engagement, email is both a top tool and a vector for leakage, new threats, and emerging risks. Outlook and other email clients are on every desktop and mobile. The study revealed very interesting results. Some are not a surprise, like the fact that 95% of IT leaders worry about the insider threat, both malicious as well as accidental. But even companies with traditional and probably clunky encryption in place had surprising findings, with over 55% of employees leaking data, doing so because they weren't provided with tools they could use each and every time.

EA How does the Egress platform work and how do customers integrate your tools with their existing email and collaboration ecosystems?

TP With a decade of success in securing email content for millions of users globally, we've had the opportunity to have both unique insight and data that can now be combined with powerful machine



It just takes one click and it's game over for privacy compliance and hello to massive CISO pain.

learning technology to detect and handle very difficult risks. For example, if you think about how financial services firms establish risk with their customers in the US, they use the notion of a risk score – your credit rating - to determine the level of risk in offering services to you. Why haven't we done that for things like email and collaboration tools? Well, that's exactly what we now have. We've applied this risk scoring concept by combining granular DLP technology and behavior analytics to solve problems that traditional DLP simply can't or can't scale to in a business and be managed. For example, a really big problem in industries like finance or healthcare is the problem of employees sharing the wrong content with the wrong recipient – becoming the accidental inside threat. Firms deal with lots of producers and consumers of data and the business leaders will be those that respond swiftly and accurately to customer needs. However, it's no secret in the industry that mistakes happen all the time – wrong content to the right person, right content to the wrong people, and so on. It just takes one click and it's game over for privacy compliance and hello to massive CISO pain. The Egress platform can actually match content to recipients, and user interactions to other user interactions, inside and outside the enterprise intelligently – so human mistakes can be detected in real-time. The system is smart too. It learns good behavior so that users are given advance feedback of bad behavior before hitting "Send" and potentially costing them their job and causing the company a world of regulatory pain. The beauty of this is that with cloud delivery, it's just a matter of plugging into the email system like Outlook and configuring policy. We take care of the complexity of the machine learning methods, the analytics processing, encryption, rights management, and machine decision making. CISOs can get precise data on where there are behavioral risk hotspots and where the tool is solving real problems – a huge value to what was formerly a very, very difficult problem to solve – namely, the pervasive human error in data handling and inside threat.

EA Do you think business productivity can increase with more secure sharing and collaboration? Most people would traditionally

expect security to slow things down.

TP When tools are wrapped around the user that help them avoid making mistakes, the feedback is very positive, especially when we can catch the “Oh no!” career-limiting moments before they become massive problems. People love the fact that they have a helping hand that’s not invasive but is there in the background – a privacy risk co-pilot if you will – to guide them in managing sensitive data and enable them to get on with business when sharing sensitive data is required. So, in fact, this people-centric risk management strategy actually becomes an accelerator, not a blocker as with more traditional perimeter approaches. While cyber security training is important, it’s often quickly forgotten, so automated feedback, as well as tools to secure sensitive data, go a long way to enhancing productivity without adding complexity and overhead. In one case, we helped an organization of around 2,000 employees with an email-centric engagement process with lots of business partners losing around 40-50 hours of FTE time per accident investigation and hundreds of such incidents per year impacting privacy compliance. If you think about it, that’s forensic team members at potentially hundreds of dollars per hour taking time that’s not adding to the bottom line. It’s a million-dollar problem and can be solved at a fraction of the cost to a business, let alone the time loss.

EA What is the role of data classification in the overall data security architecture? Do enterprise teams do an acceptable job of understanding and classifying their data?

TP Classification is a long-established process, but often misunderstood or maybe even only implemented on paper versus in day to day IT processes. How many times have you heard “We have a classification policy” only to find it never used except for the odd rubber stamp? If classification decisions are left to users, they often get them wrong by guessing, based on their perception of risk. Our study also showed variation based on generation and role. It’s not uncommon in some enterprises to find people in roles that don’t reflect what they actually do or aren’t

updated with change, which can affect how they are allowed to classify data, which then amplifies the misclassification risk. For instance, should a customer service employee be able to classify data as COMPANY-SENSITIVE or as CUSTOMER-EXTERNAL? Classification of content should ideally be automated and based on a risk score at the time of sharing and access. This involves a combination of the content, the people, where it is going, and under what conditions it’s accessed at that time. There’s no point in classifying something as SECRET and sending it to a recipient at a domain where the risk, hygiene, and reputation can’t be determined in advance. The key to success is to present the risk in a meaningful way that people can understand in advance of data sharing, showing identified content classification as real-time user feedback. The combination of machine learning and fine-grained DLP with this intelligent user feedback approach solves two problems: One, it supports correctly classifying based on the calculated risk and context of data – ultimately answering the question – what is the likelihood this will be breached? The right level of protection strategy can then be automatically applied to secure it. Second, user feedback brings a level of situational awareness and education to the user about what they are handling – continuously ensuring their responsibility as an employee is understood, but not in an annoying way that traditional pop-ups tend to bring to the table. It has to be smart.

EA Do you have any near- or long-term predictions you can share about data and email security? Are things improving generally?

TP The irony is that while attacks to steal data over the last few years focused on app security weaknesses, as businesses moved to the cloud and hardened their app stacks and code base, and enterprises have implemented tighter controls for PCI, HIPAA, and so on, the weak link now is back to the person – and the attackers know it. We’re seeing the next wave of phishing attacks luring people into mistakes. Enterprises often have notices that the employee is the firewall – and it’s so true, now more than ever before. At the same time, nobody is telling employees to work less and do less. The pressure is on to compete and succeed, so the combination

is a ticking time bomb of people-centric risk. It really is the dawning age of the assistive user-centric IT power tools for people that use machine learning as an enabler that goes well beyond traditional perimeter blocking and tackling. AI is a key enabler. We're seeing the same technology in all walks of life and CISOs are more than happy to arm their employees and business partners with the best tools for the next wave of cyber-combat and defense in depth. It really is the time for AI assisted traditional controls focused on specific risks to nail them – we're at the very dawn of this new era.

**VPN/
SECURE
ACCESS**

Secure remote access began in the 1990's as a practical means for enterprise workers to gain remote login to the corporate LAN to work on weekends and evenings (or during snow storms). Gateways were established that allowed for such remote access, often with just a password for validation, and many of these original access mechanisms reside on corporate LANs today, albeit often with enhanced two-factor authentication.

The first challenge that occurred for secure remote access involved mobiles (originally Blackberry devices and enterprise servers), which required different handling than home PCs for gaining admission to the corporate LAN. Various solutions such as container-based tunnels and per-app VPNs to enterprise-hosted applications found their way into the enterprise in the 2000's and this created a bifurcated secure remote access environment for PCs and mobiles.

The second challenge for secure remote access involved public cloud-based services. Where the initial presumption in the design of remote work solutions was that enterprise apps would be hosted on the corporate LAN, the approach evolved to where apps typically reside in cloud-hosted systems, often located outside the corporate firewall, and thus outside the location where secure remote access gateways had been installed.

The result was a hybrid arrangement, which exists to this day, where users with their mobiles and PCs use a variety of techniques to access on-premise and cloud-hosted applications. Some would call this the essence of a hybrid arrangement, where others might simply call such set-up a total mess. Regardless of the moniker used, the hybrid approach does not lend well to orchestrating common, uniform procedures or policy enforcement.

Where most organizations are shifting is toward a zero trust security approach, where the secure

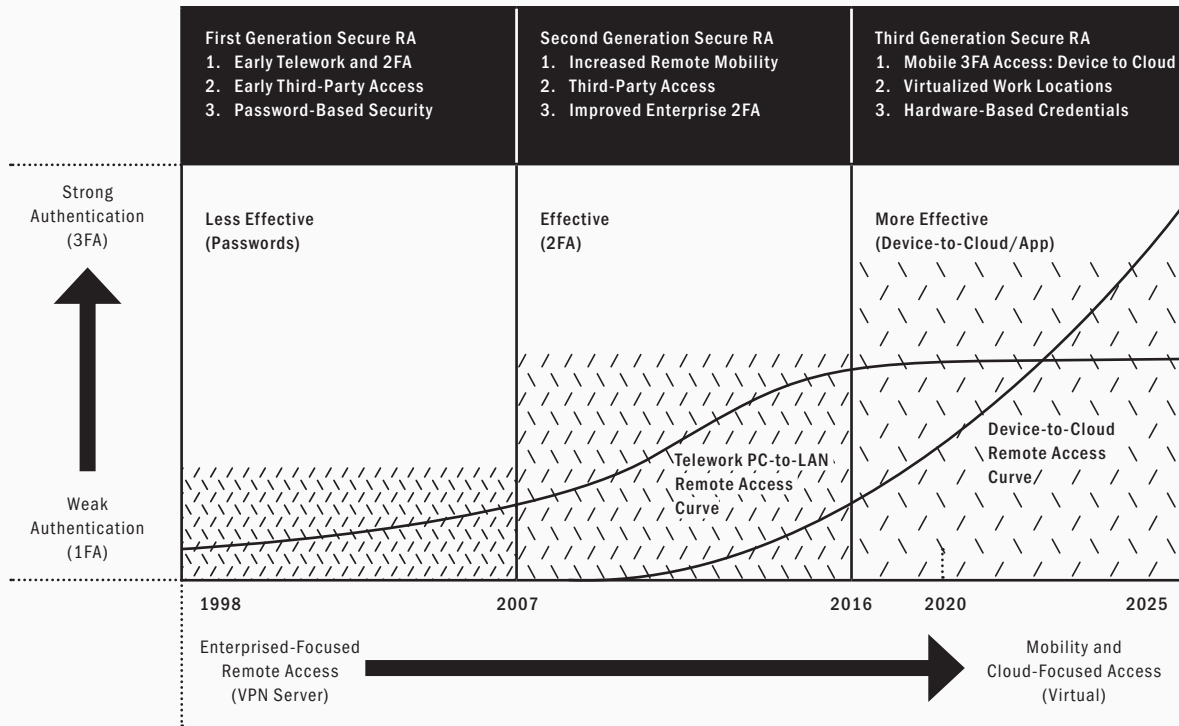
access gateways reside in generally accessible network locations, with no reliance on any perimeter for protection. This provides all the benefits of arbitrated security with none of the architectural weaknesses of legacy perimeter LANs. The introduction of zero trust to secure access will be one of the most important characteristics of the enterprise network in 2020.

2020 Trends for Secure Remote Access

First generation secure remote access supported the growing need for telework, and the typical security scheme was less effective regarding threat. Second generation secure remote access improved matters with the introduction of two-factor authentication. Third generation secure remote access, present and future, is moving in the direction of highly-effective, highly-secure, zero trust solutions that are integrated with modern cloud and mobility (see Figure 1-16).

Weak authentication using one-factor for early secure remote access from home PCs and laptops to the corporate LAN, has been replaced with more factors – up to and including three-factor authentication in some cases (e.g., mobile device biometrics, MDM-managed certificate, and user supplied password). This is excellent news for enterprise security teams, since many attacks traditionally included unauthorized remote access to the LAN.

Figure 1-16. Secure Remote Access Trend Chart



The biggest debate regarding secure remote access involves the degree to which the user experience integrates with existing procedures. The best cyber security vendors specializing in secure access solutions understand that without careful attention to minimizing the number of steps (preferably down to zero) required to establish secure connectivity, the associated solution will not be welcomed by users. Ease of use is not an option, but a firm requirement.

This implies that the establishment of VPN connectivity through a designated application, as well as the early and existing focus on virtual desktop initiatives (VDI), will have the great disadvantage of not minimizing the number of steps to establish secure access. The most successful solutions in the coming years will have to be largely invisible to users, and the resulting risk reductions will be well-worth the additional design time and effort.

The future of secure remote access lies in device-to-cloud, where mobility and embedded controls ensure that authentication, encryption, and integrity are in place. The use of public clouds to host enterprise applications will eventually remove the need for telework-based access to the corporate LAN. This function will remain in hybrid mode for several years, so traditional PC and laptop solution needs will remain in place during that transition period.

Readers should also underline zero trust security in their secure remote access planning for the coming years. The approach combines and optimizes so many different factors that it seems unlikely that any other solution will compete. Obviously, zero trust architectures will come in many different sizes, shapes, and configurations, but the absence of reliance on a perimeter will characterize every deployment.

ANTI- MALWARE TOOLS

One aspect of the anti-malware ecosystem that remains up for debate is the degree to which AI and machine learning techniques can remove the human being from the judgment equation – for both file-based and fileless malware detection.



The earliest successfully commercial computer security control was traditional anti-virus software loaded onto the Windows PC. Since its inception in the Nineties, this control has experienced uneven success detecting increasingly subtle malware, but has never wavered from its ubiquitous presence on endpoints. This stubborn application stems partly from compliance requirements, but also reflects some advances made by anti-virus vendors.

The original concept of anti-virus, now more commonly and more accurately referred to as anti-malware software, involved matching up known signatures with a scan of the operating system. Because these signatures were based on trivially side-stepped algorithms such as file names, variants became the scourge of the control. Vendors tried for many years to keep up through amazing diligence with malware samples, but this has not been an optimal strategy.

The good news is that the incredible experience and capability of the larger, legacy solution providers, combined with creative detection enhancements from start-ups and other security vendors, have resulted in much more impressive means to detect malware than the community might recognize. Behavioral heuristics and other powerful techniques have been used to expand the aperture for anti-malware software (but signatures are still useful).

An additional powerful control has been the interactions anti-malware vendors establish between their deployed software base and cloud security analytics used by their research teams. Samples can thus be sent to cloud for rapid analysis or even expert human review to determine a verdict on the file. This process has been streamlined to pseudo-real time in many cases, which is a welcome advance for enterprise security teams.

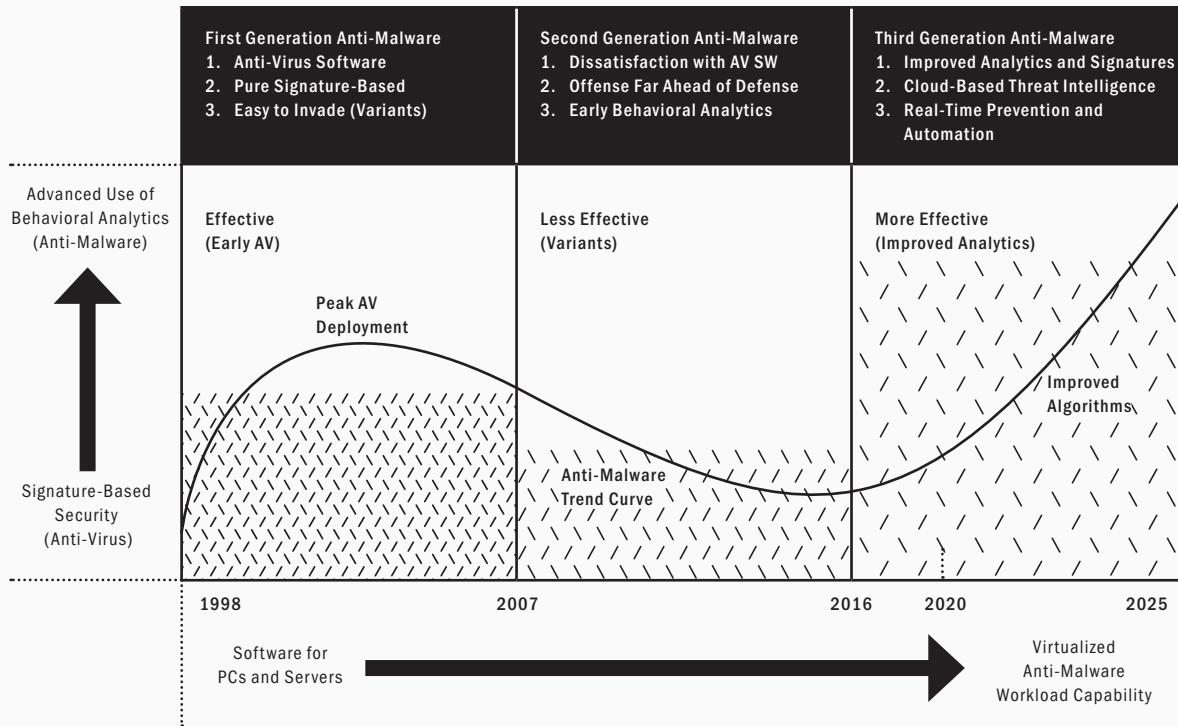
Security teams have also innovated in many different directions for anti-malware, including the use of machine learning, deep learning, and other powerful analytic means to detect the presence of malware. Tools have also been developed to ensure that intruders cannot evade anti-virus systems by detecting the specific paths used by malicious actors in practice. These advances (including for fileless exploits) increase the accuracy of anti-malware systems.

2020 Trends for Anti-Malware Software

First generation anti-malware solutions were effective in their early task of detecting viruses on PCs. Second generation anti-malware solutions were clearly less effective as variants abounded across the security community. Third generation anti-malware software solutions are demonstrating much more effective success at detecting exploits through a combination of better algorithms, cloud assistance, machine learning, and other techniques (see Figure 1-17).

The algorithmic trending for anti-malware has clearly shifted from traditional signature-based anti-virus to behavioral and more advanced machine learning analytics. Machine learning is particularly well-suited to training processes, including by humans, where examples of previous malware

Figure 1-17. Anti-Malware Software Trend Chart



variants are used to help identify new variants (e.g., a simple prepend or post-pend of a single character to a known bad file name).

Virtualization also introduces new challenges and opportunities for anti-malware software. As cloud-hosted workloads require malware detection and mitigation capabilities, such protections are likely to begin to emerge in cloud security controls such as CASBs and micro-segmentation security systems. Cloud security compliance controls will increasingly drive specific anti-malware objectives for workloads and virtually hosted systems.

The future of anti-malware software lies in dramatically expanded use of AI and machine learning. In addition, more intimate real-time correspondence between anti-malware software located adjacent to an asset, and powerful cloud-based processing, perhaps crowd-sourced, will render immediate verdicts on detected samples. These advances will combine to continue the

improvements in anti-malware software that have occurred. One aspect of the anti-malware ecosystem that remains up for debate is the degree to which AI and machine learning techniques can remove the human being from the judgment equation – for both file-based and fileless malware detection. One would hope that at minimum, the automation would make this process mostly real-time, and thus minimize the likelihood that malware is causing damage while security teams are trying to perform human-time analysis.

One wildcard with respect to malware is the increasing likelihood that nation-state developed attack tools find their way into the open ecosystem. This is a disturbing trend, because nation-state offensive researchers accelerate the process of driving existing malware intensity to new levels. One can only hope that this trend diminishes, because nation-states that expose military-grade malware create unnecessary risk for citizens and businesses around the world.



**AN INTERVIEW WITH DAN WOLFF
DIRECTOR, ENDPOINT PRODUCT MARKETING, BITDEFENDER**

ENDPOINT SECURITY FROM AN ICONIC COMPANY

EARLY cyber security companies developed large portfolios by combining solutions for both business and enterprise, often with a focus on Internet and anti-virus security. Bitdefender is no exception to his rule, having created an enormous customer base who rely on its endpoint security software every day to prevent malware from creating unnecessary risk. Based in Romania, Bitdefender has enjoyed global reach and is one of the iconic participants in our industry.

That said, Bitdefender recently introduced new security solutions for businesses using cloud infrastructure in conjunction with endpoints. The Bitdefender endpoint protection offerings combine exciting new technologies with mature infrastructure support for customers into an exciting platform for business. We recently connected with Dan Wolff, Director of Product Marketing, Endpoint Security, at Bitdefender, to learn more about how their GravityZone platform reduces enterprise security risk.

EA Let's start with an overview of the company, including its wide range of products and services for consumers and business.


DW Bitdefender is a global cybersecurity leader protecting over 500 million systems in more than 150 countries. Since 2001, Bitdefender innovation has consistently delivered award-winning security products and threat intelligence for people, homes, businesses, and their devices, networks, and cloud services. Today, Bitdefender is also the security industry's technology provider-of-choice, licensed for use in over 38% of the world's security solutions. Recognized by industry, respected by vendors, and evangelized by our customers, Bitdefender literally provides the world's best prevention that millions rely upon.

EA Help us understand the differences between endpoint protection platform (EPP) and endpoint detection and response (EDR). I know that Bitdefender supports both security objectives.

DW Endpoint protection platforms (EPP) have been around for many years, endpoint detection and response (EDR) has emerged in the last few years in response to the fact that most endpoint solutions miss attacks infecting company environments in ways invisible to IT administrators. Incident response includes investigation and threat hunting tools that detect the location, affect, and source of threats previously invisible. Today, there is demand for both, which has caused the EPP and EDR markets to converge. Every EPP vendor now has an EDR offering, and every EDR vendor has an EPP capability. The difference with Bitdefender is our highly effective endpoint protection which makes EDR work much better, with less burden for understaffed and inexperienced security teams. We call this low-overhead EDR.

EA Let's talk about GravityZone. Perhaps you can give us an overview of the platform and its use in the enterprise.

DW The GravityZone platform was developed for Bitdefender to support the development of over 30 layers of protective technology, as well



Cloud workload protection is essential, it is not optional.

as on-premise and cloud-based deployments. Its architecture is distinct, in that it maintains a single console for all technologies and functions (such as EPP, patching, and encryption). It also supports our single agent approach, which significantly lowers the administrative overhead of endpoint protection.

EA Your platform does a great job addressing enterprise architectures that reside in the cloud. What are the technology trends in this area from the perspective of cyber security?

DW Technology trends in the cloud have customers adopting cloud in two specific ways. First, they are adopting security from the cloud in the form of IT-as-a-service, including security-as-a-service. GravityZone is a great example of an effective endpoint protection security solution from the cloud. Second, customers are adopting cloud, in terms of creating specific and custom workloads that support business processes – which includes software built in AWS and Azure. Customers are also moving virtual machine workloads to the cloud so they can close their datacenters, stop purchasing expensive hardware, and enjoy the increase in productivity and utilization that the cloud can provide. However, moving to the cloud introduces new challenges based on its shared security model. That is, companies must share security responsibility with the cloud provider, in addition to their own responsibility for the software or applications being developed to cloud. This requires enhanced knowledge of cloud development models, as well as understanding of the native security tools available in the cloud. It is imperative that customers understand all of the configurations and settings they control in the cloud environment. Because cloud workload protection is essential, it is not optional.

EA Tell us about Bitdefender's layered MSP security suite. It sure looks like a comprehensive platform for service providers.

DW Bitdefender listens to MSPs and their specific requirements for managing a vast array of clients – large and small. There are several unique challenges that MSPs have that enterprises don't have. One

is client adoption. For example, they might wonder how to get a new customer up and running quickly and remotely. This requires a resilient architecture that allows them to easily create a new tenant. It also introduces requirements for tenant isolation – meaning that the data from one customer in its own tenant is always separate from the data of another customer. Products have to be designed to handle this, and GravityZone for MSP has been designed for this purpose. Another issue is billing, which introduces the need to track usage, numbers of endpoints, activation dates, renewal dates, and termination processes for each client independently. Integrations via API with customer management solutions that are specific to MSPs (like Kasaya) are also essential. Bitdefender has done the hard work of implementing these architectures and capabilities to help MSPs, which have responded, in turn, by purchasing our solutions.

EA Any near- or long-term predictions in the protection of endpoints and mobiles?

DW Threats to endpoints are never-ending and attackers are always finding new and creative ways to steal data and extract money out of unsuspecting endpoint and mobile users. This challenges endpoint detection vendors to continuously innovate, as the threat vectors become real and more sophisticated. An additional long-term issue around endpoint protection is the skills shortage. Customers can't hire enough security expertise, especially when they have complicated tools. Many customers have multiple endpoint protection products – sometimes as many as six or seven different security agents on a typical endpoint. This overloads IT teams and increases the number of incidents that require investigation. This is driving new security innovations in incident and task prioritization, including risk analytics that bring the most risky devices to the top of the list so they can make sure the limited IT administrative resources can address the most critical items first.

ENDPOINT SECURITY

The most complex, and arguably crowded, vendor space for cyber security involves the protection of endpoints. While such reference to endpoints is often generalized to include a variety of different devices, the sweet spot for cyber security vendors involves desktop and laptop computers that are issued and managed by enterprise teams for employees to use on the corporate LAN. This extends to bring-your-own-device (BYOD) programs as well.

Endpoint PCs and laptops have traditionally been primarily Windows PCs, which have tended to be quite vulnerable to a variety of security exploits. Opening a malicious link via an email phish is generally viewed to be most dangerous when done on a corporate Windows PC connected to the enterprise LAN. In contrast, opening the same link on your personal iPad or iPhone is often viewed as considerably less dangerous from a security perspective.

As such, most endpoint security solutions tend to target this general threat to PCs and laptops, with servers protected using other means. The commonality of methods stops there, however, as the field of endpoint security includes a complex, varied, and often confusing assortment of techniques, methods, agents, management systems, algorithms, and on and on. Enterprise security teams regularly express concern that endpoint security is tough to get right.

For most teams, the endpoints strategy can be viewed in three separate contexts: First, there is usually an installed baseline anti-malware tool, often from a major vendor such as Symantec, McAfee, or Kaspersky. Second, there is often an advanced, analytic-based security agent that is designed to either complement or eventually subsume the existing baseline tool. Third, there is the management system that supports installation,

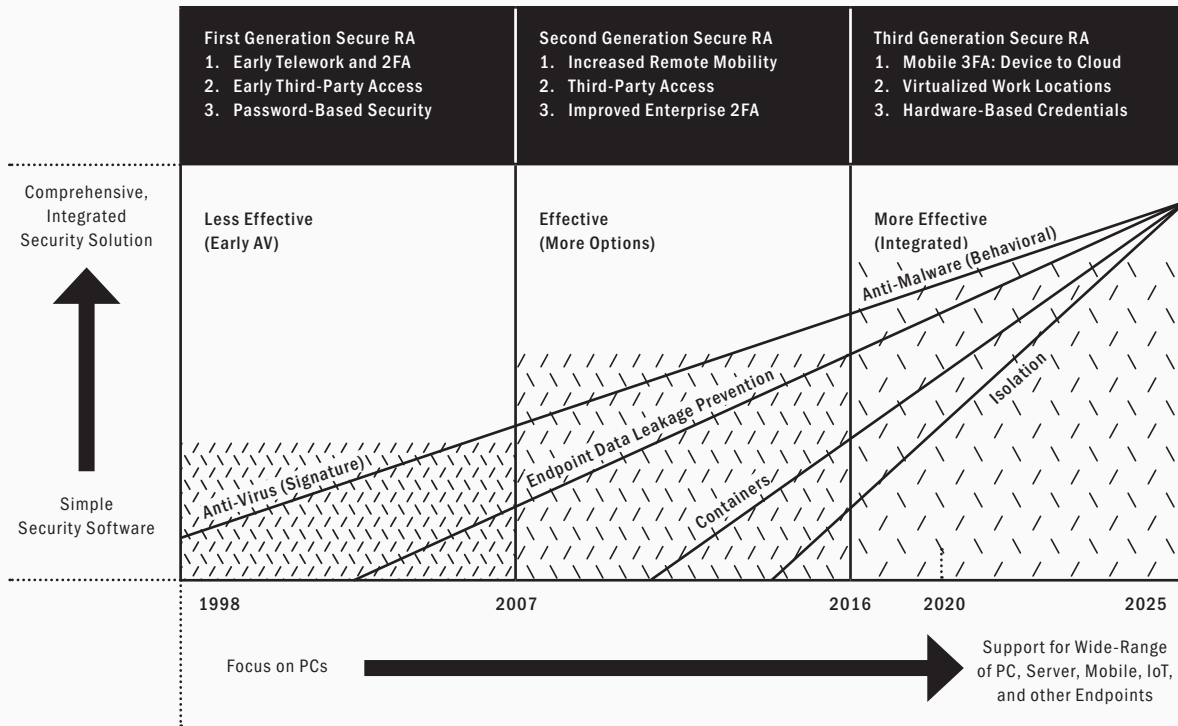
update, support, and the like. Virtualization provides a powerful means for protecting endpoint systems. This can be done through containerized solutions that prevent malware from reaching resources on a PC. It can also be done through isolation, often in the form of a remote isolation gateway, that prevents content from infecting an endpoint via the browser. Solutions even use virtualization to create multiple guests on an endpoint to allow for differentiation of protected and open computing.

2020 Trends for Endpoint Security

In general, endpoint security has evolved from less effective, first generation anti-virus solutions, through effective endpoint solutions in the second generation, toward more effective third generation solutions with many different advanced, integrated options (see Figure 1-18). The various evolutionary tracks include (but are not limited to) anti-virus (now anti-malware), data leakage prevention, user entity behavioral analytics, security containers, and isolation.

Across the board, these endpoint security techniques all benefit from the use of advanced heuristics including machine learning and AI techniques from the best security vendors. In addition, the assistance of cloud methods and automated tools for rendering rapid verdicts for potential malware samples, has

Figure 1-18. Secure Remote Access Trend Chart



dramatically improved currently-available solutions for keeping endpoints clear of exploit software.

The evolution of endpoint security has shifted during the three generations from simple security software point solutions toward comprehensive, integrated solutions. In addition, the basic support for early PCs running Windows operating systems has expanded to include more comprehensive support for a wide range of endpoint types including Mac OS, servers, mobile devices, IoT, and other endpoints.

The future of endpoint security involves more intense use of AI and machine learning, simply because these technologies fit the problem of malware identification quite well. The essence of automated learning involves the use of live or test samples as the basis for detecting future instances of the same thing, albeit slightly modified (like different pictures of cats). This will substantially reduce the risk associated with endpoints.

An additional future trend will be massive consolidation of the disparate means for protecting endpoints. One should expect a continuing flurry of mergers, acquisitions, and partnerships that will result in more embedded, user-invisible endpoint security solutions that will be cost-effective, easy to use, and much more suited to the progression of enterprise computing toward mobility-enabled hybrid cloud usage.



AN INTERVIEW WITH SAM CURRY
CPO/CSO, CYBEREASON

ADVANCED ENDPOINT PROTEC- TIONS FOR ENTERPRISE

THE EARLIEST computer security solutions focused on PC endpoints and how to use signature-based protections to prevent viruses. Since then, security solutions for endpoints have advanced considerably, with a clear focus on balancing preventive methods with the practical realization that attacks are inevitable. To that end, endpoint detection and response (EDR) has become a primary focus in more enterprise environments for their PCs, mobiles, and other devices.

Cybereason provides a world-class EDR solution that makes use of next generation anti-virus along with advanced analytics for dealing with potential incidents. We had the opportunity recently to connect with Sam Curry, CPO/CSO of Cybereason, to learn more about EDR in general, and Cybereason in particular. Below is a brief summary of the discussion.

EA How does the Cybereason platform support endpoint detection and response?

SC The Cybereason platform is designed for endpoint detection and response (EDR) first-and-foremost. Collection is done non-intrusively, and focuses on behaviors rather than traditional indicators of compromise (IOCs) or known-bad stimulus-response. The base telemetry of the platform is about what is happening – good or bad. That is assembled on a back-end that is a model to preserve context. With a small signal-to-noise ratio, and rendered for asking security questions, it becomes relatively trivial to elevate malicious operations, or Malops, as we call them. These are high fidelity forms of alert unlike any other platform. They are, in effect, kill chains. However, it doesn't stop there. Malops are both more actionable by analysts and response teams, and also able to remediate much with the platform and immunize the same vectors in the future. The platform is the definition of how to do EDR and to upscale security personnel and processes.

EA Cybereason supports so-called next generation anti-virus. Tell us how this works.

SC Cybereason does pre-execution static file analysis, meaning that right before a file executes, and after it has been subjected to optional Cybereason or third-party signature scanning, it is rendered and run through machine learning derived models to determine the likelihood of something being benign or malicious. The machine learning is based on the combined wisdom and insight of Cybereason's back-end models looking at the entire history and evolution of malware. This means the next file has a high degree of likelihood to be scored as malicious if it is malware, even if it has never been seen before. Cybereason also does post-execution dynamic behavioral analysis, because some files behave after launching in a way that is inimically bad. Ransomware is easy to spot being ransomware, and Cybereason knows how to limit damage – namely, to take action without interruption to the end user.



No matter how good the controls and measure taken, a human will think of innovative ways to get around any machine.

EA What's the importance of active threat monitoring in the management of cyber risk in the enterprise?

SC No matter how good the controls and measure taken, a human will think of innovative ways to get around any machine. This means that the human, whether from a managed service team or native to the customer using Cybereason, can spend time hunting. The Cybereason platform has all the right telemetry. Nothing can happen in the environment without Cybereason seeing a piece of it. The Cybereason platform renders this in a way that can answer questions and let analysts swim through the data without having to stop and figure out how to get the data. That means threat hunters and services can focus their time on efficient work, on the rarest of advanced attacks, and not spend their time backstopping an ineffective control. Cybereason customers and services analysts typically can do advanced hunting at a ratio of one analyst to greater than 150,000 systems per analyst, which is not just best practice, it's really a next-practice in cybersecurity.

EA Do you see visibility as a growing demand from enterprise security teams? What sort of information are they interested in obtaining and analyzing?

SC Everyone wants to find ways to be more efficient with their people and processes regarding security. This means that demand for not just basic capabilities, but for ongoing refinement and improvement, is essential. Behavioral data is the most critical data in any environment from a security perspective, and it has the most universal applicability to security problems. Enterprise security teams need to solve the cyber problem of catching at a higher percentage more-and-more attacks to the left in the kill chain, and resolving them faster. The behavioral data can also improve the IT security hygiene portion of security decisioning. This includes what to patch first, which accounts to secure, and what policies to enforce hardest or

to retire. The ability to extend both within cyber and beyond into the rest of security and IT is enormous.

EA Any near- or long-term predictions for EDR and next-generation anti-virus (NGAV)?

SC NGAV originally looked like it would disrupt the traditional EPP market, but for the most part, it has become the new normal. Anti-virus companies are all doing some NG, although I believe Cybereason is among the best. EDR is the new disruptor. While no one will throw out their AV/NGAV, because that would be foolish in the extreme, no one is looking to it to stop the most advanced attacks. That is almost all the province of EDR and its little brother, MDR, and that is where the differentiation lies. Therefore, I predict either consolidation or outright change of the guard with EDR being what matters, and in two years AV/NGAV and the rest of the EPP stack will be a set of IT check boxes that gets awarded to the EDR vendor of choice, even if we persist in still calling the space as a whole EPP (Gartner), ESS (Forrester), or some other catch-all label.

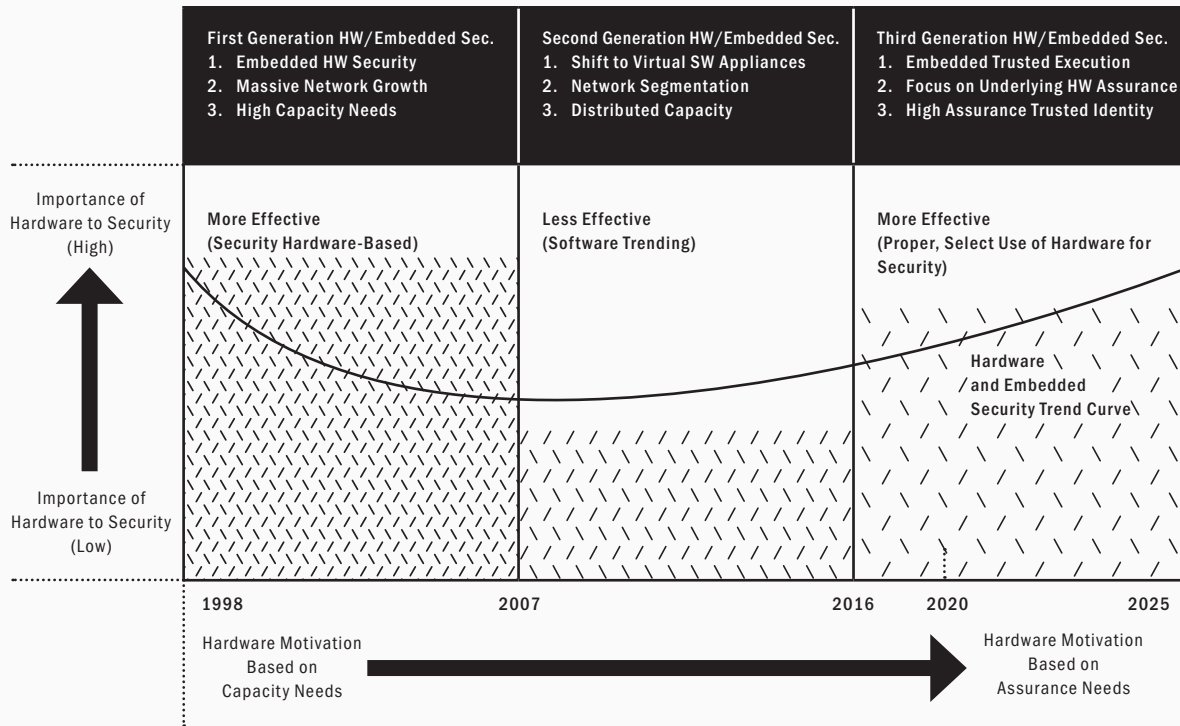
19

HW/EMBEDDED SECURITY

It is fashionable in this era of virtualization and software-defined everything, to say that hardware and embedded systems are no longer relevant in modern computing – and that if any desired function can be implemented in software, then it should be done in that manner. What this view misses, however, is the optimal design balance that seems a more reasonable goal between hardware and software.

Security experts should be explaining that hardware is best deployed when high levels of performance and assurance are desired, and these are not uncommon requirements in most settings. The use of hardware should thus be viewed in terms of optimal usage, rather than as being supplanted by software running solely on generic CPUs, arranged row-like and ready to be replaced with new appliances when they need update or show signs of wear.

Figure 1-19. Hardware/Embedded Security Trend Chart



The security community benefits from hardware in the following areas: (1) Embedded endpoint and mobile device hardware such as Trusted Platform Modules (TPMs) or Hardware Security Modules (HSMs) for high assurance; (2) optimized hardware for specialized applications such as browser or IoT isolation; and (3) hardware appliances for ultra-high performance requirements. In each case, the hardware plays an important role in achieving desired security objectives.

It is also worth mentioning that various creative solutions in cyber security have tended to utilize an attractive balance of hardware and software in their implementation. Everything from DDOS mitigation to high-assurance remote browsing can benefit from the judicious and careful integration of hardware into the design. The clear advantages of using software for most cases does not preclude hardware being a great choice in certain instances.

2020 Trends for Hardware/Embedded Security

First generation use of embedded hardware for security was effective and consistent with the threats and technology of the time. Second generation cyber security saw a clear shift and bias away from hardware toward software, but the result was less effective for many reasons – most unrelated to the shift away from hardware. Most of the shortcomings stemmed from significantly increased attack methods with increasingly reliance on perimeter.

Stated another way – the speed with which cyber threats began to progress in the late 90s and early 00s, made it clear that the rigor and capacity associated with hardware might not be sufficiently vital to justify the relative inflexibility of making changes quickly. As a result, software – even with its myriad of familiar exploitable bugs – became a more attractive option for most security controls. This accounts for the effectiveness dip experienced during this era.



Daniel Leone, Unsplash

Present third generation use of hardware and embedded means for reducing cyber risk generally includes a more effective and balanced mix of hardware and software – taking full advantage of the primary strengths of both (see Figure 1-19). Higher assurance and performance requirements have gradually shifted as the main motivations for selecting hardware security implementations over corresponding software-based designs.

The future of hardware/embedded security will continue to involve optimal design and implementation balance with software. The growth of operational technology (OT) and Internet of Things (IoT) will also drive this balance of software with embedded security. New IoT devices, for instance, should include functional protections at manufacturing time, and this will often involve embedded hardware implementations that coordinate with software controls.

One would also expect that in the coming years, an optimal balance will be achieved between the current obsession with software-based everything, hosted virtually in the cloud with the traditional advantages of locally managed hardware. This balance will ensure that small, medium, and large organizations deploy the correct combination of hardware and software across their enterprise.



AN INTERVIEW WITH TOBY WEIR-JONES
CHIEF PRODUCT OFFICER, BAYSHORE NETWORKS

ACTIVE OT SECURITY VISIBILITY & MITIGATION

THE first goal in protecting operational technology (OT) is to recognize that the connectivity of your industrial environment has probably expanded far faster than your growth in staffing and expertise required to protect your plant. As a result, you now have a very basic safety problem: lots of risk, and no practical ability to mitigate it.

This is not a matter of assigning blame. It's a simple resourcing issue. There are very few skilled industrial network security analysts, and those who are available are in huge demand. They command enormous price tags and have the luxury of endless career mobility, even in the hottest job markets nationwide. If you're a regional operator, the chances of finding one of these professionals – or training and keeping one in-house – are very slim.

Bayshore Networks has developed a commercial solution that resides inline on the OT network and provides real-time inspection and protection of OT assets and activity. Rather than offer it as a single monolithic solution, the company has divided it up into tactical point solutions for specific use cases, allowing customers much more straightforward evaluation and budgeting requirements while slowly building up the installed base. We recently met with Toby Weir-Jones of Bayshore Networks to learn more about OT active mitigation from cyber threats.

EA Do you still have to convince OT companies that they need to focus on cyber security?

TWJ Most operations technology (OT)-oriented companies now recognize that they need to pay close attention to cyber security issues, but the challenge is they're not sure exactly where to start. They're being bombarded by complicated product messages without a lot of clear thought leadership on best practices. We've adjusted our focus towards a core set of critical OT security activities which should be monitored in every OT environment, along with recommendations on what mitigation steps can be performed without disrupting operations or safety.

EA Where should an OT security professional focus their efforts?

TWJ They need to understand not only what's "out there" on their networks, but also what they can do, safely and constructively, to improve their OT security within the safety and maintenance parameters that production environments demand. Improvements in configuration, or network segmentation, or policy can often be done without requiring downtime on the floor, and Bayshore is the only ICS security tool which can provide real-time mitigation to protect OT devices at the payload level. This allows safer operation, with less downtime, all while improving your security posture.


EA Tell us how your solution works and how it can be used for visibility and mitigation?

TWJ Bayshore offers three products oriented around the same core engine. That engine understands and decodes a wide range of native OT network protocols, at wire speed, with incredibly low latency. It lets us get all the way down into the last bits of payload, make decisions on a whole range of risk factors, and return permitted packets back to the wire. The first product using this is called SCADAFuse.

It sits right in front of a PLC and acts as the last line of defense. If traffic from unauthorized sources, or of unauthorized types, or at unauthorized times, tries to touch the PLC, SCADAfuse prevents it and sends an alert to the operator's control room – their SCADA HMI – via a built-in modbus server. It can be set up in 15 minutes, evaluated for purpose in a week, and costs less than a week's worth of field engineering time for a single automation technician. The second product is our remote access solution, called OT Access. It's available as both a hosted solution (for managed service providers or other cloud-friendly deployments) and a fully on-premise version. It is designed to provide access control to OT assets with the absolute minimum exposed connectivity, along with the same content inspection and policy enforcement using the Bayshore policy engine. The third product – SCADAwall – is designed to take the traditional hardware data diode and make big steps forward on value and flexibility. It provides the same core feature – non-repudiable data transmission across the diode – but with live file object capture and inspection, for malware, OEM hash checking, and known ICS CERT vulnerabilities.

EA What trends are you seeing in OT security, other than perhaps greater awareness?

TWJ The customers have been flooded with visibility pitches for the past few years, and they are realizing that awareness is only the very first part of an effective OT security solution. Ultimately, they need to know what to do next, and how much of that can be done on their behalf by their tool or their service provider. OT threat mitigation is all about preserving production safety and continuity unless you absolutely can't, and then providing the best detail and recommendations so everyone has a transparent and objective understanding of why the OT team needs organizational support for major risks. The vendors who will succeed in this evolving space are already positioned to enable these 'shades of gray' and satisfy the demands of not



Improvements in configuration, or network segmentation, or policy can often be done without requiring downtime on the floor.

only the OT security team, but the corporate IT security team as well.

EA Any new features or capabilities that your team is currently working on?

TWJ Absolutely. Bayshore's strategy is to bring its payload-level policy controls to the entire OT environment. This includes the network inside the plant, the transition layer to other corporate or external networks, and the remote access gateway required for trusted ingress. With the three products I mentioned above, it's an exciting time to invest in the Bayshore platform and we are confident our solutions will readily distinguish themselves from the visibility and asset management providers on the market today.

20

ICT/IOT SECURITY

The distinction made here between industrial control system (ICS) and Internet of Things (IoT) is that ICS includes devices associated with highly consequential impact upon breach, including life and safety-critical implications. IoT devices, in contrast, are essentially in-band IT devices that support innovative new functions such as recognizing voice commands, controlling consumer items, and providing entertainment, fun, and productivity for citizens.

While it might seem controversial to some, we choose to focus our main emphasis here on ICS security as a unique situation – and to treat IoT devices as endpoints that require the same types of IT protections as other endpoints, including mobile devices. This follows the observation that ICS has its own unique technologies and support systems, and the security consequences are typically enormous.

In fact, technology experts will agree that ICS security (and select IoT) represents one of the greatest new challenges for data and system protection. The security obligation here focuses specifically on operational environments such as factory floors, manufacturing plants, embedded systems, machine designs, robots, drones, smart weapons, connected cars, wind turbines, and many other aspects of societal and national critical infrastructure.

ICS security has been challenged for a couple of reasons: First, legacy ICS infrastructure barely took cyber threats into consideration at design time – a decision reinforced by many years of quiet time in terms of cyber threats. (Note that almost all IoT is non-legacy.) And second, the various ICS technologies and protocols employed are inconsistent with standard IT methods, which made generally available commercial tools largely unusable for ICS in OT environments.

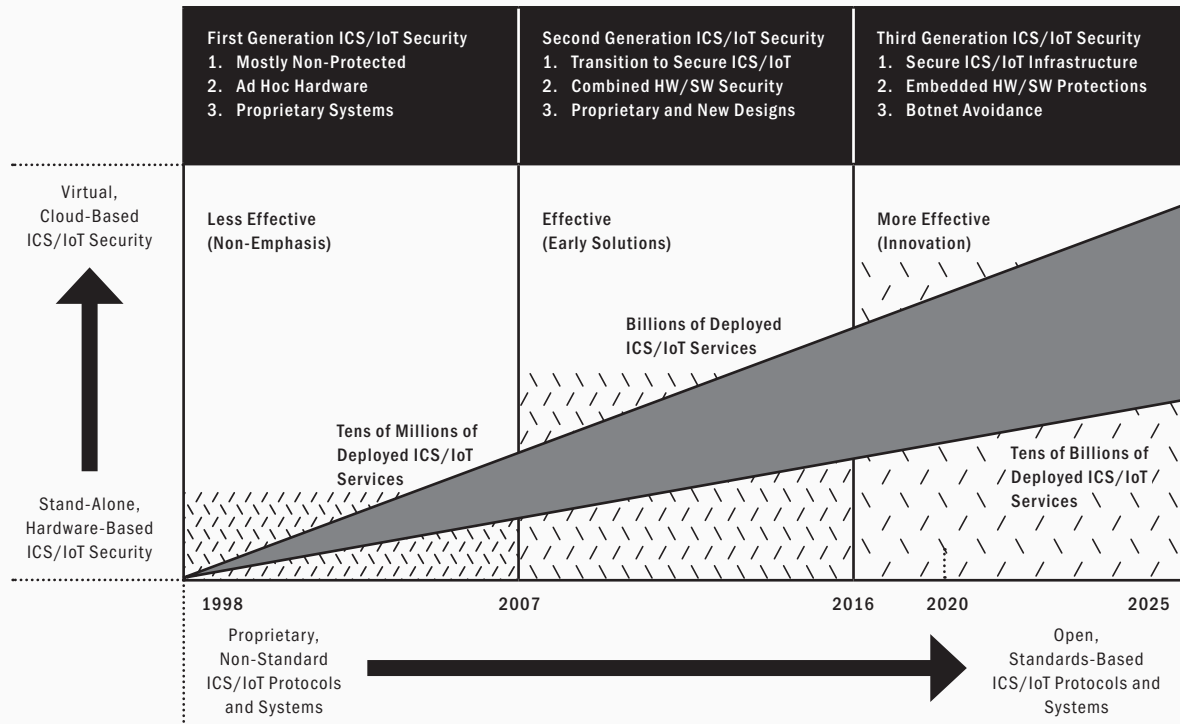
Neither of these conditions have changed, but the attention placed by both malicious offenders and industrial defenders has increased considerably. This is mostly because the offense became more active, largely due to the high consequence and enormous gain achieved by successfully breaching an ICS system. In the gravest cases, OT exploits can lead to significant loss of life, which might be the objective for a truly evil actor involved in a diabolical cyber initiative.

2020 Trends for ICS/IoT Security

First generation ICS security from 1998 to 2007 was arguably non-existent in almost all OT environments, with some larger early adopters as exceptions. Second generation ICS security from 2007 to 2016 introduced some effective early solutions, albeit with uneven adoption and deployment. Third generation ICS and IoT security from 2016 to 2025 will involve more effective solutions deployed uniformly across industrial and IoT environments (see Figure 1-20).

A major trend in this evolution involves stand-alone, hardware-based ICS and IoT security solutions shifting toward more virtual, cloud-based protections for both ICS and IoT. In addition, proprietary ICS and IoT protocols and systems are being gradually replaced with open, standard-

Figure 1-20. Industrial Control System Security Trend Chart



based protocols and systems for cyber security. The convergence of IT and OT will drive greater deployment of common, standard security solutions. Security solutions for ICS and IoT have tended to fall into several different categories: Some systems focus on managing direction of flow between IT and OT; others focus on enforcing policy at gateways between IT and OT; and still others embed their controls directly into OT devices and systems at the lower layers of the familiar Purdue model. These methods are complementary but have not been typically well-integrated in OT environments.

The future of both ICS and IoT security lies in the convergence of IT and OT. That is, increasingly, cyber security protections will not require redesign for non-IT usage, but will rather operate natively. This implies that OT infrastructure will shrink around the devices they currently manage, and most of the computing and networking supporting ICS and IoT devices will be based on standard IP protocols and technology.

An additional trend that will affect the future of ICS is the increased attention placed by nation-state militaries in attacking the critical infrastructure of its adversaries. The United States and Russia, for example, have openly postured their advances in placing malware into each other's electric power grids. The consequences of any mishandling of these attacks by either side would seem enormous.



AN INTERVIEW WITH BILL DIOTTE
CEO, MOCANA

SECURING INDUSTRIAL CONTROL & THE INTERNET OF THINGS

THE incredible promise and benefits of the Internet of Things (IoT) for modern society are tempered somewhat by the significant security risks that emerge, especially for critical infrastructure and safety-related applications. Factories, autonomous vehicles, modern homes, power plants, and many other IoT and industrial control environments must address emerging security threats in order to fully realize the potential for advancement through intelligent automation and computing.

Mocana focuses on providing just such risk reduction for IoT and ICS customers dealing with this growing risk. Their platform provides end-to-end coverage against attacks ranging from malware insertion to advanced nation-state campaigns. We spent time with Bill Diotte of Mocana to learn more about the IoT and ICS landscape from a security perspective, as well as how the Mocana platform addresses risks for its customers.

EA You talk frequently about the Internet of Trusted Things. Can you explain the concept?

BD The Internet of Trusted Things is a fundamentally new way of thinking about security, where IoT devices can protect themselves rather than relying on network-based security. For years, we've depended upon network-based security approaches like network segmentation, firewalls and detection to protect our devices. IoT security requires a different approach because IoT devices often live in untrusted networks where it is simply impractical to use traditional IT security strategies. For IoT to scale securely, we need to enable devices to protect themselves with strong authentication, encryption, and integrity built right into the device. These devices should have a trusted identity, be tamper-resistant, and be able to communicate securely. Imagine a world of billions of devices that can actually protect themselves. The complex world of network security could be dramatically simplified. This is the vision of the Internet of Trusted Things.

EA How does the Mocana platform provide end-to-end protection for industrial and IoT-based systems?

BD When Mocana talks about end-to-end protection, we're not just talking about device-to-cloud security. We're talking about protecting devices throughout their lifecycle, from the birth of the device to the end of its life. It's important that strong security controls be built into systems at the time they are being designed rather than after the fact. The device and the processes for provisioning and managing the device should be protected during development, manufacture, onboarding and management. Mocana's TrustCenter security lifecycle platform and TrustPoint on-device security software protects the device during its entire lifecycle, end-to-end.

EA What's the role of automation in the Mocana platform? Is this an essential element of any IoT security system?

BD There are as many vulnerabilities in the processes for managing security as there are



**We make it
easy to scale
the provi-
sioning and
management
of the security
lifecycle.**

hardware and software vulnerabilities in the device itself. Provisioning devices, updating credentials (keys and digital certificates), and updating firmware are often done using manual processes that require a field technician or administrator to perform the task. Manual processes are prone to human error, compromise, and scalability challenges. How do you manually update millions of devices securely? Mocana's platform automates the orchestration of the security lifecycle. We make it easy to scale the provisioning and management of the security lifecycle.

EA Do the constrained resources in a typical IoT system create challenges in providing proper cyber security?


BD IoT systems are oftentimes resource-constrained, meaning that they have limitations on power, processing speed, bandwidth throughput, and memory. These constraints limit the type of cybersecurity that can be used to protect a system. For example, a highly constrained device might have as little as 64KB of memory whereas a server class system, might have 2GB of memory. When designing applications, developers need to be as efficient as possible to minimize the resource requirements to fit the constraints of the device. This means that the software must be designed to use the smallest amount of memory and power to get the job done. These constraints will limit the key size, cryptographic algorithms, and security controls that can be employed.

EA Any near- or long-term predictions about industrial control and IoT security?

BD Both the industrial and IoT sectors will undergo a lot of change over the next decade. Here are my predictions. There will be a major cyber attack in the next five years that will have a significant impact on human safety, and governments will intervene to create stronger cyber protection regulations. Industrial cybersecurity compliance standards will be overhauled to address the advances in networking, hardware and software technologies, and modern attack scenarios. The growth of IoT and edge computing

will make it challenging to monitor and trust IoT networks. Companies will focus more on hardening platforms and endpoints to improve security. Artificial intelligence and telemetry will be providing additional context to correlate device characteristics with security processes and events to make better security decisions. Manufacturers and IoT service providers will monetize security to drive services revenue.

**MAIN-
FRAME
SECURITY**

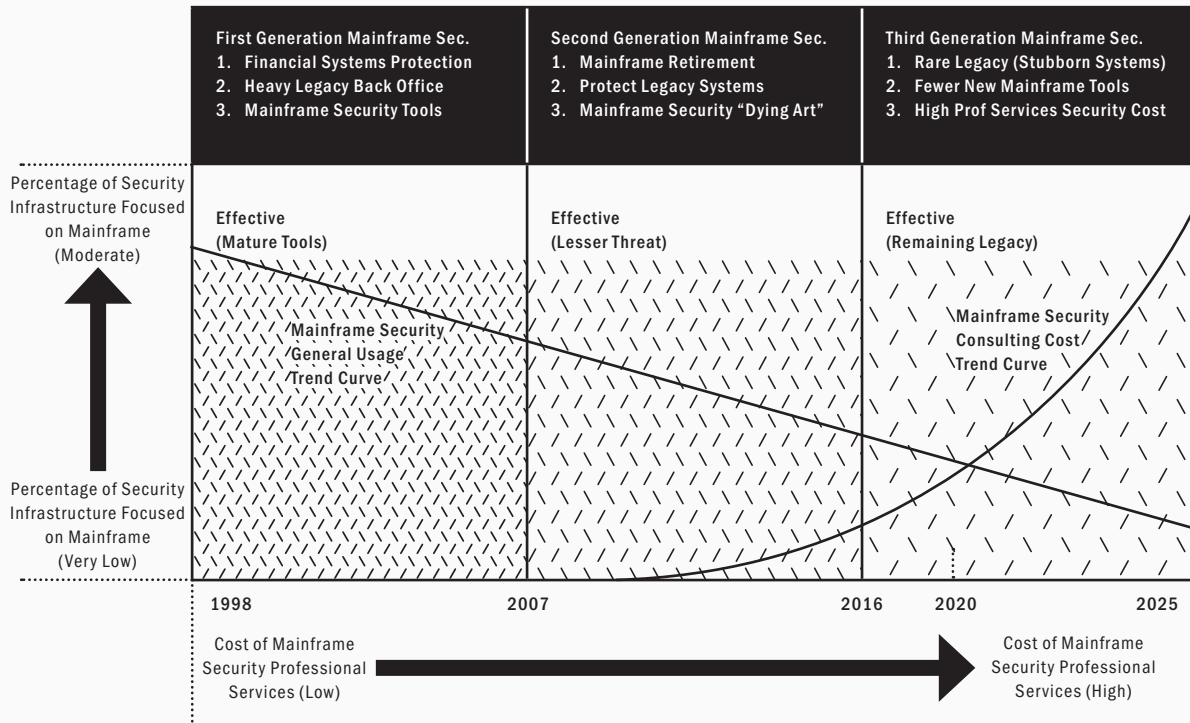


The percentage of security infrastructure focused on using mainframe security tools has gone from moderate/high to very low, and many would refer to mainframe protection as a “dying art.”

It is tempting to consider mainframe security in 2020 as being long gone, but the reality is that many companies and agencies continue to rely on mainframes and their applications. Reasons vary, but the core issue is that inertia is a powerful driver of infrastructure support, and many IT, software, and network teams have decided that it is simply easier to just leave the mainframes in place for the near-term, than to swap them out.

The resulting challenge is that traditional mainframe security protections, including tools for data governance, encryption, transfer, and audit, remain in place and require time and attention. The experience and skills of people trained to perform such mainframe-based protection are beginning to seriously wane – and it is conceivable that the skills shortage (through attrition and retirement) will be the final driver to shut down mainframes.

Figure 1-21. Mainframe Security Trend Chart



One great irony with respect to mainframe security is that the associated centralized concept of amortizing the best available mainframe administration and protection talent into one place is closely related to modern cloud security processes. In fact, it is not uncommon for pundits and observers to draw direct comparison between cloud security and the earliest efforts at mainframe security.

An additional irony is that during the heyday of mainframe security – perhaps during the mid-1970s through the mid-1990s, one could easily make the case that the associated cyber threat was far less intense than it is today. Now, most experts would (correctly) view this as primarily driven by the relative immaturity of offensive techniques; but one should not ignore or even discount the fact that when mainframes ruled, security problems were less intense.

2020 Trends for Mainframe Security


The effectiveness of mainframe security has been high from its inception to the present. Few would argue that mainframe controls have been weak, although the processes and policies of early enterprise were, in fact, poorly done (see Figure 1-21). The percentage of security infrastructure focused on using mainframe security tools has gone from moderate/high to very low, and many would refer to mainframe protection as a “dying art.”

The corresponding consulting fees that can be obtained from the remaining mainframe experts should be expected to rise dramatically, as companies continue to rely on these systems without the abundant availability of administrators who know IBM z/OS and the like. Enterprise teams are thus advised to accelerate retirement of their mainframes to avoid the need for costly consulting fees.

The future of mainframe security lies mostly in some technology museum. Future versions of the TAG Cyber Security Annual will likely drop this control from the fifty, but it remains today, simply because so many larger companies continue to run

mainframes. Government agencies apparently have quite a few mainframes as well, and presumably IBM and others will continue to support this business, which is likely to be quite high margin.

An interesting career paradox for cyber security experts regarding mainframes is whether the time required to learn the corresponding technologies is worth the effort. This is a question asked often by graduate students considering consulting careers. Perhaps the best answer is that whatever is decided had better be done quickly, because mainframes are dying and pretty soon the need will drop to zero.



During the heyday of mainframe security - perhaps during the mid-1970s through the mid-1990s, one could easily make the case that the associated cyber threat war far less intense than it is today.

MOBILE SECURITY

Mobile security has shifted from an optional consideration for smart devices that provide conveniences for workers, to a mandatory requirement for all mobile devices, systems, and infrastructure that support essential business operations. This is a dramatic shift – one that is mostly accepted by business and government teams around the work. Vendors have obviously noticed this shifted emphasis on mobile protection, and are offering a portfolio of solutions.

A curious and somewhat nagging issue, however, is that far too many businesses, especially smaller ones, still opt to not explicitly manage their mobile devices. (Apple's Genius Bar at the local mall is often the primary source of mobile management for smaller entities.) Biometric unlocking is the primary mobile device control in many environments, which is fine to reduce the risk of lost devices, but insufficient to deal with exploits such as malware.

The history of cyber security strongly suggests that with increased emphasis on mobility, and its central role in emerging zero trust access to cloud-hosted enterprise applications (e.g., Google's BeyondCorp model), that the associated risk will increase as malicious intruders find creative ways to exploit even the best designed software from companies like Apple. Enterprise teams who do not recognize this inevitable fact operate at their own peril.

It is also important to observe that the walled-garden approach taken at Apple, which ensures that all downloaded apps are passed through and vetted by Apple, has resulted in a relatively secure processing environment. It is not uncommon, for example, to hear security teams recommend that executives open their email (which might include dangerous attachments) on their iPhones versus on their LAN-connected Windows PCs.

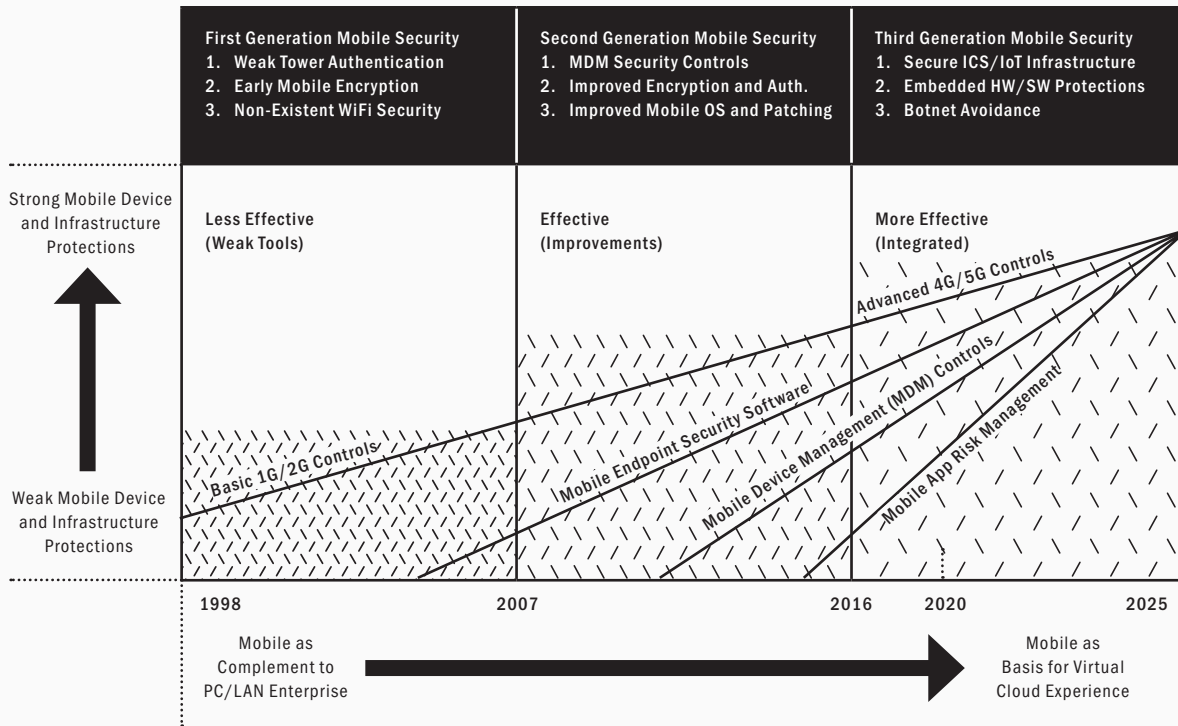
The IoT world is adjacent to mobile, especially for applications such as connected cars – soon to be autonomous, and smart homes. Mobility infrastructure brings cars and homes to life and will have to also include the requisite controls for cyber risk. Connected cars, in particular, introduce considerable mobile security risk, as intruders might suddenly have the ability to direct serious exploits toward a fast-moving vehicle carrying a bunch of humans on a highway.

One would imagine that the emerging mobile ecosystem for cars, homes, and the like will thus have to provide a suitable means for the usual sorts of cyber security controls to support identification, authentication, access, logging, encryption, and on and on. This is not a surprise, but there will be some friction between the mobile service providers, cloud hosting providers, car and home manufacturers, and application developers around who takes the lead.

2020 Trends for Mobile Security

Mobile security has transitioned from weak controls in the first generation of use from 1998 to 2007, to effective controls in the second generation from 2007 to 2016, to more effective and integrated controls in the third and present generation (see Figure 1-22). This evolution has been characterized

Figure 1-22. Mobile Security Trend Chart



by a shift from weak device and system protections to much stronger protections based on more solid foundational components.

Early mobility security was viewed largely as a complement to the traditional PC/LAN enterprise infrastructure. That is, most business users in the early days of mobility viewed their flip phones and early Blackberry devices as a nice-to-have convenience, but certainly not as a critically essential component of their day-to-day work experience. This is reflected by the largely fixed, stationary, non-mobile nature (with cubicles) of the typical office environment of the time.

Modern mobility security, in contrast, is viewed as an essential basis for the emerging cloud-based virtual work environment. What used to be called telework is now simply called work; hence, the threats to any enterprise team will now increasingly encompass traditional PC and computing assets, as well as mobile devices – whether bring-your-own-

device (BYOD)-managed or company issued. It should come as no surprise that threats will continue to shift accordingly. The future of mobility security is an integration with traditional enterprise security. That is, one should expect that mobility will become an assumed component of every enterprise, regardless of size, scope, or mission. This is good news, because teams will soon no longer view mobility security as an add-on to their protection scheme, but rather as an integrated, embedded element in their security approach.

Connected car, smart homes, and related IoT security will represent enormous new areas of business for vendors, and new areas of threat for consumers, business, and the rest of society. It seems a non-stretch to assume that the next truly consequential hacks will come in these new aspects of our lives. Hackers have already demonstrated the ability to break into live, moving vehicles. We should expect much more of this.

**PWD/
PRIVILEGE
MANAGE-
MENT**

Decisions about passwords have traditionally been left in the hands end-users who often make colossal errors in judgment in their selection, use, and sharing. When this involves passwords for critically essential resources in an enterprise, we often refer to the credential-based authentication information as a privilege. As one might expect, mishandling or poor decision-making with privileges can lead to more serious consequences.

To deal with both problems, password management and privilege management tools have emerged that simplify the corresponding tasks. (Commercial vendors typically market tools for one or the other tasks, but often not both.) Whether for consumers or enterprise users, and whether for passwords or privileges, the general idea is that an automated tool simplifies the interface to the user, and then securely manages back-end authentication usage and handling.

Both privilege and password management tools are getting easier to use, more commonly accepted, and better integrated into the usage patterns of consumer and enterprise users. Secure constructs such as password and privilege vaults, for example, are becoming more frequently cited in enterprise security policy requirements, and even showing up in security compliance frameworks.

One challenge to the use of secure vaults involves the complexity and challenge of ensuring proper coverage across all privileged passwords for all relevant applications. To that end, vendors have begun to build solutions that focus on the process of privilege management without need for a vault. Generally, two-factor authentication is an important element of this and all password and privilege management schemes. Passwordless experiences are becoming much more discussed as a requirement for enterprise, as is the decision to avoid a centralized

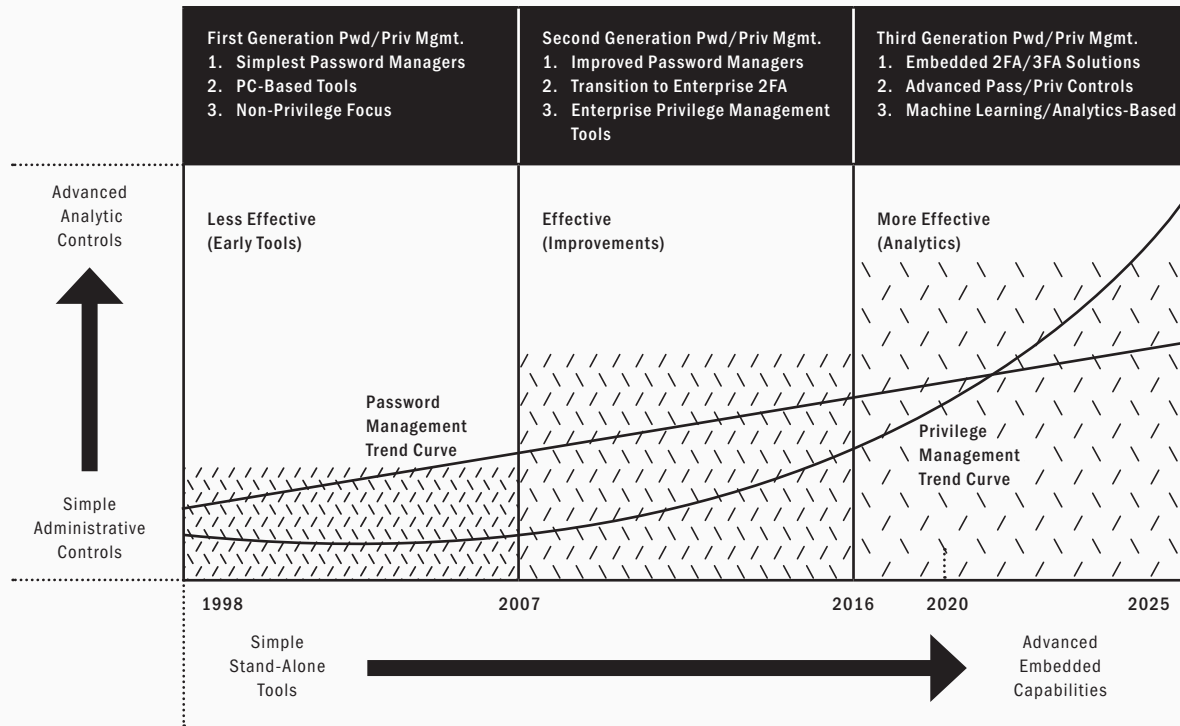
store of authentication information. It stands to reason that decentralizing the administration of passwords, for example, dramatically reduces the potential that a malicious actor can find one central place where a treasure trove of authentication information can be stolen at once.

2020 Trends for Password/Privilege Management

First generation privilege and password management involved early tools in the late 90's that were not as well-understood by customers as they are today. Second generation tools from 2007 to today saw considerable usage and security improvements; and third generation tools will become even more effective, as machine learning and advanced analytics find their way into the algorithms and utilities (see Figure 1-23).

The trend for both password and privilege management can be summed up pretty-well by the transition from simple, stand-alone administrative tools to more advanced, analytic controls, especially in the context of enterprise use. The capabilities are becoming more embedded into identity and access management (IAM) infrastructure, and even emerging Internet of Things (IoT) authentication and authorization.

Figure 1-23. Password/Privilege Management Trend Chart



Both capabilities will also benefit from increased use of cloud and virtualized as-a-service computing, if only because these emerging services increase the demand for non-homogeneous authentication and authorization for consumers and enterprise users. One might thus expect to see password and privilege management support integrate with cloud security solutions such as cloud access security brokers (CASBs).

The future for privilege and password management continues to be positive, with privilege management tools in the enterprise likely seeing exponential growth due to increased demands from a compliance perspective. Password management is likely to see continued linear growth, as the typical consumer will remain somewhat uncertain about the best way to manage passwords, often just utilizing federated authentication between social media sites.

It is worth mentioning here that some debate exists within the security community about whether a true password-less experience is a reasonable and attainable goal. This debate is somewhat orthogonal to the password and privilege management functions, as these capabilities will travel with whatever contextual or adaptive credential validation is in use by enterprise and consumers in the coming years.

Biometrics, obviously, provide an important complement to passwords and privileges, in the context of adaptive multi-factor authentication. It is expected that both passwords, privileges, and other artifacts related to strong authentication will compete based on the ease of integration with adaptive validation, as well as on which can effectively minimize required proof actions by users.



**AN INTERVIEW WITH ADAM BOSNIAN
EXECUTIVE VICE PRESIDENT, CYBERARK**

**INSIGHTS
INTO
PRIVILEGED
ACCESS
SECURITY**

THE management of privileges may be one of the most under-attended aspects of modern enterprise cyber security. This can be directly attributed to the complexities of IT infrastructure and the situation in far too many cases where the inventory of privileges is unknown. Such ignorance of good privileged access security is problematic, because adversaries generally start their offensive campaigns by collecting privileges. This helps explain why so little progress has been made in thwarting APTs.

CyberArk has been at the forefront of reducing privilege-related threats with an impressive portfolio of solutions for enterprise. We spent some time with Adam Bosnian from CyberArk, to learn more about recent advances in privileged access security. We also wanted to better understand how protection of credentials can truly advance the enterprise toward substantially lower levels of risk.

EA Can you start by providing background on the privileged access security market and the a heightened interest in this space in recent years?

AB Historically, business disruption is tightly connected with privileged access. Longstanding industries continue to be disrupted as a result of needing to adopt new technologies. For example, in the mid-2000s, networked computing ushered in a new era of business communications and operations. This led to the growth of online data storage and management, as well as the rise in enterprise cloud computing and machine-to-machine integrations through AI and machine learning. As the need for people and machines to access networked services and infrastructure increased, so too did the risk of dangerous breaches linked to privileged credential abuse. In the era of Local Area Networks (LANs), digital security protocols focused on fortified perimeters — keeping attackers outside of the corporate network. However, it soon became apparent that it wasn't a matter of "if" a motivated attacker could breach a network, but "when." And once a bad actor gains access to privileged credentials, they can exploit them to reach a target's most sensitive data, applications and infrastructure — rendering firewalls and other similar security measures defenseless. With the evolution of digital transformation, the privilege-related attack surface is expanding at a rapid pace with an emerging landscape of systems, SaaS and cloud-based applications, machine-to-machine accounts, hybrid environments, DevOps processes, IoT devices and more. Attackers know this well, which is why nearly 100% of all advanced attacks today rely on privileged credentials — from Edward Snowden, Yahoo! and the U.S. Office of Personnel Management, to the Bangladesh Bank and Uber breaches, to name a few. Privileged access is not just a compliance problem or a human user problem. It is, without a doubt, a security problem that encompasses users, applications and machine identities — and has the power to completely disrupt business. And so, organizations are prioritizing privileged access security to protect against the threats posed by credential theft and privilege misuse.



More than ever it is critical that CISOs and other security leaders become involved from the onset of digital transformation initiatives.

EA So many CISOs talk about digital transformation these days. How does CyberArk help organizations secure their digital technologies in this new era?

AB Organizations everywhere are pursuing digital transformation projects – migrating to the cloud, adopting SaaS, and evolving their solutions with robotic process automation and DevOps, while aiming to solve problems, create personalized experiences and accelerate business performance. The digitization of business creates greater opportunities including the ability to reduce costs, rapidly innovate, drive competitive advantage and increase efficiency. It can also create greater exposure to threats. More than ever it's critical that CISOs and other security leaders become involved from the onset of digital transformation initiatives. Research shows that by getting involved as strategic advisors early in the process, CISOs can proactively reduce risk and drive more productive business outcomes. As the market pioneer, CyberArk recognizes the importance of supporting CISOs and their role as a digital transformation enabler. That's why we continue to lead the market with a focus on simplicity, automation and risk reduction, delivering the most complete solution to protect against external attackers and malicious insiders exploiting privileged credentials and secrets. The CyberArk Privileged Access Security Solution empowers organizations to move forward fearlessly into this new digital landscape by securing access to their entire digital business and providing protection for all privileged credentials no matter what they are – human or machine – or where they are – on-premises, in the cloud or in hybrid environments. Through the CyberArk Privileged Access Security Hygiene Program, we help security leaders identify the areas of greatest potential cybersecurity risk, prioritize, and drive quantifiable risk reduction.

EA For many organizations, DevOps is a game changer. But it's also changing conversations about risk. Can you discuss the role security plays in DevOps?

AB People are fast realizing that you can't do DevOps without security. Without the security

team's involvement, risks that are not adequately assessed may simply be accepted, with the view that rapid adoption of DevOps is essential for competitiveness. Yet security can – and should – be integrated without slowing down development. Poor security practices will inevitably lead to a breach or failed audit, and force the team to stop the delivery of new features in order to catch up on technical debt. It's important that CISOs and their teams help stakeholders understand the changing risk picture and guide their decision-making for mitigation strategies that reduce risk and increase business value. Many CISOs see a golden opportunity in embracing close collaboration with DevOps teams: Automation gives the security team a way to build security into development and operations more than ever before. As security professionals have argued for years, “building in security” is what leads to greater efficiency, stronger competitiveness – and better security.

EA Robotic process automation (RPA) is also getting a lot of buzz these days. What should organizations considering RPA keep in mind?

AB RPA has the potential to deliver huge benefits to organizations in terms of increased efficiency, improved accuracy and significant cost savings. What's easy to overlook, however, are the IT security risks that RPA deployments can bring. Consider that in a typical enterprise RPA deployment, an organization may utilize thousands of software robots in production, which are activated and deactivated on-demand. These bots can perform a huge number of automated, functional tasks every hour – or even every minute. Each one of them requires privileged credentials to connect to target systems and applications to perform assigned duties. If these credentials are left unsecured, they become ripe targets. An attacker who gains access to the RPA password storage, console, or source code can take full control of the bots. Given the number of bots deployed in production at any given moment, these unsecured credentials can expand the attack vector exponentially. All of this means that as organizations embrace RPA, security teams must manage and protect privileged account credentials used by RPA bots and administrators,

just as they would any other privileged user or process. Further, CISOs and security leaders have a timely opportunity to drive conversations with the business about the value of applying strong cybersecurity to transformative technologies. Through the C3 Alliance, CyberArk's global technology partner program, we deliver more out-of-the-box integrations with top RPA solutions and secure more in-production deployments than any other privileged access security vendor.

EA You referenced the CyberArk C3 Alliance. Can you expand on CyberArk's approach to security integration partnerships?

AB Today's security and compliance environment is rapidly changing, and there's no “silver bullet” solution or vendor that can fully address every challenge. Organizations need a robust ecosystem to help navigate the digital transformation landscape, especially in industries like banking and insurance that are undergoing significant disruption. That's why we view security as a team game and have nurtured an enthusiastic and fast-growing ecosystem of more than 125 partners that can provide organizations with holistic, tailored solutions to meet their evolving security needs – today, tomorrow and far into the future. Nothing better illustrates our “team game” philosophy than the CyberArk Marketplace. With more than 2,000 downloads per month, it is the premier destination for privileged access security-related technology integrations for organizations around the globe. As organizations accelerate their digital transformation strategies, the CyberArk Marketplace features integrations with foundational technologies and processes such as cloud, containers, DevOps and RPA. CyberArk Marketplace users can search for effective solutions for mitigating emerging risk in their own environments, submit their own integrations to address evolving issues, build upon existing integrations to develop customized solutions and contribute to industry dialogue and solve cybersecurity challenges faster and smarter together!



AN INTERVIEW WITH TIM KEELER
CEO & CO-FOUNDER, REMEDIANT

JUST-IN-TIME SECURITY FOR PRIVILEGED SECURITY

CYBER security experts agree without exception that hackers target privileged access in their offensive campaigns. This stands to reason, simply because elevated access allows an attacker to target the most important applications, the most critical business processes, and the most valuable resources. Security privileges thus become an important aspect of any modern enterprise security protection strategy and require special attention from CISO-led teams.

Remediant has pioneered just-in-time security for privileged access, designed in a manner that avoids need for special agents or vaults. The Remediant SecureONE platform supports control and visibility into the distribution, usage, and protection of enterprise privileges. We caught up recently with Tim Keeler, CEO and Co-Founder of Remediant, and we asked him to provide some insights into the Remediant offering and into privileged security in general.

EA What was the original founding motivation for Remediant?

TK Back in 2015, Paul Lanzi and I saw that enterprise security teams tasked with managing privileges were struggling. We also saw that existing – now legacy – privileged access solutions weren't scaling as companies began their transition to cloud, virtualization, and other modern IT initiatives. As we began consulting for organizations dealing with breach response, we saw the same attack vector over and over again in organizations that had no privilege access management (PAM) capabilities, as well as companies that attempted to deploy password vaulting solutions with a varying degree of success. Something different had to be done. Along with these observations, comes our current belief that for most enterprises, the privileged accounts have already been compromised. This suggests that our platform needs to include support for response and remediation – which, incidentally, helps explain our name.

EA How does privileged access relate to the attack surface of an enterprise?

TK It's well-known now that the attack surface for enterprise breaches includes any place where an access decision is being made. In the early days of computing, this was an easy thing to control, because data traffic moved through well-defined gateways, and could be easily mediated by firewalls. But today, the modern distributed enterprise is evolving toward a zero-trust, least privilege-based model, with less dependence on perimeter gateways and more emphasis on secure access. When you combine this with the notion of elevated privilege, which is required for one's most important assets, then you can see how the attack surface would be so closely related to privileged access. Our main narrative is we focus on protecting the access and less about the password.

EA Tell us about how the SecureONE platform works.

TK The SecureONE platform is a best-in-class privileged access security solution for



The move to the Cloud and cloud-like models is inevitable.

enterprise that integrates with existing or planned infrastructure to support a variety of different protection goals, including support for transition to cloud. Our platform supports automated evaluation of privileged access (Just In Time Administration), continuous inventory of privileged access distribution, API integration with workflows and Web interfaces, and continuous monitoring of access attempts, all without installing agents. The platform also supports compliance reporting, audit log management, and incident response. At all point during its evolution, the platform was designed to handle scale and scope for the dynamic digital enterprise. Furthermore, we have focused our efforts on ensuring that SecureONE is simple to use, with as few clicks as possible to accomplish tasks, and with minimal reliance on human processes, which are always inferior to automation. Our total cost of ownership to design, deploy, and operate has proven to be significantly less than existing competitors. This sets our solution apart from most legacy vaulting solutions. That is, we are designed, via automated controls and emphasis on simplicity, to support the growing needs of organizations moving workloads to the cloud, as well as managing legacy on premise ecosystems. In contrast, most legacy solutions are trying to adjust their existing systems to meet the needs of teams that are accelerating the pace in the transformation of their IT infrastructure.

EA Your team often mentions just-in-time security. How does that work?

TK That's a good question, because so many of our customers are interested in reducing the risk of high privilege for administrators. We do this by reducing the amount of privileged access in an enterprise through our self-service, on-demand capabilities. That is, an administrator is provided access to some critical resource for only the time that is necessary, and via their own account credentials. In fact, Microsoft has recently published that removal of local admin and putting Multi-Factor Authentication in front of all accounts can reduce risk of compromise up to 99%. Such powerful, just-in-time capability reduces the risk of administrator credentials being compromised and used for attacks such as phishing or ticket forgery. It is also highly

consistent with the current design goals of zero trust security and least privilege administration. Everyone understands that removing persistent local administrator privileges/sudo is the goal for proper endpoint security, but few are able to do this at scale. We provide that set of capabilities and make it easy to use.

EA Is it easy to integrate the SecureONE platform into an existing enterprise architecture?

TK We understand that no enterprise is a greenfield, and that a variety of different security tools will be deployed to the typical architecture. On average, large enterprises have over 80 security tools in their portfolio. To that end, we have designed SecureONE to feed data into commercial SIEM, log management, and security analytic platforms so that privilege risk can be factored into any real-time secure posture assessment in the SOC. We also integrated directly with the organizations IAM, UBA, and MFA functions, which are all adjacent to the privileged access requirement. Our Scan and Protect Modes are designed to make inventory easy to integrate, and to remove the need to install software on endpoints. Since our inception, we have always had an API/automation first strategy. Our enhanced telemetry around privilege access also makes other security efforts like the SOC, Insider Threat, 3rd Party Risk, and Audit and Compliance stronger due to the additional intelligence and protection we provide.

EA Any near- or long-term predictions about insider threats and how best to manage privileged accounts?

TK We expect digital insider threats will continue to dominate the time and energy of many enterprise security teams. When compromised or disgruntled insiders gain privileged access to important resources, the attack scenarios can become overwhelming. Our hope, however, is that as we work with our customers, and as privileged access security becomes a more mandatory aspect of every enterprise security architecture, that this risk can begin to be contained. This is an important goal, because it substantially reduces the overall attack surface – and that is our ultimate goal at Remediant.

**MULTI-
FACTOR
AUTHENTI-
CATION**

The use of multi-factor authentication for the validation of a reported identity is now accepted as a basic tenet of cyber security. Most enterprise applications now require at least two factors for access, but the selection of such factors involves every combination of proof methods one can imagine. Some users might need a password and biometric; others might use a password and mobile text code; others might use a certificate and device identifier; and so on.

Such diversity of factors is a defensive advantage from the perspective of complicating matters for offensive actors, and most users will tend to settle into whatever authentication cadence they've been asked to learn. Furthermore, most proof factors have become surprisingly easy to provide (or derive); thumbprint biometric use on the mobile, for example, is trivial for anyone to use and offers a valuable initial proof factor.

Most development teams and solution vendors would prefer to see a standards-based approach to authentication. Influential standards groups such as FIDO (Fast Identity Online) are emerging globally and supporting common frameworks to address interoperability for stronger forms of user authentication. The FIDO group, in particular, has gained considerable traction and now has the support of many heavy-hitting organizations.

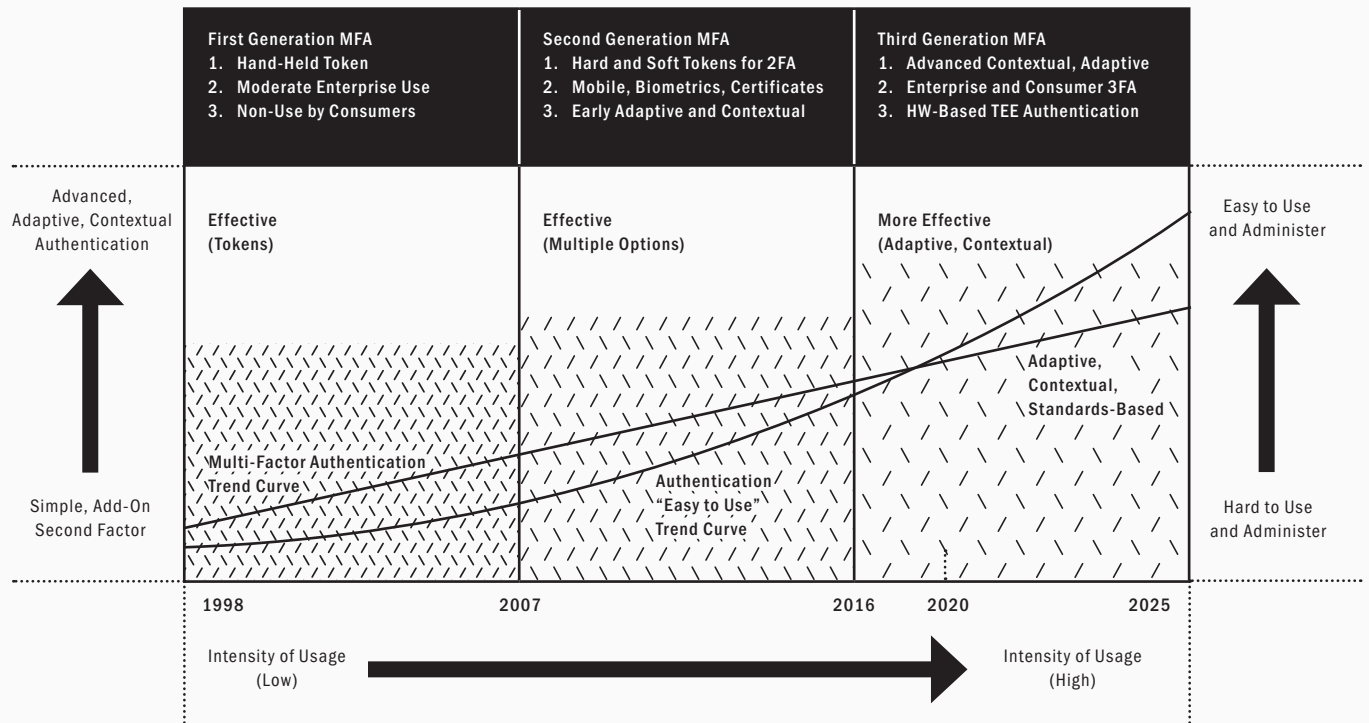
It is also generally accepted in the community that contextual authentication that senses relevant environmental attributes is a valuable goal. Furthermore, adaptive authentication that dynamically adjusts to these sensed attributes offers a more dynamic means for users to be authenticated, and holds promise that eventually, multi-factor authentication will require zero action on the part of the user. This goal cannot be achieved quickly enough for most users.

2020 Trends for Multi-Factor Authentication

The use of multi-factor authentication has been effective through all generations of usage, but has become especially effective in this third and present generation. The emerging adaptive, contextual solutions that are more standards-based have come a long way from the early hand-held tokens that emerged in the industry decades ago, and that were so dominant in the industry for many years (see Figure 1-24).

The most obvious transition has been from a single, add-on, second factor – such as handheld tokens – to the use of advanced, adaptive, contextual authentication. Adaptive authentication deals with the dynamic nature of behavioral activity, whereas contextual authentication provides complementary use of the specifics of a given authentication challenge, including attributes such as location, device type, and user behaviors.

Figure 1-24. Multi-Factor Authentication Trend Chart





Luca Zanon, Unsplash

The ease-of-use for strong, multi-factor authentication has come a long way, with clumsy fumbling around with often-lost physical tokens to cleverly integrated solutions that do not cause great additional work for users. Ease of administration is also a clear trend, especially as standards-based solutions begin to emerge. More recently, the best vendors have also included decentralized storage to reduce the risk of credential compromise against central stores.

The future of multi-factor authentication involves improved security through decentralization (including for authorization), as even greater introduction of embedded contextual and adaptive proof. The extension of stronger authentication to Internet of Things (IoT) and operational technology (OT) has also begun and will accelerate as these initiatives continue to develop. One should also expect in the coming years a more intense effort

to integrate artificial intelligence and machine learning into the adaptive, contextual process. This will naturally complement more decentralized methods for handling authentication and credential information, and should result in highly secure, highly accurate authentication with a minimum of obligation for users.

It also stands to reason that mobile devices and the supporting infrastructure will continue to play an important role in contextual, adaptive authentication. Text and call-back verification processes today will evolve to solutions supported by carriers that use location and other attributes known to the provider to validate reported identities. This approach should impose minimal (or zero) obligations on the user to do much of anything to authenticate.



AN INTERVIEW WITH GEORGE AVETISOV
CEO, HYPR

TRUE PASSWORD- LESS SECURITY

THE idea that an enterprise would store passwords and shared secrets in a centralized repository is just asking for trouble from a security perspective – and yet this has always been the norm when it comes to user authentication. The elimination of shared secrets and transition to a true passwordless architecture forces attackers to divert their attention away from a single centralized target and really changes the equation for how critical resources are protected from cyber threats.


HYPR is a New York-based cyber security company that develops advanced technology in support of a true passwordless security for the enterprise. We spent time with HYPR's CEO, George Avetisov, to better understand the HYPR authentication platform, and to obtain his insights into credential protections and the prospects for how enterprise teams can move in the direction of no longer needing passwords for authentication.

EA George, what are the realistic prospects for companies adopting a passwordless experience? Is MFA now the preferred method of authentication?

GA The prospect of going passwordless is very realistic. Enterprises have never before been so determined to deploy passwordless security to consumers and employees. And they're not talking about adding layers of MFA, but actually eliminating the use of a password altogether. Take a look at the 2019 Internet Trends Report and you may be surprised to find that global adoption of MFA has actually stagnated. The added friction, increased cost, and questionable security benefits have all been factors. But the reality is that legacy MFA never really solved the core problem of shared secrets. It simply built a layer on top of them. Hackers have figured out how to take advantage of shared secrets such as passwords and OTPs, as tools like Modlishka and SNIPR have made it easier than ever before to mount automated large-scale credential reuse attacks. When it comes to passwordless security, the timing has never been better, and the urgency has never been greater.

EA How does the HYPR platform work? Can you share an overview?

GA When you look at the security landscape, you'll find that more than 80% of breaches have one thing in common: They're caused by stolen passwords and shared secrets. Shared secrets are the primary target for hackers and have remained the number one cause of credential stuffing, fraud, phishing, and large-scale breaches. HYPR is the first authentication platform designed to eliminate passwords and shared secrets. By moving authentication keys to the device, HYPR forces hackers to have to attack each user one at a time – drastically increasing security and shifting the economics in the enterprise's favor. Enterprises achieve this vision by integrating into the HYPR Mobile Client into



The world is closer than ever before to seeing a fully passwordless Internet experience.

their applications and deploying the HYPR True Passwordless Server. This fully interoperable approach enables big and small businesses to quickly deploy True Passwordless Security cross-cloud, cross-platform, and in their own app within a matter of days.

EA For browsers like Chrome and Safari, does your platform integrate with their FIDO-compliant methods of authentication?

GA The HYPR Authentication Platform is FIDO-Certified end-to-end and built from the ground up to enable true passwordless security across the user experience. As such, HYPR supports all FIDO-Compliant methods of authentication such as Yubikeys and browser based WebAuthn. In mid-2018, the FIDO Alliance and W3C web standards organization announced that the new Web Authentication standard (WebAuthn) would be supported by all major web browsers. This major development would bring strong authentication to browsers such as Chrome, Safari and Firefox and enables large companies to standardize password-less security across the web experience. The arrival of WebAuthn was a huge driver in the adoption of passwordless authentication by making it possible for service providers to adopt the technology at the browser level. The world is closer than ever before to seeing a fully passwordless Internet experience.

EA What directions are the major compliance standards taking in terms of decentralization and passwordless authentication?

GA The PSD2 regulations are a great example. Section 9.3 of the Regulatory Technical Standards (RTS) specifically describes the use of “separated software execution environments” for achieving Strong Customer Authentication (SCA). This means passwords and legacy 2-Factor authentication are no longer good enough to secure customer applications, as they rely on centralized passwords and shared secrets that do not

make use of a secure software execution environment on the client side. As the goal is to reduce Account Takeover Fraud and secure the customer authentication experience, these requirements are a clear validation and proof that the industry is leaning towards leveraging passwordless authentication that eliminates shared secrets.

EA Any near- or long-term predictions about authentication and protection of credentials?

GA We will see many new attacks on the mobile device side. As authentication becomes more and more decentralized, hackers will focus their efforts on the mobile device. Stay tuned.

25

VOICE SECURITY

Most enterprise security teams have tended to forget that over the past few years, voice communications have become increasingly mobility-based, and thus, increasingly vulnerable to a range of new cyber threats. While it is true that the conventional public switched telephone network (PSTN) was less directly vulnerable to modern IP-based attacks, this claim simply cannot be made about modern voice services, especially when using mobiles.

The good news is that mobile service providers have tended to do a good job improving their underlying communications infrastructure protections toward enhanced voice security. Encryption algorithms have improved, as have the basic voice service infrastructure elements, often due to compliance pressures. The challenges to voice security are thus not as severe as they might be – but enterprise teams should recognize the risk and take immediate action.

Voice security tends to fall into three categories of concern: (1) Encrypting traditional and mobile voice communications when the threat has great potential consequence (e.g., when senior executives travel); (2) Protecting voice communications from eavesdropping at the infrastructure level (e.g., SS7 vulnerabilities in traditional infrastructure); and (3) Ensuring robust, highly-available services for critical applications including first responders.

References above to voice security can and should include adjacent references to texting, messaging, and other forms of over-the-top (OTT) communications. Increasingly, voice-over-IP (VOIP) and related means for speaking with friends and business associates using Internet connectivity (most often involving open WiFi service somewhere in the communication) has become the norm. Voice security for OTT is thus more imperative than ever.

2020 Trends for Voice Security

Through the three most recent generations of voice security, the associated controls started with mostly effective PSTN controls, through less effective early security for Voice-over-IP (VoIP) and mobility, toward the current generation, where excellent over-the-top (OTT) encrypted voice solutions and improved underlying infrastructure controls give enterprise teams good protection options (see Figure 1-25).

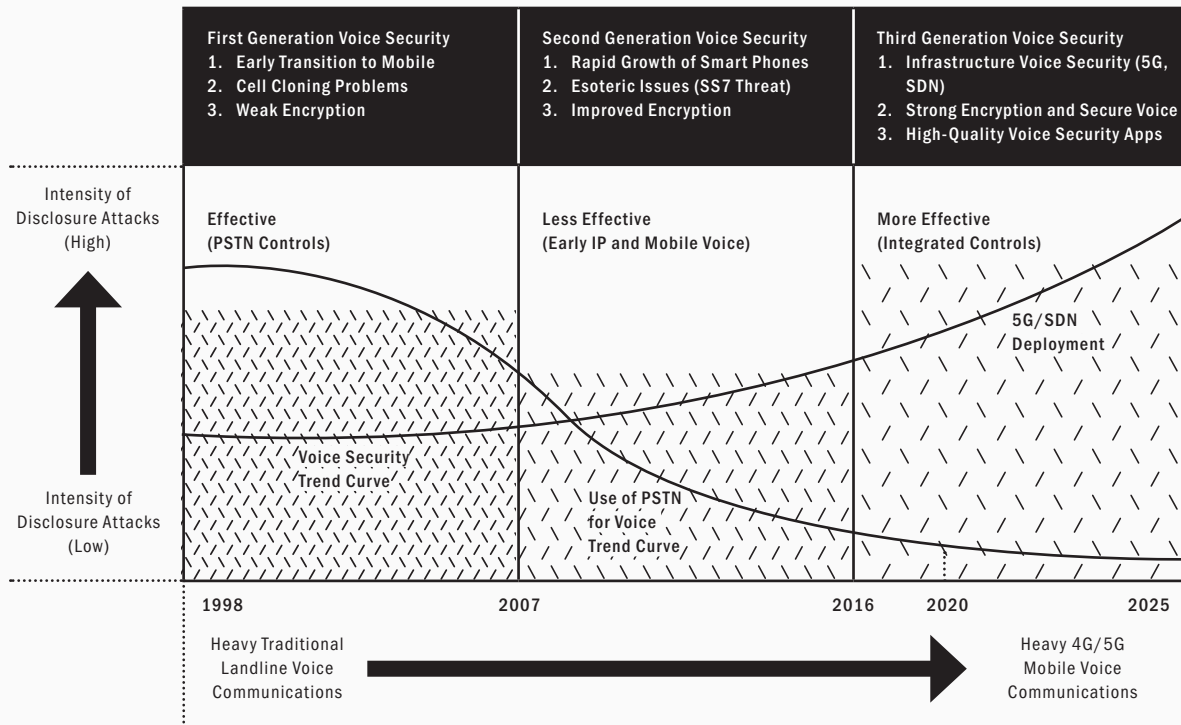
While the intensity of voice attacks is becoming ever more intense, many CISO teams have been surprisingly passive (or ignorant) regarding this threat. The transition from landline PSTN toward emerging 5G mobile services with its largely SDN-powered infrastructure offers greater flexibility for introducing new security for voice. But this is only true if security teams select the best OTT solution for mobiles, especially for traveling executives.

The future of voice security will be heavily focused at the application OTT level with end-to-end encryption providing round trip protection between endpoints. This will be true for mobile, VoIP, and application-based communications such as conference bridge and video conferencing utilities, which are generally non-encrypted today. Compliance controls for secure voice are likely to


increase in their intensity as well. It is worth saying that in the coming years, voice leaks are likely to play an important role in the transition of voice security from an add-on to an essential strategic component of every CISO’s operational playbook. When senior executives start to see their voice communications on WikiLeaks and other Internet-facing sites, the demand for encrypted OTT applications for voice will grow accordingly.

Finally, it is now time to put to rest the archaic practice of demanding that executives traveling to untrusted regions turn in their devices in favor of a temporary burner phone. The entire concept is flawed from top to bottom (e.g., foreign governments can tap burners), and reasonable alternative solutions using OTT encryption apps and infrastructure work much better. Let’s hope we see this old, inconvenient practice die soon.

Figure 1-25. Voice Security Trend Chart



**DIGITAL
RISK
MANAGE-
MENT**



The future of digital risk management lies in the convergence of interests between corporate brand and marketing teams, with zero understanding of security, and the cyber security teams, with less understanding of marketing interests, but who certainly understand cyber threats.

Digital Risk Management – also often referred to as brand protection – might be the greatest control in the enterprise that is not properly addressed directly by most enterprise security teams. This lack of security attention – and many exceptions do exist in larger organizations such as banks and telecommunications firms – is surprising, because fraudulent activity affecting and negatively influencing brands have increased considerably.

The most common digital risk and brand-related attacks involve domain misuse, hijacking, and other business identity-related breaches and fraudulent actions. This can involve the use of adjacent domains to spoof identity for phishing, or even domain squatting for illegal impersonation of a business – but in all cases, the attack techniques used range from subtle action to blatant use of obviously spoofed domains.

Two reasons such brand and reputation protection functionality have been less prominent with security teams to date include: First, a brand is an intangible asset – one that cannot be easily embraced, catalogued, and financially valued (unless you are Coca-Cola or Google). Second, some data breaches might suggest to casual observers that even after a major breach, brand reputation rarely suffers and that companies tend to bounce back (e.g., Home Depot, Target).

These arguments should hopefully ring hollow to the cyber expert, simply because a stronger case can be made that malicious actors have only begun to scratch the surface of the negative reputational impact that can be brought about by successful breaches. The Democratic National Committee is an example of an organization deeply wounded by their attacks – many of which involved brand-related breaches through email weaknesses.

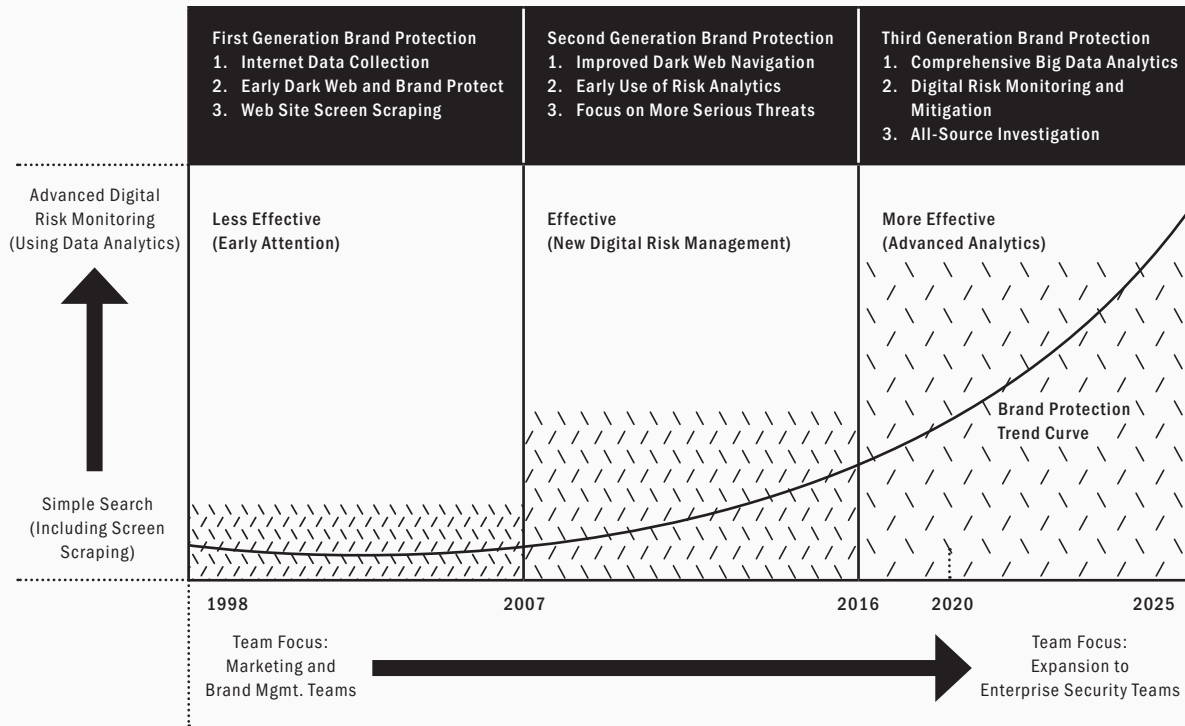
The most common solution for protecting brand involves a new discipline known as digital risk monitoring. In short, the approach relies on a comprehensive, all-source gathering of past and real-time information about an organization. This can include deep investigative collection across the surface, deep, and dark web infrastructure. The goal is to detect evidence of fraudulent activity, and the industry has produced some excellent tools and offerings.

Much digital risk monitoring is done in close proximity and coordination with email security, simply because the protections used for email infrastructure often address many of the same domain-related issues. Email security vendors now include many control functions and capabilities in the digital risk monitoring space, which makes procurement decisions easier for any enterprise buyers.

2020 Trends for Brand Protection

The effectiveness of brand protections has evolved through three generations of use from less effective early techniques, including trying to deal with early screen scraping, to more effective techniques that use advanced analytics in the context of digital risk monitoring solutions. The maturity of digital risk monitoring, including user interfaces and the skill-

Figure 1-26. Brand Protection Trend Chart



sets of risk researchers on the surface, deep, and dark web, has increased commensurately.

In addition, the focus of brand protection has shifted from marketing and brand management teams who were concerned with brand degradation from non-cyber origins, to now include focus from security teams who worry about brand degradation by malicious adversaries engaged in deliberate acts. Such combined focus has yet to include full merging of marketing and security budgets, but this might happen in the future.

The future of digital risk management lies in the convergence of interests between corporate brand and marketing teams, with zero understanding of security, and the cyber security teams, with less understanding of marketing interests, but who certainly understand cyber threats. The resulting interdisciplinary approach to digital risk will be one of the more effective controls in the future enterprise.

Finally, the role of the deep and dark web – in addition, obviously to the surface web, cannot be understated. Many of the digital risks that occur for modern enterprise teams are best identified in the context of activity only visible through intelligence gathering these more clandestine forums. To that end, digital risk management and threat intelligence solutions are often closely linked.

BUG BOUNTY SUPPORT

The use of bug bounty programs began with some of the largest global companies in the world – Google, Microsoft, AT&T, and so on – deciding that it was in their best corporate interests to work with, and reimburse cyber security researchers targeting their enterprise infrastructure. It was a good example of practical and reasonable if-you-can't-beat-'em then join-'em thinking amongst these corporate security groups.

These original bug bounty programs were mostly in-house, but the security vendor community quickly made available a collection of excellent options for commercially-managed, outsourced, or crowd-sourced bug bounty and vulnerability management services. One attractive approach has involved the use of a vetted community of hackers who carefully and appropriately probe and scan target infrastructure. The results are both useful and cost-effective.

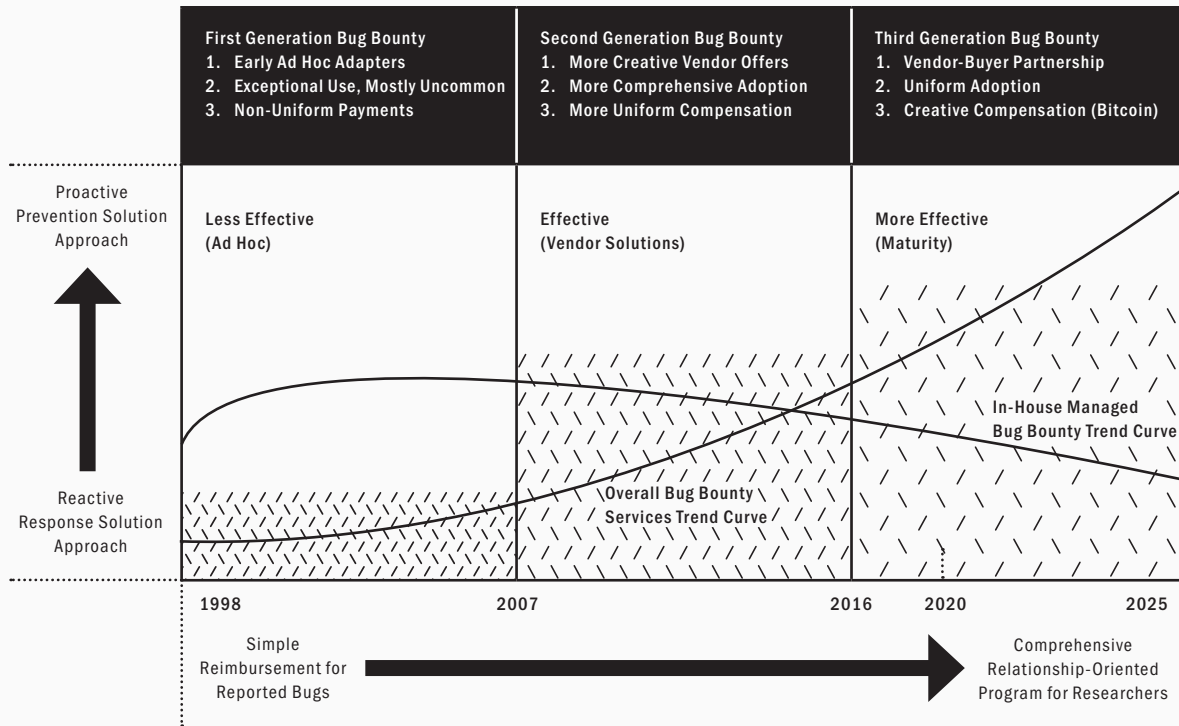
For buyers looking at vetted research communities, it makes sense to carefully review the steps followed to determine who can be part of the testing crowd and who cannot. This is an important differentiator, because if you can locate a great white hat crowd that is capable, vetted, trustworthy, and also well-trained to find exploits, then you will have an excellent resource for your security program.

Increasingly, mid and even smaller-sized companies are putting bug bounty and vulnerability management programs in place with vendors. The result is that more exploitable holes are being detected sooner by white hat hackers than would have previously been quickly identified by black hats. Obviously, all bug bounty and other testing programs cannot find every problem, but the approach pays off well in most cases.

2020 Trends for Bug Bounty Services

Bug Bounty programs in the first generation were mostly ad hoc, in-house programs with uneven results and unclear reimbursement economics; second generation bug bounty services improved the overall effectiveness, and modern, third-generation

Figure 1-27. Bug Bounty Services Trend Chart



solutions are more effective, mature, and attractive to a variety of different companies in all sectors (see Figure 1-27). Even government agencies are using bug bounty services as a risk reduction measure.

The general trend has been from reactive responses to issues, through earlier researcher detection of issues, toward truly proactive testing to prevent problems from occurring. This requires that staging and pre-deployment systems be subjected to bug bounty and vulnerability testing. An additional trend has been from simple reimbursement of researchers for bugs found to a more relationship-oriented program of cooperative trust.

The future of bug bounty services lies in more trusted relationships with vetted groups. To date, much of the work delegated to crowd-sourced testing has tended to be the Internet-facing infrastructure, simply because the external trust model need not be adjusted. In the future, however, bug bounty service providers will be given special, trusted access to

more sensitive applications and systems, in many cases, prior to their production deployment.

One interesting side issue related to bug bounty is that when a vulnerability is detected, it obviously has some value to both the targeted entity and any affected users. One might imagine a type of market evolving for discovered vulnerabilities, although the implications might not be too welcome. Nevertheless, whenever something of value is created or discovered, someone else will find a way to trade on that value. Time will tell on this one.

CYBER INSUR- ANCE

The cyber insurance marketplace has been an obviously vibrant aspect of our industry, with growth, excitement, and buzz surrounding the emergence of significant new business in this area. Board members and executives like the idea of risk transferal via an insurance policy, and CISO teams have tended to be fine with the purchase of a policy – so long as the premium payments do not come from the enterprise security operating budget.

This budgetary issue is a major consideration, of course, because CISOs would never select a policy over the purchase of a functional solution – and this should be obvious: Ask any CISO if they would prefer budget for ten new staff or for a cyber insurance policy – and I think you can guess the answer. Once (or perhaps, if) financial responsibility for insurance premiums shifts to the operational security teams, then expect growth in this area to subside quickly.

That said, the bottom line in cyber insurance is that no one – and that means no one – has much grasp on the correct financial risk equation to determine the optimal premium/coverage ratio. Instead, what tends to happen in 2019 and into 2020 is that insurance companies cover as little as they can, with premiums that are as high as they can sell. This is obviously how all insurance works, but buyers of traditional policies have more data to help them negotiate.

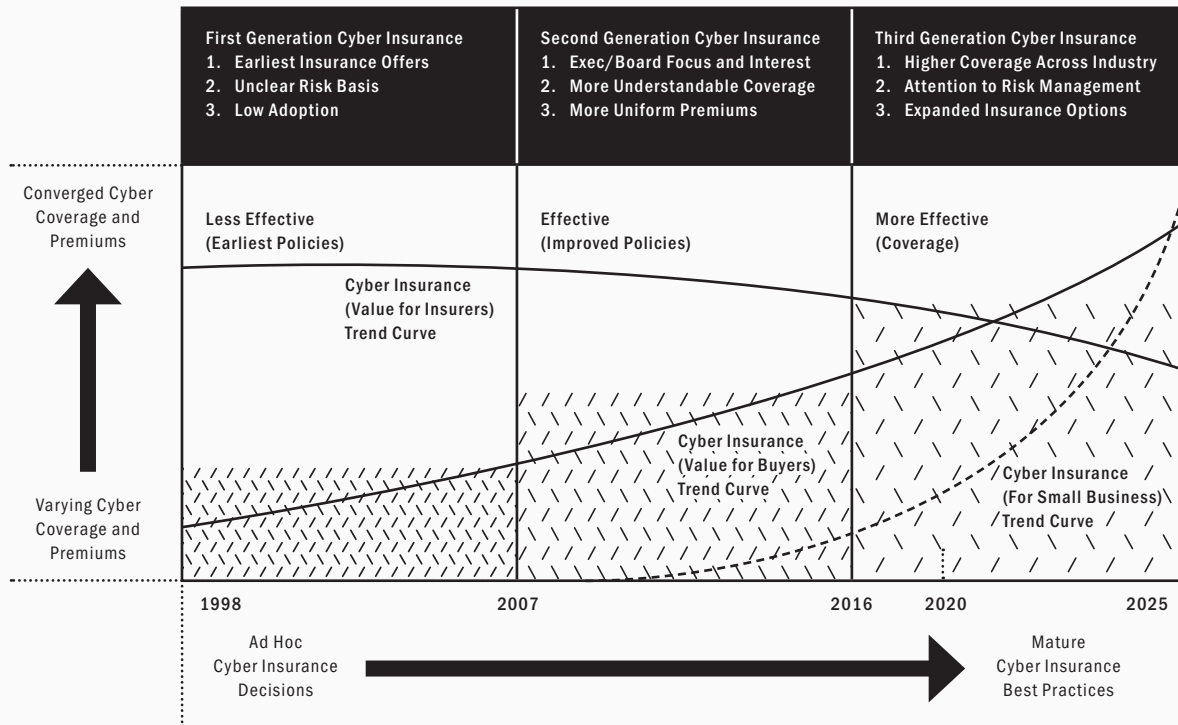
Here is an example of the challenge to writing cyber insurance: We all know that it would be highly unlikely (except in the Biblical circumstances) for a severe hurricane to hit on the same day in every US city with an NFL football team. So, writing hurricane insurance does not need to account for this impossible scenario. In contrast, any cyber expert can attest that a cyber attack can easily hit every NFL city in the same instant – and this influences the details of policies. The types of costs that enterprise teams seek to cover via insurance policies come in four flavors: First, there is the operation cost that

emerges as lost business during an attack. Second, there are the response and legal costs of dealing with the aftermath of an attack. Third, there are any government or regulatory fines that might be levied as a result of an attack. And fourth, there is the cost of reputational loss that comes with certain breaches.

2020 Trends in Cyber Insurance

The effectiveness of cyber insurance is best measured in its ability to properly transfer risk in a meaningful way from the team being insured to the insurance company. First generation policies were less effective because premiums were too high and coverage too low. Second generation policies were better, and third generation cyber insurance is already beginning to show signs of more effective risk transferal (see Figure 1-28).

Figure 1-28. Cyber Insurance Trend Chart





Mark Basarab, Unsplash

Trends include a shift from varying policy specifics across different insurance companies toward more converged insurance offerings with a common, predictable equation for calculating premiums and coverage. Buyers will shift from making ad hoc decisions about cyber insurance, toward making more informed and mature decisions about what to buy. This maturity will hopefully extend to the executive team and corporate board.

The future of cyber insurance can be summed in three basic themes: First, the buyer will gain increasing value in both risk transferal and improved coverage for lower premiums; second, the insurers will see decreasing value, but will see increased business volumes; and third, small businesses will begin to buy cyber insurance policies at increasing levels, potentially becoming the bulk of the insurance industry growth.

Great attention has also been placed on how best to integrate cyber insurance with other vendor offerings. For example, it makes perfect sense that if buyers agree to utilize some world-class assortment of security protections, that they should see breaks on their insurance premiums. This is not, however, part of the industry today (no discounts for good security behavior), but one could easily imagine partnerships emerging to offer such deals in the future.



**AN INTERVIEW WITH PETER FOSTER
CHAIRMAN, WILLIS TOWERS WATSON,
FINEX CYBER INSURANCE AND CYBER RISK SOLUTIONS**

CYBER INSURANCE INSIGHTS

FEW areas of the global security marketplace are as hot as the sale of commercial cyber insurance policies to business. The transferal of risk from an organization to an insurance company is often the optimal means for addressing the growing challenge of protecting corporate assets from cyber attack. As such, a new ecosystem has emerged to support the need for cyber insurance policies for enterprise customers of all sizes and shapes.

Willis Towers Watson is a global company that specializes in risk management, advisory services, and insurance brokerage. With a vibrant practice and great expertise in cyber insurance, the company has a unique vantage point into this important and growing business service. We asked Peter Foster, who runs the Cyber Risk Solutions team at Willis Towers Watson, to share his insights into cyber insurance and to provide an overview of how enterprise customers are using policies to transfer risk.

EA Let's start with an overview of how cyber insurance specifically transfers risk.

PF Cyber insurance transfers financial risk from the corporation to an insurance policy for liabilities arising out of the failure of security, breach of privacy (intentional or negligent), or content issues (infringement, defamation) with the publication of websites. The coverage also extends to loss of income and expense to remediate security issues following a disruption to applications whether triggered by a hacking event or a failure of software. The policy also covers breach response costs, including notification to affected parties, credit monitoring services, forensic and PR costs. One of the newer coverages extends to physical damage coverage or bodily injury loss due to or arising out of a cyber event.

EA How should an enterprise security team determine whether a given cyber insurance policy is a good deal?

PF Cyber Insurance policies are changing constantly due to developing risks. An underwriter looking to gain an edge will create a key coverage enhancement and some in the market will follow. Enterprise security should look for coverage that applies to their company or to their industry. For instance, a cyber attack against a construction company could shut down their systems and affect logistics and consequently delay projects. Some underwriters are willing to cover the costs associated with delays or loss of contract due to such an attack. This is critical today with the proliferation of ransomware attacks. No company is completely protected or secure. Through an assessment of your risks and mitigation tools, policies and procedures in place, you will identify gaps and potential loss that could arise out of the risks to which you cannot mitigate. The limitation of the risks and the overall protections in place will help your cyber insurance broker design a policy that meets your specific needs to minimize the premium cost for such a policy.

EA Is it possible for a buyer to receive better insurance terms by having better cyber security?

PF Yes. Most underwriters test your security


through core questions based on the NIST framework or ISO 27002. Your responses are compared to other similar-sized companies in your industry and region. Underwriters were less focused on the network business interruption coverage until the ransomware attacks began 2 years ago. Now we hear many more questions on disaster recovery and table top exercises to test your plan. Losses not only help brokers push new enhancements (bricking), but also help us take lessons learned to peer clients (one healthcare organization encrypting a data warehouse due to a peer's breach of their data warehouse).

EA What are the prospects for small and mid-sized business regarding cyber insurance?

PF Several insuretech products are available that have more-than-the core coverage. If your risk is perceived as minimal, but you are being pressed to show you have cyber insurance, many underwriters will add a cyber liability endorsement to your general liability policy. The issue is that the general liability endorsement is not broad and will not cover network disruption loss or the breach expense. Larger brokers have used their leverage to secure broad cover for small to mid-size businesses at a competitive pricing. Compare that coverage to what you may see in a mainstream policy or general liability endorsement or rider.

EA Any near- or long-term predictions about the cyber insurance market?

PF As we continue to see significant ransomware losses and large-scale data breaches, underwriters are adjusting pricing, especially on excess layers. The rate increase is not significant (no more than 5%) but it could be trending. The gross premium for stand-alone cyber policies is reportedly around \$4B. The loss ratios are good for many primary underwriters, but a couple excess underwriters are pulling out of large account business due to small premiums and large exposures. With all the noise around cyber terrorism, some markets are providing broad cyber coverage that will cover nation state attacks. Some markets are skittish depending on the breadth of coverage. We believe this market will be \$10B in premium annually by year end 2021.



**No company
is completely
protected or
secure.**

GRC & RISK MANAGE- MENT

A promising development in cyber security in recent years is the improved and more frequent use of automation in the establishment, maintenance, and support of governance, risk, and compliance (GRC) objectives. To support this desire for automation, commercial GRC platform deployment has exploded well beyond use by the pioneering adopters of crude, early tools. This is good news for the cyber industry, as it results in dramatically improved GRC processes.

Some excellent advances in GRC and risk management platform support include more integrated and embedded collection of data from business unit processes, more extensive coverage of DevOps software processes, and improved reporting of GRC issues to senior executives and boards. Each of these platform advances has come from practical usage-based requirements, so this is additional evidence that GRC is a mainstream tool in business.

Mid-market and SMB organizations have tended to not utilize GRC and risk management platform solutions at the same rate, however, presumably because their governance issues are less intense. With compliance demands increasing, however, one would expect to see GRC platforms moving down-market and more into as-a-service environments. This trend should be present across all sectors and will include government and academia as well.

An additional trend one would hope to see involves less emphasis on introduction of new compliance frameworks in response to political or public pressure after an incident. The idea that cyber incidents are best handled by some state, or interest group, or nation, or even company – introducing a new set of compliance requirements is gradually becoming extinct. This is good, because existing frameworks are sufficient; it's the execution that matters.

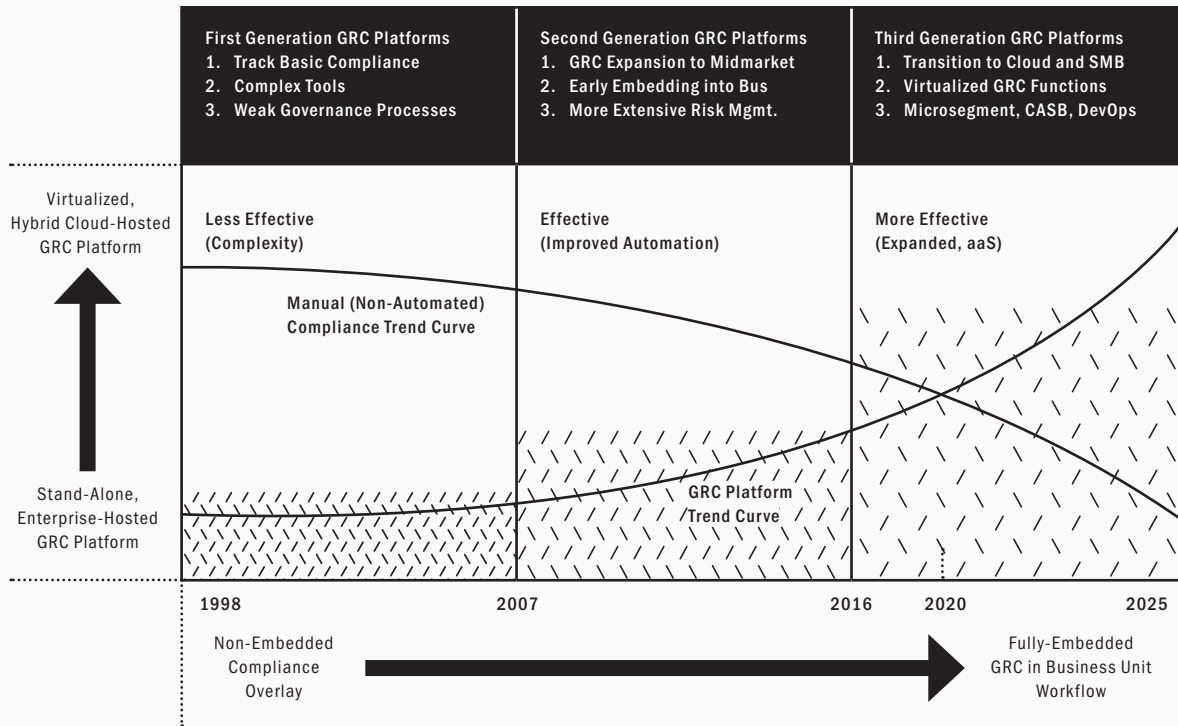
2020 Trends for GRC Platforms

The effectiveness of GRC platforms has grown from highly complex and tough-to-use early platforms in the first generation, through effective platforms in the second generation that relied on improved automation of workflow, into more effective solutions in the present, third generation that have expanded scope and are offered with a cloud-based as-a-service option for customers (see Figure 1-29).

Trends include a shift from stand-alone platforms hosted on-premise, toward virtualized, cloud hosted (or even hybrid cloud supporting) solutions that serve the governance, risk, and compliance needs of evolving organizations. A clear trend has been the shift from non-embedded compliance overlay data collection to fully-embedded GRC data collection and management within business unit processes.

The future of GRC continues to be bright, as organizations of all sizes will continue to rely on platform automation for all GRC-related activities. The market will see growth in GRC solutions for down-market, as-a-service offerings. Even the smallest companies will likely begin to use GRC to support compliance in their day-to-day activities. International use, perhaps driven by more severe privacy requirements, will be even more intense than in the United States.

Figure 1-29. Governance, Risk, & Compliance Platform Trend Chart



The impact of super-intense privacy requirements as evidenced in the General Data Protection Regulation (GDPR) arising from the European Union will gradually find a balancing point across international standards and norms. Certainly, privacy controls are essential and the GDPR has done much to advance awareness and attentiveness; but some aspects of the GDPR, such as the high fines to be levied post-breach, might require some adjustment downward over time.

INCIDENT RE- SPONSE

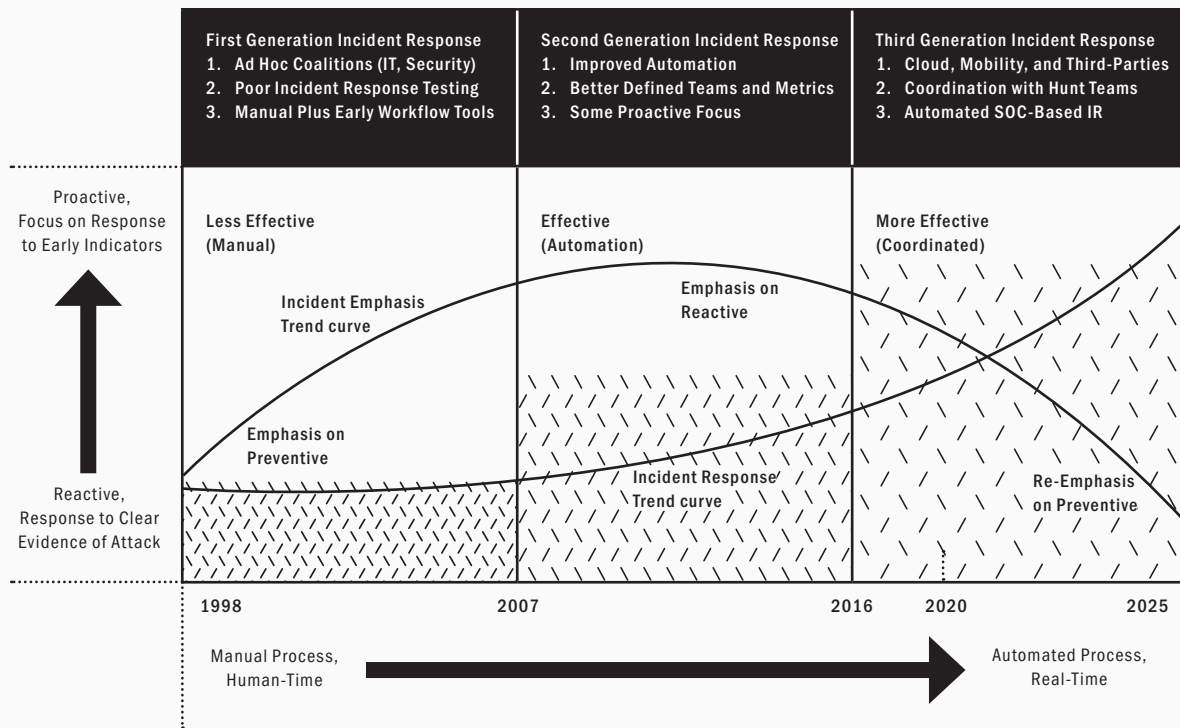
An aerial photograph of a winding asphalt road through a dense, lush green forest. The road curves through the trees, and a white rectangular redaction box covers a portion of the road in the middle-left area. The overall scene is a dense, green landscape with a clear path cutting through it.

One of the more interesting trends in cyber security is the seemingly cross-wise views that security teams should essentially just accept that attacks are inevitable, and agree to shift right on their emphasis.

Incident response involves the processes, tools, and procedures required to deal with on-going or previous cyber attacks on an organization. Traditionally, incident response has been more about cleaning up a disaster, forensically analyzing a prior cyber attack, and reconstituting hacked systems. More recently, however, incident response includes dealing with analysis of indicators, which introduces the possibility that incident response can be preventive.

A common visual descriptor used in our industry to describe cyber security emphasis is the so-called “shift-left” and “shift-right” designation. The underlying basis for this view is the attack lifecycle, which spans early indicators (on the left), across to an accomplished cyber attack mission with consequences (on the right). As such, shifting left implies being more proactive, and shifting right means being more reactive.

Figure 1-30. Incident Response Trend Chart



Incident response references the work done on the right of that underlying lifecycle. It includes the workflow, tools, databases, automation, analytics, forensics, and other resources to support all reactive work done after an attack has commenced or completed. Many of the larger commercial and government organizations today have an incident response vendor partner, but a surprisingly high percentage of mid-market and smaller firms do not.

An important component of the response emphasis involves collection and analysis of telemetry from endpoints. The so-called endpoint detection and response (EDR) marketing category has thus emerged, and several vendors provide excellent solutions for data collection, analysis, and support for hunt tool using EDR sensors, management systems, analysis tools, and reporting interfaces.

2020 Trends for Incident Response

The effectiveness of incident response has evolved from most manual, less effective procedures in the first generation, through effective incident response advances that introduced automation in the second generation. Today's modern, third generation incident response frameworks, including EDR, are coordinated with hunt teams, automated into the SOC, and much more effective at dealing with incidents (see Figure 1-30).

One of the more interesting trends in cyber security is the seemingly cross-wise views that security teams should essentially just accept that attacks are inevitable, and agree to shift right on their emphasis. This is a hard concept to dispute, because just about every industry expert or pundit has explained that stopping capable cyber actors is not possible today, and that if a nation-state wants to break into your systems, then they can do so with impunity.

Despite this observation, just as many cyber experts will agree that incident response tools can be deployed and used to deal with early indicators, rather than with emerging evidence of a completed attack. By pointing the incident response team at indicators, the security team is essentially shifting

left in their emphasis – and this would seem to contradict the earlier advice. The bottom line is that incident response teams will have to cover the entire lifecycle.

Everyone agrees, however, that the clearest trend is from manual incident response toward highly automated tools that guide workflow and manage artifacts. This is good news, because as cyber campaigns by adversaries continue to grow more advanced and complex, no enterprise security team can possibly defend using manual processes. The speed and scale of attacks require automated support, if only to keep up with volumes of data for analysis.

The future of incident response includes expansion into mid-market and SMB team processes, likely through as-a-service, cloud-based offerings. This is a natural evolution because cyber attacks to these segments are becoming more intense, and the automation associated with modern incident response platforms does not require large, highly trained teams to operate. This greatly expands their applicability and potential use.

The integration of incident response, endpoint security (e.g., EDR), and SOC hunt analysis tools is also a clear trend. This should be welcome news for cyber security teams who must currently juggle a variety of different platforms in their work. Vendors are advised to maintain a holistic perspective, and to recognize that their own commercial platform likely complements many other solution factors in the enterprise, versus providing stand-alone support.



AN INTERVIEW WITH MENACHEM SHAFRAN
VP PRODUCT, XM CYBER

SUPPORTING BREACH AND ATTACK SIMULATION

THE process of breach and attack simulation is clearly one of the important new controls in cyber security. Benefits include validation of controls over a continuous period, and exercise of attacks from the best available taxonomies of known (and unknown) methods. The result is that most enterprise teams now utilize some form of simulation for this work, and excellent automated platforms are commercially available.

XM Cyber is an industry leader in this area of breach and attack simulation with a platform that effectively integrates with other aspects of an enterprise architecture. Led by veterans with military intelligence backgrounds, the company makes good use of attack frameworks and offers an excellent validation experience. We spent time with Menachem Shafran of XM Cyber, who shared his insights into this important area of cyber security and how the company's platform is evolving.

EA How does attack and breach simulation work in the context of enterprise security?

MS Breach and attack simulation works in enterprises by continuously simulating attacks on the environments, in a safe way, without creating additional risks. With BAS tools, enterprises gain a measure of how effective their security is and where they should focus their efforts to improve it. Measuring continuously allows enterprises to detect changes that create a risk in near real-time and to act upon them, greatly reducing the risks. In most cases, the security team will review the results every few days and update their workplan accordingly while also validating the impact of changes as they are made. This is a great improvement to just looking at vulnerabilities or performing manual red team exercises every few months.

EA Does simulation require buyers to conceive scenarios or does automation cover this action?

MS Different breach and attack simulation tools work in different ways, yet most would not require the user to conceive the exact scenario. At XM Cyber, we ask the customer to define the goals, meaning the target critical assets that the simulation will try to reach. The details of how the simulation will reach the critical assets are completely automatic. The simulation will look to find the most probable attack vectors towards the assets. Using this information, we can now help prioritize remediation efforts based on the impact each finding has on reaching the critical assets. This allows organizations to focus on the most critical issues they have instead of just guessing what to work on.

EA How does the XM Cyber platform work? How does it automate the simulation process?

MS The XM Cyber platform works by installing lightweight sensors in the environments. The sensors then learn the network and run

the attack simulation in a safe and accurate manner. One of XM Cyber's unique values is the fact that the platform runs the simulations on the production environment and not on separate devices. This allows us to discover the most realistic attack vectors possible by combining vulnerabilities, IT hygiene and misconfigurations, and user activities just like a real attacker would. The simulation process is completely automatic. The platform has many attack techniques in its hacking engine, and just like a real attacker it selects the most fitting on each step of the attack vector.

EA Do you make use of any attack frameworks such as MITRE ATT&CK?

MS Yes. The XM Cyber platform is aligned to the MITRE ATT&CK framework and we show the relevant ATT&CK techniques on each step of the attack. We believe that the ATT&CK framework is a great learning tool to help security teams understand how adversaries work and an excellent way to create a common language in the industry.

EA Any near- or long-term predictions about breach and attack simulation?

MS I believe that breach and attack simulation will grow rapidly as more and more organizations start to realize they can now measure their security posture effectively. I think we will also see many collaborations between, or perhaps among, BAS vendors and other security vendors such as vulnerability management solutions and endpoint protection. Together, we will provide better value to customers by allowing them to view a more holistic understanding of the current risks in the environment.

**PENE-
TRATION
TEST/SIM-
ULATION**

Penetrating testing has always been a staple in the enterprise security team's arsenal against continually expanding cyber risk. Few would argue the obvious benefits of unleashing the power and capability of vetted, trusted white hats against some target system, before non-vetted, untrustworthy hackers find their way to the same systems. This is particularly true for any asset or resource that is publicly accessible directly via the Internet.

Now, any form of testing will always have limitations. In fact, where testing is an excellent means for demonstrating the presence of exploitable vulnerabilities, it is not a great means for convincing an observer of their absence. In this way, penetration testing serves to illustrate and highlight problems, often in an environment where management or other decision-makers refuse to accept that serious issues might be present.

Finding good penetration testing talent for hire is non-trivial, so many enterprise teams have opted to create working relationships with companies specializing in this skill. Past experience suggests that many penetration testing teams have been somewhat transient, since it is easy for a highly-trained expert to spin off into a new start-up. Acquisitions of small penetration testing teams has also been a popular means for larger consulting firms to grow.

Nevertheless, every enterprise security team is wise to ensure a close working relationship with either in-house or contracted penetration testing talent. This is often best used to demonstrate, often in a shockingly visual manner, the existence of exploitable flaws in some portion of the business infrastructure. When a business unit leader refuses to cooperate with security, for instance, good penetration test results often shift such attitudes.

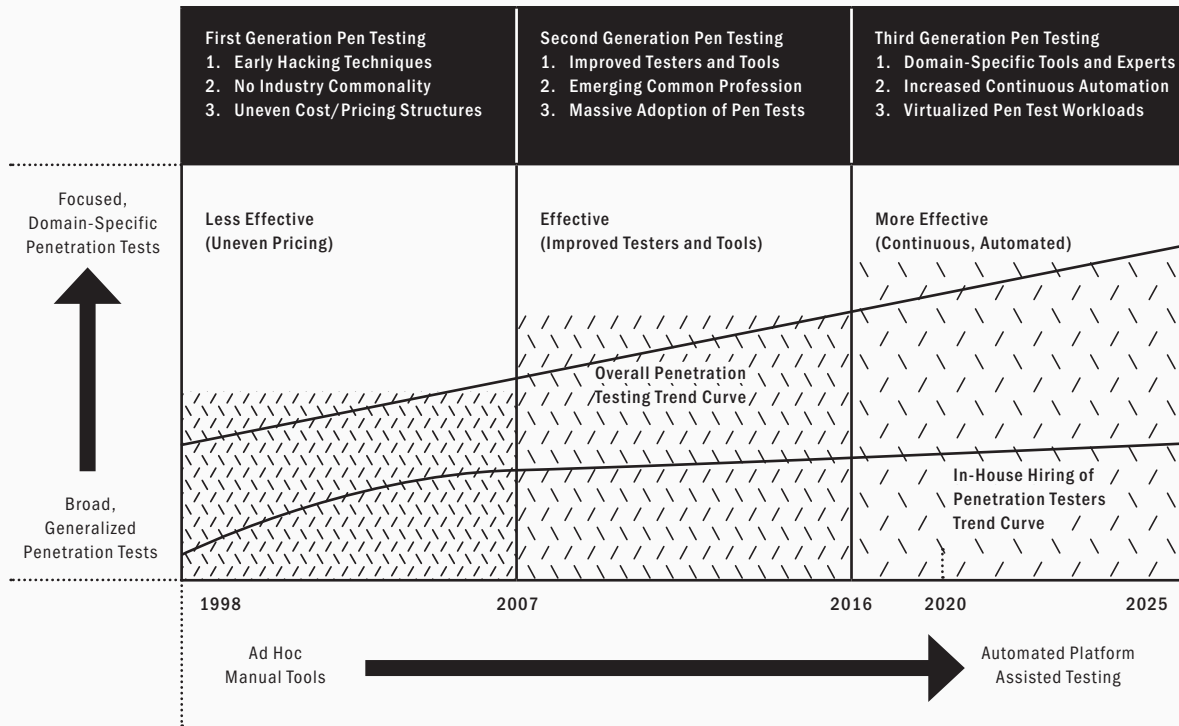
2020 Trends for Penetration Testing

Penetration testing has evolved from less effective engagements in the first generation, through effective usage in the second generation, into a more effective third generation. Advances that propelled this gradual and steady improvement included improved tester, better tools, more predictable pricing, and now greater attention to continuous penetration testing using automation (see Figure 1-31).

A clear trend has been from broad, general penetration tests toward more focused, domain-specific tests. This is good news for teams that manage specialized infrastructure or technology such as with IoT or ICS. An additional transition has occurred from ad hoc manual testing toward the use of automated control validation platforms – and this includes breach and attack simulation (BAS) platforms that provide continuous test coverage.

The future of penetration testing will continue to be characterized by gradual, but steady growth, with domain-specific testing and continuous simulation driving most of the heavier business growth. Despite clear advances in autonomous self-learning, it is highly unlikely that automation and AI will soon replace the need for experts to manage the penetration testing engagements for their infrastructure.

Figure 1-31. Penetration Testing Trend Chart



The growth of BAS and bug bounty services will put pressure on some penetration testing firms to show their value. One would expect, however, that human curation will continue for certain types of security testing, especially for test campaigns with more intense objectives (e.g. breaking into something particularly sensitive). To that end, expert penetration testing will always be a valuable capability in our industry.



AN INTERVIEW WITH JOHN DAWSON
PRESIDENT, EXACTDATA

GENERATING SYNTHETIC DATA FOR CYBER

LIKE all types of computing functions, cyber security controls must be tested. And with the complexities of modern enterprise networks, running meaningful tests requires either live production or simulated synthetic data. Obviously, the security advantages of not exposing production records, credentials, and other information make the synthetic option more desirable. But, it requires that good algorithms be available to create truly realistic test environments.

ExactData provides high-quality synthetic test data based on customer specifications. The Rochester-based company has recently begun to focus on cyber security applications, and this is good news for both enterprise teams and security solution vendors. We spent time with John Dawson of ExactData to learn more about how synthetic data can be generated from specifications and how this process can extend to network data as well.

EA What is synthetic data? What value does it bring to cyber application testing?

JD Synthetic data is created to look exactly like live production data, but is completely artificial. Synthetic data allows you to create fake documents, databases, and emails with customer names, account numbers, and social security numbers that look real, but that contain no personally identifying information (PII) or sensitive data. It allows you to develop, test, and demonstrate cyber systems with realistic data that looks like live network traffic, but that poses no security or privacy compromise risk.

EA Tell us about the technical issues required to generate high quality synthetic data?

JD Making low quality synthetic data is easy: You can obtain numerous such generators for free today. High quality or high-fidelity synthetic data generation, on the other hand, is much more difficult to do well. \$100M's worth of research has been invested in this technology area by the US Government and Commercial companies and we are the only company that has actually solved this problem and been issued patents. The difficulty is in maintaining the relationships between the data elements and other disparate databases for very large datasets. Business logic, work flow rules, statistical distributions, software requirements, use-case coverage, and maintaining the time axis all need to be correct to give the data the necessary realism for testing today's complex systems and changing cyber threats.

EA What types of synthetic data are required for cyber security? Do commercial vendors use such data to test their products?

JD Reasonable commercial solutions are available to test the performance of Network Intrusion Detection Systems and other network devices. Attack signatures are typically known using technologies such as Nessus, Metasploit, Splunk, Spirent CyberFlood, and penetration testing. Formal testing for behavior-based, intrusion detection systems is still in its infancy – until now. Publicly-available data sets are severely limited in attack



\$100M's worth of research has been invested in this technology area by the US Government and Commercial companies and we are the only company that has actually solved this problem and been issued patents.

scope (not many types of attacks), outdated (70% of works use a dataset from 2000), or propriety. This is where synthetic data plays an important role: State of the art network traffic generation. Today's "network normal" traffic is real traffic, but generally includes simple content that can be made to look more complex for more representative performance testing in the network. There is direct control of the traffic format mix, but events are not linked or consistent with other events, except by happenstance. This means that individual actions aren't necessarily in a logical, realistic sequence. Threat traffic is predefined with fixed content that can be edited manually. The threat traffic can be complex and made to be even more complex to enhance the test realism. There are no links or consistency with network normal traffic and the threat traffic is injected into a stream of simple traffic, making it stand out in an obvious way from the network normal traffic.

EA With all the breaches that have occurred in recent years, one would expect that synthetic generation of large credential databases would be an important test priority for enterprise. Are you seeing this trend?

JD Absolutely, as behavioral based attacks become more and more complex (and more prevalent), cyber security teams are realizing that they do not have a good way to test these systems. This is where synthetic data generation from ExactData comes in to fill this gap.

EA Can you generate synthetic network data and is this done through partnership?

JD We are excited to say yes. We are working with major network traffic generation companies and technologies. The basic process is that ExactData generates the synthetic data needed to emulate the most realistic conditions for the environment, industry, or company. Synthetic data includes the content, IP address structure, organizational hierarchy, document types, and subject matter-specific emails for any industry or client – but contains no PII, production, or sensitive information, because it is 100% artificial. This data is correctly

formatted in the right file format, such as .msl, for ingest into the network traffic generation solution. This solution then plays those scripts in a timed sequence, sending packets of this rich behavioral content data through the network. Network normal traffic is real traffic with complex base rate content that is all plausible. Threat traffic is naturally integrated with network normal traffic, interwoven and obfuscated for truly realistic testing, scoring, and performance metrics. This provides behavior-based control of the data domain mix in addition to the traffic mix that has become the foundation of cyber testing techniques.

EA Any near- or long-term predictions about synthetic data generation?

JD I'm amazed that there isn't more competition in this market today. We are beating some of the largest companies in the world today, ones with multi-billion technology portfolios on some of the world's largest technology implementations. We do this with a high-fidelity synthetic test data generation solution. The standard technologies used today basically use production data that has been modified. That introduces huge security risks and breaks important data linkages that increase the software development error rate and associated costs to fix these errors. For cyber, the standard data generation solutions being used today aren't realistic enough to effectively test advanced, behavior-based threats that are becoming more sophisticated, more prevalent, and expected to continue their rapid growth. My prediction is explosive growth in this technology space once the viability and value of this solution becomes more broadly known in the cyber community.



**AN INTERVIEW WITH GUY BEJERANO
CEO & CO-FOUNDER, SAFE BREACH**

AUTOMATING BREACH AND ATTACK SIMULATION

WHEN any enterprise is asked whether their applications, systems, networks, and infrastructure are secure, the response is necessarily subjective. Good metrics for whether controls are working or whether known (and also unknown) breach methods might succeed in the enterprise are rarely available. Only recently have enterprise teams begun to rely on the process of continuous validation through live simulation to test each of these concerns. This has resulted in a new branch of cyber security protection.

SafeBreach is a leader in this new field often referred to as breach and attack simulation (BAS). Their world-class platform is designed to test controls, as well as continuously execute breach methods. Through analysis and reporting of the results, enterprise teams can thus provide more accurate responses to the question of whether security is being properly deployed. We spent time with Guy Bejerano of SafeBreach to learn more about their platform and how it achieves these important goals.

EA How does attack and breach simulation reduce risk in an enterprise? What questions does it answer for the security and executive teams?

GB Breach and Attack simulation (BAS) solutions automate attack scenarios against the actual infrastructure using a complete library of known and unknown attacks, effectively carrying out continuous 24x7x365 tests on every security control in the enterprise. This catches drift in security controls immediately and allows security teams to quickly address issues. Advanced BAS solutions find complex security gaps automatically by executing safe simulated attacks and analyzing the results. They find loopholes and prioritize the remediation activities of the security teams to enable a strong security posture at all times. They also provide guidance and data on how to fix security issues. By measuring the impact of each security gap found, advanced BAS solutions enable security teams to focus on the most impactful activities and report on their progress in terms of how they improve overall security posture. Questions answered for security teams include the following: What is the security posture of the company? What is the effectiveness of each security control? What are the underlying security gaps? What needs to be prioritized in fixing based on the business risk? Questions answered for executive teams include these: Is the enterprise currently vulnerable, and in what ways? What is the organization wide level of preparedness for a specific threat of interest? How is the security team prioritizing its efforts to minimize business risk? Is the company's business or brand at risk? In the case of M&A, what is the security posture and risk of the asset/ company we acquire?

EA Does breach and attack simulation remove the need for penetration testing?

GB Automated Breach and Attack Simulation platforms provide a holistic and comprehensive view of the enterprise security posture rather than a funneled or siloed approach of vulnerability management or penetration testing solutions. Like BAS, penetration testing carries out automatic tests in the network. However, penetration testing



BAS provides a holistic, independent assessment of an enterprise security posture.

by definition interacts with production system whereas SafeBreach runs in production without interacting with production system, making it completely safe and risk free. SafeBreach's BAS solution runs continuously and network-wide, using a dynamic, playbook containing close to 7000 different breach methods, which represents all steps of the attack kill chain. This provides users with a comprehensive view of their environment's overall security posture. Penetration testing will remain a valuable tool for specific targets of interest and for new and innovative ways to reach them. However, BAS solutions are the only way to scale security testing network wide, and on a continuous basis. With today's dynamic environment and ever evolving threat landscape, the only way to keep up is automated and continuous testing.

EA Can simulations be run across distributed, hybrid cloud infrastructure?

GB Yes. Simulators can be deployed in the corporate network, the data center and the cloud and simulate all possible attack paths between them across the entire kill chain including infiltration, lateral movement, host level attacks and data exfiltration. A comprehensive BAS platform will cover multiple deployment options, support multiple flavors of operating systems and cover all major attack surfaces including network, host and email.

EA What are the types of management actions an enterprise might take based on simulation results?

GB BAS provides a holistic independent assessment of an enterprise security posture. This enables management teams to make appropriate decisions to manage risk, including remediation of security gaps. It enables the enterprise to track progress across several risk-oriented indicators to make sure security posture is improving over time and to be able to report it to executive levels. BAS enables management teams to know their current posture and which steps to take to improve it. So, it offers a concrete set of steps that can be assigned and tracked to ensure that the appropriate security controls are implemented and properly configured. Finally, BAS enables a management team to

understand the relative value of different security controls needed, to implement the right security controls. This can be of value in pricing negotiations with vendors.

EA Any near- or long-term predictions about breach and attack simulation?

GB BAS platforms are becoming a vital solution in enterprise security. They will provide an expert, always-on member of the security team that ensures that the security posture does not drift and is continuously improved. The expertise of the BAS platform will be greater than any human member of the security team, because the BAS is continuously up-to-date and runs 24x7x365 to find security drift. As organizations seek to adopt more cloud infrastructure with complex cloud services to configure, BAS will be a vital companion on the journey continually testing and recommending changes to ensure security. Think of the BAS platform as a vital team member with the best skill set in the world and with an understanding of the business risk of complex breach scenarios and an ability to recommend how to fix them. As the environment and the architecture of the network becomes more complex and distributed, BAS role in tracking and validating security posture and controls will become more vital, as the ability to manually track and maintain configuration, governance and posture will become impossible. BAS and security automation will become close companions as the remediation data produced from BAS platforms will be streamlined to trigger automated remediation workflows to continuously identify and resolve security gaps which are a result of frequent configuration changes.

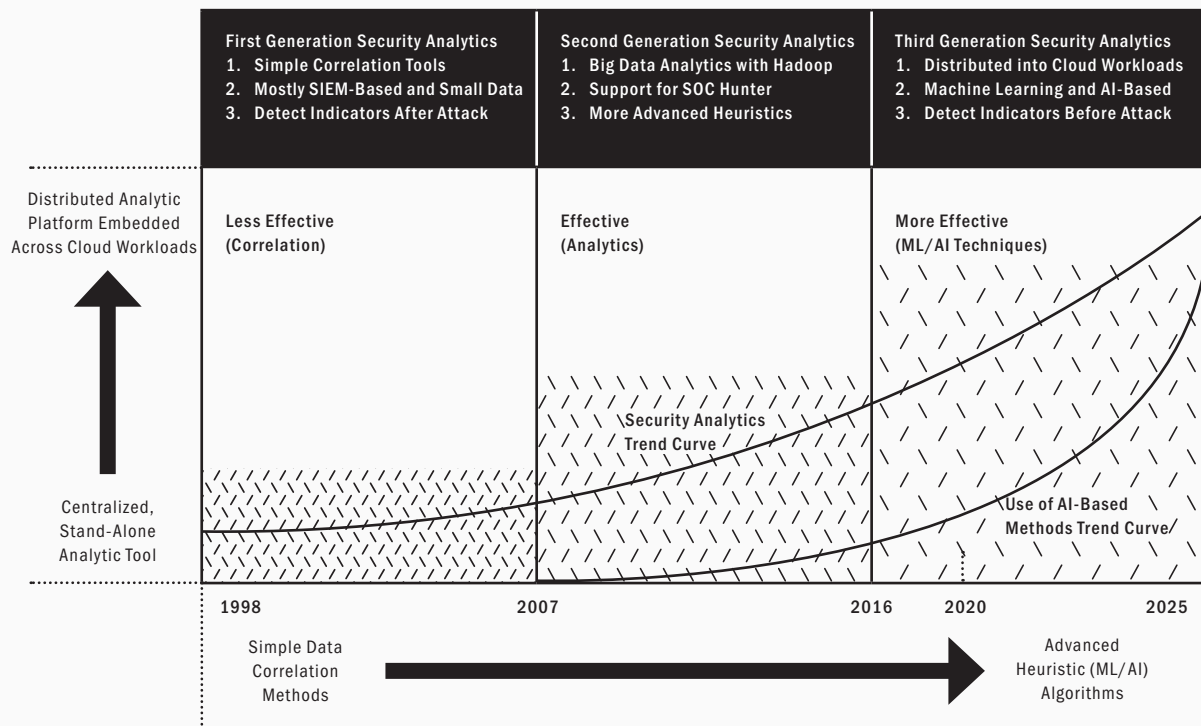
**SECURITY
ANALYTICS
/ HUNT
TOOLS**

The use of AI, and its related techniques of machine learning and deep learning, is the most exciting advance in security analytics – and arguably in all cyber security.

Just about every cyber security solution today is marketed as being powered by an underlying analytic platform, which tends to marginalize the importance of this technology discipline to cyber security. Collecting and properly analyzing data for evidence of cyber intrusions is a powerful means for improving the entire cyber defensive process, and the community has embraced analytics as an essential requirement in modern cyber defense, especially in the SOC.

The primary focus areas for security analytics tend to break into three main categories of emphasis – although products can easily include elements of any number of these attributes: behavioral analytics, which collect observable meta-data to draw conclusions about actors; real-time analytics, which involve fast algorithms that keep up with network speeds; and AI-based analytics, which includes machine and deep learning techniques to reduce risk.

Figure 1-32. Security Analytics/SOC Hunt Tools Trend Chart



Solutions for security analytics can be stand-alone toolkits to be integrated into a customer's environment; they can be embedded as a component in a cyber security appliance or other product; or they can be available as a service, often in the cloud, where the analytics provides results to customers who need a verdict rendered either as part of a malware analysis or some hunt-related activity. In all cases, so-called SOC hunt teams are increasingly involved as users.

Endpoint detection and response (EDR) solutions have also tended to serve as powerful SOC hunt platforms, because the data collected provides valuable insights into important behaviors. Insider activity, for example, is often best analyzed using hunt tools that integrate with EDR, DLP, and UEBA. Such integration is indicative of current trends for commercial tools, where analysts want more sources of data, more powerful analytics, and less complex interfaces.

Some debate does exist across the cyber security community as to the efficacy of AI, machine learning, and other advanced heuristics in dealing with exploits. Evidence seems overwhelming that when applied properly, the results for malware and exploit risk reduction can be dramatic, so long as valid data is used to train the advanced processing on powerful platforms to recognize and accurately categorize previously unseen artifacts.

2020 Trends for Security Analytics

The effectiveness of security analytics and SOC hunt tools has risen through three generations from less effective correlation methods used for indicators, to effective use of advanced analytics using all-source intelligence to improve accuracy, and to reduce false positives. Modern, third generation security analytic usage includes highly advanced algorithms using machine learning to detect variants, new exploits, and other subtle indicators (see Figure 1-32).

Security analytic solutions have transitioned from centralized, stand-alone tools to more distributed analytic platforms that are often embedded in cloud

workloads to address threats local to the asset being protected – often in a micro-segmented architecture. This is a powerful advantage, because it removes the needs for a complex, and often ineffective, perimeter to be used to detect attacks inbound to an organization.

The use of AI, and its related techniques of machine learning and deep learning, is the most exciting advance in security analytics – and arguably in all cyber security. Deep learning represents an excellent means for removing the need for tedious test training, by creating powerful arrays of neural processors that can ingest live data and learn to recognize malware and exploits dynamically.

The future of security analytics and related SOC hunting resides with advanced algorithmic developments, and soon, this will include autonomous cyber security. To keep up with the prospects of synthetic attacks that are automated to find the weakest link in the fastest and most efficient manner, automation will be required to ingest behavioral and environmental data, and then combine this with the best intelligence to make a real-time security decision.

Some debate does emerge, in the context of this increased automation, as to whether SOC hunt tools will be required in the future for human operation and use. This is an open question, but one would expect humans to remain in the loop, if only to curate the automated tools working to make real-time decisions for mitigating risk from automated offensive tools. Such human curation can be vital and non-trivial, but it can never be as fast as automated tools.



AN INTERVIEW WITH PEDRAM AMINI
CTO, INQUEST

ADVANCED SUPPORT FOR THE SOC HUNTER

THE SOC hunter has increasingly become a more central player in the detection and response process for enterprise cyber security. This follows the increasingly complex assortment of vulnerabilities and attacks that must be addressed, along with the constant need to hone and improve the configuration of automated tools in the enterprise. Both lend well to a SOC team performing hunt actions – but a proper support platform is obviously required.


InQuest provides an automated platform for SOC hunter that includes powerful means for inspecting files to detect the presence of malicious code. The platform ingests network data and then goes through a variety of analytic functions resulting in an effective risk score. Pedram Amini, CTO of InQuest, was kind enough to spend some time with us explaining how the platform and associated process work for the SOC team supporting enterprise risk analytics and response.

EA Tell us about the InQuest platform and how it supports the SOC hunter.

PA At the end of the day, our platform aids human analysts through its actions as a tireless mechanized SOC analyst. Data is collected from a variety of sources at scale, exposed and analyzed with human-level scrutiny, scored with consideration from numerous sources, and made available to the human analyst through robust search. Described by one of our customers as “Network God Mode,” the InQuest platform empowers the SOC hunter to pose questions that she otherwise could not answer without tremendous manual labor. The depth of data exposure through technology we coined “Deep File Inspection” is the true differentiator here for the SOC hunter. Providing the ability to analyze in real-time or leverage the power of hindsight through retrospective analysis or “retro-hunting,” as we call it. The most common file-borne malware carriers include Microsoft and Adobe office documents, compressed archives, and applet code (Java, Flash). Each of these file formats is complex, ever-changing, and requires a specialized skill-set to dissect and interpret. InQuest removes this barrier to analyze liberating the SOC hunter to focus on the threat, instead of wasting precious cycles focusing on the encapsulated delivery package.

EA How does your deep file inspection technology work?

PA Deep File Inspection, or DFI for short, is a core tenet of our solution. A static-analysis engine that peers deep into layer 7 of the OSI model. Essentially automating the expert system that is your typical SOC analyst/security researcher. Regardless of the novelty of nesting employed by an attacker, DFI will rapidly dissect common carriers to decompile/expose embedded logic (macros, scripts, applets), semantic context (ex: data in cells of the spreadsheet, words in a presentation or document), and metadata (ex: author, edit time, page count). Images discovered to be embedded are processed through a machine vision layer (OCR, perception hashing), adding to the semantic context extracted from the original file. Common evasive characteristics and encoding mechanisms



There's a large gap in the talent pool requisite for working in the SOC environment, and it's only getting larger.

are automatically discovered and decoded. The DFI process typically results in four times the amount of analyzable content. For example, 8MB of data may be extracted from a 2MB file, resulting in 10MB of total inspectable data. A general frustration voiced by SOC analysts and information security researchers is the restrictive resources available for detection analytics. In the case of IPS, resources are limited to only nanoseconds of time and kilobytes of analyzable data. IDS systems can typically delve deeper, given the addition of milliseconds of time and additional kilobytes of data. The next step up with regards to time-vs-analysis trade-off is behavioral monitoring or sandbox solutions. Capable of detonating a sample in a virtualized environment and annotating the behavior of the system for threat detection... this takes minutes. The InQuest platform addresses the time-vs-analysis gap with Deep File Inspection (DFI), that typically completes its analysis in seconds and provides megabytes of analyzable data from a variety of sources.

EA Your platform assigns a threat score to ingested data. Can you tell us how this would be used?

PA No single solution is sufficient on its own. There's no "silver bullet" so to speak. In support of that mantra, we play nice with others. Leveraging our experience with a variety of security solutions to stack together complementary tools in a robust manner. We use the term "intelligent" orchestration here to highlight the fact that InQuest supplies data-to, receives results-from, and then interprets those results before factoring them into the threat score. Just as a human analyst leans on their knowledge and experience with vendors and results, our threat scoring engine does the same, capturing the intuition of a seasoned analyst to apply an accurate threat score. Data sources that drive our threat score include IP/domain/SSL reputation, mail/web header analytics, signature/signature-less threat detection, multi-antivirus consensus, behavioral analytics, and more. With so many factors in our analysis, a single digestible threat score is the most concise way for analysts to prioritize their research on the InQuest platform.

EA What is the impact of cloud architectures on how your platform is deployed to the enterprise?

PA Whether data flows are analyzed on-premise or in-cloud, the delivery mechanism for malware is largely the same in both environments. The vast majority of malware is delivered within a file, destined to an end-user, and delivered via e-mail as an attachment or URL. InQuest Deep File Inspection can be deployed in a SaaS model to protect corporate e-mail and/or integrated to into the corporate web proxy. The explosion in popularity of file-sharing platforms ranging from Dropbox to Salesforce adds complexity for threat hunters in the lack of a centralized repository for assets. A cloud deployment of InQuest can be leveraged as a aggregation and analysis point.

EA Any near- or long-term predictions about security analytics and SOC operations?

PA There's a large gap in the talent pool requisite for working in the SOC environment, and it's only getting larger. Simultaneously, data flows and malicious behavior are continually on the rise. This trend will compound into two results. First, an increase in the application of automated solutions including AI/ML and orchestration. Second, an increase in outsourcing to vendors in the MDR and MSSP. Data consolidation across multiple industry verticals provides these vendors with a wider scale global view that can be leveraged to improve and scale automated solutions.



**AN INTERVIEW WITH CHRIS CALVERT
CO-FOUNDER & VP PRODUCT STRATEGY,
RESPOND SOFTWARE**


ROBOTIC DECISION AUTOMATION FOR CYBER

FEW would argue that automation is the secret to optimizing a modern enterprise cyber defense. The decisions that must be made in both real-time and human-time must take into account so many different factors that automated intelligence must play a role, or it becomes too likely that some preventive or reactive decision misses something important. Establishing good ROI for security also requires attention to solid decision-making with automated support.

Respond Software is a leader in the important area now known as robotic decision automation with focus on cyber security. Their platform and team are focused on helping decision-makers from the SOC to the executive suite optimize the judgment and factors that drive action. We spent some time recently with Chris Calvert, Co-Founder of Respond Software, to learn more about robotic decision automation (RDA) and how it can be applied to current challenges in enterprise cyber security.

EA You reference a concept known as robotic decision automation. Tell us about this and how it relates to security operations.

CC Making good security decisions is hard, and making real-time, streaming, complicated, technical decisions with accuracy, is basically impossible. But that is how we as an industry turn the millions of dollars we've invested in security tools into incidents that require action. The problem is, many teams put a junior Security Operations Center (SOC) analyst in the middle, and then artificially reduces the volume to a level they can handle. For example, in one SOC I recently visited, the ratio of alerts collected by their Security Information and Event Management (SIEM) platform to the number of alerts ever interacted with by an analyst was less than one in a million. So, in today's SOC, analysts look at almost nothing, and still suffer decision fatigue within 30 minutes of starting their 12-hour shift. Robotic Decision Automation (RDA), while a bit of a mouthful, hits the nail on the head. With the constant confusion in the market around artificial intelligence, RDA provides a way for us to be clear about what problem we are solving – namely, the volume of alerts generated from security sensors, and the lack of effective human monitoring that manifests as false positives and missed incidents. RDA, built into the Respond Analyst, makes automated decisions about what needs to be escalated as an incident and what can be safely ignored. When I hear the term 'AI in Security', I immediately replace it with 'Java in Security' in my mind. That is: Don't tell me what tool you used, tell me what it does. Because the Respond Analyst is 100% software, it can consider more than 60 pieces of evidence for every alert it evaluates. It helps solving this question: "Given everything else I know, what's the chance this alert is a real incident?" Today's SOC analysts would love to have time to investigate every alert, but the volume is too great. This is the perfect job for RDA, because it brings depth of analysis, scale and consistency to real-time monitoring that no human could match, freeing analysts to use curiosity and creativity to hunt for novel attacks and to focus on security efforts that can reduce overall business risk.



The Respond Analyst leverages all the information that a human security analyst would want - if only they had the time to gather it.

EA How does the Respond Analyst work?

CC You would think that would be a difficult question to answer, but it isn't. We put subject matter expertise into mathematical models and gave them a way to learn from experience. We use recent advances in probability theory (I'll skip the math details). If you are an experienced security investigator, you know how likely a successful attack is given a set of circumstances. Over decades you develop ways to think about security problems, as well as a specific set of experiences. Your experiences are subject to bias, but the structure of your thinking is surprisingly resilient. You know, for example, how excited to get about slowly spreading, older, Windows file-based malware in a Linux dominant data center. The Respond Analyst leverages all the information that a human security analyst would want – if only they had the time to gather it. This includes security data sources, threat intelligence, local context about users and systems, known vulnerabilities, behaviors, patterns, and more. It includes basically anything that can be observed, and that reduces the uncertainty of a security decision. By leveraging Bayesian math, we can also use weak evidence to influence automated decision making. The Respond Analyst is not just a set of decision models, it is an integrated decision engine. It uses integrated reasoning to consider data from multiple sources to make a common decision. By assembling evidence from all relevant security data sources, it provides multiple opportunities to detect an attack and a deeper level of analysis. The combination of these capabilities results in the Respond Analyst making ten times fewer false positive escalations, and providing a tremendous level of accuracy in detecting on-going attacks.

EA What's the role of automation in supporting good decision making by an enterprise security team?

CC If good decision-making is equivalent to accurate decision-making, then you should start by picking your battles. We know a lot about decision science these days, and the singular truth is that people only make good decisions within a narrow set of circumstances – that is, when they aren't tired

or stressed, and have enough time to gather and understand all the important evidence and enough knowledge and experience to get to a reasonably likely conclusion. Just describing that exhausted me, thus decision fatigue is a good indicator of tasks to automate. The current trend in the Security Orchestration Automation and Response (SOAR) industry is to gather additional information to equip junior analysts to make better decisions. This information gathering typically makes up 80% or more of your SOAR playbook development. When you have implemented Robotic Decision Automation (RDA) via the Respond Analyst, you no longer have to gather additional information for SOC analysts to make a decision. Rather, you can use your SOAR efforts to speed up investigation and response. This reduces the time from detection to remediation. While the Respond Analyst is often used as a decision support tool early in its employment, it completely replaces the SOC level-1 task of console monitoring, freeing analysts to hunt for novel attacks and support the security program in higher value ways.

EA How do security teams determine the return on investment (ROI) for an automated security platform?

CC There are a number of ways to measure ROI from security operations automation. The real ROI from automation is seen in its impact on your overall security program. What else could you do with the talent or money you currently spend monitoring for incidents? Here are some examples: You can, for instance, enable greater value from your security talent, thus retaining security analysts by providing them more engaging and valuable work. You can also better allocate scarce human resources to tasks that reduce the most business risk, thus gaining dramatic performance improvements. This produces much faster time-to-detection, and results in fewer and less expensive breaches. It also increases accuracy, due to a deep and consistent level of analysis, resulting in orders of magnitudes increase in coverage, as all relevant events are evaluated. The increase in effectiveness from existing security sensors is achieved by tuning them up in volume without incurring additional costs. An automated

security platform also provides a reduction in the overall cost of security operations. This includes reduction in staffing for SOC console monitoring, up to ten-fold reductions in false positives and nuisance alerts, compared to Managed Security Service Providers (MSSP) or internal SOC operations, and involves no rules or playbooks to develop and support, and no sensor tuning.

EA Any near- or long-term predictions about decision making in the SOC? Will the trend toward increased automation continue?

CC Imagine a security program where there is no human involvement between the time an alert is generated on an external sensor, and the time the enterprise adapts its defensive posture. That scenario is scary for the CIO responsible for a high availability environment, but eventually the growth in malicious attacks will surpass technical failure and user error as the most common cause of production impact, and change will be mandatory. The security operations industry is trending in a negative direction, versus the modern attacker, and I think that causes many of us to see automation as a way to reduce the average cost of failure. That is exactly the way we treated outsourcing, and it's a bad sign that we have accepted failure as the status quo. We need automation that expands our industry's average capability by orders of magnitude, just to keep up with the threats we face doing business on the Internet. In order to gain that much capability, we will have to change the layer at which we operate. Currently, we put our most junior security employees in front of a stream of events and tell them to find the best that cyber-criminals and nation states can throw at them. If we put machines in charge of finding the bad, then people can manage the resulting situations much more effectively. The future has people and machines working in concert, each at their best, to provide security for a digital society.

SIEM PLAT- FORM

Virtually every mid-to-large organization today operates a security information and event management (SIEM) in their enterprise. Often referred to as the cyber security hub of an enterprise, the SIEM ingest data from applications, systems, and networks via tailored connectors. It then normalizes this collected data into a common representation so that analytics can be applied toward an effective, actionable conclusion.

The traditional SIEM was housed on-premise in the data center, and would be administered locally via console access by trusted, in-house personnel. This evolved toward increased use by managed security service (MSS) teams operating and managing the SIEM more virtually, with a more extensive assortment of connectors. Modern SIEMs reside primarily in the hybrid cloud, with the requirement that data be ingested both on-premise and from cloud workloads.

Recently, more down-market SIEM offerings have been made available that are easily integrated with cloud deployments, and this has greatly expanded the SIEM ecosystem. One might expect to see SIEM usage even find its way into small and even micro-business infrastructure – mostly virtual – and this will have a good impact on compliance and security in these segments of the business environment around the world.

An additional trend involves the use of advanced tools that help the SIEM better orchestrate security operations across an enterprise. This begins the transition of the SIEM as a passive collection device, into a more active operations hub for enterprise cyber security. This transition will create interesting marketing integration (and collision) with CASBs, microsegments, and even next generation firewalls. High-end machine learning and artificial intelligence are also finding their way into the SIEM

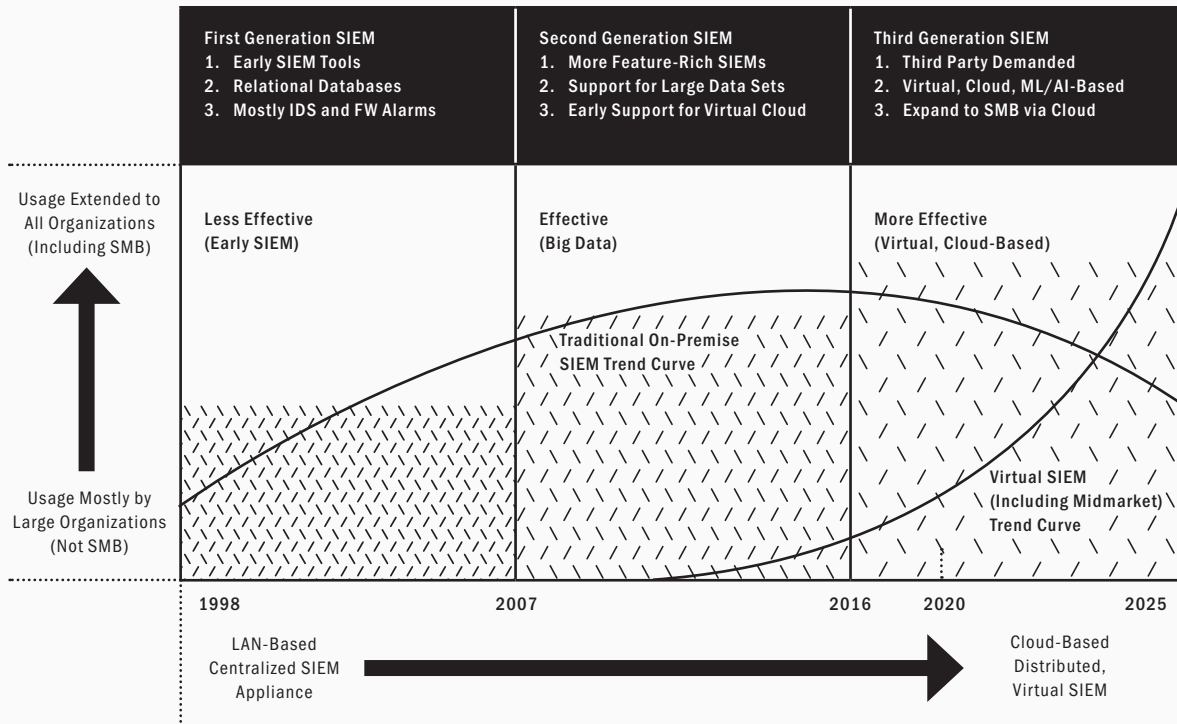
ecosystem. It stands to reason that the learning that comes from observed or test data can make SIEM decision-making more accurate. One should expect to see AI-based processing emerge as an important differentiator between different commercial SIEM offerings, even on the lower end for small and medium sized business.

2020 Trends for SIEM

The effectiveness of SIEM solutions has risen through three generations of usage from less effective early tools, through effective tools built for data analytics, into the modern, third generation where the SIEM is more effective, cloud-ready, and much easier to use. The coverage for SIEM deployments has transitions from mostly large organizations to basically all organizations in the coming years – which is a welcome evolution (see Figure 1-33).

The architecture for SIEM deployment and use has evolved from LAN-based appliances on physical servers to much lighter, cloud-based virtual offerings. A clear trend is that one should expect to see a dramatic drop-off of on-premise hosted SIEM infrastructure in favor of more virtualized coverage. This follows the reduction in emphasis on a perimeter-based LAN supporting the business and government enterprise.

Figure 1-33. Security Information and Event Management Trend Chart



The future of the SIEM is clearly in its expanded market, with the current trends into mid-market infrastructure extending to the micro-business and even family or personal systems. It would seem a natural extension of current SIEM capabilities; for example, ISPs could provide a solution for the home, perhaps hosted on cloud operating systems in generic hardware. This would help families do a better job avoiding serious breach attempts at their personal finances.

One challenge for pure SIEM providers is that adjacent commercial offerings such as UEBA and EDR are designed today to include an excellent set of data collection, analysis, hunt, and reporting tools. As these adjacent platforms continue to expand their own interoperability via increased numbers of connectors to more collection sources, they begin to resemble SIEM platforms, and this should be viewed as a competitive force in this area.



**AN INTERVIEW WITH RAN PUGACH
VP STRATEGY, JAZZ NETWORKS**

ENDPOINT ANALYTICS

ENDPOINT SECURITY has evolved from simple signature-based anti-virus solutions for PCs into comprehensive data collection and analysis solutions that address advanced cyber threats. This new emphasis includes automated platform support for the threat hunter in the enterprise SOC, trying to identify evidence of malware, insider activity, or newly initiated attacks campaigns. This capability must integrate with other security tools in the enterprise, including the SIEM.


Jazz Networks is an endpoint security company with a platform that supports these important functions, with an interface that focuses on helping SOC hunters identify suspicious behaviors. The platform includes a GUI-based analysis environment that allows for advanced queries to understand where threats in the enterprise might be brewing. We caught up with Ran Pugach from Jazz Networks to ask about how this works in practice and to learn what's in the pipeline at Jazz Networks.

EA Tell us about how Jazz Networks supports the emerging EDR marketplace for enterprise.

RP If studies on recent events are any indication, employee-driven data loss is a leading cause of breaches. From older anti-virus solutions that looked for signature matches on files to more recent and advanced EDR solutions that look at behavioral characteristics, the underlying theme is that they were all designed with a system-centric view of the environment. But if users of these systems are the ones putting an organization and its data at risk, then adding a focus on user monitoring is imperative. The primary focus of EDRs continues to be recording process and file-centric activity, but Jazz does not limit itself to looking at files or processes running at the endpoint. While providing in-depth visibility of those aspects, it additionally provides insight into applications accessed, bandwidth usage, browser uploads and downloads, Wi-Fi activity, location information, connection details, DNS activity, cloud share activity, and printing activity (to name a few). This adds to preventative measures to reduce risk, as it monitors both user and system activity prior to a data breach.

EA How does your platform support the modern threat hunter?

RP The Jazz Platform can accelerate threat hunting in the following areas: For data quality, Jazz collects its own metadata, avoiding issues related to data integrity. The kernel-level agent yields granular detail around users and the data cannot be deleted or manipulated by anyone else. To support data variety, Jazz collects a vast range of details on user behavior and activity. This multifaceted picture helps threat hunters choose from a wide variety of data and correlate related information during their investigations. For data visualization, Jazz helps with big data challenges by creating uncluttered views, detailed event timeline (with exact time frame), clean series of events strung together in chronological order, and full context. The platform brings just the most relevant pieces to the surface, with the ability to drill down and pivot between different views (like alarms to the event data details to charts) quickly.



If studies on recent events are any indication, employee-driven data loss, unwittingly or otherwise, is becoming the leading cause of breaches.

EA Do you see the hunt process as requiring new types of technologies such as machine learning or advanced analytics?

RP There is an endless amount of data for threat hunters in the SOC to collect and analyze. Traditionally, they'd have to write scripts to look at a normal processes versus new processes or to find something that's anomalous in an application – usually in the context of a behavioral profile. Machine Learning can help surface the most relevant details, identify and cluster different patterns, and assist the hunter spot anomalies much faster. These are important focus areas for us at Jazz Networks.

EA How important is it for enterprise teams to maximize automation in the protection of their endpoint resources?

RP Enterprise cyber security teams are often required to conduct a great deal of repeat tasks in the context of their day-to-day work activities. Advanced analytics and automation increase the speed and efficiency of these tasks, and for every process that can be automated, SOC teams will have more bandwidth to spend investigating the most serious threats.

EA Any near- or long-term predictions about EDR and threat hunting for enterprise?

RP In the future, the concept of endpoint will imply much more than just computers or servers. There is a huge convergence of cyber security, physical security, mobile, and IoT on the horizon, and this will come with new varieties of endpoints to monitor and protect. As a result, analysts will need to best tools in their SOC arsenal to collect the relevant data and to apply the most advanced methods available to detect the presence of risks in the enterprise.

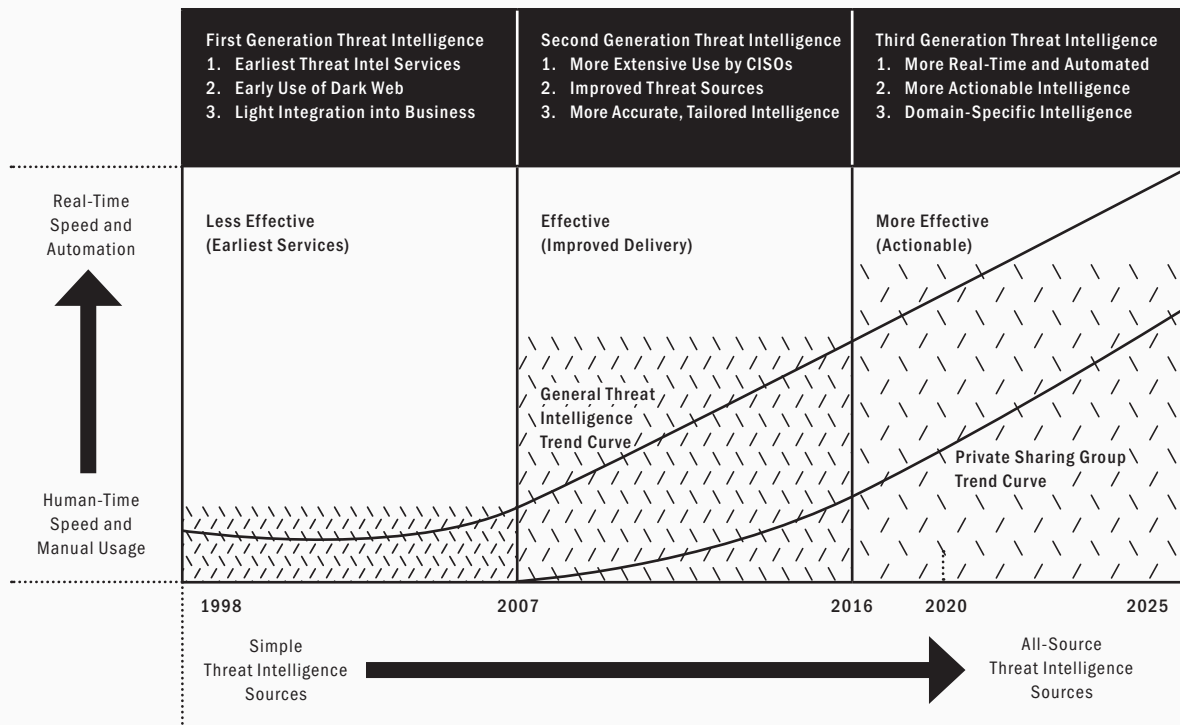
**THREAT
INTELLI-
GENCE**

Considerable threat intelligence is now derived from marginally-unsavory sources such as the deep and dark web, and the lifecycle handing of stolen credentials offers a new opportunity for intelligence.

The use of threat intelligence to enhance the usefulness of cyber security products and services, as well as enterprise processes for prevention, detection, and response is now well-established in our industry. The analogy of oil lubricating an engine seems accurate in describing how threat intelligence drives high-quality security solutions. The most traditional example is the real-time URL intelligence that has been used for years to update and maintain web security proxies.

Many vendors now offer threat intelligence as a feed, often derived from teams of experts, usually former law enforcers and hackers (which one suspects can produce an interesting mix of personalities around the office water-cooler). These threat feeds can be ingested in both structured and unstructured formats. The trend is toward automated sharing of threat data by systems that can ingest and process data with the goal of taking mitigation action.

Figure 1-34. Threat intelligence Trend Chart



Considerable threat intelligence is now derived from marginally-unsavory sources such as the deep and dark web, and the lifecycle handling of stolen credentials offers a new opportunity for intelligence. By embedding threat analysts into the early stages of credential theft and sharing between hackers, intelligence teams in commercial entities can identify this stolen information and use it as the basis for creating early detection and prevention of exploits.

Platforms for sharing threat intelligence in organized groups continue to play important roles in the cyber security community. Government-organized or even mandated sharing initiatives have been helpful, but international and competitive pressures have hampered some efforts. Commercial solutions have thus been especially helpful in creating private sharing enclaves where senders and receivers of intelligence establish a meaningful level of trust.

The general goal for cyber threat intelligence is ultimately to offer real-time context to practitioners. That is, the information and insights included in good threat intelligence helps make the enterprise security process better. This is true to help prevent threats (e.g., URL intelligence), detect threats (e.g., attack signatures), and respond to threats (e.g., hacker chatter in the dark web).

2020 Trends for Threat Intelligence

The effectiveness of threat intelligence sharing and usage has transitioned from less effective early approaches, through effective processes with improved delivery of threat intelligence, to the current more effective generation of threat intelligence usage, where the goal is actionable results. This progression is good news, because coordinated defenses are the best approach amidst growing capabilities from capable adversaries (see Figure 1-34).

A clear transition in threat intelligence has been from human-time management of often-manual processes for dealing with ingested information to

the real-time delivery and analysis of ingested data for immediate defensive adjustment and mitigation. In addition, threat intelligence has moved from collection of data from a single source, to all-source ingest from a variety of different trusted entities.

It is worth mentioning that the Federal Government includes its own unique sets of factors in the use of threat intelligence for national security and information assurance. Nation-state military and intelligence teams can collect information at a level that is impossible for commercial entities. Human intelligence and signals intelligence, for example, permit a level of attribution that would be unheard of in industrial settings.

The future of threat intelligence is toward increased automation, improved autonomy, and more real-time actionable results from ingested data. The use of private sharing groups, perhaps temporary or project-based, is likely to increase considerably, which follows the increasingly transient nature of business partnerships. One can also envision cloud services soon including threat intelligence APIs as a normal course of business with its customers.

An additional future trend is that more protection systems are likely to use threat intelligence as the basis for automated decisions – without need for human intervention and curation. This will become a requirement as automated attacks require fast, real-time decision-making, and any human-time process will make this impossible. Enterprise teams will simply have to become comfortable with this trend in the coming years.



AN INTERVIEW WITH JAMIL JAFFER
VP STRATEGY & PARTNERSHIPS, IRONNET CYBERSECURITY

BEHAVIORAL THREAT DETECTION AT THE NET- WORK LEVEL

THERE was a time when an individual enterprise security team might have had the capability to address its cyber threat without any external assistance or partnership. Those days, however, are long gone – with the tradecraft of the adversary now reaching new heights in terms of power, scope, and reach. As a result, the modern enterprise security team must partner with the best vendors, and also learn to collaborate and cooperate toward reduction of cyber risk.


IronNet Cybersecurity offers a commercial platform that ingests network data at line speed, and that employs analytics derived from a unique understanding of the tactics and procedures of advanced adversaries. We spent time recently with Jamil N. Jaffer, VP for Strategy, Partnerships, and Corporate Development at IronNet Cybersecurity to understand the platform and to obtain insights into trends in cyber offense and defense.

EA How important is it for security teams to use platforms that can address the evolving tradecraft of the adversary?

JJ Given the rapidly evolving nature of the cybersecurity threat faced by nearly every company out there today, it is critical that security teams have access to tools that are able to quickly adapt to changes in the threat environment. Behavioral threat detection at the network layer is a central component of any such capability, because while the signature of a particular threat capability is fairly easy and cheap to modify, the associated behavioral pattern is much more difficult to mask. This is particularly true when the threat detection capability being deployed takes advantage of the tradecraft knowledge of top-notch offensive and defensive actors. IronNet's patented IronDefense platform builds into its analytics, expert system, and core hunt platform, the tradecraft expertise of some of our nation's best and brightest operators from the public and private sectors. Using this applied knowledge provides IronNet's partners with better detection capabilities and significantly reduced false positive rates, and also puts the skillset and techniques of IronNet's operators in the hands of our partner's SOC operators, making them faster and better at their jobs on a daily basis.

EA What is the IronNet concept of a cyber collective and how does it work?

JJ The reality is that today, no one company can reasonably be expected to stand alone against the onslaught of attacks from a wide range of capable actors, from script kiddies and hacktivists to criminal hacker gangs and nation-state attackers. There has been a widespread recognition across industry and allied nations that to effectively combat this danger, there needs to be a significantly greater amount of threat and knowledge sharing – yet implementing such a capability has been a challenge. Moreover, there is also an increasing awareness of the need for such sharing to take place at machine-speed and on a more sustainable and repeatable basis than just occasional sharing through phone calls, emails, or posts. IronNet's IronDome capability addresses



No one company can reasonably be expected to stand alone against the onslaught of attacks from a wide range of capable actors.

this gap by sharing behavioral and other threat detections across companies, industries, and as appropriate, governments, in order to create a true collective defense fabric. Such a capability – operating at machine-speed, in real-time, and sharing a broad range of anomalous behaviors – allows not just for the creation of a common operating picture across multiple entities and industries, but also for the identification of new and unique behavioral threat patterns that might otherwise have gone undetected in a single environment. This real-time sharing capability also allows IronNet to cut the dwell time of a potential adversary that is already in partner systems significantly because it leverages a broad scope of data to identify new behavioral trends.

EA Threat trends seem to be intensifying with nation-states getting more capable in executing offensive campaigns. What are some features in the IronNet platform and supporting infrastructure that help address these trends?

JJ With the spread of nation-state capabilities to a broader range of attackers, it is increasingly critical for companies across the spectrum to be taking steps to protect against these type of threats. Indeed, when this trend is combined with the increasing threat of collateral damage—as in the case of the NotPetya attacks by Russia against Ukraine, which cost hundreds of millions of dollars to individual private sector companies that weren't even the target of the attacks—protection against such threats can be a matter of economic survival. The IronNet platform puts the capability to identify and detect such attacks in the hands of companies across the economy, and operates at scale by leveraging the collective knowledge of all of our ecosystem partners. IronNet does so by taking highly capable behavioral analytics, combining them with the applied tradecraft knowledge and hunt capabilities of some of the best operators out there today, and building all of this into a single threat detection platform known as IronDefense. IronNet then builds on this capability by linking all of our key customers together through a collective defense platform known as IronDome, which shares the threat detections and assessments made

by our partners to provide common situational awareness and to allow for the identification of novel behavioral threat patterns. This combination of a top-notch network traffic analytics platform with a massive-scale collective defense capability is what gives IronNet a unique edge in the current threat environment.

EA Do you see any improvements in public/private partnerships for cyber security in the United States?

JJ There are certainly significant opportunities for the public and private sectors to come together more effectively to defend the nation in cyberspace. The fact is that today – as it has been for a long time – the defense of our nation’s information infrastructure and all of our core economic sectors and capabilities is a shared responsibility between both public and private entities. On the government side, it has the ultimate responsibility for defending the nation in cyberspace, particularly against the most skilled and highly resourced nation-state attackers out there, taking advantage of its unique collection and response capabilities. On the private sector side, industry is taking the brunt of the economic and destructive attacks out there today, while also representing the vast majority of the attack surface. As a result, there is little option but for government and industry to work together to better defend the nation. In many ways, this will take a shift on both sides from sharing information on an episodic basis to sharing threats at scale and speed, in real-time to create a common operating picture. To the extent such a picture can be created, the government must then be willing to collect on threats to the private sector and share information, in real-time, back to the private sector. If the government is able to effectively do so, the private sector can then leverage this information to be better defended against such attacks. IronNet’s platform is one element in creating such a collective defense capability.

EA Any near- or long-term predictions about cyber threats and corresponding security solutions?

JJ In the near term, it is likely that the threat landscape will continue to evolve rapidly, with private sector entities continuing to bear the lion’s share of the burden of both disruptive and destructive attacks, as well as the burden of leading on defense. This means that implementing a strong behavior-based, network threat detection capability is critical, as is leveraging the collective knowledge of multiple entities and multiple industries at scale. If industry is able to do so, there is a significant possibility of cyber defense getting better much faster than would otherwise likely happen. In the longer term, if industry can tip the government to the nature and type of threat behaviors it is seeing, and the government is willing to do its part to collect and share information in real-time with the private sector, there is a significant possibility that we can, as a nation, actually get ahead of some of the most significant threats out there.



AN INTERVIEW WITH JEFF SPENCER
CO-FOUNDER, HYAS

CYBER ATTRIBUTION INTELLIGENCE

DETERMINING the source of a cyber-attack is recognized by most in our industry as one of the most challenging tasks for an enterprise security team. The simplicity of spoofing and the relative anonymity of the Dark Web contribute to this challenge, but the primary root challenge is the complexity of infrastructure. Weaving an attack from one compromised host to another, and another, is an easy way to hide the source of a threat.

HYAS provides a world-class capability to enterprise security teams who choose to address this attribution challenge. As one might expect, security analytics as one might find in a SOC are greatly assisted, perhaps even enabled, with the context of accurate attribution. We recently caught up with Jeff Spencer, Co-Founder of HYAS, to learn more about how the company enables enterprises to solve many of the challenges of cyber attribution.

EA Why is determination of accurate cyber attribution such a difficult activity?

JS As you know, Ed – threat actors range from cybercriminals vandalizing systems for profit to nation-state actors targeting critical infrastructure. In the vast majority of cases, the actor would like to hide their identity. This might be to avoid law enforcement, hack backs, or other forms of retribution. As a result, threat actors have developed a host of strategies to obfuscate the infrastructure they use to carry out their attacks. Some common examples are; working from a compromised host, using non-attributable services like dynamic DNS and privacy protected domains, spoofing source IP addresses, and many others. The net result is that it's quite challenging to attribute infrastructure back to an actor and determine their intent using traditional security tools and threat intelligence. Because of this, most organizations have not focused on attribution because it was just too difficult. Recently however, we find that law enforcement, enterprise security and fraud teams, and other groups are increasingly wanting to identify the specific threats and threat actors targeting their organization, and focusing on the infrastructure threat actors use is one of the best ways to do that.

EA How does your solution offering address this challenge?

JS We provide cyber attribution intelligence by collecting and deriving information from a variety of traditional and non-traditional DNS sources, and help weave the intelligence into a clear picture for the organization of where a given attack likely originated. Obviously, we cannot do the types of things a nation-state might do with planted spies, signals intelligence, and other advanced means for collecting information. But in the context of legal, reasonable intelligence gathering, our Comox platform is the best resource in the world.

EA How do customers make use of this intelligence?

JS Customers use the Hyas Attribution and

Response Platform through subscription access to the web portal and also via API. Threat intelligence and Fraud teams are using the platform to bring attribution into their investigations where it wasn't possible or realistically feasible before. The feedback we've gotten is that this type of attribution is not available anywhere else, so we are confident that we are on the right track. Attribution has several layers of meaning to our customers: 1) Differentiating the attack by two kids out of a suburban UK home vs Class A office space in St Petersburg Russia, 2) Understanding which attacks are attacking the entire Internet vs the ones targeting just the customer and maybe their suppliers, 3) Preemptively blocking threat actors' infrastructure before it's used in an attack, and 4) Gathering the evidence to taking the actor off the street.

EA What's been your approach to supporting law enforcement?

JS I'm glad you mention this, because law enforcers have a different goal, obviously. Where an enterprise team might be providing information for their board, or might be using the data to enhance the accuracy of some SOC-based threat hunting, law enforcers are trying to bring offenders to justice. This is certainly complementary to what we enable for enterprises, but the motivation is different. We're honored to help law enforcers with this important task.

EA Any near- or long-term predictions about cyber attribution?

JS We'd like to think that our solution will help make attribution intelligence a standard tool for every analyst. We fully understand that the ease with which threat actors can hide will always make attribution a challenge, but that's why it's essential for analysts, CISOs, enterprise security staff, and law enforcers to take a close look at the Hyas platform. We believe we can provide substantive help to any organization's security program with the addition of attribution intelligence.

APPLICA- TION SECURITY

Perhaps the most challenging aspect of enterprise cyber security involves dealing with the unique and sometimes legacy issues of application software. Few would argue that applications, including mobile apps, exhibit the highest degree of update and change in all of computing. Where infrastructure software and systems might be installed and left intact for months or years, applications can experience meaningful changes on an hourly basis.

If you add the fact that software engineering remains a craft with little hope of producing bug-free code in non-trivial products, then you have a tough environment for securing apps. This helps explain the many approaches in this area: Static code review, app scanning, software maturity, behavioral visibility, application telemetry, containerized protections, risk scoring, and micro-segmentation are all promising risk reductions for apps.

One clear trend involves more active analysis of applications, and many vendor focus on and offer run-time application self-protection (RASP) solutions. The trend with many RASP offerings involves a shift toward telemetry generation first, with active mitigation support coming second. This seems a rational deployment methodology, given the challenges of dealing with the unique complexities of modern applications for both Web and mobile.

Most experts agree now that the most common root cause for advanced exploits and breaches in the enterprise will be found at the application level. It is also not uncommon for different vendor solutions that purport to do the same general function (e.g., scanning) to produce wildly different output. This can be unsettling for an enterprise security team, and really highlights the unscientific methods for application security that are still followed by many teams.

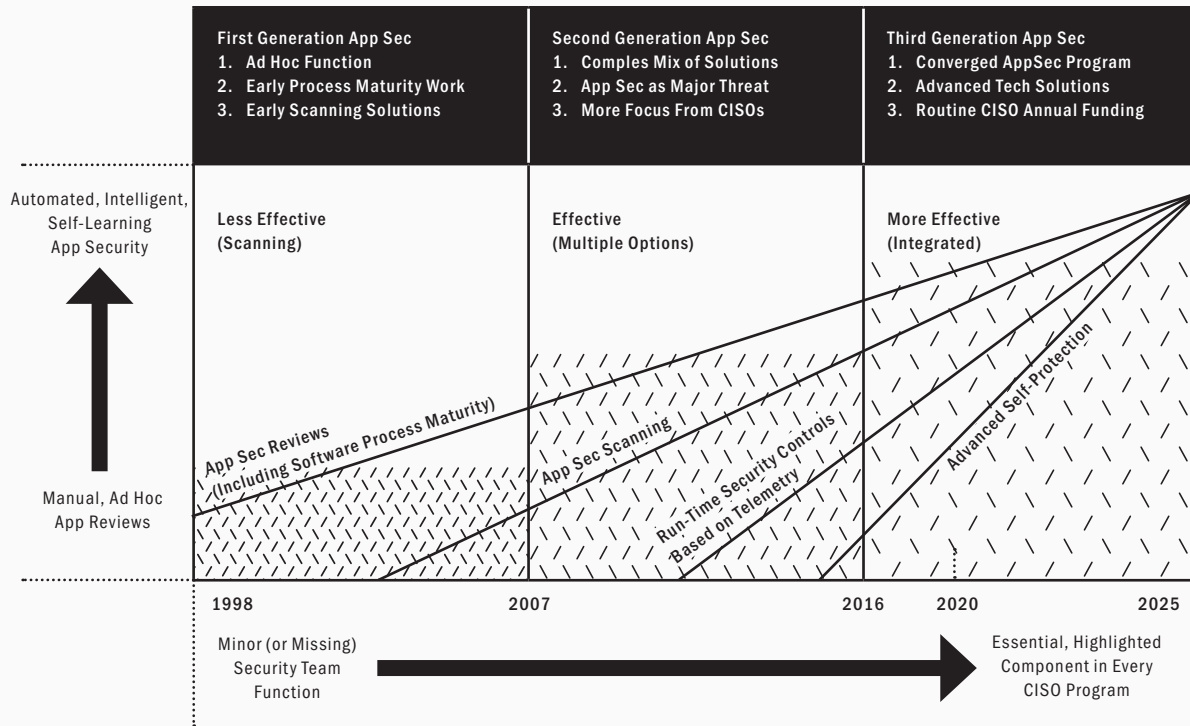
An additional major consideration for enterprise security teams is the use of SaaS-based critical business applications such as SAP or Salesforce. Such use of SaaS applications implies the need for cyber security support, both from the SaaS vendor, and from additional expert-based offerings that fill in gaps during periods of non-patching, offer additional security training, and provide overlay tools to integrate SaaS security into more general systems such as SIEMs.

2020 Trends for Application Security

First generation application security was less effective, because it focused on simple methods such as scanning that helped, but were insufficient to address the threat from software. Second generation application security became effective from many new options including improved maturity models, run-time security controls, and early self-protection. Modern third generation options are more effective and are beginning to converge (see Figure 1-35).

Early, ad hoc manual code reviews for in-house apps have transitioned to automated, self-learning, run-time security for application security. This is a massive shift, and does provide a significantly improved level of security for application-level software including mobile apps. In addition, this function – which was originally a non-component

Figure 1-35. Application Security Trend Chart



of most early enterprise security teams – is now considered an essential, highlighted component of every CISO program.

The future of application security involves convergence, especially for run-time protections in cloud workloads and containers. That is, rather than select from a menu of different and largely non-integrated options for application security, the emerging generation of enterprise security teams will have a common, unified philosophy for application security. The tools and processes used to ensure AppSec goals will be provided in a more integrated, cohesive manner.

An additional future is a more intense reliance on SaaS-based business applications. One would expect the native security support from SaaS vendors to continue to improve, but boutique commercial security offerings for popular SaaS tools such as SAP will also continue to improve. Enterprise teams will have to find good ways to integrate third-party security management programs with these improved SaaS security support systems.



AN INTERVIEW WITH MICHAEL ASSRAF
CEO & CO-FOUNDER, VICARIUS

MACHINE- LEARNING ANALYSIS TO SECURE CODE

ONE of the great challenges in cyber security involves keeping track of your software, applications, and operating systems – and, in particular, maintaining an understanding of whether they have sufficient security, including patches. This is an especially tough challenge for real-time critical applications that cannot be easily paused, updated, and then redeployed. And for proprietary software, it is often not even possible – especially if an obscure third-party developed the code.

Vicarius offers a world-class security platform that helps an organization determine where their risks reside. The company's machine learning-based cloud platform for malware and software analysis provides an effective prediction and detection capability for enterprise security teams. We caught up recently with Michael Assraf, CEO and Co-Founder of Vicarius to learn more about their platform and the methodology they recommend for reducing risk in the enterprise.

EA Michael, how have enterprise teams tried to protect software in the past, and what have been the limitations?


MA Patching has been the primary means for dealing with security issues detected in software, and this will certainly continue. But this is not an easy process, and furthermore, for older software or operating systems that might be running in the enterprise, it might not even be possible. Upgrading software to new versions, for example, can sometimes cause run-time issues for applications, especially when the underlying software or the application is poorly coded. At Vicarius, we focus on helping our customers deal with these common software security limitations.

EA How does Vicarius address this problem of protecting software from exploitation?

MA You are correct to describe our mission as protecting software from exploitation, and this includes both known and also yet-to-be-discovered software vulnerabilities. Our solution, called Topia, is a platform designed to offer patchless protection for software without the need to reboot or restart your systems. These are also, by the way, challenges in certain critical environments when a conventional patch is required. Our approach focuses on analysis using machine learning to highlight issues and provides means for mitigating any discovered exploits. In our vision, to disrupt a legacy market, you need to provide both previous and next-generation features. So, alongside our patchless and vulnerability prediction capabilities, we allow the customer to explore the same-old CVE data and apply security patches under one consolidated platform.

EA Can you explain your map, reduce, and eliminate methodology?

MA Yes, these steps form the basis for deploying Topia. They involve mapping CVE and any binary-level vulnerabilities that have



We focus on improving the three nagging issues in software protection: patching, zero-day vulnerabilities, and proprietary code.

been detected, including new ones. The process also involves reducing risk, which can be significant – often as much as 95% of the business issues for your software. This is done by involving contextual attributes of a client's environment rather than the generic CVSS-based prioritization. The last step is to act against the exploitation of these threats, which involves real mitigation that can be either protecting patchlessly or by installing a real patch. Our approach is not just a passive technology.

EA How do you accomplish these goals on the platform?

MA Topia can be deployed on-premise or SaaS. Our tiny clients can be deployed on any popular Linux distribution, as well as Windows XP and above. We're trying to be OS agnostic and provide an easy coverage for hybrid environments. Our customers use Topia to review their software, and this often involves focusing on the most critical applications, as you would expect. The binary analysis we perform is especially useful for home-grown proprietary code that does not have some corresponding public reporting process. So, Topia is often the only means for identifying issues in these applications. Our algorithms use training data in a machine learning context to spot binary patterns that correspond to software exploits. Once detected, these can be acted upon immediately by the software team.

EA What will be the role of software patching in the future? Do you see this process eventually going away?

MA Much of this existing patching process relies on detection by the community resulting in CPE-CVE signature-based vulnerability detection. While this has been useful, it is time consuming and uneven in coverage. We don't expect to see patching go away completely and we even allow customers to go this way. But our mission is to offer an alternative and, we believe, superior way to protect software. We also expect zero-day security problems

to increase in their intensity as nation-state military teams continue to improve their offense.

EA Any near- or long-term predictions about software protection from exploits?

MA We certainly like to think that things will get better as a result of our platform. We focus on improving the three nagging issues in software protection: patching, zero-day vulnerabilities, and proprietary code. All three areas benefit from our technology, so we are excited that we can contribute to a more secure future for many enterprise and government organizations who run critical application code in support of their mission.



AN INTERVIEW WITH SAMEER MALHOTRA
CO-FOUNDER & CEO, TRUEFORT

ACHIEVING APPLICATION VISIBILITY, CONTROL & PRO- TECTION

WHEN a software workload supports a business, collecting accurate run-time telemetry is easier said than done. Nevertheless, enterprise security teams must address this challenge because establishing visibility into applications is the most important step toward securing them. And with applications now serving as the lifeblood of modern businesses, this task is vital to the security and compliance of the entire enterprise.

TrueFort specializes in world class application visibility, control, and protection for the enterprise. We had the good fortune to connect with Sameer Malhotra, Co-Founder and CEO of New Jersey-based TrueFort, to learn more about his platform and how it supports modern networks with comprehensive application and workload security.

EA Sameer, what are the primary steps involved in establishing application security in the modern enterprise?


SM It all begins with knowing what your applications should do – your policies – and then baselining what they actually do. And that's a major disconnect for most organizations today. You then need to map and bring policy, configuration, and profiled behavior into alignment. Once done, it is important to automatically and continuously monitor application behavior against those policies to detect anomalies with a minimum of false positives. You then need to be prepared to investigate, tune policy, and take action to remediate when anomalies do occur. At TrueFort, we have focused on simplifying that process for our customers by automating all aspects from data acquisition to controls.

EA What is the primary role of visualization and mapping, and how can this information be collected in real-time?

SM Visualization and mapping are only possible when you collect deep and continuous information – and not just on an application's static configuration. That's a snapshot. You need to monitor application behavior and relationships over time to understand the dynamic context. And that can only be collected from within the workload, but not inline so that it impacts application performance and the business. Then, once you can visualize their active state and whitelisted behavior, stakeholders – whether security, infrastructure, app owners or DevOps teams – gain a common understanding of their environment and are better prepared to create and collectively manage policy.

EA How important is it to profile the behavior of applications?

SM Unfortunately, today's typical configuration-based approach misses execution events. That's because traditional security tools approach workloads from the infrastructure level. They might focus on whether events are anomalous or not, and therefore end up missing attacks in progress, or managing large volumes of false positives. Without



Visualization and mapping are only possible when you collect deep and continuous information.

the environmental application context, it is extremely difficult to decide if an event is anomalous. As a result, tracking behavior is foundational to profiling applications for anomaly detection – however you get there. To establish zero trust, you need to understand relationships comprehensively.


EA Do you see segmentation frequently with your clients? How does this affect the process of establishing visibility?

SM Yes, we see many customers implementing basic network segmentation using static intelligence as the first step. Ultimately, however, they soon realize this approach is not enough and that they need dynamic information from the application layer to effectively profile, tune policy, and monitor real-time events to secure the workloads the segmentation is intended to protect. Then, because comprehensive visibility is needed to construct effective segmentation policy, it gets prioritized. But how you get that visibility and how comprehensive it is determines how easy it is to operationalize a segmentation project, and how successful it is at protecting the environment. Visibility based on automation and behavioral analytics rather than traditional, ‘snapshot-oriented’ configuration management, is the best approach to successfully implementing segmentation that actually gets the job done.

EA Can you share your thoughts on application security in general in the context of today’s push to cloud-based infrastructure?

SM Securing applications, the lifeblood of most businesses today, is still often based on an old, pre-Cloud configuration-oriented approach. And that’s because many breaches still come from failed configurations. But while managing configurations is still important, there’s still a lot of potential exposure. Analytics-based security that uses real-time monitoring and response to anomalies is vital, especially in dynamic, non-snapshot-oriented environments like the cloud.

CONTENT PROTEC- TION



The future of content protection lies in stronger forms of encryption, data protection tools, and intellectual property security in virtualized, cloud-hosted infrastructure.



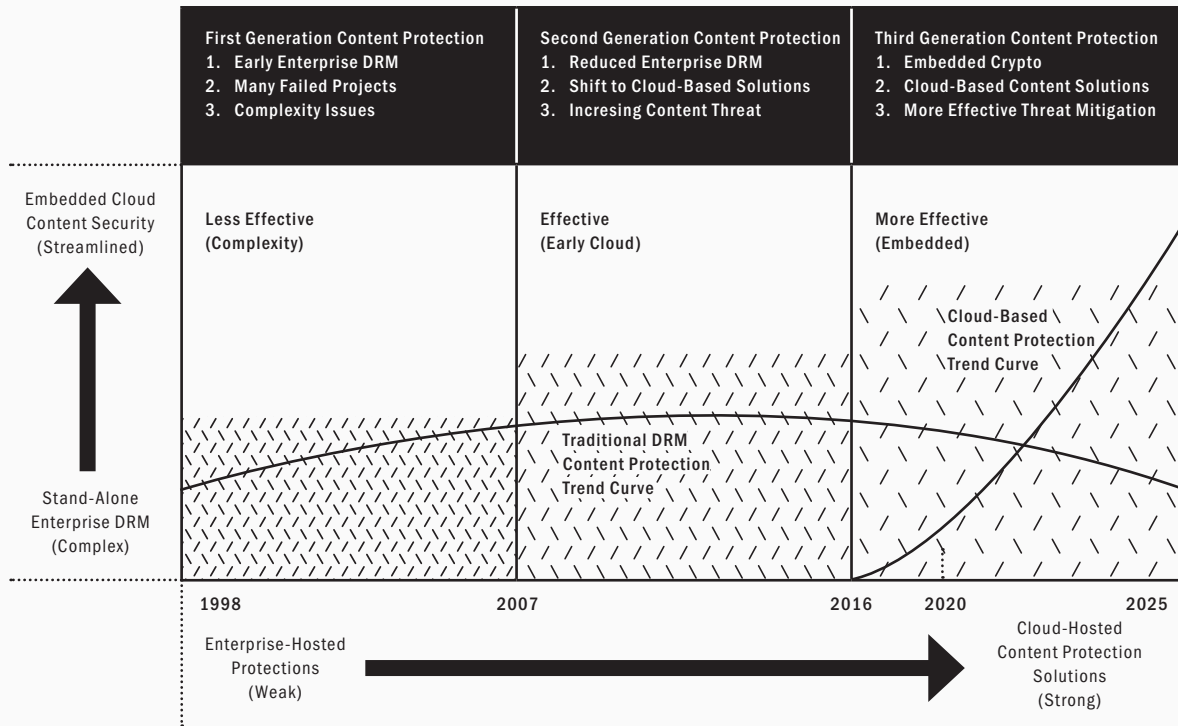
Content protection (also called copy protection) has traditionally been rooted in the use of digital rights management (DRM) technology, which many consumers, especially young ones, do not like. Consider, for example, the continued bumpiness and uneven approaches used to protect and monetize movies, television shows, apps, games, media, music, and other content across non-heterogeneous platforms such as Microsoft Windows, MacOS, iOS, and Android.

The protection of this type of media content is largely outside the scope of this report, because it is an issue that 99% of CISO teams do not have to contend with. But the deployment of enterprise DRM to provide protection of intellectual property is an enormous concern for every CISO team – and is hence considered an important control area. The bad news, however, is that previous enterprise DRM with PKI-enabled infrastructure has proven highly complex to run.

The good news is that with the rapid adoption of cloud-based, as-a-service data handling, the securing of intellectual property using content protection tools will grow considerably. This is a natural extension of how cloud storage, cloud data management, and cloud security are being handled. One would expect smaller firms to adopt encryption and related content protections in cloud more readily than larger firms, which will come later.

A major requirement to support this DRM-like adoption in cloud and as-a-service solutions will be ease of use, and integration with common, existing tools such as Microsoft Office tools for dealing with business files. Furthermore, the underlying PKI controls will have to be hidden and managed from enterprise teams to avoid the complexities that have held back business content from being access-controlled with strong, mandatory protections.

Figure 1-36. Content Protection Trend Chart



2020 Trends in Content Protection

Less effective early enterprise DRM solutions could not find a growth curve, and with the dissolution of the perimeter, will continue a downward trend. Instead, cloud-based protection, including encryption of data, have already found that growth curve and will be a successful new enterprise control. This results in stand-alone DRM moving to embedded content protections in cloud, resulting in stronger security (see Figure 1-36).

Content protections for media will gradually shift toward increased enterprise relevancy as more businesses opt to utilize creative video, social media, and other forms that might have previously not been considered common for use by companies. This might create some intersection in the DRM community between consumer and business use of encryption and key management. Nevertheless, the encryption and access control for media will remain largely separate from similar tools used to

protect business information. The future of content protection lies in stronger forms of encryption, data protection tools, and intellectual property security in virtualized, cloud-hosted infrastructure. Enterprise teams will include more routine inclusion of source selection requirements from enterprise teams for these types of data security capabilities when companies are selecting vendors to support storage and other functions to be implemented in the cloud.

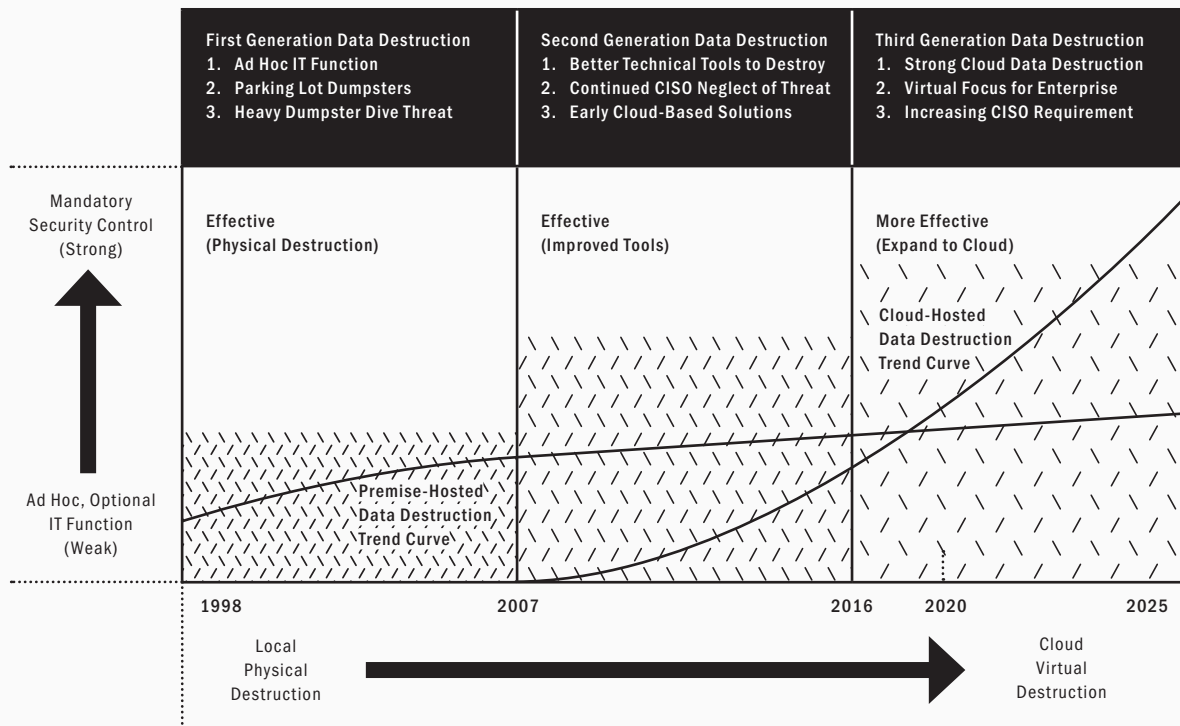
It is also relevant from a security perspective that enterprise teams more frequently communicate with their constituents using video and other forms of media. It thus becomes reasonable to expect that traditional means for encrypting and storing sensitive enterprise documents will shift in emphasis toward the content and copy protection of sensitive enterprise video, audio, and other media.

DATA DESTRUC- TION

Perhaps the least attended-to requirement in the CISO arsenal is data destruction – and this is somewhat mystifying – at least to this analyst team. Consider the following: One of the most well-established and insidious challenges every enterprise security group faces each day involves the malicious theft of data, information, and intellectual property. Such resources typically exist in the form of files, records, presentations, folders, and other stored receptacles.

This would imply, one would guess, an obsessive focus on deleting, destroying, and removing every such piece of information that is not essential to the function of the enterprise. It would also imply, one would guess, that data destruction methods follow a basic principle of minimal storage. That is, information should be stored in its most limited and isolated manner for as short a time as possible – like handling radiation.

Figure 1-37. Data Destruction Trend Chart



The reality, however, is that most security teams have either non-focus or limited visibility into how IT or local business unit teams handle this important function. In smaller businesses, there might be zero emphasis on policies for storing company data; in mid-sized companies, a policy might be in place, usually for printed materials that should be shredded. In larger companies, records information management (RIM) policies are generally established, but mostly ignored.

Cloud services can potentially change the equation here, but only if enterprise security teams begin to more forcefully demand this function in every as-a-service capability they select and use. Standards exist for proper destruction of data, and RIM policies are in place – so this is not a technically challenging issue. The problem is one of emphasis: Ask ten CISOs about how they do data destruction in the enterprise or cloud, and expect a non-answer.

2020 Trend in Data Destruction


The effectiveness of data destruction methods has remained effective through three generations of usage. With cloud services, the techniques are even more effective. The challenge instead has been around the attention, application, and enforcement of data destruction tools – both hardware (for physical media) and software, to ensure attention to minimal storage of corporate information (see Figure 1-37).

The trend one should expect in the coming years is that this function will eventually progress from a weak, ad hoc option to a strong, mandatory control. In addition, the function as a local physical destruction option, including shredding in the office, will transition to a cloud-hosted virtual option, where less paper is involved and more standards-based destruction of unneeded information will become the norm.

The future of data destruction resides in the cloud. Older images of companies shredding paper will gradually evolve to virtualized functions that are automated and properly attended-to in the cloud.

Legal provisions will continue to play an important role here, because some important corporate data must be maintained; but in all cases where data can be deleted, it will be – and the cloud providers will have this responsibility to implement the destruction.

An obvious additional trend for data destruction will be more stringent requirements levied against third party companies. This is an easily negotiated additional requirement, and makes perfect sense, especially for third-parties that handle sensitive information. One would expect the requirements to cover both physical, tangible destruction, as well as secure means for performing virtual destruction of information.



**Ask ten CISOs
about how
they do data
destruction in
the enterprise
or cloud, and
expect a non-
answer.**



AN INTERVIEW WITH MIKE MCKEE
CEO, OBSERVEIT

ADDRESSING DATA LOSS FROM INSIDER THREATS

THE insider threat is, without a doubt, the most insidious and difficult of all security challenges for the modern enterprise. Because compromised or disgruntled employees (or third party members) take advantage of the trust that is inherent in being an insider, this problem requires a fundamental rethinking of how corporate data and assets are protected. It requires safe, reasonable monitoring and fast, efficient response – both of which have been tough to implement in the past for security teams.

Boston-based ObserveIT has been developing and deploying world-class user behavior analytic solutions for many years. Enterprise team benefit from their advanced algorithms and non-intrusive functionality, to the point where user behavioral analytics are being viewed as essential protections for employees, rather than nosy surveillance. We caught up with Mike McKee of ObserveIT to learn more about user behavioral analytics and the current state of the art in this important control area.

EA How intense is the insider threat in the typical enterprise?

MM Up until now, cybersecurity has been about malware, external threats, and network security. Traditional infrastructure-based security prevention solutions have been designed to keep unauthorized users out. Unfortunately, the majority of today's data breaches involve validated accounts, either misused or stolen. Indeed, if you look at the Verizon Data Breach Investigation 2019 Report or Forrester's recent Best Practices: Mitigating Insider Threats 2019 report by Joseph Blankenship, they both find that at least half of all recent data breaches have an insider related component to them – whether they were accidental or driven by malicious in user intent. Ponemon Institute research also confirms that breaches caused by negligent and malicious insiders are on the increase. Their 2018 paper found that they have increased by 26 and 53 percent respectively in just two years. As insider threats are not solely a technical problem, most enterprises find it much harder to use legacy, external facing cybersecurity tools to detect and mitigate these types of threats. The Verizon 2019 report also found that a massive 70% of the insider related breaches were not detected until months – even years – after they took place. When it comes to investigating an insider breach, enterprise security analysts must typically work through multiple activity and reporting logs that come from a variety of sources, none of which are correlated to each other. This is a time-consuming and manual effort meaning that the enterprise spends weeks to months attempting to pull together what happened, who did what and why. Sometimes, user attribution is beyond their best attempts. ObserveIT enables any organization to detect these insider threats as they happen, identify the source, understand their intent, and ensure that the enterprise responds appropriately.

EA How does ObserveIT's technology address the challenge of understanding user behaviors?

MM Our lightweight agent collectors sit at the user level to monitor user actions with applications, on the web, within their endpoint across screen, mouse, and keyboard activity, be it local and remote access.



70% of the insider related breaches were not detected until months - even years - after they took place.

With continuous behavior analysis, it provides full, granular visibility into user and file activity at all levels, delivering context-specific insights into the 'how' and 'why' of a user's behavior that helps establish intent and anticipate activity. Crucially, with an Insider Threat Library detailing 350+ real world insider threat scenarios in place, the product can be configured so that security teams are alerted to a multitude of risky behavior or activity by insiders. Overall, this means that security teams can quickly investigate alerts as and when they happen, drawing on easily searchable metadata as well as other features like automatic video recordings of user activity to understand the intent behind that person's behavior. Without ObserveIT, security teams are forced to rely on solutions that aggregate insights based on inconsistent data sources, inhibiting their productivity and leading to user and data blind spots.

EA Does the ObserveIT capability support data leakage prevention (DLP)? Does it remove the need for a separate DLP platform?

MM ObserveIT is a cutting-edge solution designed to combat data loss because of insider threats through real-time detection, activity monitoring, deterrence, education and discretionary prevention. Going beyond traditional DLP solutions, ObserveIT provides customers with a full 360 view – monitoring users, establishing intent and tracking all data interaction and movement in real-time (copy&paste, authorized/non-authorized removable storage, screenshots, cloud upload or email transfer, and more) and when required, streamlines the investigation process. It is the only software solution on the market that unifies user activity, data activity, and user behavior analytics into a single interface. As such, we augment most data protection and governance programs with granular user context and data movement visibility, meaning that many of our customers have removed their DLP platform altogether.

EA How does de-perimeterization affect and influence insider threat programs if enterprise teams are scattered across heterogeneous infrastructure?

MM Network perimeters still exist in many organizations, but they're becoming more and more irrelevant. With more workers working remotely, a boom in freelance and contract staffing, plus the increasing consumerization of enterprise IT as every year goes by, enterprise IP and sensitive data is stored, moved and worked on in a variety of locations. As such, locking down your office network perimeter will not stop all the leakage of data that is already stored and worked on from outside your office walls. By turning the focus for data security efforts to be on the trusted insider – whether full-time employees, contractors or partners – and monitoring their actions and their intent around moving data, regardless of where they are, the enterprise will significantly reduce their risk of data compromise. Using a highly visual management console, ObserveIT also delivers prevention prompts and policy reminders when a user acts suspiciously or makes a mistake. In doing so, it delivers a holistic solution - solving multiple insider use cases, safeguarding valuable assets no matter where they are accessed and upholds employee productivity.

EA Any near- or long-term predictions about insider threats?

MM Regarding threats, I would offer the following: In the near term, as organizations complete their cloud journeys, we can anticipate continued data leaks due to unsecured and poorly permissioned cloud storage and cloud servers. The boundaries between cloud vendor responsibility and organization are still being worked out. In the medium term, more supply chain driven attacks as more and more of our supply chains are based on software. They will be driven by users with privileged knowledge but not privileged access stealing data and sabotaging systems. In some part, nation-states and their affiliates will continue to incentivize insiders to target specific nationally sensitive assets. And in the longer term, we are confident that these threats will be more contained by better equipped security teams and the response will be automated and reduce the impacted systems, data and employees rapidly. Regarding cyber protection, we would expect that every company

that is dependent on core intellectual property for success will have a separate insider threat team and a broader governance council. We also expect to see an increase in the creation of insider-related incidence response playbooks that involve IT and security sharing data with non-technical teams. In a similar vein, HR, legal and cybersecurity teams will become closer friends within the enterprise as they must increasingly work together to prevent and manage insider incidents. In particular, there will be more correlation of HR and business systems with cybersecurity technologies.



AN INTERVIEW WITH DAN FISCHER
EVP, SERTAINTY

EMPOW- ERING DATA

NOW that enterprise teams can no longer rely on the cover of a firewall-protected perimeter to secure their data, new methods are required to enforce access policies. In the best case, such protection is done in a way that empowers the data owner to decide the type of accesses that are considered acceptable. But this is not easy in the typical heterogeneous ecosystems that modern businesses must deal with. The only reasonable solution is to focus on the data and how it can play in inherent role in security.

Sertainty has been developing solutions for data security for several years, and has pioneered the concept of empowered data using cryptographic controls embedded into data files. The result is a highly portable and flexible solution for protecting data ranging from unstructured enterprise information to media content. We caught up with Dan Fischer, EVP of Sertainty, to learn more about empowered data and how Sertainty customers are using the solution for advanced protection.

EA Your team references a concept known as Data: Empowered. Can you help us understand what this means and how it relates to your technology solution?

DF Sertainty provides a data layer platform and development toolkit for integrating security intelligence into software applications. Our unique UXP Technology protects data by transforming the file into a self-reliant proxy that is controlled by its owner. This powerful control, combined with network security protection, identity verification, and governance, is enforced by our Sertainty Intelligence Module, and is the basis for the name of our solution: data:empowered. This approach is well-known and often referenced by industry experts. Grant Schneider, for example, who serves as the federal CISO, stated this recently: “We have to move to where our data is far more aware, and where our data is essentially helping to protect itself, so it knows where it is, who is trying to access it, and a lot of context around it so it can be protected whether it is on a computer that is lost in a parking lot, or left on an airplane or someplace else that it is not secure. Or is on someone else’s cloud that we might have concerns about.” Sertainty has been granted a patent for its Intelligence Module and our intent is to establish data:empowered as the standard in the market for data that is “far more aware” and not only detects anomalies, but mitigates risk in real-time.


EA How can an enterprise protect its unstructured data more effectively?

DF Data is currently inert, lacking an inherent ability to either control its own fate, or mitigate risks while at rest, in transit, or under process. Data loss and theft of valuable information are thus symptoms of this passivity. At Sertainty, we’ve rethought this problem and put it in terms of data as an attack surface. If implemented at scale, our concept would imply that attackers would no longer be able look at endpoints as an attack surface. Instead, data becomes the endpoint, and thus constitutes the new enterprise perimeter. We make it possible to resolve data loss by fusing our configurable Intelligence Module to the data file so that technology providers and their customers can better monetize valuable

information, while mitigating risk in real time. Data:empowered is a data file that can act and react. The Sertainty UXP Technology promises to aid in the protection and governance of unstructured data (such as txt, csv, Word, Excel, pdf, jpeg, video) without compromising user productivity. The Sertainty brand stands for uncompromising performance, protection, and privacy.

EA How does the Sertainty solution help enterprise teams improve governance and control of their data?

DF We enable enterprise teams with the ability to embed policy controls into the data. This involves not just the rules, but, the controls. The Sertainty Intelligence Module manages the fate of data, and enforces policy at the data layer. According to a recent data privacy survey by Egress, barely one in five organizations implement encryption policies, while sharing sensitive data intra-system. And only one in three implement encryption policies, while sharing sensitive data inter-system. This can be explained as follows: First, there are not enough skilled cyber-pros to go around. To integrate the many and diverse cyber-technologies, both hardware and software, into a cohesive solution that defeats the inside attacker, is a complex and expensive proposition. And this requires the skills of trained, experienced, and trusted cyber pros to minimize the initial investment, as well as optimize the on-going operational effectiveness and costs. Second, not only is there a shortage of skills capable of building security into the applications themselves, but the development tools available fall short of making it easy to optimize performance, data availability, and protection. There are more vacancies for these roles than there are people, or AI, to fill them, along with a void in data layer tools that automate these protection and performance processes. Jeff Snyder, Founder of CyberStratos reinforced this theme with the following observation: “How do you close the gap?” he asked. “How do you expand the throughput of the trusted cyber-pros, and how do you implement secure software development practices when you don’t have the ideal tools and the skilled resources?” For many SMBs and Enterprises, they shift these responsibilities and accountabilities to the cloud.



Cloud workload protection is essential, it is not optional.

This introduces a new question: Which would you choose, invest in attacking ten thousand different entities with ten thousand different pay-offs, or attack one in the cloud, with ten thousand pay-offs? These skill and dev-tool gaps also translate into supply chain exploits. The strength of any given supply chain is defined by its weakest link. Aside from the insider threat, more successful attacks begin with one of their smaller and less equipped suppliers. With the Sertainty data layer technology platform and tools, a developer combines intelligence with user data to transform that data file into one which enforces owner-specified controls and context. The result is a Sertainty UXP Object, and this exemplifies data:empowered, which does not relegate control to the supply chain.

EA What are some common use-cases where the Sertainty technology helps embed intelligence into the enforcement of data security policies?

DF Our workflow tools address the interoperability issues of disparate or siloed systems, cloud migrations, safe VM2VM transmissions, and the sharing of sensitive information via app-to-app (M2M) workflows. In these cases, the complexities of data security and policy enforcement become unmanageable as the data transitions from rest to transport and back to rest. This can be represented as follows: end2end2end2end. The Sertainty technology eliminates dependency on certificates and removes the burden of key management. It eliminates the dependency on tunnel encryption and related management – and this is done inter-system and intra-system. Our workflow tool is meant to be an easy way for SMBs and Enterprises to implement a simple data:empowered workflow solution without having to depend on either the infrastructure or the communications path or protocol.

EA Any near- or long term predictions about enterprise data security? Do you see cloud services having an impact? How about artificial intelligence?

DF Obviously, the great technology themes of our time, such as 5G, deep learning, machine learning, blockchain, biometric authentication, and quantum computing, will have great impact. But we are

confident that our data:empowered solution can also have a massive impact. Data provides both input and output to all the great themes mentioned above, so data:empowered offers the potential to advance each in a way that enables the coexistence of each without compromising privacy. Our data:empowered solution enables both data manipulation and data protection at the same time – and it's available today.

DATA ENCRYPT- TION

Data encryption has been largely synonymous with computer security for many decades. In academia, entire courses on security might include 90% of the lectures on encryption. While this might make for excellent and interesting class discussions and exercises, it misses the point on the role that encryption plays in modern cyber security as an underlying foundational method in the context of broader protection methods. It is a means to an end; not an end.

The data encryption business has been hazardous for many commercial vendors since the early days of our industry. The challenges have been many – including the difficulty of providing easy-to-use administration tools, the technical issues of algorithmic and protocol interoperability, the legal and political debates that arise between law enforcement and industry, the ambivalence of most users about properly storing data encrypted, and on and on.

Perhaps the only reason encryption has seen some business success through practical application is the obsessive influence the compliance community has had on its use. Every security compliance framework demands encryption of data – both at rest and during transmission – and this has resulted in reasonable adoption and use of encryption. But as a commercial business, it's not realized its full potential (and this might change with cloud).

All this said, the modern enterprise will continue to require and demand the strongest forms of encryption for data at rest and in motion. Both are required in every security compliance framework and by every business auditor, so the requirement will not change. What hopefully does change is the ease with which such encryption support is offered across heterogeneous services provided in hybrid cloud environments.

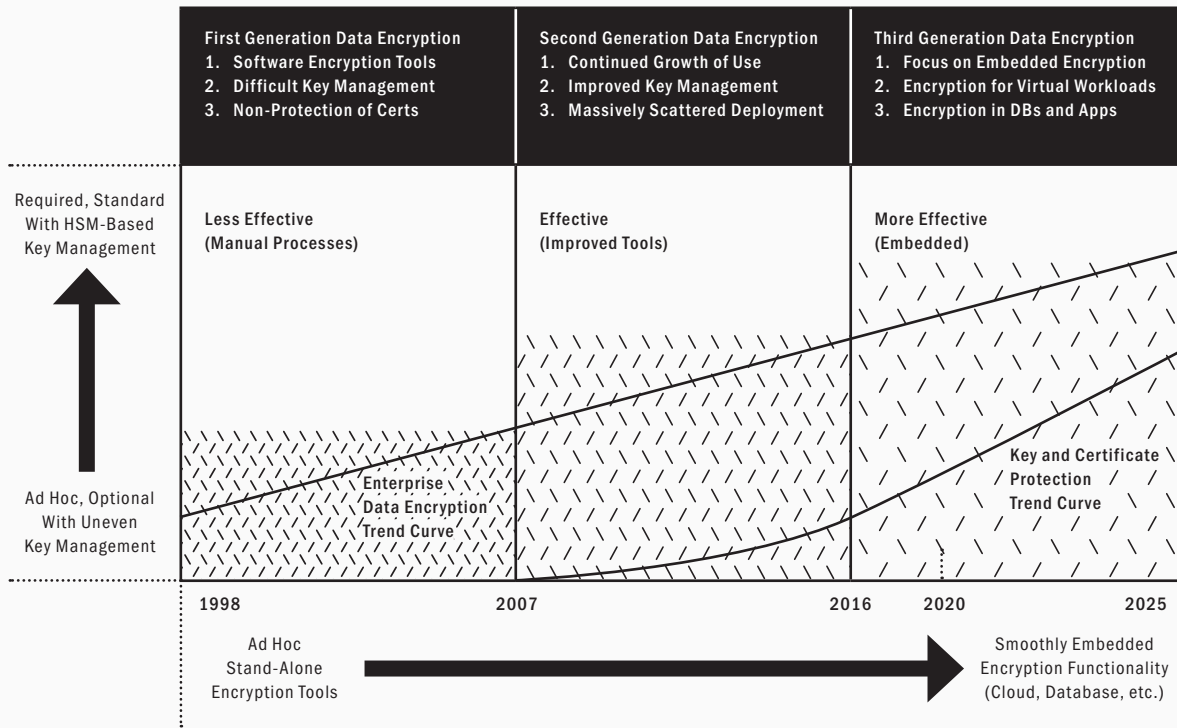
Such expanded support for data encryption will become embedded into SaaS, cloud, and related virtual offerings for enterprise. Routine encryption will also become more accepted as a mandatory business requirement for email, which is a shameful omission in the way organizations communicate today. The big question is whether companies can make decent profits supporting and selling this security control.

2020 Trends for Data Encryption

The effectiveness of data encryption in the context of enterprise protection has transitioned through three generations from manual techniques that didn't scale well to large groups, through effective solutions with improved automation, into the present approach of more embedded data encryption. Such an integrated, embedded methodology reduces the need for key management and related administration (see Figure 1-38).

Key management is shifting from ad hoc techniques and tools to more standard approaches, often using the power of hardware security modules (HSMs) to assist in the protection. Stand-alone data encryption is being replaced by tools that are embedded smoothly into cloud workloads, databases, and even the data representation itself. All these are positive

Figure 1-38. Data Encryption Trend Chart



shifts which will help make data encryption more accessible down-market.

The future of data encryption, from the perspective of vendor success and growth, is in cloud and other services, including software-defined networks (SDNs) where the telecommunications provider will offer advanced encryption not only for data in motion, but also in storage. Encryption algorithms will continue to improve gradually and will face existential replacement needs in five to ten years due to advances in quantum computing.

Cryptographic lifecycle management is another interesting trend, especially with the specter of quantum computing looming in the distance. Such lifecycle management involves finding and building an inventory of the places where cryptography is used in a given enterprise network. The goal is to ensure that weak cryptography is replaced by more modern solutions, especially in cases where quantum might create a real threat.



AN INTERVIEW WITH IAN CURRY
VP MARKETING, CORD3

CORD3'S AP- PROACH TO ENTERPRISE ENCRYPTION

ENCRYPTION is the most familiar and mature of all security technologies, having been around for as long as humans have been communicating. With the advent of computing, encryption was the natural choice for protecting stored and networked data, and one could argue that the present security community benefits from at least fifty years of experience applying encryption to data, and managing the attendant support activities including key management.

But the reality is that practical application of encryption to the enterprise has been surprisingly uneven, perhaps even poorly done, for many organizations. We recently spent time with Ian Curry of Cord3 to better understand the encryption challenge and to obtain insights into how the Cord3 UNITY platform can provide an effective means for enterprise teams and users to apply encryption to files, applications, and other artifacts of modern computing.

EA Tell us about how your UNITY solution delivers encryption to the enterprise for files and users. How transparent is the process?

IC Cord3 encrypts data so it is strongly protected at rest on servers. We deliver this encryption separately from applications and users by deploying Cord3's UNITY intercepts, which sit in the network between user end points and servers. This separation enables Cord3 to deliver consistent, policy-driven data protection, including encryption, across applications that also protects data against privileged credential attacks by internal and external attackers. Cord3's encryption process is completely transparent to users. Users simply click the Save button in their normal applications and Cord3's encryption process happens separately from applications and users on our UNITY intercepts. There are no changes required to applications or any software deployed to user end points or servers. Cord3 takes care of the entire encryption process, so users and applications do not have any keys to manage. Cord3's encryption of data at rest only uses AES with 256-bit keys, so encryption is fast and strong.

EA How does your platform operate with applications, and how is the key management performed?

IC One of the most compelling aspects of Cord3's solution is that it requires no changes whatsoever to applications on user endpoints or servers. Cord3 is an overlay technology that is easy to deploy. Customers simply deploy UNITY intercepts between users and servers. The UNITY intercepts perform all the encryption and key management operations on behalf of applications and users. Cord3 uses a separate, random symmetric key for each data asset (e.g., a file or an email).

EA Tell us about privileged credential abuse and how the Cord3 solution reduces this risk for the enterprise.



Cord3's encryption process is completely transparent to users.

IC Privileged credential attacks are involved in virtually every data breach. These attacks come in two forms. The first occurs when privileged credentials are used to extract data at rest directly from storage media. Solving this type of attack requires strong encryption of data at rest, which Cord3 delivers in an easy-to-use, transparent manner completely separate from applications. The second occurs when internal or external attackers use privileged credentials to access data by logging into an application. If the attacker attempts to access data without going through a Cord3 intercept, the data is inaccessible because it is strongly encrypted – the application will not be able to open the data. If the attacker attempts to use privileged credentials to access data through a Cord3 intercept, the intercept will deny access to that data. Since Cord3's intercepts are separate from applications, our intercepts make a separate access control decision from the application itself. From Cord3's perspective, a privileged credential is the same as any other credential, so we can deny access to data by privileged credentials using the same approach we use to manage access to data by any other user.

EA For enterprise teams with resources scattered across the Cloud, does your platform provide suitable means to extend the encryption?

IC Cord3's solutions can work in cloud, hybrid, and enterprise configurations. Our UNITY intercepts can operate in virtual appliances in the cloud or hardware appliances in the enterprise and on the edge of the enterprise. Using Cord3 for the cloud means that customers own their security and are not dependent on, or inextricably tied to, the security offered by a cloud service provider. In 2018, The US Department of Homeland Security released a report stating that customers of managed security service providers, which includes cloud providers, need to be aware that they are significantly increasing their exposure to privileged

credential attacks. By implementing Cord3 for cloud data protection, customers can own their security and manage this exposure.

EA Any near- or long-term predictions about enterprise encryption?

IC For the near-term, we predict that enterprises will recognize the technical, user, and management benefits of separating encryption from applications. For the longer-term – five years and beyond, we foresee quantum computing having a major impact on public-key cryptography. We predict it will take 20 years or longer for new algorithms to be developed and proven – and then integrated into solutions, to replace existing RSA and ECC algorithms. Cord3 only uses strong symmetric cryptography for protecting data at rest. As a result, Cord3’s encryption is already quantum-ready and customer data will be well-protected when quantum computing breaks RSA and ECC.



AN INTERVIEW WITH TYSON MACAULEY
CPO, INFOSEC GLOBAL

ADVANCED CRYPTO- GRAPHIC LIFECYCLE MANAGEMENT

THE use of cryptography is the most universal of all security methods and remains one of the most effective means for protecting information ever invented. But in the enterprise, it is not uncommon for a security team to have little understanding of where and how encryption software has been deployed across the infrastructure. This can lead to unknown crypto routines that might need updating or even removal. With quantum computing risks looming, this will eventually become a more serious issue.

InfoSec Global provides support for an important enterprise activity known as cryptographic lifecycle management where automation is used to detect and inventory the use of encryption in designated systems. We spent time with Tyson Macaulay of InfoSec Global, to learn more about this function. We wanted to know how it can be applied, and whether the timeframe for such action is sooner than most teams would expect.

EA What is meant by cryptographic lifecycle management?

TM Cryptographic lifecycle management includes the discovery, inventory, assessment, policy, update, de-commissioning, and on-going monitoring of the cryptography across the IT estate. This involves focus on cryptography deployed across a variety of assets from cloud services to IoT endpoints.

EA Do most organizations have any idea where their cryptographic functions are located?

TM No. Decisions about the what, where, and how of cryptography have been historically delegated to the bottom. This implies that individual developers and system administrators were expected to act in good faith, but without oversight. Cryptography thus appears scattered around systems and buried in binary applications, often in ways barely documented, and sometimes not at all. The rate at which cryptographic vulnerabilities are impacting organizations is increasing. The most common indicators of unmanaged cryptography are outages due to the expiry of forgotten certificates, and unauthorized disclosure of personal data due to the configuration of vulnerable algorithms.

EA How does the InfoSec Global technology work?

TM We have two complementary products: A crypto-inventory and discover product called AgileScan, and an API toolkit to implement cryptographic agility called AgileSec. The AgileScan product automates the location and reporting of certificates, keys, algorithms, and libraries from cloud to IoT – in compiled applications or stored on filesystems. AgileSec, in contrast, transforms cryptographic functions from hard-coded and unmanaged software to a plug-n-play, centrally managed security infrastructure.

EA What timeframe should be assigned to quantum computing as a threat to cryptography?

TM Most of our enterprise customers assume that quantum computers become a serious risk around 2025 and have launched cryptographic migration programs now (2019/2020) or have them budgeted for near-term focus. However, this timeframe is not about selecting and implementing quantum-safe crypto. Rather, it is about implementing cryptographic agility, thus making crypto plug-n-play, versus moving to statically encoded, hard-to-change crypto (again).

EA Any near- or long-term predictions about the use of cryptography in the enterprise

TM In the short-term, cryptography has to be brought under central management by security organizations. This means that they need visibility, which they currently lack. Most immediate efforts are around gaining visibility, in order to form long term strategies for managing the cryptographic footprint of an enterprise. In the long term, cryptographic agility is – hands down – the solution for managing cryptographic risks around vulnerable algorithms, regulatory changes, flawed implementations, and ultimately quantum-computing risks.



AN INTERVIEW WITH DAVID GIBSON
CMO, VARONIS

ADVANCED DATA SECURITY

COLLECTING real-time, security-related data in an enterprise is a mature protection concept, but is much easier said than done. Application-level monitoring, for example, is easily undermined by malware in the underlying operating system, so the collection process must be carefully designed to avoid this problem. Furthermore, the intensity of the insider threat continues to grow, so security monitoring is no longer just done for compliance. Rather, it is required to protect an enterprise from real internal threats.

Varonis provides a world-class solution for protecting data, with an emphasis on reducing threats from insiders and external attackers that hijack accounts and systems, improving visibility and context, and substantially improving cycle times for incident response. We connected recently with David Gibson, CMO for Varonis, and asked him to share some insights into his platform, as well as how data security trends are driving solution design for enterprise at Varonis.

EA David, what is the current state of the data protection and how can analytics help reduce the threat?

DG I think it is now well-established across the entire cyber industry that the insider threat is a serious concern for most enterprise security teams, but what's also becoming clear is that attackers easily hijack insider accounts and systems. This is especially true in Zero Trust environments, where the protection of a firewall-based perimeter is no longer a primary control in the modern enterprise. Advanced analytics, such as what we have in the Varonis platform, provide a practical means to use collected empirical data about real-time behaviors to reduce this risk. Analytics requires a world-class platform with sufficient reach into the most commonly found utilities, and this has been one of our main focus areas at Varonis.

EA How does the Varonis platform work? How does it collect and support analysis of data?

DG The Varonis platform uses distributed enterprise collection points to collect and generate real-time metadata streams including Users and Groups, Permissions, Access, Active Directory, Perimeter, and Content. We extend visibility in Active Directory, Windows operating systems SharePoint, Exchange, Linux, Office 365, NetApp, Nasuni, Box, and many more tools and systems. The goal is to provide context for security managers to better understand how to fine-tune privileges, optimize access permissions, identify data owners, and automation to effect change quickly. A commit engine allows for any proposed changes, such as for user access, to be simulated in a sandbox to ensure correct operation. The topology of all this is simple and hierarchical: The Varonis Data Security Platform collects data from a Varonis Probe/Aggregator. Varonis Collectors, which feed the Probe/Aggregator, are distributed across the enterprise to pull data from the relevant



The enterprise is moving toward increased use of cloud infrastructure for many critical use-cases.

operational sources such as Active Directory and Office 365.

EA What are the specific product components of your solution offering?

DG Our offerings are all part of the Varonis Data Security Platform, which protects data in the cloud and on-premises. DatAdvantage maps file systems and permissions, tracks activity to determine who can and does use data, and highlights where users have too much access through analytics and machine learning. Our Data Classification Engine discovers sensitive content and puts it in context, so that it is easy to see who the users are. DatAlert analyzes all the metadata we collect to identify and alert us on behavioral abnormalities that may indicate a breach. Automation Engine safely fixes permissions exposures, like global groups and malfunctioning access controls. DataPrivilege automates authorization (granting, revoking, and certifying access. Data Transport Engine automates the disposition and mitigation of data. Data Classification Labels allow classifications to become persistent on sensitive files. DatAnswers, which supports search for data subject access requests and discovery. Edge detects threats to data by analyzing perimeter devices. Policy Pack automatically identifies GDPR and CCPA data. And finally, Box Security Events addresses Box enterprise data.

EA Does cloud infrastructure complicate data protection, perhaps by making visibility tougher to obtain?

DG Obviously, the enterprise is moving toward increased use of cloud infrastructure for many critical use-cases. In the cloud, there is no perimeter, so controls (access controls, auditing, classification, and alerting) around the data become precious.

EA Any near- or long-term predictions about enterprise data security?

DG Enterprise teams who really want to protect their data will have to get serious about deploying a world-class platform, one that can deliver the collection, visibility, monitoring, and support needed as threats to data increase. Secure access must allow for anytime-anywhere access to resources scattered across hybrid infrastructures. Our team at Varonis is excited to evolve with our clients toward the best possible support for enterprise data security and compliance.

DIGITAL FOREN- SICS

Digital forensics remains a vital investigative technique to be used by experts to make sense of artifacts that might provide evidence of cyber exploits or malware. In the past, this discipline was the sole concern of highly-trained experts with advanced tools, often from law enforcement. But today, the digital forensics space is being populated by individuals who require less training and can achieve good results with accessible, affordable security tools.

The emphasis in digital forensics was also previously around reactive response to a past cyber or criminal incident; but today, this emphasis has shifted to the right in the overall attack kill chain. This implies that instead of treating the forensic process of dealing with just evidence of past attacks, it can also deal with early indicators of attack. Some forensics vendors see this as an opportunity to slide into the endpoint protection space.

Nevertheless, the core focus of digital forensics remains the same: It is a vital and growing discipline focused on extracting intelligence from artifacts to draw conclusions about physical or electronic hacking, criminal activity, policy violations, and the like. To this end, as the potential behavior of interest moves more toward cloud, mobility and other emerging areas, then digital forensic tools and techniques must shift accordingly.

Another useful advance in digital forensics is that the tools for recovering and investigating material from systems and devices, especially mobiles, have become more powerful and much easier to use. Where this branch of forensic science was once only an option for highly trained experts, today it is a much more accessible activity – one that can even be performed by new analysts equipped with some basic training.

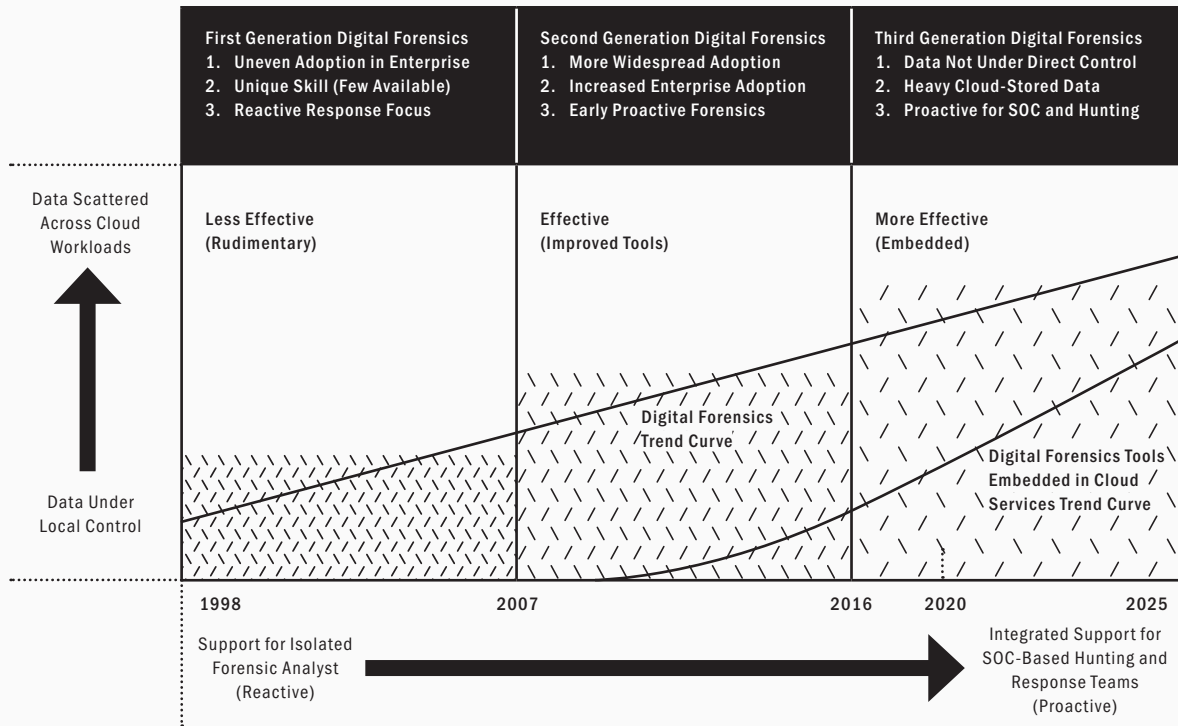
2020 Trends for Digital Forensics

The effectiveness of digital forensics tools has risen from its first generation, rudimentary beginnings to the more effective, embedded tools in use today. This is good news for forensic analysts and even law enforcement, but social and political policies play an important and vital balancing role to ensure that these tools are properly positioned in terms of power and capability. Apple's famous debate with the US FBI about decryption exemplifies the issue.

The most comprehensive transition that is occurring for digital forensics is the shift from stand-alone tools for an isolated analyst working after an event has occurred toward a much more integrated platform of support for hunting and response teams searching for evidence of past, but also on-going incidents. This implies that digital forensics tools, when applied to indicators, can be preventive (see Figure 1-39).

An additional on-going transition in the digital forensics space involves a shift from data under local control – such as on a captured disk drive or mobile device – to the analysis of data perhaps under remote, SaaS, or third-party control. Obviously, law enforcement can seize such captured data under the proper circumstances, but for commercial digital forensic analysts, this option might not be available.

Figure 1-39. Digital Forensics Trend Chart



As such, one should expect to see more intense use of digital forensic options from cloud service providers handling data of interest. This can be done in a professional service context, or it can be automated into the as-a-service environment. The publication of APIs for digital forensic analysts interested in determining the low-level characteristics of some stored artifact would not seem out of the question.

The future of digital forensics lies in emerging virtualized support for artifacts that are scattered across hybrid architectures. This will not remove the need for specialized analysis of specific devices such as mobile phones, but will create an enhanced means for establishing context around the forensic analysis of a given incident or exploit. Commercial digital forensics platforms will evolve to provide this broader view.

In addition, the debate will continue about whether commercial vendors of devices, systems, and software should be compelled to include back doors for law enforcement. Obviously, this debate will include different points of view in different countries, but for global providers such as Apple and Microsoft, the debate will necessarily require a more nuanced conclusion. Expect this to intensify in coming years, especially for AI-based technologies.



AN INTERVIEW WITH JOHN HAYES
CTO, BLACKRIDGE TECHNOLOGY

IDENTITY-BASED SOLUTIONS FOR NETWORK SECURITY

A significant weakness in any IP-based enterprise is that easily spoofed source addresses complicate access decisions based on incoming packets. Instead, what generally happens is that best-effort approaches are taken to inspect source address ranges, to direct the inbound traffic to a hosted gateway that will provide application-level security decision-making. This has the obvious drawback of allowing potentially malicious packets into the enterprise and to also move laterally within it.

BlackRidge Technology offers a creative solution to this problem using an identity-based enhancement to the TCP/IP protocol suite. A special gateway called a Transport Access Control (TAC) gateway is used to interrogate incoming packets for evidence of proper source authentication before traffic is permitted to proceed. We spent some time with John Hayes, CTO of BlackRidge Technology, to learn more about the approach and its implication on zero trust security.

EA John, what specifically is the weakness in the Internet protocol that your team set out to address?

JH As you know, Ed – the original TCP/IP protocol suite does not include native support for strong authentication. Security gateways must therefore do the best they can to determine the source and intent of any packet that initiates a new session. The traditional five-tuple used in packet filters has been the most popular means for making such decisions, but this is not a sufficient level of assurance in networks that must protect truly valuable assets.

EA How does the BlackRidge solution to this problem work?

JH We've created and integrated an identity-based solution that works at the protocol level to identify incoming packets using a special gateway. The scheme we've invented is called Transport Access Control or TAC – and it allows a BlackRidge TAC Gateway to be positioned at the network entry point or in front of valuable assets, perhaps next to other access or edge security components. Incoming packets are then interrogated using an identity authentication scheme that is much stronger than inspection of easily spoofed source IP addresses. Using BlackRidge TAC, our customers can ensure that only approved traffic ever enters a trusted domain or enterprise.

EA You've suggested that the TAC scheme is consistent with the goal of zero trust in an enterprise. How does that work?

JH When packets are received from the Internet, it is 100% appropriate to view their associated source information with low confidence. It is this notion of confidence as a factor in determining trust that we find interesting. That is, we envision a confidence scale where assurance activities move the needle on the scale, depending on the strength of the action. When a packet arrives with a weak source address, we assign low confidence to its origin, but once the TAC gateway has interrogated the packet and authenticated its source identity, we can move the needle on the confidence scale.

EA Do you find that higher assurance environments demand the type of protection offered by the TAC?

JH Certainly, we see the higher assurance customers as the earliest adopters of our technology, if only because the urgency to protect infrastructure is so high. But we believe that any organization with security policy requirements for secure access, and certainly any organization that provides identity and access management services for third parties, will really benefit from our solution.

EA What future directions do you see in this area of identity-based network security?

JH Well, zero trust security is going to increase in importance as a design philosophy, and this is good because it is consistent with trends in cloud and IoT architectures. We also expect to see security policies for identity-based controls become more tightly enforced. The idea that network traffic can enter a network segment without authentication and access restrictions is just asking for trouble. We believe this will be rectified – and we're excited that BlackRidge will be an important part of that equation with our identity-based Transport Access Control.

**IAM &
IDENTITY
PLAT-
FORMS**



The cloud introduces considerable new opportunities, but also tough challenges, for organizational IAM infrastructure and applications.

Every enterprise security team will attest to the increasingly fundamental role that identity and access management (IAM) technology, systems, tools, and processes all play in the protection of organizational assets. This has always been true, as evidenced by the lopsided percentage of the overall IT security budget that usually finds its way to IAM. With the dissolution of the perimeter, IAM takes on a new security significance.

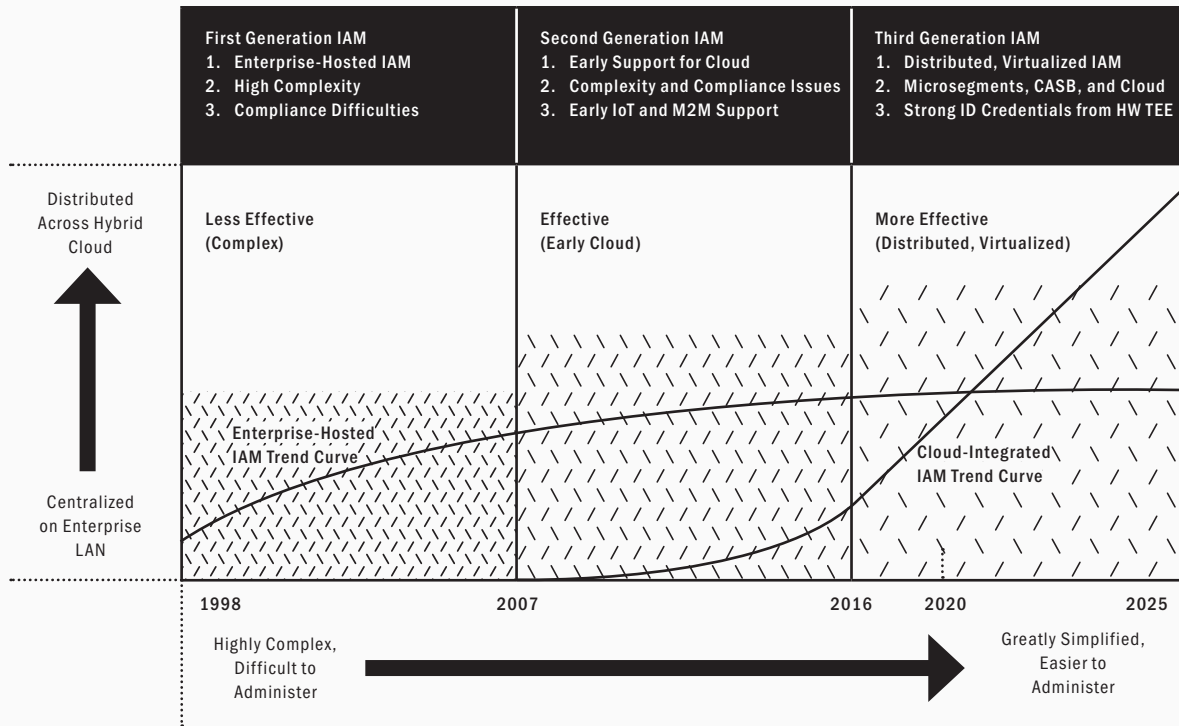
The cloud introduces considerable new opportunities, but also tough challenges, for organizational IAM infrastructure and applications. Obviously, it is more straightforward to operate and deploy an IAM system onto a perimeter-protected LAN, if only because so-called east-west visibility can be assumed to most relevant resources. Despite IAM's historical reputation for complexity, its operation was, in fact, assisted by a flat enterprise network.

So, now with the transition to hybrid cloud architecture, the IAM becomes the primary control for access to resources, replacing the firewall. That is, rather than presenting hackers with an initial hurdle in the form of packet filtering or application-level policy enforcement in a firewall, the new arrangement requires that access to the cloud gateway be permitted for publicly-hosted resources. This implies that IAM will be required to differentiate good from bad users.

With this adoption of IAM as a primary control will also come increased attentiveness from the compliance and audit community – as if IAM experts have not had enough of this already. New cloud-based IAM solutions have generally been designed with security in mind, rather than pure compliance. One might expect that with IAM-in-the-cloud offerings, the overall attention assigned to automated support for audit is likely to increase.

Related security technologies considered in-scope with IAM include password and privilege management, two-factor authentication, and secure access. In many cases, the IAM vendor offers these adjacent functions as part of the overall commercial platform. This simplifies management, but is not always feasible in environments that have gradually upgraded both legacy and new IAM infrastructure.

Figure 1-40. Identity and Access Management Trend Chart



2020 Trends for Identity and Access Management

The effectiveness of IAM has evolved from less effective deployments that were highly complex, through a second generation of effective installations that began to address some cloud usage, into the present more effective IAM solutions which are distributed and support virtual computing. This gradual evolution toward better IAM has been made possible by attention across this sector in reducing complexity (see Figure 1-40).

A clear transition has occurred during this evolution from centralized systems installed on a LAN toward more hybrid IAM systems distributed across premise, network, and cloud systems. In addition, increasingly decentralized control of identities for authentication, access, and authorization is also consistent with the hybrid arrangement. IAM is thus considered an important aspect of cloud infrastructure for business.

The future of IAM will see three trends: Continued integration into cloud infrastructure, continued focus on simplification of administration and use, and continued drive toward more secure, decentralized storage and management of credentials. These are positive trends, consistent with emerging compliance needs. IAM will thus see continued growth across all industrial sectors, including smaller businesses becoming more reliant on these solutions.

Through all this change, however, one factor will remain constant – namely, that the design and operational success of any IAM installation will be inversely proportional to the complexity of the system. Enterprise teams are therefore advised to focus on simplification of process, economy of workflow for tasks such as authorization, and modular design of the underlying IAM components (which allows for introduction of innovative technologies).



**AN INTERVIEW WITH ANDREW SELLERS & JASON CRABTREE
CTO & CEO, QOMPLX**

INTELLIGENT DECISION MAKING FOR CYBER

INTELLIGENT decision-making matches up well with the cyber security goal of driving action based on as much relevant information as can be gathered and analyzed. As a result, many companies have tried to build decision engines that learn from behavioral patterns and optimize risk-related recommendations. No enterprise team would fully outsource the selection and deployment of prevent, detect, and response actions, but all are at least considering integrating some form of this approach into their decision operations.

QOMPLX (previously known as Fractal Industries) is a leader in advanced decision engine platforms. Their solution has been applied to a variety of different contexts, including cyber security. Specifically, they have built a solution that collects identity-related information from the enterprise – Kerberos and Active Directory data, in particular – to increase assurance that identity and authentication are being operated properly. We spoke with Andrew Sellers and Jason Crabtree of QOMPLX to learn how this works in practice.

EA Your team references “Reimagining Complexity. We embrace it, so you don’t have to.” Can you explain what this means?

AS Every organization that endeavors to bring a data-driven decision system to market has to wrestle with the complexity of ingesting, normalizing, and schematizing heterogeneous to derive insights. The work these teams perform to build data infrastructure through the integration of point solutions often doesn’t specifically address practical business use-cases. Instead, they hire legions of data engineers and data scientists to instantiate, operationalize, and maintain a technology stack, instead of focusing on how an understanding of the data enables better business efficiencies. In contrast, we provide an integrated platform with enterprise-ready core services and turn-key workflows to facilitate the collection, organization, persistence, transformation, and visualization of data using a unified ecosystem of tools in an intuitive, browser-based application. This way, our clients can focus on solving business problems, rather than the complexity of their data fabric.

JC As Andrew suggests, we allow our clients to have superior focus within internal efforts by providing them an enterprise ready and massively scalable data fabric, so they can focus on differentiated aspects of their own business and their own unique data.

EA Cybersecurity has become an obviously important component of your solution application. Tell us a bit about how this came to be. Did you have cybersecurity in mind when you developed your solution?

AS We always knew that we wanted to build our application to have the highest standards of performance and scalability. From our past careers, we always knew that timely and actionable analysis of cyber telemetry across a global enterprise was out of reach of the current market offerings. Any data analytics platform that could find insight from the volume of data generated by network sensors would be robust enough to meet the needs of other domains. We consider cyber security to be the

benchmark for judging the suitability of a technology to meet the demands of the market for data-driven decision making.

JC Given our team's experience in managing and designing large networks, we realized that heterogeneous data fusion to support just-in-time, just-in-place, and just-in-context decision-making was a critical gap. One of the most glaring issues that was a huge part of the design inspiration was how to address Kerberos and Microsoft Active Directory (AD) security and our approach to massive stream processing and telemetry collection was heavily influenced by the specific requirements associated with near-real time detection of golden and silver ticket attacks via stateful protocol validation.

EA Guys, your team focuses specifically on identity assurance for cyber security. How does this work?

AS One of our flagship experiences that showcases the capabilities of the QOMPLX OS platform is the Identity Assurance module. It assures network defenders that the machinery for establishing identity inside their IT environments is trustworthy by adding external validation to trust authority provisioning and user authentication/authorization requests. This capability means that identity in other sources (e.g. logs) are trustworthy and actively combats the concerning trend where adversaries are leveraging increasingly commoditized open source tools for forging credentials to surreptitiously persist and collect data for months and years. QOMPLX OS's streaming analytics and time-series analysis have made this highly differentiating capability possible such that we can offer SLAs for deterministic detection of forged credentials in minutes from anywhere in the world.

JC While we definitely look at the same heuristics that have become industry standard for Kerberos and AD-related solutions, we decided to add external state to validate the Kerberos protocol itself. This was harder, because it required collecting every single part of the Kerberos authentication

handshake across global networks for clients. But doing it the hard way allowed us to support high confidence detections that are actually fit for the SOC. We've been able to demonstrate this for large organizations and deal with large numbers of DCs, Kerberized services, and complex trust relationships.

EA Can you help us understand the deployment process for your Q:CYBER into the typical enterprise?

AS One of the differentiating aspects of Q:CYBER is how we efficiently deploy to customers and begin finding insights based on extensive automation of our sensors. Our Kerberos agents are configured and installed using a client's existing systems management platform. We provide a unified experience for forwarding and aggregating telemetry for analysis via midservers, which are high availability collection points, automatically deployed in minutes across an enterprise. The midserver can facilitate transport of additional sources of information, including windows event logs and sysmon data. Once data is collected, we offer standard packages for actionable detections or automation rules plus the ability for users to define statistical and model-driven detections inside an intuitive, browser-based interface. These workflows then feed existing SIEM tools or manage incident response using a built-in workflow.

JC Automation around configuration and deployment actions was a key requirement for us. We automate much of the time-consuming tasks associated with installation of sensors, transport of data across the WAN, and actual ingestion of arbitrary log and sensor data into our platform for analytics. The goal was to make it faster and cheaper to improve visibility on the network, including novel data sources like the Kerberos agent capabilities which fill visibility gaps for attacks like Silver Tickets.

EA Any near- or long-term predictions about identity assurance? And also, more generally, about advanced AI for cyber security.

AS The concept of identity will become harder to proactively manage as enterprises move from consolidated architectures toward services consumed from multiple providers across

multiple environments with less intuitive trust relationships. Today, IT environments are moving from consolidating all directory services, and now must wrestle with associating users with tools like Slack messaging, social media accounts, and other service providers, where trust is federated or doesn't exist at all. Current protocols aren't designed to compensate for the loss of shared secrets, and this limitation will only become more problematic as the attack surface for identity-based exploits extends as the formerly well-defined perimeters of trust deteriorate. Tools that mitigate risks associated with identity compromise will become even more central to the best cybersecurity risk management programs. Regarding the future of AI in cyber security, the potential of moving towards event-oriented architectures with better data models – and one powerful example is enterprise knowledge graphs – is immense, and will enable more relevant and predictive AI applications. It's difficult to recover from a poor data model and architecture, despite continued improvement in AI models, which is why many schema-less data-lake efforts were declared successful by technologists, but found lacking by business clients. A simple way to view the shift towards a more diverse and integrated set of data stores and analytics processing engines, when coupled with appropriate data flow orchestration, is that industry will get closer to realizing the big promises made 10-15 years ago and still in the coming-soon category. Until data is better organized and transformed, AI will not realize its potential to transform network defense.

JC Andrew is definitely correct. We recommend evaluating assumptions at the core of the security program. One of the reasons we dove deep into Kerberos and Active Directory – we support Windows and Linux environments – was that so many aspects of the enterprise IT security programs depend on authentication and SSO working as intended. We believe in validating the Kerberos protocol as a key part of identity strategy, because it ensures that users are consuming the intended services in line with expectations from administrators. This helps them avoid common issues where behavioral analysis programs and insider threat programs fail, since they are basing

analytics on improperly attributed actions when credentials are being forged or misused. We're big on blocking and tackling, which means doing things in the right order. If we can use a declarative rule, we do so. We like to focus on data quality and consistency, then start laying in basic rules, which can be powerful in the context of streaming fixed-point semantics. Then we work up to model-based security via statistical models or various types of machine learning for detections. We often see clients prematurely trying to go to AI/ML, and while these techniques can be powerful if done correctly, which includes leveraging visibility from multiple sensors on the network, they aren't operationally advisable without getting the infrastructure and data right first. There is no God-algorithm here that addresses all the issues in cyber, so we focus on combining narrow bits of math and data as individual strands which are weaved together to create a mutually-supporting fabric for detections, automation, and decision-making.

COMP- LIANCE SUPPORT

Every business understands the importance of a security compliance program, if only because modern regulatory and audit requirements demand attention to this area. Credit card usage, customer data storage, third-party support, and on and on – all require attention to ensuring a minimum level of security protections; hence, the security compliance industry has thrived, with products and services available to assist businesses of all sizes.

The most common commercial engagement in security compliance involves use of a consultant to provide either pre-audit advice, formal attestation, or post-audit improvement. This can be done by trained consultants in the context of a well-established compliance standard such as the Payment Card Industry (PCI)/Data Security Standard (DSS); or it can be done by established experts in the context of generally accepted security practices.

Many commercial tools that assist with the compliance process tend to focus on security risk. In fact, an enormous industry sector has emerged for collecting security risk-related artifacts, analyzing and synthesizing them into a coherent view, and then presenting these risks as a dashboard for executives. The usefulness of risk analysis, management, and reporting tools is two-fold: They help with compliance, but they also help with pure cyber security.

Many risk-related enterprise processes have been supported to date using rudimentary tools such as Microsoft Excel, where subjective, probabilistic estimates of attack likelihood and monetary consequences are used as the basis for rounds of Monte Carlo simulations. This is not an optimal approach for complex environments, so vendor solutions have emerged to improve on this critically important function.

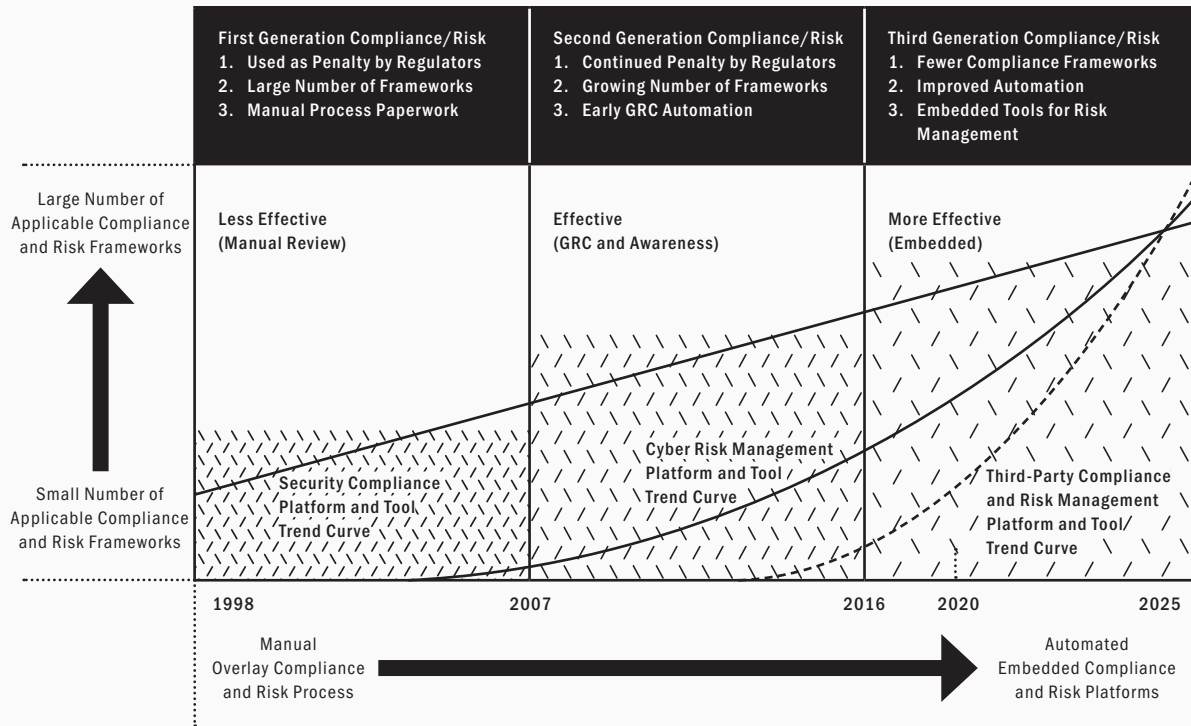
An additional major factor for both compliance and risk involves third-party coverage. Most of the major breaches that have happened in the past few years have involved third-party suppliers, partners, and support teams. Automation will be required to deal with this massive growth in third-party initiatives, including outsourcing and offshoring. As the work scatters across a more complex organization, the compliance and risk must follow.

2020 Trends for Security Compliance and Risk

The effectiveness of both security compliance and cyber risk management tools has increased from less effective platforms in the first generation, through an effective period of both compliance and risk support, to a more effective third, present generation. Security compliance support has increased gradually and linearly; risk management support is in a more accelerated growth curve for both commercial success and effectiveness of solution (see Figure 1-41).

The accelerated success that risk platforms have experienced can be traced to their dual value proposition for both compliance and security. For example, if an executive team or board would like information on compliance metrics or on general cyber security posture of the organization, a risk reporting platform with good visualization would

Figure 1-41. Security Compliance and Risk Trend Chart



provide an excellent means for providing this information clearly and accurately. A transition for both compliance and risk is that the pure number of applicable frameworks has grown dramatically. This is an aspect of our industry where growth is probably not a good thing. When additional frameworks are introduced to an environment, the compliance and security teams will rely on the automation to just map existing practices to the new requirements. This introduces more bureaucracy, and rarely results in changes to operations.

An additional transition for compliance and risk has been the shift from largely manual processes that are overlaid onto business unit systems and procedures to more automated and embedded compliance and risk platforms. This is a welcome shift given the larger number of applicable frameworks, as well as the speed and scale increases in most modern business sectors. The automation helps compliance and security teams keep up with the volumes.

The future of security compliance and cyber risk involves more automation, more embedded controls, and expanded focus across increasingly hybrid cloud environments. Less compliance and risk data will come from the local LAN, which is dissolving, and more will come from third-party programs. Manual compliance and risk management will gradually fade into executive processes that interpret and utilize insights from the automation.

That said, human beings will still obviously curate compliance processes, including during the development lifecycle for automated systems. This suggests that compliance for DevOps might be one of the more consequential future considerations in the coming years. Such application will require, obviously, that the compliance and risk management controls do not introduce delays into the development lifecycle. This is done through economical use of automation.



AN INTERVIEW WITH CHRISTOPHER KENNEDY
CISO & VP CUSTOMER SUCCESS, ATTACKIQ

CONTINUOUS VALIDATION OF ENTERPRISE CONTROLS USING ATTACKIQ

EVERY enterprise security team knows that various forms of testing will always be required components of any protection strategy. This can range from laser-focused penetration tests by white hat hackers to much broader testing of controls by assessment professionals. In all cases, however, the time that lapses between tests, and often the methods, and most importantly, the constraints imposed, affect the efficacy of the validation function that testing is intended to serve. The way we test and the time between them isn't effective. This challenge grows larger with the increased speed of processes such as DevOps.

The AttackIQ team has been focused on addressing this gap by offering a suite of continuous validation solutions in its breach and attack simulation platform. We recently sat down with Christopher Kennedy, CISO and Vice President of Customer Success for AttackIQ, to learn more about how their solutions are being used in the enterprise. We were particularly interested in the degree to which such continuous validation can help reduce the overall cyber security risk to the enterprise.

EA Can you help us understand the nature and importance of continuous validation in the context of cyber security?

CK There's a major gap in the enterprise cyber security lifecycle today, where validation of controls is under-represented as a construct. This is a foundational systems engineering problem in the industry. Common standards don't dutifully specify the what and how to do this better in a technological era where it's both a must do and new capabilities are emerging to improve it. As a result, organizations tend to validate their controls using ad hoc audits or periodic penetration tests. This is a particular challenge, because security teams already have to deal with a growing and dizzying array of security technologies, configuration complexities, and products ambiguous value lifecycles. It's therefore hard to know the best solution through time, much less determine whether it is working effectively. The data is all there. A recent Ponemon Institute survey showed that 53% of the interviewed IT and IT security practitioners (whose organizations spend an average of \$18M each year on security) don't have confidence in their security posture. Wow. The 2018 Verizon DBIR stated that of the incidents they analyzed, 80% of the affected organizations had all the security technology in place to avoid the issue, but either a security control configuration or operational process is what failed them. This point is further reinforced in a deeper review of any of the recent breaches in the news, Equifax, Marriott, Capitol One, etc. I'm here to tell you, I've seen the effectiveness of an advanced and determined attacker, but the reality is, organizations are failing against common hygienic basics. A key reason is they aren't emphasizing testing and validation enough. These security technology investments are not fire and forget. In the last few years there have been significant advancements in more effective frameworks like MITRE ATT&CK and technologies such as AttackIQ that can allow an organization to test and validate at scale.



**Technology
is now the
lifeblood
of almost
every
business.**

EA Does that complexity make continuous validation more difficult?

CK Certainly. Technology is now the lifeblood of almost every business. The CIO and CISO play a critical role in enabling company strategy today. This places tremendous pressure on these executives to manage technology and security effectively to deliver corporate value. Hybrid technology environments from corporate data centers, mobile infrastructure, and cloud services create a significant complexity challenge that is compounded by the diversity of security technologies often required to protect them (and even further complicated by the varying level of skill and expertise of the people behind those controls). I saw a recent survey suggesting that modern enterprises have over 75 security control PLATFORMS alone. Furthermore, commonly adopted risk management rubrics are highly subjective, academic, and largely temporal – often not fully illuminating the true security challenges for the organization. It's a hard place to be, trying to set an investment path with all this divergent optionality in technology and security, often armed only with an academic understanding of the risks you're willing to accept. Continuous security validation, also referred to as CSV, affords a new approach to assuring one's security posture. By emulating real attacker behaviors, you can base the control maturity assessment of your risk program on the most probabilistic attacker tactics and techniques. Protect yourself from the ways you know a real attacker would exploit you. Armed with this approach, you can invest where you really need to, and you can defend key assets against the most viable threats. Many of our customers at AttackIQ get it, and are framing their investment in CSV to enable more real time threat modeling, where they can rationalize the security stack they have, address protection failures and configuration gaps, and eliminate security capabilities that are failing or duplicative through end to end testing based on continuous attacker emulation.

EA How is the AttackIQ platform deployed – and can you explain the nature of the scenarios that are run in the enterprise?

CK Our platform is based on a simple-to-deploy distributed client server architecture that is purposefully optimized to emulate point of breach attacker behavior. Philosophically, we believe point of breach controls are the most important, because you want to minimize the attackers' dwell time in the environment. Controls that protect in the later phases of the attacker kill chain are important, but at that point the attacker has already made significant progress against their goals. This is the most expensive place to defend. Our "post-breach" based approach enables the deployment of lightweight assessment engines to assets that you assume are breached. These "agents" then safely emulate attacker activity on that asset, thus enabling the measurement of the effectiveness of your control stack. The agent safely does all the work, executes all the tests, and cleans up any residuals from the tests automatically. The backend brain of the process is managed either on-premise or via our SaaS. A particularly discriminative architectural component of our platform is our production asset orientation. Though a viable but costly approach, there's no requirement to stand up "synthetic attacker hosts" or orchestrate a testing laboratory. Our assessment engines are engineered to run safely on real business assets so you can emulate attacker behaviors and exercise the controls on your most critical business assets – just as an attacker would. This is absolutely critical.

We support direct integration with major security control and SIEM/SOAR platforms to enable end-to-end security ecosystem testing. These integrations allow the management console to serve as the single pane of glass to drive testing across the security ecosystem. Already have another tool to drive security workflows? A robust API allows direct integration to those platforms as well. Our goal ultimately is to make testing administration as

pervasive, lightweight, and flexible as possible. Although Gartner has classified this product space as "Breach and Attack Simulation," we think our platform is broader than that. First, the platform is more "emulation (test on production assets) than simulation (test on lab or synthetic assets)" based on the dialogue above, but our testing "content library" really shows how BAS is just a subset of what we do. We have the industry's most robust content library, which constitutes an exceptionally deep and capable pre-established set of tests or "scenarios" that an analyst can use day one, out of the box. There are three major categories of content in the library: ATT&CK based emulation, Continuous Validations, and Threat Intelligence. As one of the earliest adopters of MITRE ATT&CK, we have the most comprehensive array of ATT&CK aligned attacker behavior emulations ready to go and these are continuously evolving based on the diligent work of our dedicated threat emulation development team. But beyond ATT&CK TTP emulations, we have also developed a wide array of common "security validations" that are often not yet linked to MITRE ATT&CK, but are critical to validating continuously (think of open S3 buckets or broadly exposed VPC configurations as examples of these tests). This is a particular investment area for us, where we're already working with major IAAS providers to develop emulations for the attacker tactics and techniques they are most concerned about. Through this support, and given our early alignment and partnership with MITRE, we intend to help MITRE expand the cloud-centered TTPs of ATT&CK.

Lastly, we also have temporal OTX-based threat intelligence feeds that can be leveraged. The scenario library is organized into simple, easy to consume templates, so customers can run more comprehensive kill chain activities such as: "Ransomware, windows credential theft," and so on. We also integrate community and industry threat intelligence, so customers can take advantage of the recommendations of that analysis, such as the Red Canary Top 10 Tactics 2019. Another particular differentiator in

industry is our entire library is open and exposed to the customer – meaning the customer can see, learn from, and modify every scenario in the library by reviewing the Python based code. Customers can also create their own scenarios and templates directly using existing threat intelligence tailoring for privately defined security controls. The open library is a great training tool as well.

EA What type of constraints do you place on scenarios? One would imagine that enterprise teams would want confidence that they can ensure the integrity of the testing and to avoid outages or other issues.

CK Do-no-harm is a fundamental tenet of our platform, and this requires no lab to facilitate emulation. Our platform is designed to be safely deployed into production enterprise environments. This is critical, because all the scenarios in the platform are extensively tested to ensure their safety before release. Although we have broad coverage of emulation tests across MITRE ATT&CK, there's still a reasonable percentage of highly destructive scenarios that we cannot cover, because it would be impossible to emulate safely. We're finding the penetration testing teams, who usually operate with significant ROE to minimize operational risk, prefer this platform because of the openness and safety. We've built RBAC profiles to scope user behaviors, and are building other safety features to protect users from taking the advanced capability too far unintentionally.

EA Do you see continuous validation growing in importance across the compliance and audit community? One would guess that auditors and assessors would like the continuous nature of the testing.

CK Absolutely – spot on. I see significant evolution, for instance, in automating blue/red/purple team assessments, and connecting and mapping those activities to answering regulatory remits. Continuous, evidence-based compliance dashboarding as an idea, opposed

to the endless array of interviews, meetings, and navigating the ambiguity of regulatory expectation will be especially attractive to the compliance and audit community.

EA Any near- or long-term predictions in this area of continuous validation?

CK Right now, I see MITRE ATT&CK as having an explosive impact on the industry – serving as the anchor of CSV platforms, helping industry drive efficacy into their products, and reshaping security teams – including purple teams, threat hunters, automated compliance. Correspondingly, I see CSV reshaping risk management in the enterprise. A couple of big picture things I expect to see include continued evolution of ATT&CK with cloud TTPs, mobile, and more industry involvement (such as the Center for Threat Informed Defense). I also see further adoption and standardization across sectors, addendums to standards and regulatory bodies further defining and requiring SCV programs, improved connection between pre-ATT&CK and ATT&CK and other risk management functions (like 3PA) which will better enable real time risk management based on known attacker behaviors; and application of machine learning to create and assess attacker kill chains before the attackers fabricate them. and industry threat intelligence, so customers can take advantage of the recommendations of that analysis, such as the Red Canary Top 10 Tactics 2019. Another particular differentiator in industry is our entire library is open and exposed to the customer – meaning the customer can see, learn from, and modify every scenario in the library by reviewing the Python based code. Customers can also create their own scenarios and templates directly using existing threat intelligence tailoring for privately defined security controls. The open library is a great training tool as well.



AN INTERVIEW WITH KISHOR VASWANI
FOUNDER & CEO, CONTROLCASE

**DEMOCRATIZING
COMPLIANCE-
AS-A-SERVICE
USING
CONTROLCASE**

CERTAIN aspects of the cyber security obligation for companies have tended traditionally to be reserved primarily for larger companies. Compliance is one of these aspects, and its techniques and tools have tended to evolve consistent with the need of larger organizations. Governance, risk, and compliance (GRC) tools, for example, have tended to be expensive and feature-rich to deal with the complexities of large business processes and workflow.

More recently, however, small and medium-sized business have begun to experience an increase in compliance requirements for cyber security. This places considerable burden on organizations that have never considered such issues in the context of compliance. We recently caught up with Kishor Vaswani of ControlCase, to learn more about how they are now providing popular and effective cyber security compliance support via subscription solutions for small and medium sized businesses.

EA ControlCase is in the business of providing certification services for the past decade and has evolved to include many certification and attestations, but what other value propositions do you have for the market place?


KV ControlCase initially started as an organization more than a decade ago providing one or two certifications, but since then we have over 15 certifications/assessments (including PCI DSS, ISO 27001, HITRUST, SOC2, NIST 800-53, CSA to name a few) within our portfolio of certification services. We currently provide the following solutions: We can perform certifications and assessments for all types of organizations, we support continuous compliance mainly for Fortune 1000 enterprises, we offer compliance as a Service (CaaS) mainly for all mid-size organizations, and we are a managed security services provider for all mid-size organizations.

EA What is a continuous compliance offering?

KV Continuous compliance means attaining compliance across your IT and business environments, and then maintaining it on an ongoing basis. Continuous compliance is all about developing a culture and strategy within the organization that continually reviews compliance position to ensure that industry and regulatory demands are being met while also maintaining secure systems. Continuous compliance includes quarterly review of 20-25 high impact data points. It also includes technical review of vulnerability scans, log management, asset lists, and other available automated systems. Finally, it includes continuous compliance as a quarterly scorecard of compliance. This involves the familiar green/yellow/red scheme found across multiple compliance regimes.

EA What are the benefits of the Continuous Compliance offering?

KV The main benefits of continuous compliance include eliminating the need for potential major last-minute audit findings, reducing effort for final audit by approximately 25%, reducing the risk of technical shortcomings such as quarterly scans, missed certain assets, and logs from assets not reporting.



Continuous compliance as it sounds means attaining compliance and increased security across your IT and business environments, and then maintaining and retaining it on an ongoing basis.

EA Tell us how about your other solutions compliance as a service (CaaS) in support for your clients.

KV ControlCase Compliance as a Service (CaaS) solution was built for organizations who wish to offload and outsource all their compliance and certification-related needs. As part of the CaaS solution offering, we enable clients to manage their compliance seamlessly using access to compliance experts, SkyCAM portal that converts over 15 international regulations to English-like questions, and automation in evidence collection required for compliance/certification regimes.

EA Which compliance frameworks do you see as being the most important moving forward, especially for small business? Do you expect to see consolidation?

KV As the industry heads to a direction where cyber threat and security lapses are common news items, there are many different regulators and standards which come through by virtue and significance. In today's world, if you throw a dart at the list of Fortune 5000 organizations, it will land on an organization which will need multiple compliance/certificate requirements to meet regulatory standards, internal security standards, compete with peers in the market place etc. Here are the standards ControlCase sees as common needs - PCI DSS, ISO 27001, HITRUST, SOC2, NIST 800-53, CSA.

EA How does your One Audit solution work?

KV The One Audit service provides the ability for organizations to perform a single assessment and certify/comply with multiple regulations, including but not limited PCI DSS, ISO 27001, HITRUST, SOC2, NIST 800-53, and CSA. The features and benefits of One Audit lie in the fact that there are fewer internal resources required from the organization, as well as reduced audit preparation and execution time. It thoroughly simplifies the multiple regulatory requirements into a simple English-based evidence collection questionnaire, where responses serve as evidence for multiple control objectives for multiple regulations.

EA What do you mean by automation in continuous compliance, can you provide more details?

KV At any point during the course of the year, a company has about 70% of their assets out of compliance at some point in time. The idea of continuous compliance is to manage and address these before they escalate and become an issue during evidence collection for certification. Now if this is to be achieved manually, it takes a lot of personnel effort and hence we have built automation into the process of managing continuous compliance with our GRC portal. This includes API's integrated with world-class GRC solutions, such as Archer and ServiceNow. It also eases the process of monitoring and quarterly reviews of evidences, which then eliminates the need for last minute audit findings, and reduces effort by 25% during the final phase of certification.

42

VULNERABILITY MANAGEMENT

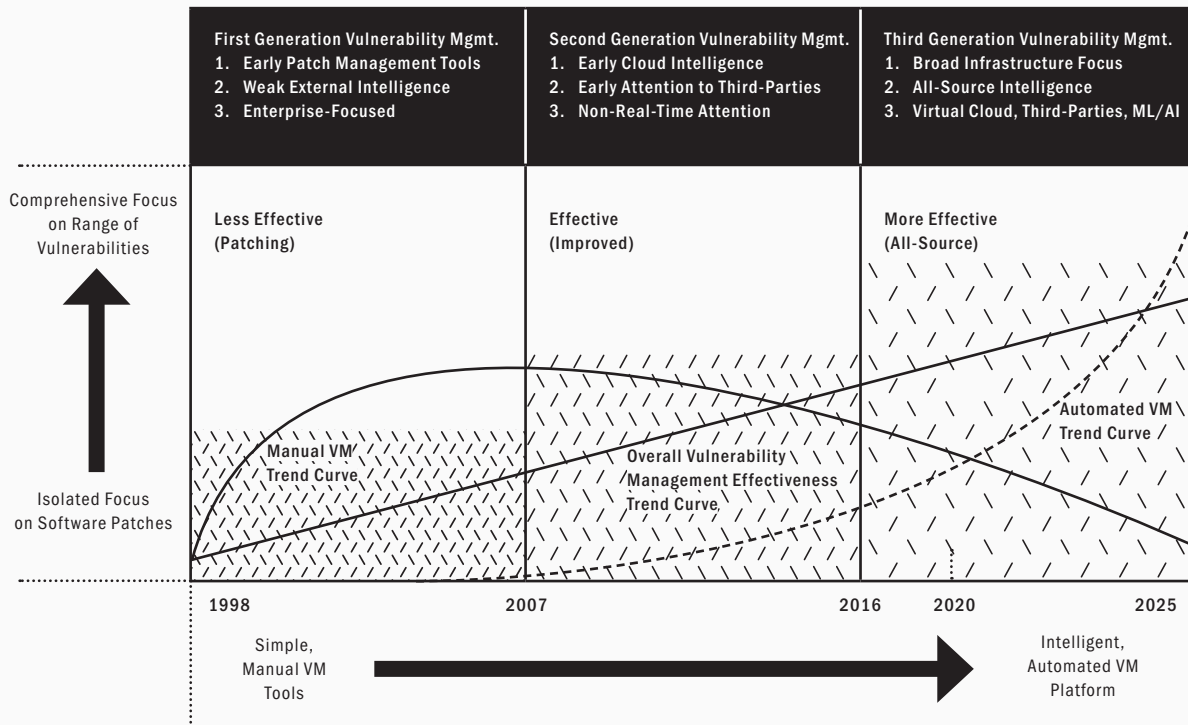
Vulnerability management for enterprise began its life in the 2000's in the business of patch management for servers. It has since shifted rapidly from this modest beginning to one of the most essential cyber security processes for identifying, categorizing, tracking, managing, and remediating the massive assortment of cyber-related vulnerabilities that modern organizations face across their servers, endpoints, databases, systems, networks, and so on.

The modern vulnerability management process requires a variety of information, access, tools, techniques, and capabilities, because it tends to reach into every aspect of business unit activity. For example, vulnerabilities can be obvious, such as highly-public exploits that affect all servers in the data center; or they can be hidden and subtle, such as an obscure software bug in a small proprietary application used in a limited manner by a small portion of the company.

This need for wide vulnerability management coverage has resulted in a shift toward greater use of automated discovery, control, and even remedy. That is, vulnerability management has shifted from the days of manual reviews based on Excel spreadsheets of identified issues toward platform-based orchestration of more extensive coverage. This also now includes vulnerability management for cloud and mobile assets as well.

Many existing security consulting teams have found a natural evolution from professional services with clients engaged in vulnerability risk toward the provision of an automated platform for helping to perform enterprise-wide vulnerability management. This is a welcome process, because such experience-based creation of automated platform support based on real projects will result in high-quality advances to vulnerability management offerings.

Figure 1-42. Vulenrability Management Trend Chart





Qingbao Meng, Unsplash

2020 Trends in Vulnerability Management

Vulnerability management was less effective in its first generation of use, due to overly manual processes that missed important issues. The second generation of vulnerability management was characterized by improved methods, including early automation. Current, third generation vulnerability management is more effective with fully automated platforms ingesting relevant data from all-sources (see Figure 1-42).

Transition has occurred in this area from isolated focus on software patches in the early days toward a comprehensive focus on a range of different vulnerabilities in traditional server and application areas, as well as emerging cloud and mobile. This is characterized by intelligent, automated VM platforms that are on the verge of incorporating

advanced heuristics including machine learning to improve accuracy. The future of vulnerability management lies in more embedded collection tools and management controls. Like GRC functions, VM works best as an integrated component, rather than as an overlay. As such, expect to see most new systems come with pre-defined interfaces for VM platforms to ingest data and to serve up required mitigation based on identified vulnerabilities.

An additional future vision for VM is that as computing becomes more inherently automated, including during development, the need increases for vulnerabilities to be identified and addressed automatically in real-time. Human-time involvement in any enterprise VM process will thus become impractical simply because humans cannot process information and react quickly enough to keep up with an automated infrastructure (and automated attacks).



AN INTERVIEW WITH PAULO SHAKARIAN
CEO & CO-FOUNDER, CYR3CON

PREDICTING ATTACKS WITH AI

FEW concepts in the cyber security industry are as enticing as the use of artificial intelligence (AI) to predict attacks. While this idea is no longer just part of some distant future, it's implementation in practice is non-trivial and requires development of powerful algorithms and capabilities. Meaningful data must be collected, analyzed, categorized, and then quickly used as the basis for proper action by enterprise cyber security teams.


We recently had the good fortune to connect with Dr. Paulo Shakarian, CEO and Co-Founder of CYR3CON. Shakarian is an amazing technologist and entrepreneur with an impressive personal background – including two combat tours in Iraq. Below is a summary of our discussion, including details he shared with us about how his AI-based platform does, in fact, support the accurate prediction of cyber attacks from collected intelligence. It's a fascinating story.

EA How does the CYR3CON platform predict and prevent cyber attacks?

PS We predict which software vulnerabilities are going to be exploited in the wild. And this is where we need to move vulnerability prioritization, because disclosures have skyrocketed over the last three years and teams need to predict what's going to be used in an attack. That said, this is a difficult task, as under 3% of vulnerabilities are used by hackers in attacks in the wild. Finding a needle in a haystack with reasonable accuracy can only be accomplished through advanced artificial intelligence techniques. Further, our algorithms provide a probability of exploitation, which can be used to rank-order the results of a vulnerability scan. This gives our customers a predictive ranking by which to tackle remediation efforts. Key to doing this correctly is to fuel the predictive algorithms with data that is automatically mined from hacker communities to derive intelligence about potential threats. Any type of prediction needs indicator data, and if you are going to predict the actions of attackers, the indicator data must come from the hacker community. This information provides context around the prediction. Having just a numerical prediction value does little to build trust in the system. However, when you have context from the hacker community, the threat becomes clearer.

EA So, let me see if I understand – the idea is that enterprise teams would get priority-based information from CYR3CON, which they can then use to prioritize their work?

PS Yes, that's correct. One of the challenges for enterprise teams is that vulnerability prioritization is all over the map from different experts. This is due to the subjective nature of those opinions – which is typically not driven by strong data about the attacker. To illustrate, I recently blogged about an old Microsoft Office vulnerability (CVE-2017-11882) which was being used by hackers to exfiltrate information. We saw evidence that the vulnerability was severe, because hackers were actively discussing how to leverage the vulnerability before it was seen in the wild. But when it was assigned severity ratings from the larger



We predict which software vulnerabilities are going to be exploited in the wild.

research teams, we saw references such as “very low risk” and “exploitations less likely.” Perhaps these assessments are OK in a vacuum, but they ignore the hacker community and how they share information and build on experience. Our premise at CYR3CON is that empirical data from real conversations can help predict which vulnerabilities will be used in an attack.

EA So, what’s wrong with CVSS scoring – don’t enterprises need to use that for compliance reasons anyway?

PS CVSS was never designed to predict what hackers are going to do in the future. Rather, it was designed to provide a single metric to assess the importance of a vulnerability. It was also not designed to triage vulnerabilities, because around 60% of vulnerabilities are ranked at the high or critical level, which is what enterprises normally patch for compliance reasons. This is twenty times more than the number of vulnerabilities actually exploited. But more importantly, the CVSS score is distributed the same way for both exploited and non-exploited vulnerabilities. So, while CVSS helps firms reach compliance, it still opens up the enterprises to two major problems. First, it does not provide a high level of triage, because you don’t instantly patch everything. You instead decide which vulnerabilities pose an imminent threat. Second, when dealing with low and medium ranked vulnerabilities, enterprise defenders need to know which ones hackers will most likely sneak in an exploit, as these often go ignored. By providing an attacker-driven probability of exploitation, CYR3CON addresses both of these problems.

EA So why not just have an analyst research each vulnerability?

PS There are many vulnerability management and threat intelligence groups that do a great job of doing threat research. But the key issue is scale. That is, when you have thousands, hundreds of thousands, or even millions of vulnerabilities, is it realistic to do threat research on each one? Even if we could, would the human judgement on probability of exploitation be accurate, consistent,

or objective? The reality is that it makes sense to do this with artificial intelligence, machine learning, and data mining techniques. Our platform easily scales to provide results for large enterprises, and the research is reduced to a click or a Python script that can be run in seconds with a tiny fraction of the analyst's time. In many ways, CYR3CON can inexpensively up-level an analyst, allowing them to scale, be more accurate, and more objective in how they assess what vulnerabilities will be exploited.

EA What types of information are you looking for in the hacker community to provide advanced warning?

PS The key is not only collecting the right kind of data, but having the feedback loop to ensure that the data we collect is meaningful to prediction. Many firms collect data from various sources, often with an eye for manual use cases. Our data collection is streamlined to support predictive efforts and we have optimized it as such. Indicators gathered from the hacker community not only depend on what the hackers are saying, but underlying aspects of their social structure, as well as metadata about the sources that we mine. These techniques are part of the proprietary base that drives our platform, but we've been open in the community about how this general area of technology works. We include a downloadable eBook on our website, and I've been a co-author of a couple of books on the technical foundations of this approach.

EA Do you worry that hackers will sense that you're collecting this data and will stop talking?

PS That seems unlikely. Just as enterprise teams rely on workflow, email, and collaboration tools to coordinate their activities, the hacking community relies on discussion in forums to share, learn, cooperate, and yes – also brag. When we climb into this community, we gain insights that are literally impossible to derive anywhere else. Also, our approach considers socio-cultural variables that include aspects of the hackers' expertise, reputation, community, and history. These are variables that are time-consuming for hackers to fake. In fact, we have conducted red-team tests against our

algorithms and found them to be robust against poisoned data. Beyond that, this provides context around the prediction. The feedback we are getting is that enterprise teams find the context invaluable, and have been using our solution to drive accurate prioritization of vulnerabilities and corresponding preventive actions. Further, the contextual information provides justification required for major and expensive remediation projects.

EA Any thoughts on the future of AI for cyber security?

PS I like the prospects for using artificial intelligence in more cyber security applications. The recent advances in algorithms and platform support have changed the equation, and that's a good thing for our industry. Obviously, we need to keep an eye on how hackers might also use automation. Botnets and other automated tools make their exploits so much more powerful. But I'm generally bullish on the prospects of reducing risk using powerful AI-based technologies such as we use at CYR3CON.

INDUSTRY ANALYSIS

Industry analysis for cyber security involves the expert provision of advisory guidance, trend information, and relevant insights for the working cyber security professional. It is a vital component of vendor source selection, and when used properly by an enterprise security team, can save time, budget, and effort across the enterprise cyber security ecosystem, across all phases of the kill chain. Few consider industry analysis a control, but it most certainly is.

For example, when an enterprise security program is being created, managed, augmented, or assessed, the advisory guidance from experts should play an essential role in future-proofing the characteristics of that program. Without such guidance, security managers and executives are basically guessing at trends, mostly based on vantage points that exist within the walls of a private, proprietary enterprise. This can increase risk.

Most industry analysis to date has come from large companies providing two-dimensional grids. They score vendors based – presumably – on objective assessments of their ability to provide a good solution and their insights into the needs of their customers. In practice, however, these grids, waves, and quadrants are expensive, and have tended to serve more as marketing fodder, with relative placement often determined by pay-for-play factors.

This Security Annual is an attempt to shift the cyber security industry analysis picture toward more egalitarian, free, unbiased assessment of security technology vendors, commercial solution offerings, and defensive cyber trends. Good analysis is an important component of security protection – no less important than great consulting support, penetration test insights, or world-class functional architectures.

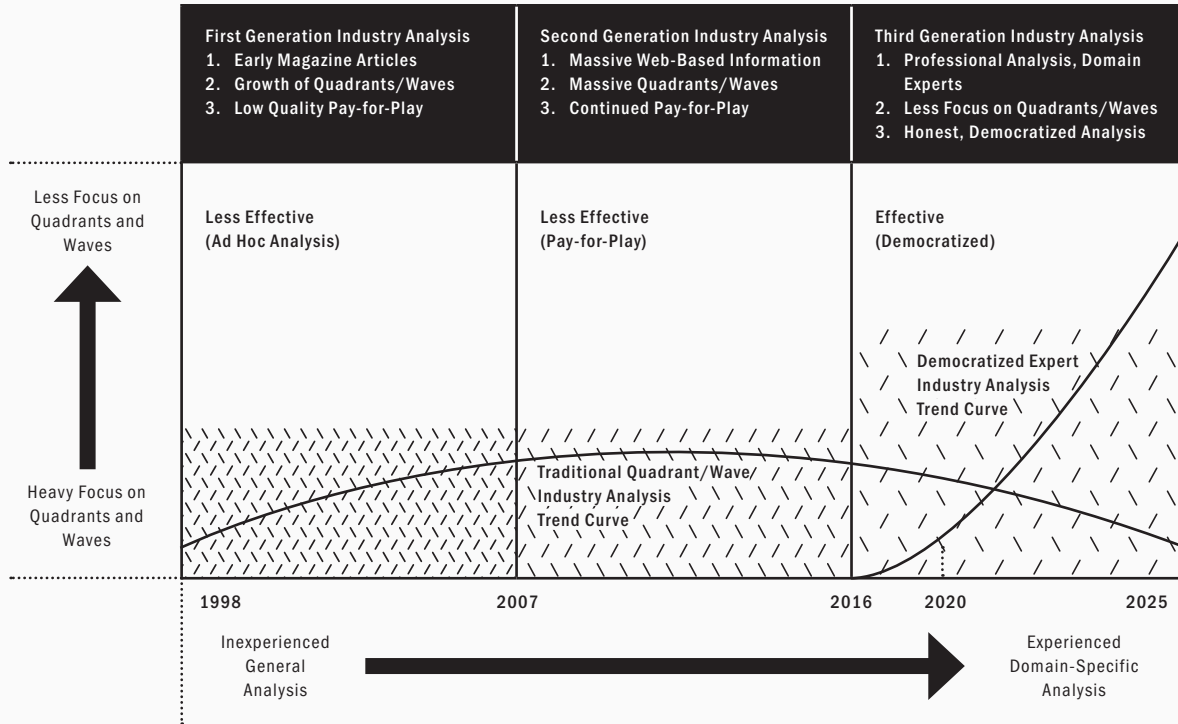
2020 Trends in Industry Analysis

The effectiveness of industry analysis through its first two generations of use has been less effective, simply because the discipline has not been properly attended to across the cyber security industry. The present generation includes more expert guidance – including this Security Annual – and should create an important new resource for enterprise security teams making decisions about their cyber risk (see Figure 1-43).

The transition away from quadrants, grids, and waves is the best example of improved analysis in our industry. Every other aspect of our business, financial, and critical infrastructure sectors includes independent, unbiased assessment of the quality and effectiveness of tools, products, methods, and solutions available for purchase. This transition is welcome and will significantly improve the ability of enterprise teams to build cyber security solutions.

An additional transition is that generic guidance from broad, non-specifically trained writers will be replaced by experts with many years of training in domain-specific areas. General industry reports, for example, that are created on industry control system security simply cannot be produced effectively by writers using a browser to search keywords in this area. Luckily, enterprise teams are no longer assigning much value to these reports.

Figure 1-43. Industry Analysis Trend Chart



The future of industry analysis for cyber security lies in democratized, domain-specific guidance provided to enterprise teams by domain-specific experts who are unbiased and motivated only by the need to help reduce risk. This will change the nature of the provision of this information toward more democratized means such as social media, video, and other more accessible means for publishing timely guidance.

Industry analysis will also become more automated. Where market reports served previously as the sole means for sharing information and guidance, searchable information with powerful tools for analysis will become the norm. Even this Security Annual includes now an automated means for vendor investigation at <https://www.tag-cyber.com/vendors>. This on-line utility replaces what was previously a large PDF document. Expect this trend to continue.

**INFORMA-
TION
ASSUR-
ANCE**

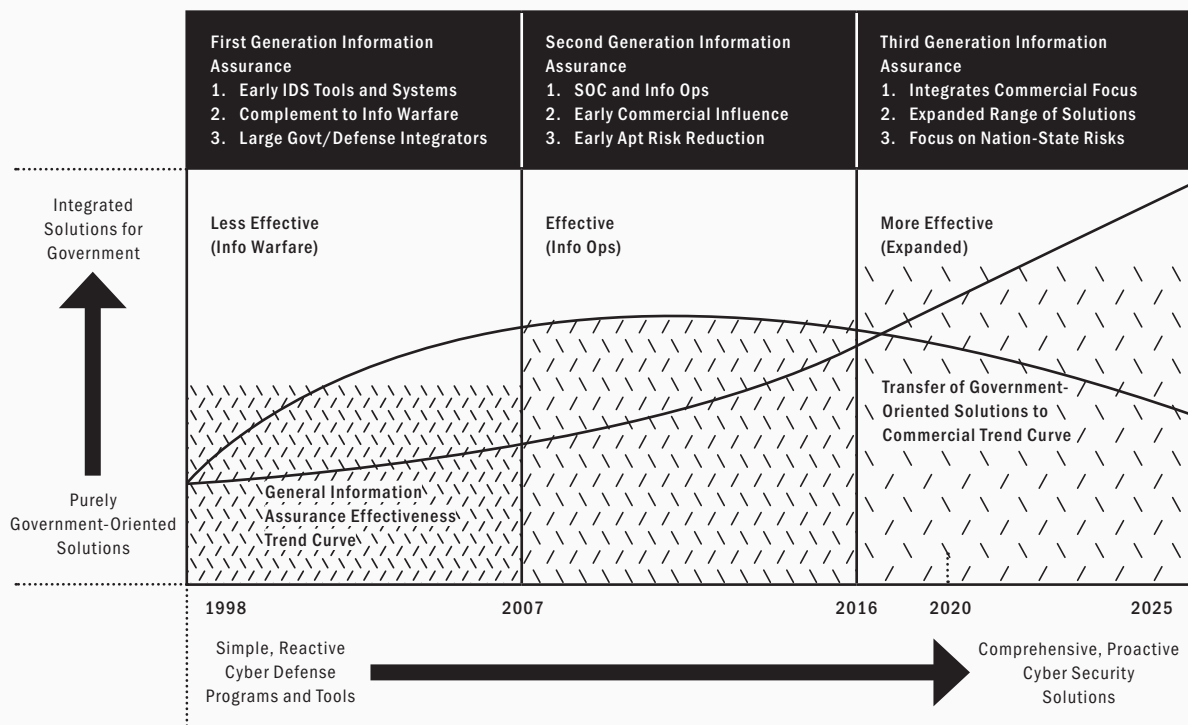


The most prominent trend in information assurance has included a shift from purely government oriented solutions – created and integrated specifically for government – toward more integrated solutions that include the best elements of commercial and government focused technology.

The military sector adopted the phrase information warfare to designate its offensive use of computers and networks to achieve tactical and strategic goals. The corresponding term information assurance emerged to designate a more defensive approach to achieving military goals. As a result, cyber security solutions – often from commercial teams supporting military customers – are now collectively referenced using this moniker.

Information assurance solutions have tended to be characterized by three specific aspects: First, they are designed to be easily consumed by military organization; this often includes ease of procurement through military purchase schedules. Second, they are often a combination of hardware, software, and professional services, which is not surprising given the unique needs of the military. Third, they are characterized by unusually high levels of assurance and trust.

Figure 1-44. Information Assurance Trend Chart



Many information assurance vendors in the defense industry have tried – usually unsuccessfully, to transfer their solution offerings to the commercial space. This would make sense on the surface, because banks and other large companies should covet the high assurance aspect of information assurance offerings. In practice, however, the unique marketing culture, lengthy sales cycles, and support processes have not transferred well.

The good news is that the government industry – across intelligence, defense, civilian, state, and local sectors – continues to have a healthy appetite for information assurance offerings from the best vendors. Since the barriers to entry in this marketplace are significant, including a willingness to put up with enormously long sales cycles, the companies offering information assurance products and services should see continued success and growth.

2020 Trends for Information Assurance

The most prominent trend in information assurance has included a shift from purely government oriented solutions – created and integrated specifically for government – toward more integrated solutions that include the best elements of commercial and government focused technology. The result has been a gradual progression from less effective early solutions in the first generation to more effective, expanded solutions today (see Figure 1-44).

In addition, early information assurance approaches included mostly simple, reactive cyber defense tools and programs – often based on intrusion detection. This has transitioned toward more modern, comprehensive and proactive cyber security solutions. Federal government customers in the US and abroad now enjoy world-class, highly effective offerings to protect national critical infrastructure from cyber threats.

The future of information assurance lies in even more advanced solutions to ward off information warfare actors who will use synthetic, imitation,

and intelligence-assisted attack methods to create warfare havoc. The resulting increase in military and national threat will require that information assurance vendors keep up with the latest and greatest defensive techniques including the effective use of AI and machine learning.

Cloud infrastructure and the advantage of zero trust security have also found their way into the information assurance equation. Nearly every military organization now covets the low capital requirements, high flexibility, and minimal costs of virtualized cloud services. Information assurance offerings thus include migration and support paths for government customers to utilize cloud capabilities – usually from the major providers such as Amazon and Microsoft.



Federal government customers in the US and abroad now enjoy world-class, highly effective offerings to protect national critical infrastructure from cyber threats.

MANAGED SECURITY SERVICES

The managed security services (MSS) sector will see more intense business changes in the coming years than any other aspect of the cyber security ecosystem. Initially created to remotely monitor the health and status of firewalls deployed to customer gateways, the MSS solution space gradually evolved to include a range of outsourced features marketed to customers today. Modern MSS vendors now extend far beyond device monitoring at a DMZ.

The canonical MSS architecture has been relatively stable for many years amidst steady growth of the industry. It includes systems – hardware or software – being deployed into a target customer environment, with logs, alarms, alerts, and other telemetry being pulled back to a virtual or physical security operations center (SOC) for handling. An MSS vendor might include status monitoring of deployed systems, or might perform monitoring with no management.

Telecommunications firms have been particularly well-positioned for MSS, simply because the management and monitoring functions match their normal telecom function so closely. This has allowed for easier business case approvals than in other firms with less applicable infrastructure. This advantage will continue for SDN deployments, where virtualized MSS will be an enormous growth engine – should telecom firms decide to follow this path.

The reason the MSS space will see so much change in the coming years can be summed up in one word: Virtualization. With enterprise teams now having the ability to create virtualized functions, on-demand, and in the cloud, the corresponding need for MSS shift considerably. Rather than having to deal with remote hardware issues, MSS teams will provide analysis and response using telemetry pulled from cloud based security tools such as SIEMs.

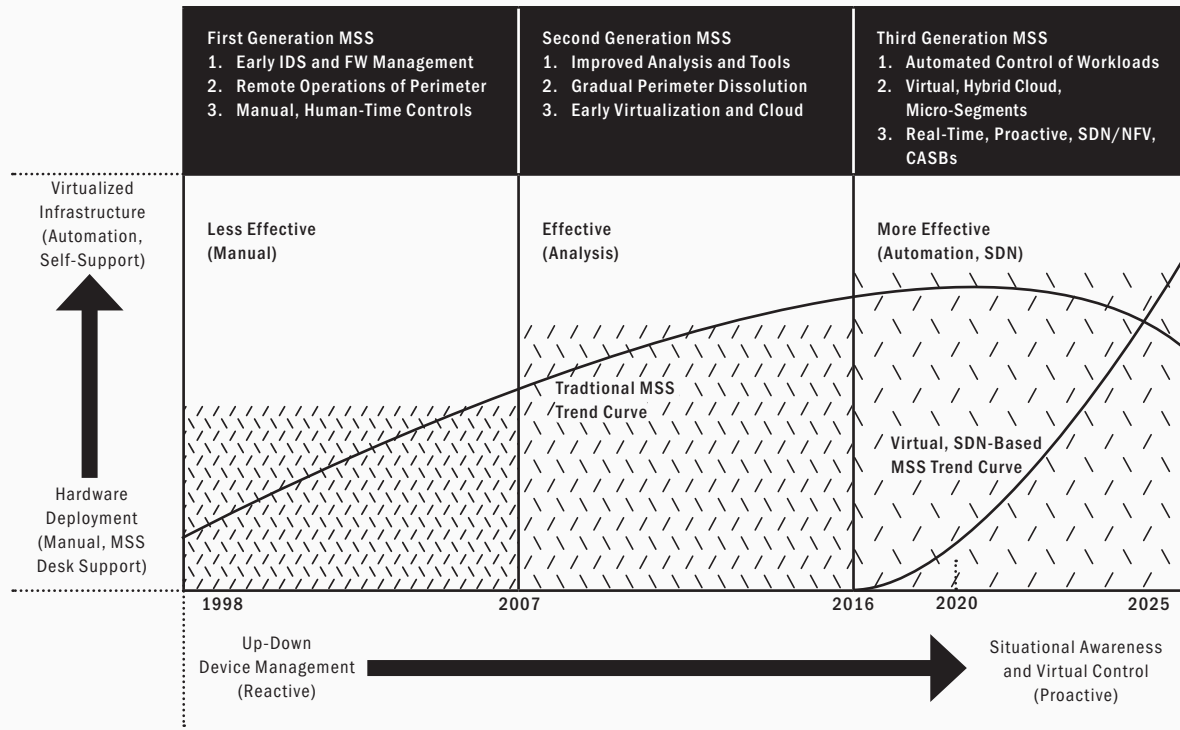
This might seem like a simple adjacency to their current function, but the existential risk emerges that major cloud providers will embed such analysis into their solution offerings. With the potential for automated, AI-based tools to support real-time security decision-making for subscribers, cloud providers might begin to disintermediate the MSS provider. This begs immediate attention from MSS vendors to differentiate and highlight their continued value.

2020 Trends for Managed Security Services

The effectiveness of managed security services (MSS) has transitioned from less effective early systems that collected intrusion detection alarms, through effective MSS offerings that began to include analysis in the monitoring function, into more effective current generation MSS that can handle virtualized deployments. The obvious shift coming will involve SDN-based MSS using dynamic service chains as the primary mechanism (see Figure 1-45).

A transition has occurred from pure hardware deployments with manual support and help desks, toward virtualized deployments of software that benefit from automated support with many self-service features. This transition to automation reduces costs for MSS teams, but also tends to improve the quality of support for customers. It

Figure 1-45. Managed Security Services Trend Chart



allows more on-demand provisioning requests and even modifications in some cases.

The up-down orientation of early management functions in the MSS has transitioned away from this health and status capability toward a more integrated, situationally-aware, and virtualized control of deployed systems. This results in MSS teams becoming a more capable security operations center (SOC) partner with an improved assortment of available services for business and government customers.

The most obvious and attractive such capability involves greater use of advanced analytics to detect indicators and to identify – and even prevent – cyber threats to customer infrastructure. These analytics have shifted from simple correlation tools to behavioral analytics with meaningful underlying mathematical models. Additional introduction of AI and machine learning tools to the MSS SOC will provide even great benefit for customers.

The future of MSS lies squarely in continued virtualization and a clear trend toward software-defined controls. Telecom firms with SDN-based infrastructure are best positioned to take advantage of this obvious match between MSS needs and dynamic service-chaining technology in SDN. Some question remains how aggressively existing MSS firms will pursue this high-growth opportunity. Ones that do not will see reduction in business growth.

The aforementioned threat to MSS vendors from the major cloud providers is also a major consideration for everyone involved. Buyers should spend time with their MSS vendor to understand why, for example, their SIEM monitoring capability will exceed the capabilities inherent in security resources from the cloud provider. This might be easy for an MSS to justify today, but one suspects that the challenge from cloud providers will grow.



AN INTERVIEW WITH PETER SMITH
FOUNDER & CEO, EDGEWISE

AUTOMATED SUPPORT FOR ZERO TRUST MICROSEG- MENTATION

EVERYONE agrees that the firewall-based perimeter no longer works. But the reality is that most enterprise teams maintain their perimeter as a primary control for audit, and as an on-going staple in their cyber security architecture. The main reason for this persistence is that meaningful roadmaps to alternative approaches have been elusive. Zero trust security is helpful, because it offers a vision for replacing perimeters, but enterprise teams still struggle to get moving.

Edgewise provides an innovative platform that supports transition to zero trust security based on the design of microsegmented workloads. This method offers real hope to security teams who covet the flexibility of a virtualized cloud environment. We spent time with Peter Smith, Founder and CEO of Edgewise, to learn more about how the company is supporting this important initiative and how enterprise teams are accelerating their architectures toward zero trust.

EA So many are talking about zero trust security today. Can you offer a brief overview of the concept?

PS The zero trust approach was created by John Kindervag while he was an analyst at Forrester Research. Trust in an IT system should be considered a vulnerability that can be exploited by adversaries to perpetuate data breaches and cause disruption to the business. A better way to approach security is to take the position of “don’t trust but verify” -- aka zero trust. This broad concept can be applied to many aspects of security which is why so many people are talking about it. For zero trust to be effective, it needs to be applied to specific domains of security as discussed in the answer to the next question.

EA How do zero trust security and microsegmentation work together?

PS The goal of microsegmentation is to prevent attackers’ lateral movement inside a company’s cloud and data center environment, protect business applications from compromise, and prevent data breaches. Traditionally, address-based controls (as used in firewalls) are used for microsegmentation. While address-based controls are good for perimeter protection, they unfortunately are not suited for protecting internal networks because attackers, after they have made initial landfall, can simply piggyback on approved firewall rules to move laterally. To provide better security, the zero trust networking principle is applied to microsegmentation. The internal network is assumed to be hostile. The most effective way to achieve security in this untrusted network is to verify the identity of all applications, users, hosts and workloads communicating on the network. Every communication must be verified and risk-based policies must be continually reviewed and monitored to ensure protection is always present.

EA Tell us about the architecture and set-up of your platform and how it supports enterprise teams moving toward zero trust.

PS Edgewise is a software as a service which makes deployment and management very simple.



Edgewise microseg- mentation happens in mere minutes— with just one click.

Edgewise uses machine learning to reduce the operational complexity typically associated with micro-segmentation. Edgewise policies are automatically built in its cloud service and are enforced by its agents running on hosts in the customer's environment. Edgewise is designed for high performance, scalability and resiliency. Edgewise ZT Auto-Segmentation supports enterprise teams by providing differentiated value: First, microsegments are created automatically with our 1-Click Auto-Segmentation. Legacy microsegmentation involves multiple steps that can take months. Edgewise microsegmentation happens in mere minutes—with just one click. From asset inventory to mapping data flows to deploying policies for enforcement, our microsegmentation is quick and simple. Second, policies are built (without manual intervention) by the Policy Recommendation Engine. Based on the identities of all communicating software on your networks, Edgewise eliminates risk by building policy recommendations using our patented machine learning technology. All software updates are captured instantly, meaning, your days of manual policy creation are in the past. Third, risk is reduced through policy compression. At the heart of Edgewise's policies is a model of every application connection across your environment. Using a combination of exposure, reputation, behaviors—and of course, software identity—Edgewise creates risk-driven policies that are 25x fewer than those of traditional microsegmentation tools. Fourth, security outcomes are provable with Exposure Analysis (risk analysis). Edgewise automatically builds a real-time application topology map of your environment based on the software and services communicating. As you apply segmentation policies, see how risk is reduced as attack paths are blocked and critical assets are protected with the highest level of confidence. Fifth, Software identity is verified through cryptographic attributes with Zero Trust Identity. All software in an Edgewise-managed environment is fingerprinted using a combination of cryptographic identity attributes. Software identity is the basis for every access control decision. Per our zero trust model, if software can't be verified, it can't communicate, regardless of previous permissions. This ensures the strongest level of protection for your workloads,

independent of network changes. Sixth, segments adapt to accommodate app updates and changes. Traditional microsegmentation requires ongoing manual policy creation and exception handling because it can't easily account for software changes and auto-scaling clusters. In contrast, Edgewise segments are based on the identity of communicating software and not the network itself. This means that segments can adjust as new applications and hosts are added, verified, and permitted to communicate. The result: hardened security minus operational burden and complexity. And seventh, security monitoring tools are enriched with app data via the API. You can feed your customized Edgewise application communication logs directly into your SIEM, which enables you to prioritize security events better, detect anomalous communication faster, and reduce alert fatigue, all while monitoring the health of your Edgewise implementation. Edgewise provides the broadest support across all environments, whether it is bare metal on premises, virtualized private cloud, the public cloud, or any combination thereof. Environments can be static or highly dynamic. Edgewise supports 10 distributions of Linux (with over 800 patch levels dating back to 2.6), Windows 7 onwards, and any Windows Server operating systems. Supported container environments supported include Kubernetes, Docker, and AWS Elastic Container Service (ECS). Edgewise's platform and products are API driven and can integrate with existing security tools and DevOps processes, enabling easy zero trust microsegmentation.

EA What is the role of DevOps in zero trust?

PS DevOps cares about speed, agility and scalability of applications from development through production. Traditional security is seen as a hindrance in achieving these goals. A well-implemented zero trust security solution can deliver strong protection without getting in the way of DevOps's operational goals. It is simpler for DevOps to work with a zero trust solution because security is decoupled from the complexity of the underlying network. Software-identity based security is more aligned with DevOps practices. A zero trust solution is built to be automated which enables

it to be easily integrated into a DevOps process. For example, application-centric security policies can be programmatically applied to new versions of software without requiring manual intervention. Zero trust policies can automatically adapt to and scale with application services regardless of where they are deployed—on-premises or in the cloud.

EA Any near- or long-term predictions about zero trust security?

PS In the near term, end users will demand vendors demonstrate and how they implement zero trust principles into their security product and prove the return on investment to the business. Vendors must provide concrete steps for end users to get started with zero trust. In the long term, practitioners will recognize that zero trust is a journey and will look to make it a general best practice.

SECURITY CONSULT- ING

The security consulting industry has been, and will continue to be a steady growth engine in our industry, with excellent prospects for small, medium, and large companies offering all types of professional services to businesses. The market for excellent security consultants will also expand from large enterprise into a much broader base, including business customers of all sizes and shapes – and this does not preclude the micro-business community.

Security services for cyber security range from high-level assessments of compliance, program effectiveness, and aggregate cyber risk – usually designed for executive consumption – to more detailed testing, probing, and even code reviews, usually designed for subject matter expert or working level consumption. It is accurate to imagine just about every possible permutation of service between these two ends of the spectrum.

It is not easy to isolate the components of security consulting as an industry sector, simply because so many adjacent areas of professional service exist. Information assurance for government, crowd-sourced vulnerability management, penetration testing, beach and attack simulation (BAS), and compliance/risk management are all consulting activities, most of which are included in the portfolio of offerings from security consulting firms.

Furthermore, the small barriers to entry to become a security consultant will ensure continued flux and turnover for this sector of the market. That is, any individual or group of individuals with some skill or persistence can establish a consultancy in cyber security. In addition, product vendors often see great opportunity to tighten their relationship with customers – or just add some additional cash flow – through the provision of consulting services.

Fees paid to security consultants will differ based on the type of work being done, location of the work, skill level of the consultant, and size of the enterprise customer. Typical rates in the northeast portion of the United States might be in the \$200-\$500 per hour range for expert consulting to a typical enterprise customer. Special projects might warrant higher rates and a long-term engagement might allow for a lesser hourly rate. (And yes, these are high fees.)

Small companies who require security consulting services, but who cannot afford these types of fees, must be creative. The Genius Bar at the local Apple retail store is not set up for security consulting, but many small businesses use them as such. On-line resources and free advice from ISPs, MSPs, and other vendors sometimes helps. This TAG Cyber Security Annual, hopefully, helps to fill this gap as well.

2020 Trends in Security Consulting

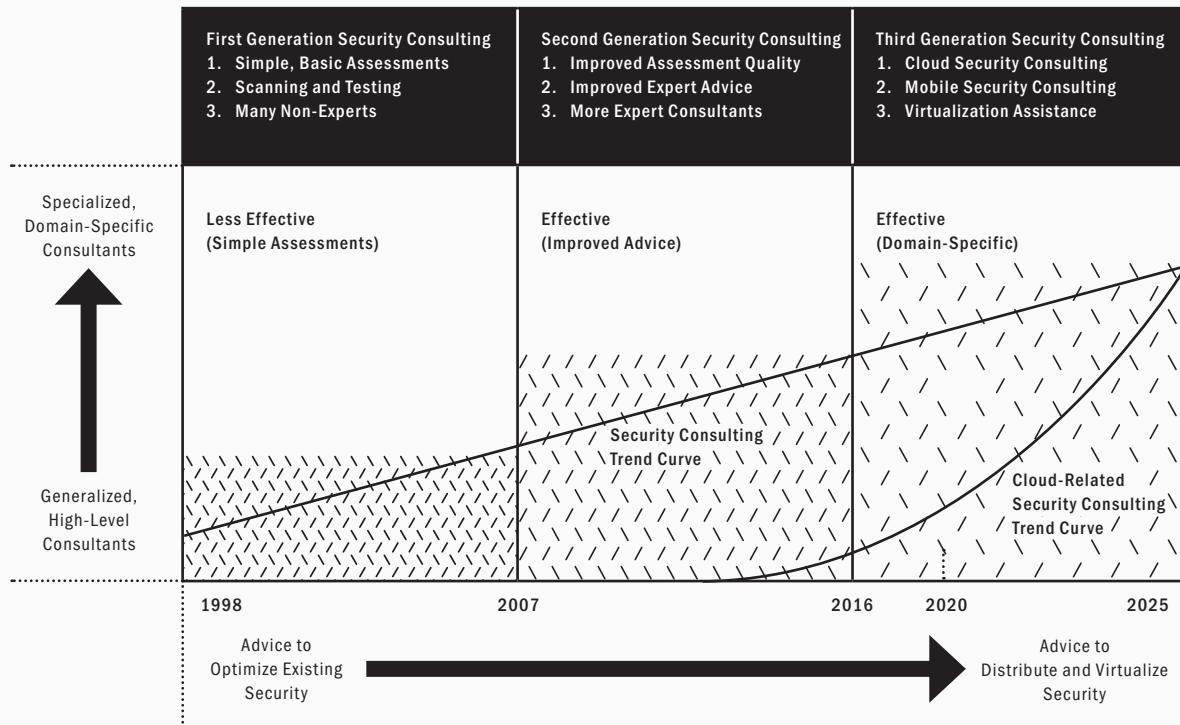
The effectiveness of security consulting services has transitioned from less effective simple assessments in the first generation from 1998 to 2007, through effective engagements with improved advice from 2007 to 2016. There are presently more effective security consulting services that include domain-specific advice on matters ranging from Internet of Things (IoT) to enterprise mobile security (see Figure 1-46).

The transition from generalized, high-level consulting toward more specialized, domain-specific consultants has mirrored the development of new domains, including critical infrastructure areas such as industrial control. The advice provided by security consultants has also transitioned from basic, general guidance on optimizing enterprise security toward architectural guidance, usually involving distribution and virtualization of resources.

It is this growth potential that also implies that buyers beware of non-experts touting their security consulting capability – often at low rates. When the demand for services increases beyond the ability of an industry to offer suitable solutions, then inevitably, groups will step in to fill the void. Be certain to check the credentials and background of your consultant before you decide to take their advice.

The future of security consulting lies in more advanced, domain-specific services, including advice and guidance for enterprise teams moving in the direction of full public cloud use. Risk-based services with focus on executive reporting will also be an enormous growth area as CISOs move up in the corporate hierarchy. The need to provide cyber risk information through consultation engagements will create considerable growth in this area of the industry.

Figure 1-46. Security Consulting Trend Chart





AN INTERVIEW WITH MIKE COTTON
SVP ENGINEERING, DIGITAL DEFENSE, INC.

NEXT GENERATION VULNERA- BILITY MAN- AGEMENT

FOR many years, managing vulnerabilities meant keeping track of the latest patches. This was especially depressing, because just as an enterprise team made sufficient progress with one patch, there would be two more to deal with. Luckily today, organizations can take a more holistic and proactive approach to managing vulnerabilities. This is done through automated enterprise visibility, scanning, and security architecture planning (and yes – patching is still part of the process).

Digital Defense provides a world class SaaS-based platform for enterprise vulnerability management – one that includes support for identifying, evaluating, and mitigating the most important cyber risks. Resident in the cloud, the Frontline platform supports both security and compliance. We asked Mike Cotton, SVP of Engineering from Digital Defense to help us understand the platform and how it serves customers.

EA What is meant by next generation vulnerability management?

MC Traditional networks are evolving. As more organizations adopt cloud, IaaS, and outsourced network resources, boundaries are becoming more elusive. Security platforms must adapt to provide the most comprehensive coverage and capabilities for new technologies and network architectures. Frontline.Cloud is designed to scale easily for distributed, hybrid networks. A fully SaaS native cloud offering, Frontline.Cloud introduces an intuitive, easy to use, accurate, and affordable vulnerability and threat management solution to serve as the cornerstone data set for cybersecurity programs. Today's malware and attacks are more sophisticated than ever. As a result, in an attempt to better protect their network, security professionals are implementing more security protections creating complex cyber security ecosystems and more siloed data. The security ecosystems can't perform at peak effectiveness if the data sets aren't shared. Digital Defense's vulnerability and threat data enriches and enables the security ecosystem applications to make informed decisions for each asset increasing the likelihood of thwarting an attack.

EA Do enterprise security teams require SaaS solutions for vulnerability management? How does this compare with a hosted solution?

MC SaaS solutions are attractive to many security teams as it reduces the overhead associated with maintenance and upkeep of a traditional on premise or hosted security solutions. This frees up additional resources for more focused activities like remediation and directly improving network security. SaaS solutions for vulnerability management are also more favorable when networks are distributed or the architecture is hybrid in nature, providing flexible deployments to ensure coverage of all network assets, regardless of where they reside, on site or in the cloud. As more organizations adopt cloud infrastructure as a service and outsource application hosting, native SaaS vulnerability management solutions become a highly desirable option, and in some cases, the only option.



**Today's
malware and
attacks are
more sophis-
ticated than
ever.**

EA Tell us about the range of services you provide enterprise teams. My understanding is that it includes valuable capabilities such as web application scans and penetration testing.

MC Digital Defense has been helping organizations determine their security risk posture for almost two decades. We offer an industry recognized, award winning fully integrated cloud vulnerability scanning and management solution leveraging patented proprietary scanning technology, a fully capable modern web application scanning solution, automated threat hunting solution and analyst-driven penetration testing. We like to think like an attacker and simulate an attack and provide the tools and information to users to secure their networks against those tactics. Frontline.Cloud is fully integrated into popular security ecosystem platforms. With an industry standard REST API and integrations with industry leading communication fabrics, like Palo Alto Cortex and Cisco ISE, security professionals and further enhance their security operations with interconnected enriched data sets to improve ecosystem performance.

EA How does your Frontline.Cloud platform work? Can you provide us with a high-level view of the architecture?

MC Frontline.Cloud is the native SaaS platform providing access to Digital Defense's Frontline family of security offerings. Digital Defense's scanning technologies intelligently audits external and internal network systems comprehensively for vulnerabilities to evaluated security risk. Frontline.Cloud fully resides in Amazon's AWS cloud. External scans originate from our cloud appliances to evaluate external and cloud assets. Internal scanning appliances, hardware or virtual, are deployed in client networks to securely assess internal assets and transmit findings to the Frontline.Cloud platform where the data can be managed. Our cloud native architecture is advantageous to both the client and Digital Defense; allowing clients to quickly implement a solution in traditional, cloud or hybrid environments with zero capital requirements and very little

overhead; as well as permitting Digital Defense to offer a global footprint to scale to clients of any size and address data residency requirements.

EA Any near- or long-term predictions about vulnerability management and cybersecurity in general?

MC We're already at a point where the human operators can no longer shoulder the load alone effectively and efficiently enough to counter all potential attacks. There will be a shift from report and fix to more real-time remediation workflows, assisted by automation to fix or mitigate on the fly. The speed and automation of attacks against the scale and scope of networks is too extensive to protect with delays of days or weeks to address flaws. Security ecosystem platforms have to communicate and be capable of producing a smart automated real-time response as incidents are detected or occur based on broad human operator guidance. Digital Defense is already starting to lay the groundwork for real-time security intelligence through automation.

47

SECURITY

CAREER

SUPPORT

Providing and funding programs of security career support might appear an extravagant luxury for executives and practitioners, but nothing could be more distant from the truth. If enterprise managers would like to retain world-class staff, while also ensuring a constant in-bound stream of new talent for their cyber security groups, then they will have to build effective programs for supporting the careers of new and existing security staff.

Such programs should include heavy emphasis on learning, skills assessment, and coaching – all of which are growing areas in cyber security professional services. But security career support also requires a good working relationship with the best recruiting firms offering services to growing teams. External recruiting is sometimes viewed as evil, often coupled with the practice of firing existing staff; but more often, it involves finding and adding talented individuals.

The two canonical approaches to recruiting in our industry have been so-called contingency recruiting and retained search. In the contingency case, the recruiting company works on a negotiated percentage for staff that are located and ultimately hired. In the retained case, the recruiting company is paid an up-front fee. Presumably, retained search results in a more comprehensive analysis, but no scientific studies exist to substantiate this view.

The increasing recruitment of freshly graduated computer science majors to cyber security has been a growing aspect of the industry, and is a welcome trend. Most computer science programs include some degree of introduction to cyber security, and younger employees tend to be savvy in their understanding of modern technology, cloud and mobile services, and cyber security services.

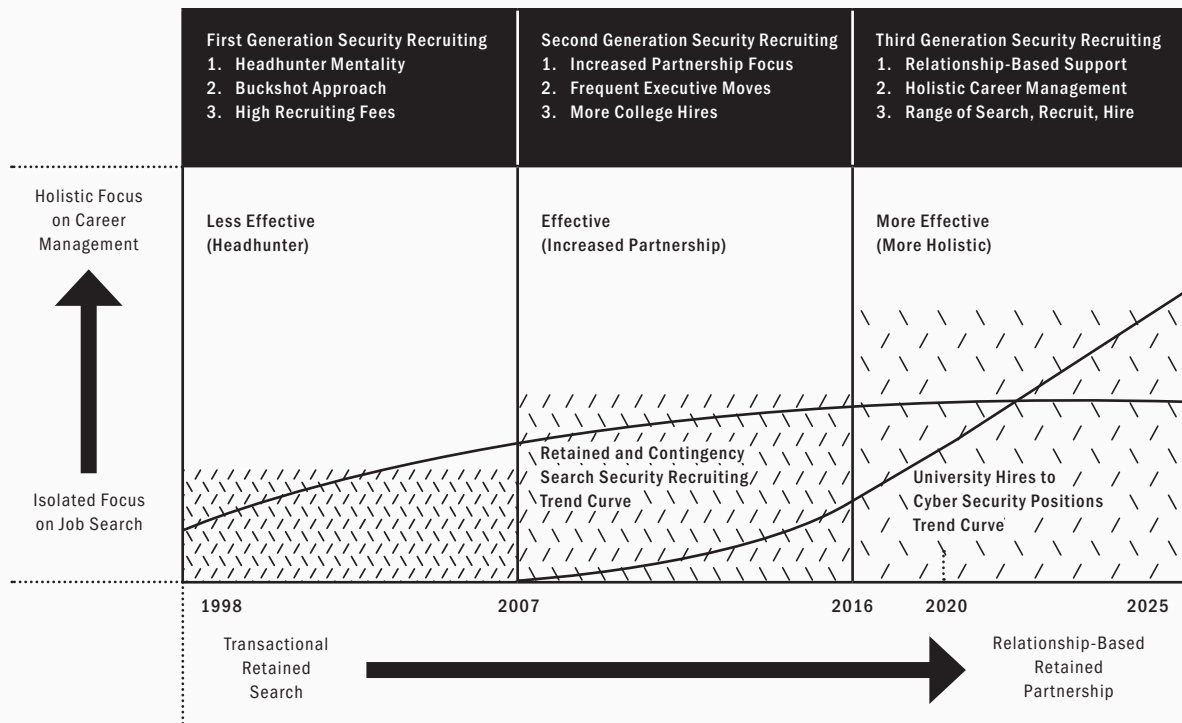
More scientific support for career decision-making is beginning to emerge gradually. TAG Cyber, for

example, now provides an on-line Myers-Briggs-type personality trait assessment tool called CyberEXP that helps professionals better determine their innate traits for cyber security. One can only hope that professionals have access to more tools and resources that can help them optimize career decisions in our industry.

2020 Trends in Security Recruiting

First generation security recruiting from 1998 to 2007 was less effective and involved mostly headhunters with sometimes unsavory practices. Second generation security recruiting from 2007 to 2016 was characterized by effective practices with increased partnership focus. Current generation security recruiting is more effective and includes a holistic approach to executive, middle management, and new hire recruiting for cyber (see Figure 1-47).

Figure 1-47. Security Recruiting Trend Chart





Eberhard Grossgasteiger, Unsplash

Security recruiting has shifted from an isolated focus on specific job search toward a more holistic focus on career management. This is also characterized by a shift from transactional retained and contingency search deals toward a more relationship-based approach followed by the security recruiting firms as well as enterprise teams looking to build their talent from both internal and external sources.

One trend that works slightly against the security recruiting business has been a slight, but growing trend toward internal development of talent. Early generation security executive positions had no younger bench to draw from, but this is different today. Most enterprise security teams now have several years of experience as a group and this will create internal candidates for new executive positions.

The future of security recruiting is all about holistic relationships that are less transactional and more career-focused. That is, the best cyber security recruiting firms will take the time to understand the long-term goals of their customers and will tailor their support and services to meet those needs. This might even include assistance identifying newer employees directly recruited from their university programs.

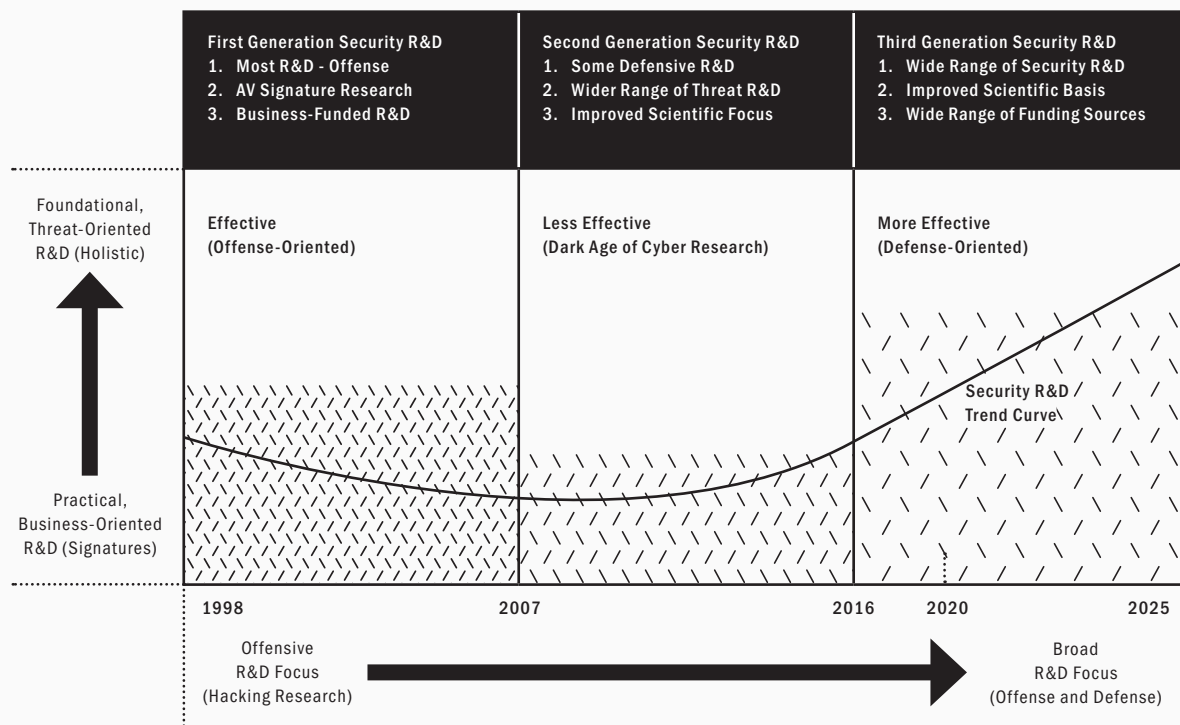
Technology and apps will also play vital roles in the coming years for security career support. That is, AI-based decision support will help managers and other practitioners weigh more factors in making decisions about the best job or career given their strengths and interests. This might seem futuristic, but with people using technology and apps to make decisions about dating and other personal issues, career assistance would seem a likely near-term step.

SECURITY R&D

To date, the security research and development (R&D) community has existed within academia, federally-funded research and development centers (FFRDCs), university affiliated research centers (UARCs), government and military agencies, and other non-profit organizations. It remains unclear why more successful commercial opportunities have not emerged in the marketplace for pure and applied research teams providing cyber-oriented R&D for customers.

The value of security intellectual property (IP) has certainly not shrunk in recent years, so this relatively quiet attention to security R&D as a commercial pursuit is surprising. Nevertheless, any commercial organization that would like to research some aspect of security will have to turn to internal resources, academic organizations, or a non-profit. The defense industry is perhaps an exception, with many system integrators including R&D as an offering.

Figure 1-48. Security Research & Development Trend Chart



Note that by security research, we do not mean investigation of vulnerabilities or black hat pursuits of finding exploits in systems. While many refer to this as research, we choose to call this vulnerability management and penetration testing. Finding errors in someone's bad code or holes in someone's horrendous system design just doesn't seem to fit the bill in terms of what we would call world-class cyber security research. It's important, but it's not research.

2020 Trends in Security R&D

The early days of computer security in the 1980's and 1990's included quite a bit of good research in trusted computing design, high assurance computing, security policy modeling, information flow mathematics, and on and on. It was a substantive component of the industry, as evidenced by the degree of focus afforded such research concepts in the earliest major computer and information security conferences (see Figure 1-48).


In the 1990's, the research environment downshifted as commercial interests overtook research interests – except in academia and non-profits. A second generation ensued which we might refer to as the Dark Age of Cyber Research. During this period from 2007 to 2016, all advances in security seemed connected to a start-up or commercial engagement, simply because the business prospects of security were too irresistible to ignore for most innovators.

The present generation of cyber research will shift back into focus with a more defensive-orientation than the original offensive focus that characterized many earlier efforts. With most organizations, especially in government, now beginning to understand the value of pure and applied research, it should be easier for research teams to procure funding and even commercial profit in their engagements.

The future research focus areas for security will track the major advances of the day – including

autonomous computing, artificial intelligence and machine learning, increased automation of industrial control systems, smart medicine, and on and on. In each of these areas, foundational research is required to provide a suitable base on which to design and building meaningful operational systems.

In addition, as computer science hopefully become more scientific (with laws and repeatable experiments), one might expect to see a more professional research focus in cyber security. The good news is that excellent questions have emerged for cyber security that require expert investigation, such as the role of quantum computing in cyber, methods for improving software quality and correctness, and establishing the boundaries of AI for solving cyber problems.



Finding errors in someone's bad code or holes in someone's horrendous system design just doesn't seem to fit the bill in terms of what we would call world-class cyber security research.



AN INTERVIEW WITH ART GILLILAND
EVP & GM ENTERPRISE PRODUCTS, SYMANTEC

WORLD-CLASS SUPPORT FOR ENTERPRISE SECURITY

FROM the earliest days of our cyber security industry's existence, Symantec has been at the forefront of business and consumer protection, helping to maintain protection of systems, applications, software, and networks. Today, Symantec has reached iconic status with a rich portfolio of security solution offerings, all of which have evolved alongside the enterprise and technology industries, helping to protect everything from cloud infrastructure to mobile devices.

We were fortunate to spend time with Art Gilliland, EVP and GM of Enterprise Products at Symantec, to gain insights into the direction of our industry. With such a unique vantage point as an industry leader, Symantec must address challenges in every sector with organizations of every possible size and shape. As such, it stands to reason that the company would have useful insights for all of us. Below is a brief summary of our interview with Art Gilliland of Symantec.

EA Like so many iconic companies, Symantec has obviously had to evolve its technology and solutions as the world has undergone so many changes. Can you talk a bit about how you've evolved?

AG It's true that the company has had to evolve to meet the changing security needs of businesses, and in line with that, we've evolved our solutions in a number of important ways. The first step in this evolution has involved innovation. Sophisticated methodologies and monetization of attacks have made the stakes higher than ever. Symantec's combination of internal innovation and acquisition enables us to field the best-in-class infrastructure security for endpoint, network and web gateways, email, and cloud applications. The second aspect of our evolution is through integration. We've seen businesses struggle with the fragmentation of their security stack. By integrating all of our best-in-class technology, we've reduced cost and complexity for our customers. This is highlighted by our Information Protection suite, a set of technologies that identifies sensitive data, secures it with access policy and encryption, and monitors ongoing risk of data use. By providing a single set of policies, an incident console and risk analysis across network, email, endpoint and cloud apps, we are fully adapting to the very dynamic world of cloud. And the third aspect to our evolution involves solutions through our open ecosystem of partners. With a robust set of open API's and our Technology Innovation Partner's Program (TIPP), we've completed 250+ integrations with 120+ partners in the last three years. This extends the benefits of our Integrated Cyber Defense beyond our own technologies to further reduce the cost and complexity of cyber security. Finally, and perhaps most importantly, we've integrated our powerful set of security technologies to enable customers to migrate safely to cloud. Best in class CASB and software defined perimeter (SDP) technologies enable new security models to access SaaS, IaaS and private cloud apps. Workload protection and assurance secures IaaS applications and DevOps accounts. And cloud-delivered security stacks for web and email – services with Proxy, demarc, sandbox, DLP, threat isolation and other capabilities – all ease adoption and operation and offer



We've integrated our powerful set of security technologies to enable customers to migrate safely to cloud.

comprehensive protection via a fully consolidated web access and email cloud service.

EA With so many security products and solution offerings, is it difficult to prioritize your investment in new capabilities. What are the factors that drive your strategy?

AG When it comes to prioritizing our investments, we work with our customers to understand their changing environment and then tap into the innovation that comes from our development architects as well as from emerging technologies in the marketplace to understand where our priorities need to be. We also have the world's largest civilian investment in threat research, and that gives us a unique view into the evolution of threats which further helps us understand where we need to invest in our solutions. All this, combined with our huge R&D organizations, helps create a strategy for investment that has led to continuous innovation in areas like cloud, data protection, endpoint and network threat protection.

EA How does the research from the Symantec Research Lab find its way into the products and solutions you offer customers?

AG The Symantec Research Lab (SRL) is constantly working on a myriad of projects, looking for the opportunities that they present to build on the capabilities within our standing products as well as to form the basis for new offerings. Not all the research coming from the Lab will make its way into our products, but all of it ultimately leads to the evolution of cybersecurity protection for enterprises. It also contributes to the high level of innovative thinking that drives all the work we do. A typical example of how a technology might find its way into our products via the SRL is the work we've done around tracking the trillions of events we capture from our data feeds. Recently, members of our product teams came to the SRL asking for a new approach to keep up with these events. This led us to train a system based on our leading threat analysts and massive civilian cyber defense dataset. Using a technique called active-learning within the ML toolbox, we were able to help our customers fix

twice as many incidents with the same workforce. And because of how this is delivered to our customers, it is an immediate benefit to them. Another example is how we deployed our User Behavior Analytics (UBA) in conjunction with AI to uncover suspicious activities when our CASB team came to the SRL asking how we could help their customers uncover Insider Threats when there was no specific pattern of behavior to look for. Without UBA and AI, finding these suspicious activities was like looking for a needle in a haystack. With the SRL AI solution, however, our CASB customers are now able to discover structural anomalies over time that are incredibly performant while also avoiding false positives.

EA Is there a secret to how Symantec customers can integrate existing or third-party solutions into their enterprise security architecture?

AG The secret, if there is one, is in our open ecosystem architecture that has led to our highly successful Technology Integration Partner Program (TIPP). Through this program and by leveraging our APIs and our ICDx integration framework, our Symantec team has been able to develop key relationships with third-parties to extend the value of our integration efforts, thus driving down the cost and complexity of cyber defense for customers.

EA What are some of the newer offerings in your platform and how do you see your focus evolving in the coming years at Symantec?

AG Symantec's platform offering is already far ahead of the rest of the industry in so many areas, and we're driving innovation to extend that lead. We're focused on making our technology simpler to purchase, utilize, and adopt. Our platform offers a complete Endpoint Defense with EDR and coverage for mobile platforms; a full web security and email security stack in the cloud; and the most complete information protection everywhere. It's about extending the state of the art to deliver the most effective integrated cyber defense. It's also about making it simpler for customers to migrate securely to the cloud and to transform security operations everywhere. That's our aim.

**SECURITY
TRAINING
& AWARE-
NESS**

Security training can be delivered as general security awareness for anyone in contact with organizational assets, or as expert training and certification for practitioners who need more advanced education in cyber-related technology, procedures, or policies. Both approaches are moving toward more creative, hands-on, multi-media training, often delivered virtually, in ways that support the most flexible learning environment.

Security awareness is an efficient form of enterprise risk reduction, simply because user behaviors contribute directly to the success (or failure) of many different security attacks. Even the most advanced persistent threats (APTs) from nation-state actors will generally include exploitation of human weaknesses. So, training employees to be savvier, especially about email phishing probes, is an excellent investment.

Getting the right message to employees can be difficult, simply because people are busy, and most security awareness programs are crushingly dull. The use of situational video, cartoons (such as the Charlie Ciso series from TAG Cyber, which is being tailored to awareness programs every day), and other humorous material has increased the effectiveness of getting proper security messages to employees, and even consumers. Let's hope this continues.

Expert training and certification in cyber security also provide good returns on investment, although the quality of the training will vary. Security conferences, such as the massive RSA gathering each year, generally include many professional training opportunities. Increasingly, though, courses tailored to specific disciplines such as firewall administration or cryptographic protocol management, are available for practitioners.

2020 Trends in Security Training

First generation security awareness programs were less effective, generally offered as stiff directives from early security practitioners with weak training skills. Second generation security awareness became effective as early use of video and some on-line options were made available. Third generation security awareness programs should be expected to become more effective, with maximal use of creative, multi-media training options (see Figure 1-49).

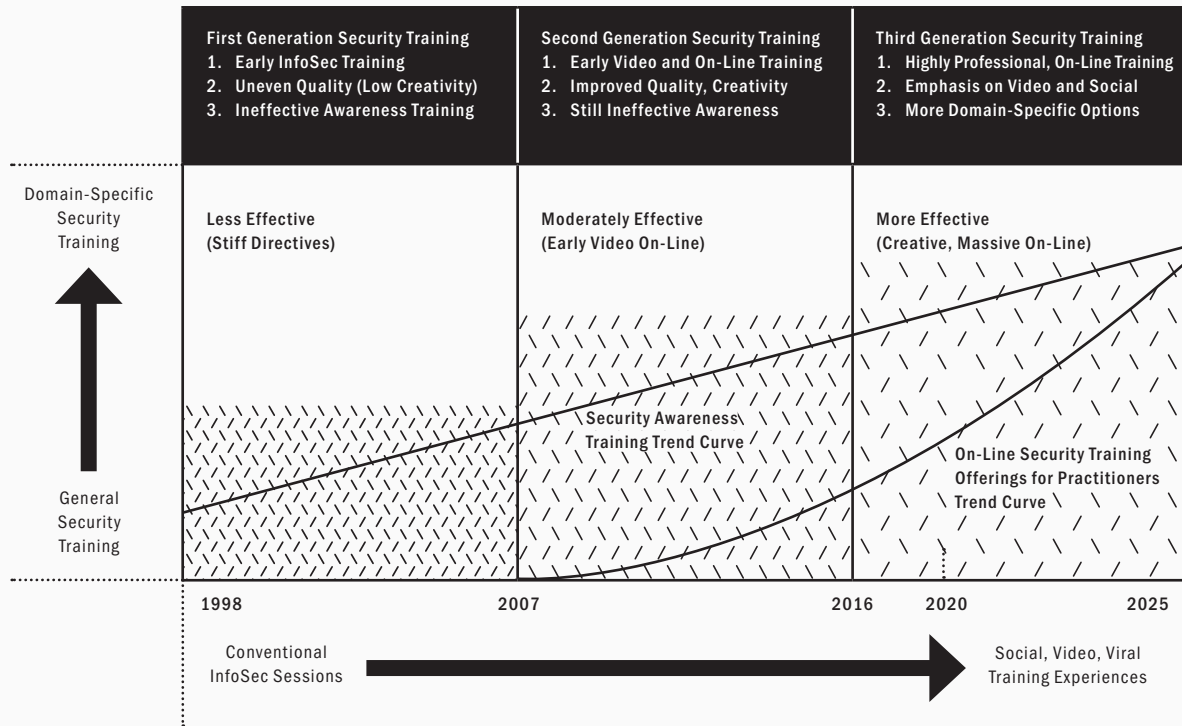
Expert training and certification in security was less available in the early years, mostly obtained through conferences, books, and other materials. Good on-line options for experts who need domain-specific training in cyber security have begun to grow dramatically, and this represents an excellent advance for practitioners. Virtually every aspect of cyber security technology, procedures, and practice have great options for on-line learning today.

The trend for both awareness and expert training as been from general coverage toward more focused training on domain-specific areas. Additionally, the early conventional InfoSec sessions of the 80's and 90's for general and expert audiences, have been replaced with social, viral, and video training options. Certifications continue to lag somewhat, although the Certified Information Systems Security Professional (CISSP) is still popular.

The future of training for both general awareness and expert learning involves even more creative options for video and social learning, as well as greater use of massive open on-line courses that allow learners to progress at their own pace. The quality of these courses has steadily increased to the point where some match the best available options from even the best universities.

Expert cyber security training will also need to evolve in the coming years, presumably toward greater domain specificity. For industrial and IoT applications, in particular, the training will need to combine the best elements of industrial engineering with computer science. This will not be easy, because the respective disciplines have been so separated to date. But commercial interests and needs will prompt convergence in training.

Figure 1-49. Security Training Trend Chart





AN INTERVIEW WITH RYAN COREY
CEO & CO-FOUNDER, CYBRARY

CYBRARY'S UNIQUE APPROACH TO CYBER CAREER LEARNING AND SUPPORT

THE challenge of educating and training cyber professionals has not been traditionally met through obvious means. Courses, conferences, books, on-line materials, and other resources are certainly available, but clear methods for vetting the educational quality of the experience have not been readily available. This has caused most cyber professionals to piece together a self-learning plan through word-of-mouth, on-line reviews, and ad hoc judgment.

Cybrary addresses this void with a world-class curriculum of on-line and instructor-led training solutions and career resources for the cyber security professional. Ryan Corey, CEO and Co-Founder at Cybrary, took us through the various offerings at Cybrary. We were interested in how professionals can take advantage of Cybrary curriculum to optimize their careers toward mastery of a specific technical or compliance interest, or through advancement into senior management.

EA Tell us about Cybrary. What types of learning solutions do you offer?

RC Cybrary is a security enablement learning platform that enables organizations with the tools they need to assess, develop, and measure their technical organization's security skills. This, in return, provides the ability to identify gaps, increase efficiency, and reduce risk. Our differentiated creator network of over 2000 unique contributors, positions Cybrary to deliver our customers the fastest moving catalog in the industry, housing more relevant and up-to-date content than any other provider on the market. We have more than 2.5 million professionals on the platform, including 96% of the Fortune 1000.

EA What's the role of learning in cyber career management?

RC At the University of Virginia, for example, students live by the credo of Thomas Jefferson who once said "you are never a senior in knowledge." Learning is a lifelong aspect of anyone's career and life, not just cyber. With the expansion of attack vectors and increase in endpoints, there is a desperate need for just in time, continuous learning across the profession at every level.

EA How hard is it for cyber professionals to maintain or develop cutting edge skills?

RC It's really hard. There are several reasons that employees are unable to develop the latest skills. The hardest aspect is time: According to ESG-ISSA although 93% of cybersecurity professionals "must keep up with their skills or else the organizations they work for will be at a significant disadvantage against cyber-attackers, 66% claim that cybersecurity job demands often preclude them from skills development." This puts cyber professionals at a terrible disadvantage to deal with the latest attacks and to continue developing their skills.



We can both spark the innate curiosity in technology of these individuals and improve security across the organization.

EA Do you work with your students to develop a customized learning program?

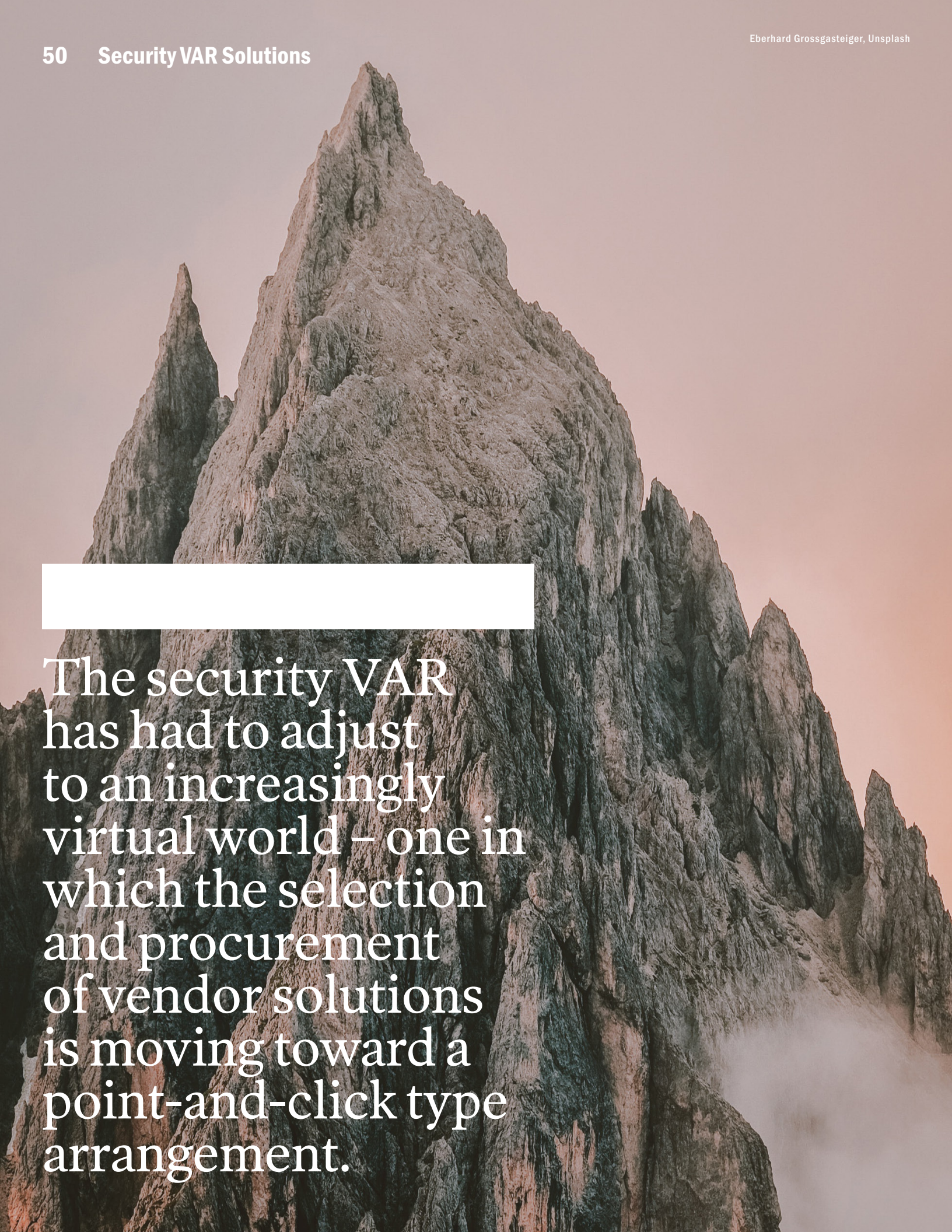
RC Yes, we have two ways of offering customized career paths. The first is our insider pro program, which is our consumer product. This provides pathways for several careers across red team, blue team, management, and advanced practitioners. We combine a best in class curriculum formed by the best practitioners in the globe. The second is our business product. We work with hundreds of businesses to develop the careers of their workforce. We have extensive curriculums across every work role in the NICE/NIST framework which provides a business with everything they would need. Also, if we do not have something in our catalog that is of need, we have several thousand creators on our site that provide us with the best content in cyber today. The combination of our vendor providers and our massive community of creators gives us the largest and fastest growing catalog in cyber today. Over 75% of our content has been created in the past year, which shows that we are keeping up with the latest trends in the space.

EA What do you see as the future of cyber security training and career development?

RC Cyber security training will be across the entire organization. This is a term that we call security enablement. Individuals across the organization will be empowered to incorporate security into their daily interactions with business systems. The security department will no longer be the separate department it is today. This full integration of security should help organizations reduce cost and operate more efficiently. The key areas employees across an organization need to learn are cloud security and data science, and how these fit directly into their day to day operations. As we empower more individuals across the organization to incorporate this key knowledge, we can both spark the innate curiosity in technology of these individuals and improve

security across the organization. If you are an expert in the field, you have a responsibility to guide this movement. There are too few professionals and leaders in the profession today for what faces us. Therefore, solving individual problems is not enough. We need more leaders to join our community and mentor the next generation of cyber and IT professionals. We need more great instructors to create learning that will guide the education of all professionals. This massive problem will take a community that supports each other every step of the way. Cybrary is the only platform that is positioned to offer this community at scale.their real-time security efforts on the much more vulnerable inner layers: Application and Data.

SECURITY VAR SOLU- TIONS



The security VAR has had to adjust to an increasingly virtual world – one in which the selection and procurement of vendor solutions is moving toward a point-and-click type arrangement.

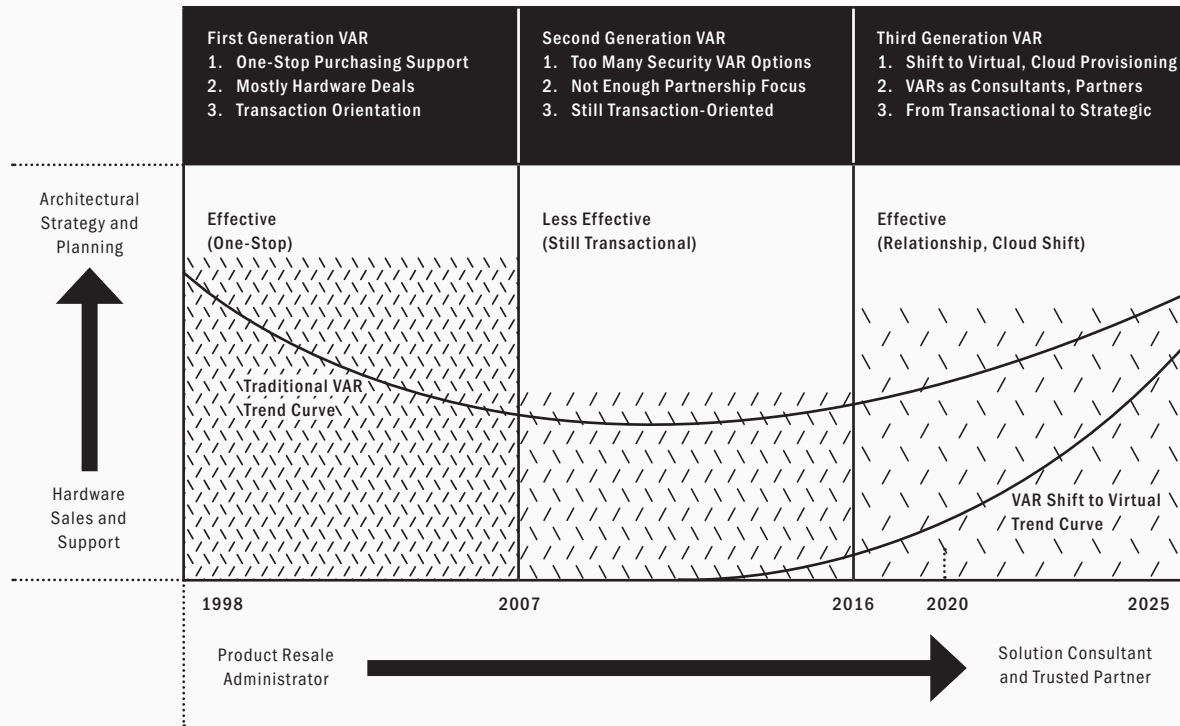
The earliest purpose of the security value added reseller (VAR) was to assist with the selection, procurement, payment, maintenance, integration, update, support, and replacement of cyber security solutions for the enterprise. This function was particularly valuable in the context of the relatively lengthy cycle times for introducing new hardware and software-based systems such as firewalls and intrusion prevention systems.

The original benefit for vendors was also quite powerful, in that the best security VARs offered channel opportunities that many smaller start-ups couldn't otherwise fathom. Even larger vendors benefitted from the expanded channel, especially in remote regions of the globe where a local VAR knew the language, culture, and customs of potential enterprise customers of their supported vendor products.

More recently, the security VAR has had to adjust to an increasingly virtual world – one in which the selection and procurement of vendor solutions is moving toward a point-and-click type arrangement. This is both a challenge and an opportunity for the best VAR teams, because with this general transition away from hardware purchases (not all, obviously) will come the need for good professional services to guide enterprise teams toward the right approaches.

An important area in which security VARs are advised to focus is the transition to cloud-based services for most enterprise team. Selecting and integrating the best available tools for micro-segmentation, CASB integration, cloud-based IAM, and cloud compliance will require the trust and support that security VAR teams have already established with their clients. This will give the security VARs an advantage over many existing security consulting teams.

Figure 1-50. Security Value Added Reseller Trend Chart



2020 Trends for Security VARs

The effectiveness of security VARs during the first generation was based on one-stop shopping as part of the enterprise relationship. This was followed by a recent second generation of security VARs, where too many companies were vying for a reduced number of transactions, with weak focus on emerging cloud systems and virtualized data centers. The emerging third generation will be effective and focused more on relationship-based work (see Figure 1-50).

A transition has occurred in security VAR solution provision from mostly hardware sales and support toward emerging support for hybrid cloud architectural support in the areas of strategy and planning. An additional transition has occurred from the administration of product resale, toward the emergence of security VARs as solution consultants and trusted partners for enterprise security teams.

The security VAR will continue to see a massive shift toward relationship-based consulting with higher end services at higher margins for companies moving toward hybrid cloud arrangements. This is good news for the best security VARs who will seize the opportunity, but terrible news for any security VAR that is determined to resist change and cling instead to older business models that will not work in a hybrid cloud-oriented world.

In the end, the needs of the enterprise security buyer will inevitably change with virtualization and cloud, so the best VARs will focus on changing accordingly. As suggested above, the deep relationships between good VARs and their customers, of every size and in every sector, will create an excellent opportunity for consultation, advice, and guidance on everything from architecture, to policy, to security operations.



AN INTERVIEW WITH BRUCE FLITCROFT
CEO, TENFOUR

PRIVATE DO- MAIN, SECURE GLOBAL IT INFRASTRUC- TURE

NETWORK security requires attention at all levels – and the underlying infrastructure components must be carefully addressed for higher application levels to be protected. Increasingly, enterprise teams are opting for a model in which network functionality is provided on a subscription basis via an ‘as-a-service’ offering. If done properly, this approach results in cyber security being embedded in the lower levels of the network – and all security experts know this to be the strongest model.

TenFour has been offering enterprise customers a portfolio of global IT infrastructure and network capabilities in a subscription model. Their unique subscription service automatically includes advanced cyber security features, which is attractive because it is both embedded and also efficient. We spent time with Bruce Flitcroft of TenFour recently, and asked him to provide an update on this important IT and security approach and how it is being applied to support and protect modern enterprise teams.

EA Your team has pioneered so-called IT infrastructure as a service. Tell us how this works.

BF We build and own exceptional, private domain global IT infrastructure that is simplified, has fewer defects, and costs less to operate than traditional models. We’re not a cloud computing company, but we’ve taken the cloud model and extended it beyond compute and storage to core components, platforms, and services, such as routers, switches, wireless access points, IP phones, IoT devices, and so much more which has traditionally been “uncloudable.” Our customers pay one simple subscription price per month.

EA How easy is it to streamline IT infrastructure security into your service model?

BF By incorporating best practices at every stage (Plan, Build & Run) within each of our platforms we can ensure that all the components are up to date and secure. TenFour has established a Reference Architecture for each of the infrastructure platforms and continually evolves and tests against use cases and configurations to insure a best in class service. We also engage in a set discipline to test and deploy security patches and OS upgrades as needed and in a timely manner.

EA Tell us about your cloud-first strategy. One would presume that most of your customers must be operating a growing portion of their infrastructure in the cloud.

BF The move to the Cloud and cloud-like models is inevitable. For the last decade, businesses in almost every industry have shifted away from traditional product delivery models to subscription-based services. The subscription e-commerce market has grown by more than 100 percent a year over the past five years. These services have redefined customers’ experiences, giving them what they want and on their own terms. Rather than putting the focus of the business on the ‘product’ or the ‘transaction,’ subscription economy companies live and die by their ability to focus on and serve the customer. We saw this shift coming in 2012 and that’s why we developed the first IT



The move to the Cloud and cloud-like models is inevitable.

infrastructure Cloud model. But for years, we were running two business models: our IT subscription service (including Transitional Managed Services) and our VAR service. We recognized that the future of IT was quickly abandoning the VAR type of model. That's why we announced in June that we are shifting the business away from VAR to focus all of our resources, personnel, and operations on delivering IT infrastructure as a service and building out a robust customer success program that focuses on exceeding customer business goals. Our model delivers the flexibility, reliability and security that help power digital transformation and build a foundation for successful business outcomes. We're excited by this shift and to lead the charge toward more innovative enterprise IT solutions. Not only because of the prospective benefit to our business, but because of what it means for our customers and the IT industry at large.

EA How does the TenFour team keep up with the latest vulnerabilities, patches, and other security issues on behalf of clients?

BF Our NetSec service provides the first line of defense by monitoring for a wide array of threats, including malware, intrusion, DDoS attacks, and internal traffic anomalies. By using a variety of industry-trusted services and products, we provide up-to-the-minute protection. Plus, we minimize the number of equipment variables and standardize our security measures across the IT infrastructure we provide, so your surface attack area doesn't expand even as your business grows and your infrastructure extends out to the IoT edge. To get to you they need to go through us. We provide all the Network layer security and most of the Host/System layers. Our service is embedded with AAA, NetFlow, SGT, 802.1X, patch management and syslog—these are included as core capabilities. Additional advanced cyber security capabilities - Next-Generation Firewalls, Enterprise Security Management Platform (ESMP), Security Visibility Platform (SVP) and Domain Name Services - can be added as IT Units (ITU) in the consumption-based model. With our network security services, our customers' underlying network infrastructure contains the requisite protections so that their teams can focus

their real-time security efforts on the much more vulnerable inner layers: Application and Data.

EA Any near- or long-term predictions about IT infrastructure? Do you expect to see more companies move to a subscription service?

BF Enterprises have focused on first defining their Digital Strategy; now it's about execution and subscription services are certainly on the rise across industries from entertainment, to insurance and now to IT infrastructure. We are seeing an increase in interest on how to speed the delivery of IT and make it more agile, flexible and secure. Enterprise IT departments increasingly do not want to own their own IT infrastructure. The forward-looking driver is the need to focus on new technologies—AI and automation—that will drive innovation, stronger customer engagement and top line growth. Whatever the use case, their IT staff does not have time to deal with yesterday's problems as they focus on adapting to their new roles and skills required for the Digital Age. But with IT that was built for a different era, IT leaders struggle with getting ahead of the technology debt and the new security challenges. We are seeing enterprise IT increasingly embrace IT Infrastructure as a Service to eliminate technology debt and build a more secure foundation. More and more security features, such as log management, access controls, intrusion detection and firewalling, are just going to be a requirement of the standard service and not sold as standalone elements. TenFour has taken this approach by embedding network security as a core service of its IT infrastructure subscription.



**AN INTERVIEW WITH TAMER HASSAN
CEO & CO-FOUNDER, WHITE OPS**

ADVANCED BOT MITIGATION

THE most sophisticated botnets look and act like humans when they take over accounts, commit payment fraud, click on ads, visit websites, or fill out forms. What makes bots dangerous is the ease with which a cybercriminal can scale up their activity. That is, anything that can be done by a human can be done faster and cheaper with an attack by a million bots, which makes it an appealing option for growing a nefarious business.

White Ops is a global leader in the prevention, detection, and mitigation of sophisticated bot-based attacks and fraud. The White Ops bot mitigation platform determines the humanity of more than 1 trillion interactions per week (soon to be 1 trillion per day) by using multiple layers to spot bots when they appear, and then eliminates the impact those bots have on their targets, all without impacting the end-user's experience.


We spent time with Tamer Hassan, Co-founder and CEO of White Ops, to learn more about how his platform works and the success of the recent 3ve takedown (the largest botnet organization ever defeated) that White Ops led in collaboration with the FBI, Google, Facebook and many other partners across the globe. Tamer was recognized by Fast Company as being the No.1 most creative person in business this year based on his efforts in the 3ve takedown that led the FBI to its biggest ad-fraud bust ever.

EA Tamer, is the detection of a botnet just a simple matter of doing a Turing test, or is there much more to the algorithms? What's the difference between a simple bot and a sophisticated bot?

TH It's not as simple as it used to be. Today's bots have gotten incredibly sophisticated and do a remarkable job at mimicking humans. And more than 75% of bots are on residential machines, meaning they share space on a device that actual humans are using, making it harder to spot when it's a bot as opposed to a human. The tests we run have to be dynamic by design. We change them on an hourly basis to make sure that cybercriminals can't stay ahead of our efforts to evade or reverse engineer our algorithms. We also make use of machine learning to identify bots that might be harder still to spot in a vacuum. For example, if we see a group of machines in the same location with the same screen brightness level at the same time, that would suggest that those machines are probably not being operated by humans. Finally, we have a team of threat intelligence analysts who are proactively hunting for threats to give us another advantage. Their work informs our detection algorithms so that newly observed tools, tactics, and methods are accounted for before they become widespread.

EA So where does fraud fit into this conversation?

TH Bot fraud can take a broad variety of forms, each of which has a different impact on the victimized business. Consider account fraud, which is a common way cybercriminals gain access to personal information and credit card information. Many of these attacks are based on credential stuffing or account cracking, both of which are made a great deal simpler and more malicious with the use of sophisticated bots. Another attack involves inventory fraud, through which bots can deprive businesses of customers by holding reservations without making a purchase. Influence fraud can occur when bots use social media platforms to create fake engagements to promote and highlight specific content. All of these pose challenges to organizations of all shapes and sizes.



The odds are good that one of the devices your readers uses every day has either been victim of or the target of someone operating a botnet.

EA You're saying the threat isn't just to businesses but also to end-users?

TH That's right. End-users are the victims of bots just as much as the largest enterprises. The odds are good that one of the devices your readers uses every day – their laptop or tablet or smartphone – has either been the victim of or the target of someone operating a botnet. That doesn't mean the reader did anything wrong per se, just that maybe an app that got installed had some code written into it that runs something else in the background or becomes a part of the botnet and helps the cybercriminal target another organization. The challenge is in getting ahead of those criminals. They change their tactics constantly to avoid detection. What is critical is to play the long game, where we detect, stop it and go to the source where we can actually disrupt the economics of cybercrime by putting the bad actors in jail like what occurred with the 3ve takedown.

EA What sort of success has White Ops had in getting enterprises on board with bot mitigation?

TH Increasingly, enterprises are pulling us in, as they are being targeted by botnets and they want to know what they can do to stop the attacks and prevent future ones. They discovered that simple bot mitigation offered by vendors today are not enough. They need a product that can stop sophisticated bots that act and look more and more like humans. We see significant opportunities to help financial services, insurance, ecommerce, travel, entertainment, and tech brands asking for our help to mitigate sophisticated bots.

EA How does White Ops platform work?

TH White Ops provides both passive detection and active prevention of bot traffic, and we do that through a monitoring payload that looks at each interaction. There are a few vehicles for that payload, depending on the situation, but it's how we can see into the traffic that's coming through and determine if it's human or not. The active prevention is built on a low-latency REST API. Every interaction that we scan checks into our global detection

cloud, which has data on all of the bot activity we've ever seen. That historical data, combined with our machine learning technology, lets us make a bot-or-human prediction in milliseconds. We've also got a dashboard that lets customers track their valid and invalid traffic rates over time and build reports to better understand the behavior and sophistication of the bots that they see.

EA What does the future look like for the White Ops platform?

TH We're working to enhance our bot mitigation platform every day, finding new threats and building detection capabilities around them, especially around sophisticated bots that center on account and ticketing fraud. We're expanding our technology to new systems and use cases to protect organizations in places and in ways where bots are starting to appear. And we're building integrations with Web Application Firewall (WAF) and Content Delivery Network (CDN) providers to ensure our technology can work elegantly with other web application security solutions. White Ops is a pro-privacy, pro-human organization. Our privacy-sensitive code detects bots without tracking humans. And that privacy-centric approach has earned the trust of our partners and allowed us to reach an enormous global scale. Our code, running in countless websites and apps every day, affords us a footprint larger than any single anti-virus or threat detection platform on the internet. This approach is enabling us to fulfill our mission to protect the internet and more specifically, our enterprise customers by verifying the humanity of every online interaction and disrupt the economics of cybercrime.



AN INTERVIEW WITH MARIANO NUNEZ
CEO & CO-FOUNDER, ONAPSIS

SECURING CRITICAL BUSINESS APPLICATIONS

The use of cloud-based applications has dramatically transformed the way businesses manage their critical functions and processes. SaaS-based services provide flexible, ubiquitous means for an organization to serve up capabilities without need to maintain capital or administer system infrastructure. But with this added flexibility comes a renewed need to deal with cyber threats – and enterprise security strategies must be adjusted because much of the responsibility is outsourced to the SaaS provider.

Onapsis specializes in helping organizations reduce the threats to business-critical applications platforms such as SAP and Oracle E-Business Suite (EBS), to maximize uptime while keeping them secure and compliant. Their approach supports modernization and digital transformation initiatives by enabling cross-functional teams to discover risk, optimize workflows, control change, and automate reporting. We caught up with Mariano Nunez of Onapsis to learn more about protecting SAP, Oracle EBS, and other business applications from attack.

EA Share with us how Onapsis was conceived and how it has now grown into the company it is today.

MN Onapsis was founded in 2009 with a small team of cybersecurity researchers who realized the massive risk organizations were facing by not securing their business-critical applications. We were the first to detect this problem and create a solution for it, providing the vulnerability analysis, actionable insight, and continuous monitoring organizations need to ensure these essential systems are secure and compliant. Today we're a global operation serving hundreds of the world's leading brands, including many of the Global 2000, and we expect this growth to continue as digital transformation and cloud migration projects expand across the enterprise.

EA What are the risks associated with use of critical business applications, and SAP in particular?

MN It's important to understand that these systems - ERP, supply chain management, CRM, BI, etc. - that form the backbone of an organization are incredibly complex and highly customized. This complexity makes it very difficult to assess and protect these environments, from both internal and external threats and it's very common to find outdated systems, misconfigurations, poor access control and other vulnerabilities. Adding to this is the lack of visibility from InfoSec teams - how can the security experts know what needs to be fixed if they don't know what's there? The Onapsis platform provides a window into these systems so everyone - IT, InfoSec, Compliance - can see what exists, where there are vulnerabilities or audit concerns, and how to remedy.

EA Does SaaS-provision of business application introduce any new security considerations for enterprise?

MN Yes, while there are a number of great



How can the security experts know what needs to be fixed if they don't know what's there?

reasons to move applications to the cloud, it also comes with some significant security concerns. Namely, once they are moved, internal teams are often flying blind and unable to track or control who accesses or modifies the applications. Onapsis restores this visibility, enabling organizations to identify code vulnerabilities, configuration drift, compliance violations, and other threats so they can cloud with confidence.

EA What is next for Onapsis? Are there additional areas of in-depth security coverage that you'll be focusing on?

MN With our acquisition of Virtual Forge earlier this year, we are able to provide more in-depth code analysis, including one click remediation capabilities so organizations can quickly protect themselves from the most common vulnerabilities. SAP and Oracle EBS can contain millions of lines of code, so automating code assessment and fixes are essential for these teams. Another area we are focusing on is compliance and audit requirements, such as SOX and GDPR. While most organizations understand the security risks of not protecting their business-critical applications, what many don't realize is that these systems, since they process protected information like financial, customer, and employee data, play huge roles in regulatory audits. Material weaknesses found within these applications can bring an organization out of compliance, the consequences of which can be significant fines, reputation damage, and even jail time for executives.

EA Any near- or long-term predictions about critical business application security?

MN As suggested above, we see critical business applications playing an increasingly important role in the overall mission of the organization. To that end, we would expect to see threats increase, particularly those from external attackers looking for easy access to the organization's most critical data or

“crown jewels”. I also anticipate more system migrations - whether to the cloud or S4/HANA, as SAP is requiring by 2025. This drives home the need for visibility into these systems, including system and code vulnerabilities, with ongoing monitoring, remediation capabilities, and automated governance to ensure they remain secure during the migration process and no matter where they ultimately live. In the end, our goal is to protect the applications that run a business so companies can confidently, and securely, achieve their overall mission goals.

TAG CYBER PERIODIC TABLE OF FIFTY CYBER SECURITY CONTROLS

ENTERPRISE CONTROLS	NETWORK CONTROLS	ENDPOINT CONTROLS	GOVERNANCE CONTROLS	DATA CONTROLS	INDUSTRY CONTROLS
01 IDPS/Deception	09 CA/PKI Solutions	17 Anti-Malware Tools	26 Digital Risk Management	35 Application Security	43 Industry Analysis
02 DLP and UEBA	10 Cloud Security/CASB	18 Endpoint Security	27 Bug Bounty Support	36 Content Protection	44 Information Assurance
03 Firewall Platforms	11 DDOS Security	19 HW/Embedded Security	28 Cyber Insurance	37 Data Destruction	45 Managed Security Services
04 Network Access Control	12 DMARCSec Email/DMARC Security	20 ICT/IoT Security	29 GRC and Risk Management	38 Data Encryption	46 Security Consulting
05 Unified Threat Management	13 SDNSec BGP/DNS/SDN Security	21 Mainframe Security	30 Incident Response	39 Digital Forensics	47 Security Career Support
06 Web Application Firewall	14 Network Monitoring	22 Mobile Security	31 Penetration Test/Simulation	40 IAM and Identity Platforms	48 Security R&D
07 Web Fraud Prevention	15 Secure File Sharing	23 Password/Privilege Management	32 Security Analytics/SOC Hunt Tools	41 Compliance Support	49 Security Training/Awareness
08 Web Security Gateway	16 VPN/Secure Access	24 Multi-factor Authentication	33 SIEM Platform	42 Vulnerability Management	50 Security VAR Solutions
		25 Voice Security	34 Threat Intelligence		

TAGCYBER