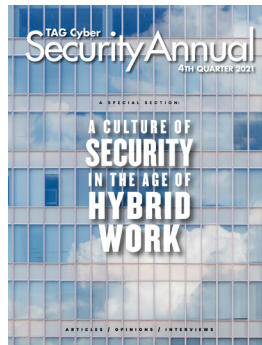


TAG Cyber •  
**Security Annual**  
4TH QUARTER 2021

A SPECIAL SECTION:

A CULTURE OF  
**SECURITY**  
IN THE AGE OF  
**HYBRID**  
**WORK**

ARTICLES / OPINIONS / INTERVIEWS



## WELCOME TO THE 2021 TAG CYBER SECURITY ANNUAL 4TH QUARTER EDITION

**W**e are so happy to offer our 4Q 2021 Edition of the TAG Cyber Security Quarterly. The content in this volume was developed by our expert team of analysts and writers with one goal in mind: To offer unbiased, accurate, and informative technical and business pieces that can help with your practical day-to-day cyber security tasks. Hopefully, this will be the case.

One dubious recent trend in cyber security is that our language has devolved into painful acronym purgatory. As we edited the articles and interviews in this report, we were struck by the endless, endless, and more endless acronyms. It's as if every cyber security expert decided to talk in a special coded form – perhaps to prevent others from butting into our precious cyber conversations. We are just as guilty as everyone else. It's a bit embarrassing – actually.

Here are just a few of the more oft-cited cyber acro-goodies: EDR, MDR, SOAR, SIEM, XDR, NGFW, ZTNA, NAC, SOC, WAF, MFA, NDR, 2FA, SSO, DLP, SASE, SD-WAN, VPN, IAM, CIEM, CIAM, IAM, IGA, EDR (oops I said that one already), CASB, CSPM, ASM, ADR, FML (OK, I put that in for fun), ISO, CSF, AES, PKI, DEVSECOPS, SECDEVOPS, DEVOPSSEC, DEVOPSSEX (when developers get frisky).

Now, every technical discipline will have its acronyms – that is certainly not a new thing. But one cannot help but wonder if we haven't taken this thing a bit too far. Here's a fun challenge for you this fourth quarter of 2021: Why not see if your team can go one day in the office without saying an acronym. If anyone can perform such a feat, then the prize should be to let that person create an acronym to name the don't-say-an-acronym game.

On a more serious note – we watched more cyber vulnerabilities enter our living rooms this past quarter, including a doozy from Apple. The idea that malware might find its way onto our iPhones without so much as a click is a terrifying proposition. Charlie Miller showed some frightening exploits on earlier iPhones a decade ago, but this new vulnerability made Charlie's work look almost primitive. Apple will need to do a better job.

As will our federal government. A recent [Senate report](#) pointed out continued vulnerabilities in our government systems, leaving citizens at risk. This theme just never seems to end – and before long, something truly serious is going to happen. Maybe that's what it will take for agencies to up their game.

## I N T R O D U C T I O N

At TAG Cyber, we deployed our Alpha Research Portal this quarter, and we are so grateful to our initial customers for helping us work out kinks in the buttons, links, and downloads. Our goal is to invent a new form of research as a service (RaaS) to compete with the tired analyst models pushed out by the likes of Gartner and Forrester.

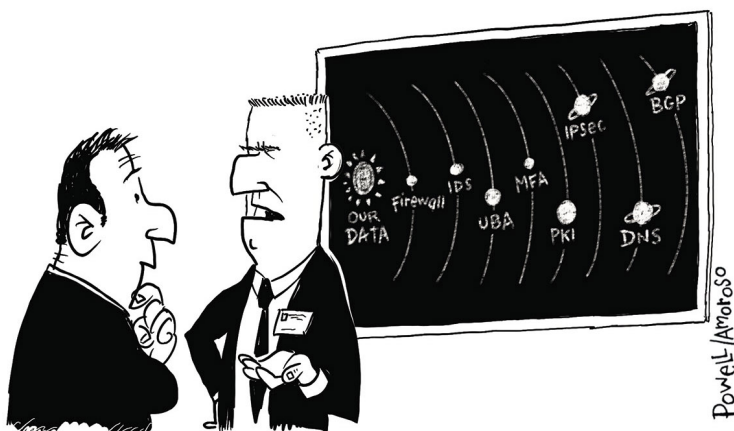
We watched with some sadness as Gideon Gartner, founder of the modern analyst industry, passed just nine months ago. At TAG Cyber, we hope to continue his legacy of being feisty, opinionated, edgy, but always knowledgeable. His namesake company has just gotten too big and powerful, with too much revenue at risk.

In contrast, as we deploy our beta RaaS portal, we hope you'll join our community as a customer. We promise to make it worth your while. Drop us a note at [contact@tag-cyber.com](mailto:contact@tag-cyber.com).

What you will get with our RaaS offering is original research, reporting, videos, articles, and advice in roughly 140 different subcategories of cyber security. If you are working on a project, then we include a RaaS option to send our analysts a question or ask for their real-time assistance. We provide this through the portal, and the model seems to be working well.

Again – we are so pleased to welcome you to this volume, and we hope that our work is helpful in your enterprise protection, solution development, course development, research investigations, and other use-cases that define our industry.

Happy reading.



*“Uh, yes – I will admit some NASA influence in the new security architecture.”*





- **LEAD AUTHORS** – Ed Amoroso, David Hechler
- **RESEARCH AND CONTENT** – Shawn Hopkins, Liam Baglivo, Stan Quintana, Andy McCool, Jennifer Bayuk, Matt Amoroso
- **MEDIA AND DESIGN** – Lester Goodman, Miles McDonald, Rich Powell

TAG Cyber LLC  
P.O. Box 260, Sparta, New Jersey 07871  
Copyright © 2021 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 authors 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 2021 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.

**The opinions expressed in this document are that of the TAG Cyber Analysts, and in no way reflect that of its Distinguished Vendors.**

October 15, 2021

C O N T E N T S

Introduction	2	Bringing an Offensive Mindset to Cyber Defense Patty Wright, Bishop Fox	50
<b>A CULTURE OF SECURITY IN THE AGE OF HYBRID WORK</b>	<b>6</b>	Supporting Intelligent Secure Access Control James Winebrenner, Elisity	53
Our Survey Shows Companies Have Remote and Hybrid Work Plans, but They Also Have Reason for Concern	7	Connected Device Security Solutions Mark Harris, Finite State	56
Policies to Tame the Risks of Hybrid Work	12	Reducing the Risk of Malicious Bots Tamer Hassan, HUMAN Security	58
Five Cyber Security Technologies You Will Need to Support Hybrid Work	16	Supporting Collective Defense to Reduce Cyber Risk Bill Welch, IronNet	61
Five Cyber Security Technologies You Will Not Need to Support Hybrid Work	17	Using Security Ratings to Protect Business Aleksandr Yampolskiy, SecurityScorecard	64
Are Companies Ready for a Return to the Office?	18	Solutions to Optimize Security for Active Directory Mickey Bresman, Semperis	67
<b>OP-ED</b>	<b>21</b>	Security and Compliance Enhancements to Permissions James Wilde, Sphere	70
Warnings, Threats, and Blurry Red Lines	22	Advanced DevOps Security Controls Suresh Vasudevan, Sysdig	73
XDR: An Alliance and a Mission	26	Cyber Security Performance Management for Enterprise Allan Alford, TrustMAPP	76
Hacking Back at Russia is a Terrible Idea. Here are Ten Reasons Why.	28	<b>ANALYST REPORTS</b>	<b>79</b>
His Cyber Training Was Not About Tech. It Was About People	30	Cyber Insurability as a Posture Index	80
<b>INTERVIEWS</b>	<b>34</b>	Mapping CVE Records to the ATT&CK Framework	83
Supporting Cyber Security for Small and Midsize Business Raffaele Mautone and Julie Cullivan, AaDya	35	Next-Generation Vulnerability Assessment and Patch Management: An Overview of Acronis Cyber Protect	91
Unifying Data Protection and Cyber Security Candid Wüest, Acronis	37	Self-Protection Data as a Means for Business Resiliency	96
Protecting Families from Cyber Threats Erez Antebi, Allot	39	Understanding Compromise Intelligence	103
Advanced Data-Driven Network Security Rahul Kashyap, Arista Networks	41	<b>DISTINGUISHED VENDORS</b>	<b>107</b>
Preventing and Detecting Lateral Movement Tushar Kothari, Attivo Networks	44		
Continuous Authentication for End Users Dr. Neil Costigan, BehavioSec	47		

A SPECIAL SECTION:

**A  
CULTURE  
OF  
SECURITY**



**IN  
THE AGE  
OF  
HYBRID  
WORK**

## OUR SURVEY SHOWS COMPANIES HAVE REMOTE AND HYBRID WORK PLANS, BUT THEY ALSO HAVE REASON FOR CONCERN

KATIE TEITLER

A mere two years ago, the idea of “hybrid work,” that is, working partly in a dedicated corporate office environment and partly from various and fluctuating remote locations, was the privilege of a select few. While remote work had more than taken hold in the corporate world by that same time period, hybrid work wasn’t yet part of the corporate lexicon.

When COVID-19 hit in full force in the United States, starting in March 2020, offices were shuttered and workers were forced into their living rooms, dining rooms, basements, and even bedrooms as their new work environments. Coffee shops weren’t open for a change of scenery. Business travel had ground to a halt. Businesses were operating at near 100 percent remote capacity wherever and whenever possible.

As signs of improvement arose, especially following the release of COVID-19 vaccines, some office workers tentatively started returning to office environments for at least part-time in-office work. Today, in Q4 2021, as we weather the roller coaster of COVID cases in the U.S., 61 percent of organizations report that their workforces continue to function remotely, according to a recent survey of 258 IT and security professionals conducted by TAG Cyber. (Figure 1)

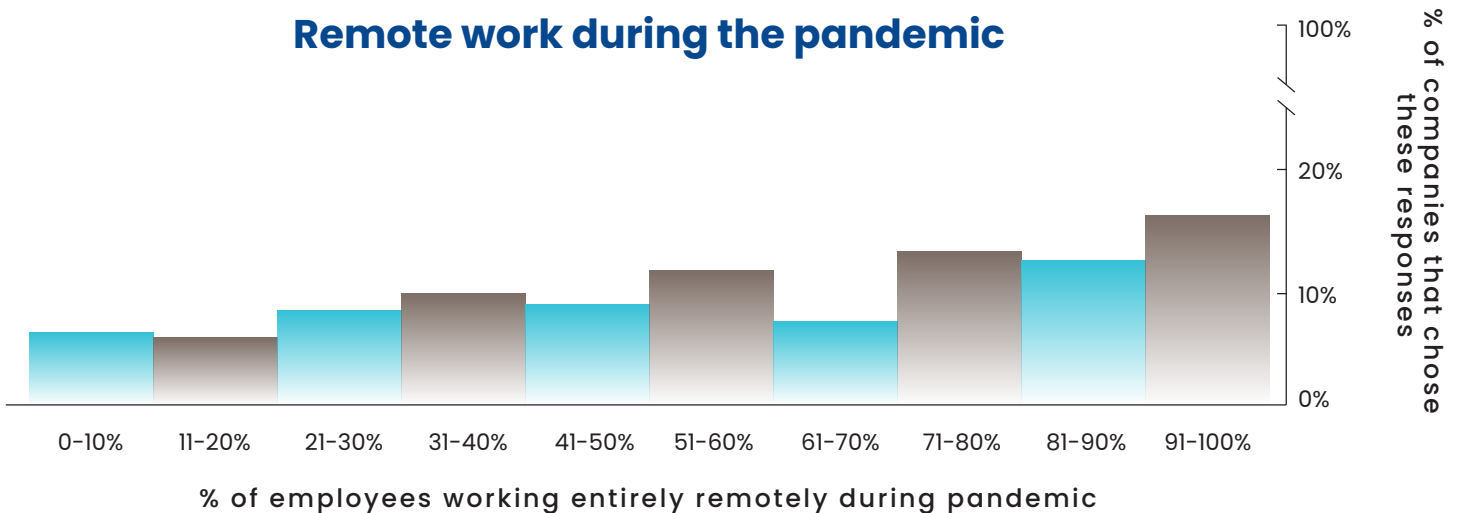


Figure 1



When broken down by company size, organizations with 1,000–4,999 employees have more employees working remotely than any other category (29.5 percent of those companies have more than 51 percent of employees working remotely).

However, when looking at companies with 91–100 percent of employees working remotely, smaller companies, those with 100–999 employees, report the highest percentage of employees working remotely (41 percent of those companies have more than 90 percent of employees working remotely).

Looking ahead to 2022, hybrid work seems to be the future. To level set, according to TAG Cyber’s definition, hybrid work differs from remote work in that hybrid workers function part time in the corporate office environment and part time in other, remote locations. Remote work, in contrast, means that the preponderance of time is spent working in out-of-office locations. This does not mean that remote workers will never visit the corporate office, nor does it mean that their working location will be static. However, remote workers are likely to have a dedicated office and spend the majority of their time working from there.

When it comes to post-pandemic working conditions, 60 percent of our survey respondents said they expect fewer than half their companies’ employees to work remotely when offices are able to reopen. (Figure 2)

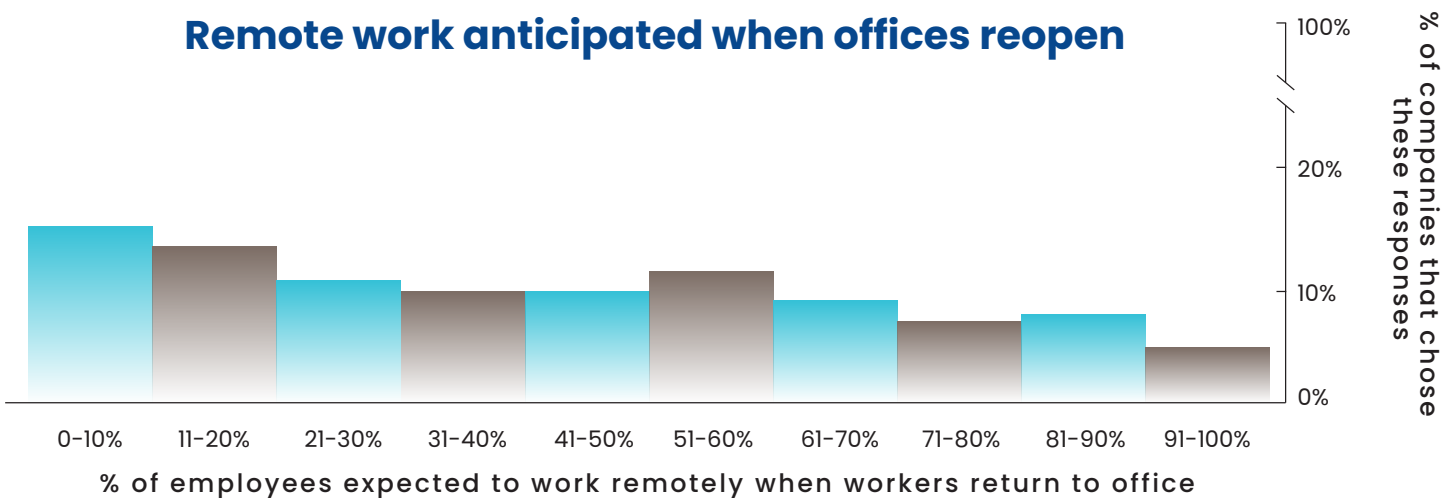


Figure 2

Smaller companies, those with 100–999 employees, are the least likely to anticipate remote and hybrid work. By contrast, companies with 5,000–9,999 employees and those with more than 25,000 employees are anticipating a higher percentage of remote workers in the coming months.

And again, fully remote work is different from hybrid work—where workers are coming in and out of the office and potentially working from various remote locations on their days outside the office, as well as potentially using unmanaged devices to conduct work when they are out of the office. These factors introduce additional risks when combined with a return to the office.

When it comes to the remote work structure alone, a clear majority of our respondents say they are fully prepared for the cyber security implications. Fully 80 percent said they already have a remote cyber security strategy in place, and an additional 12 percent said they are working on it. (Figure 3)

A strategy is one thing, but the ability to execute on that strategy is everything. Far too often in security—



whether it concerns remote or hybrid work—operationalizing plans is a major challenge. Companies lack such essentials as the in-house security expertise necessary; and the budget to hire more internal staff, to hire outside experts, or to acquire the appropriate tooling. The IT and security professionals may lack the power to affect business decisions that would improve security posture.

One area that they *are* operationalizing, when it comes to remote and hybrid work, is the management of unmanaged devices like personal laptops, phones, IoT devices, and tablets over which the security team has little to no visibility or control. This is especially true of access to SaaS applications that are now used in business settings. (Figure 4)

### Do you have a hybrid work cyber strategy in place?

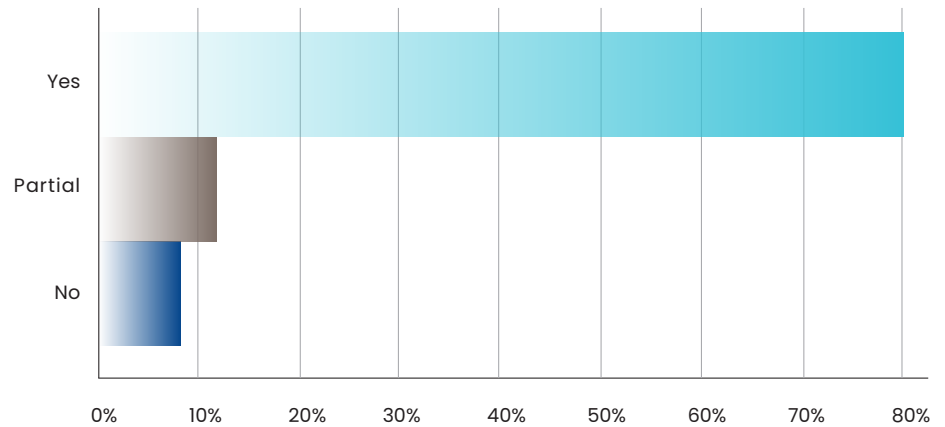
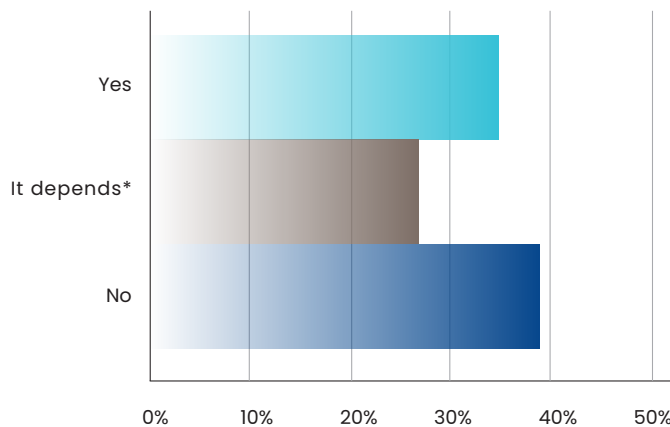


Figure 3

### Are employees allowed to connect personal or unmanaged devices to corporate resources?



\*It depends on the security posture of the device and/or the sensitivity of the resource

Figure 4

According to our respondents, nearly 40 percent of companies draw a line in the sand when it comes to personal and/or unmanaged devices accessing corporate resources. Thirty-four percent said employees are allowed to use non-work issued devices, and another 27 percent said employees can use personal/unmanaged devices for work purposes, depending on the security hygiene of the device. The latter, of course, relies on the

company deploying and using appropriate endpoint/device management tools and access controls—not to mention the onsite (or contracted) staff to do so.

We were remiss in our survey design, though, and this potentially calls the results of this answer into question. We should have asked, *How are IT and security departments measuring when and how employees are accessing SaaS applications via unmanaged devices?* Based on our extensive work with enterprises and vendors, we know that a significant number of enterprises do not have full visibility into who or what is being accessed—and how. Especially as it relates to SaaS applications.

Getting deeper into the matter of access, the next question was: *How are you currently securing remote and hybrid worker connections?* Respondents were allowed to choose as many answers as apply. (Figure 5)

Sixty-nine percent are currently using VPNs—an outdated and nominally secure connection method—for remote connectivity.

Tied for second place, at 55.8 percent, are antivirus and firewalls/next-gen firewalls used to help secure employees’ connections into corporate resources. Next is multi-factor authentication (MFA), and five points behind is encryption.

Interestingly, despite the buzz, zero trust network access is currently being used at less than 20 percent of companies. This finding may indicate end users’ understanding that zero trust is not a product but an approach. Or it may signal that, despite all the industry hype of moving toward more secure methods of access, namely continuous verification based on context and identity, end users are not yet ready to move their systems away from a “trusted” architecture.

## How are you currently securing remote and hybrid worker connections?

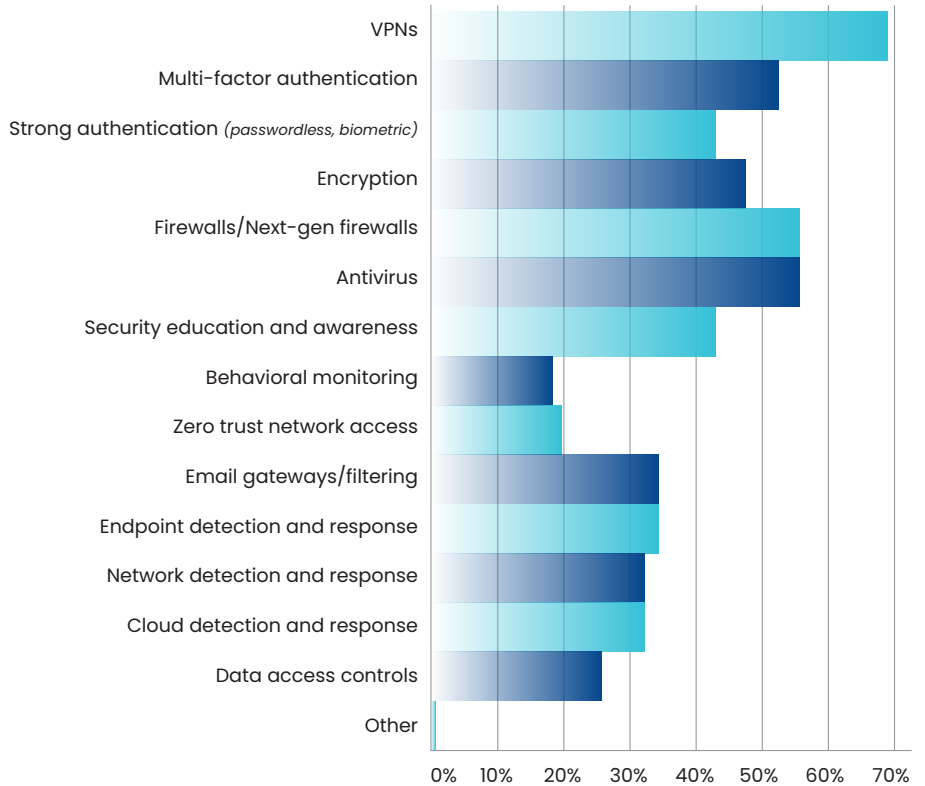


Figure 5

## Which of the following will be the greatest risk to your company’s hybrid work environment?

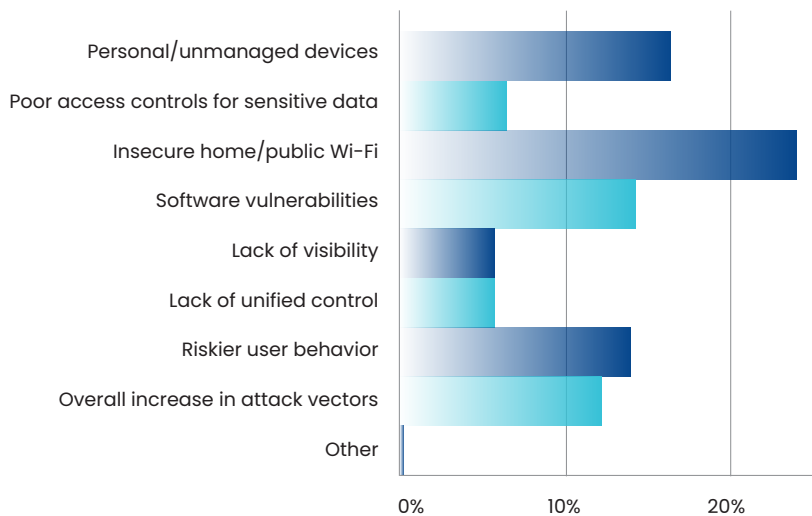


Figure 6

Regardless, the use of numerous security technologies certainly seems valuable to our survey takers. Fifty-four percent reported that their organizations saw an increase in potential attack activity as a result of remote and hybrid work. This is in light of mandated security awareness training for employees at more than 80 percent of organizations.

Looking to the future and the seeming inevitability of increased hybrid work, only 22 percent of respondents said that they do not expect the number of cyber security incidents targeted at their organization to increase as hybrid work increases.

Of the 78 percent who said attack activity will or may increase, the reasons varied. (Figure 6)

In the clear lead is concern over insecure home/public Wi-Fi, with 24 percent of the vote. With this in mind, it would be TAG Cyber's suggestion that these organizations implement zero trust access-based controls, increase use of endpoint detection and response (including built-in device hygiene assessment capabilities), and even consider behavioral monitoring (which, incidentally, was the least selected answer to the question about securing hybrid access).

Not surprisingly, respondents again expressed great concern in their answers over the use of unmanaged/personal devices. Yet, more than a third of respondents said that their organizations plan to allow the use of personal devices in the future—perhaps pressured into doing so by non-security/non-IT use cases—and nearly 50 percent said that their organizations will permit employees to manage applications from personal devices while working remotely.

Given the concern about and risks of infected personal and unmanaged devices (Figure 7), organizations must look for enhanced authentication and access options, predicated on identity (both human and machine) which conform to a zero trust approach.

When it comes to the market's opinion of methods to decrease risk in order to increase cyber security control, 59 percent of respondents said that the solution lies in security education and awareness training (respondents were allowed to choose their top 3 controls). (Figure 8)

TAG Cyber is a proponent of ongoing education in all areas; however, cyber security must be a combination of people, process, and technology (PPT), led by security experts and not left to unsuspecting users as the first line of defense. We were thus pleased to see that email and endpoint security were ranked highly by respondents (45 percent and 41 percent, respectively), followed by strong authentication (MFA and long, unguessable

### Are you concerned about employees bringing infected devices into the office?

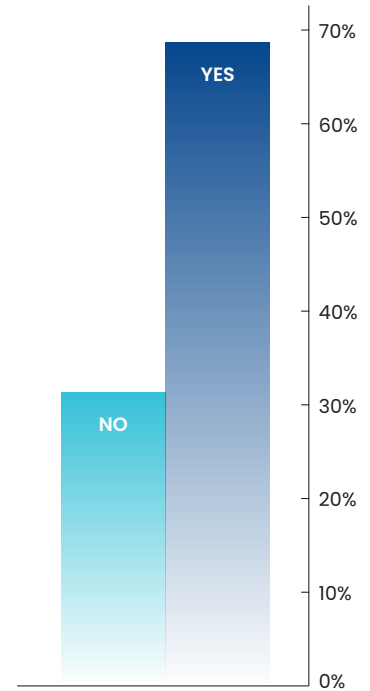


Figure 7

### Which approaches do you think will have the greatest positive impact on your hybrid work cyber security posture?

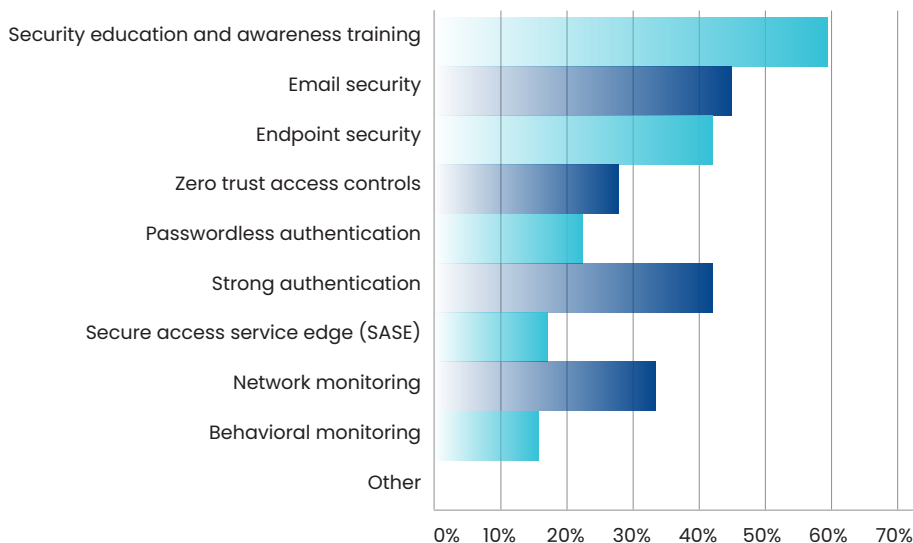


Figure 8

passwords). Network monitoring, a tried-and-true method of identifying suspicious behavior, fell in the middle of the pack, while secure access service edge (SASE), a category gaining tremendous attention in the vendor community, fell to the bottom of organizations' choices for enhanced security control.

Though this question could have included multiple additional areas of control (TAG Cyber tracks 130+ categories of vendor products), no respondent chose them as a write-in option. With all of the choices on the market, it's a good thing that our survey takers anticipate increased cyber security budgets (72 percent) to tackle the new paradigm of hybrid work.



AN INTERVIEW WITH KRISTINA PODNAR,  
FOUNDER, NATIVE TRUST CONSULTING, LLC

## POLICIES TO TAME THE RISKS OF HYBRID WORK

Kristina Podnar calls herself a “digital policy consultant.” She doesn’t have formal training in tech (she earned an MBA in international business), but she learned the old-fashioned way. She worked at a startup in the early days of the web. It was a wild ride. “We did crazy things,” she said. “We would upgrade websites without backing them up first.” The result: a famous website was down for eight hours. On a Saturday. She survived to help companies navigate the digital world for two decades, most recently under the banner of Native Trust Consulting, LLC. Along the way she wrote a book called “The Power of Digital Policy.” We thought she’d have a lot to say about our survey on hybrid work.

**TAG Cyber:** *What were some of the findings of the survey that seemed important to you, or were surprising in some way?*


**KRISTINA PODNAR:** I found the majority of the answers predictable. Do folks actually have a cyber security strategy in place? The majority of folks said yes. Do they anticipate people continuing to work from home? The answer is yes. What I thought was really interesting was when we start to delve deeper into the results and look at things like how companies currently secure remote and hybrid worker connections. That was really telling. I was expecting things like MFA—multi-factor authentication—to be much higher than it was. And zero trust network access—I would have anticipated a much higher number. It’s not so much the overarching results that were surprising, it’s really getting under the covers, and getting to the substance that was surprising. And not necessarily in a good way. Because it points back to the need for additional awareness and better security practices.

**TAG Cyber:** *Do you believe companies should establish policies and rules for employees when they are working remotely? And do these need to be written down and disseminated?*

**PODNAR:** Absolutely. In fact, what I encourage the companies that I work with is not just to develop the policies, because it’s really easy to create what I call shelfware. Shelfware is when I write down my policy, I put it in a really nice looking PDF on SharePoint, and nobody ever looks at it again. That’s not going to get you anything. Save the paper. What you really need to do is write down the policy. If you’re a small business, with maybe like 10–15 people, it doesn’t



Do you want people to do certain things before they come back into the office? Are you going to disable, for the time being, all USB devices until you can really get everybody patched up?



have to be as formal. It can be written down on a napkin if you want. But yes, make sure that everybody's aware of what the policy is and practice it. You have to be very clear about the remote workers' responsibilities. You have to provide, in some instances, monitoring services. I'm a proponent of those—things like identity and access management control.

***TAG Cyber: Should companies be monitoring their employees' behavior, and should they try to enforce the rules and policies they have established?***

**PODNAR:** I think for a lot of folks, this seems like an over-the-top approach. But it is definitely something that we're progressively seeing in security measures for remote workers. Services can actively monitor that behavior and pick up any anomalies. And I think that that's actually a good thing. Because through data collection analysis, not just by manual review but increasingly through artificial intelligence, we can start to understand what is normal behavior, and we can identify, based on each individual user profile, anything out of the ordinary. This isn't meant to threaten employees, as in, "If you go onto your Facebook account three times in a workday, I'm going to reprimand you." It is meant to monitor the fact that if I start to see you ping Facebook 17 times a day, I know that something else might be happening. We might be experiencing a cyber event that I need to look into.

We have a situation with an organization that I've been supporting where an individual decided to take their laptop and go to India pre-pandemic. And that person was not supposed to be taking their laptop out of the country. They were very diligent, they were working every day logging on to every meeting. But at the end of the day, that laptop still left the U.S. And people might go, "Oh, is that a big deal?" Well, yeah it's a big deal. Why? If you have data loss, it implicates governments and is beyond the FBI. Now we have Indian government entities that need to be involved in any kind of a data breach or data loss situation. The other aspect of that is if there's a breach and that employee's in India, the cyber insurance policy may not cover that incident. And so the organization could be out millions of dollars. All of that can be avoided if we have not just clear policies in place, but we back up those policies with monitoring.

***TAG Cyber: Many companies have cyber insurance policies. Do most policies cover remote work?***

**PODNAR:** I'm not a cyber insurance specialist. I actually know people who are, so I usually work with them and we create the policy and translate the organization's risk profile into a cyber insurance policy. Do most organizations automatically get covered? No. And this was true before the pandemic. Just because you had an insurance policy in place, it didn't automatically cover every individual who teleworked from home



one or two days a week, or decided to go work at Starbucks because it was a more productive place for them. So most organizations need to take a look and understand the extent of their coverage.


***TAG Cyber: These days when people are working remotely, they seem to have more and more video meetings, like the one we're having right now. There are a number of potential vulnerabilities. Some of them aren't even necessarily technological.***

**PODNAR:** Sometimes IT folks are outside of their sphere. They're thinking about how somebody might hack into the network. Will we experience ransomware? They're thinking about all the digital aspects, that we could have data loss or have an incident that we need to worry about. But a lot of times what folks are forgetting to do is think about the physical world that we're in. We are working remote, and often there are people around us. So if you go to work at Starbucks, who else can see your monitor from their screen next to you? If I'm talking to you from home right now, suppose I'm a doctor. I'm speaking in a regular voice, but next to me is my husband, who's also working at home. Who else is hearing your personal health information? We have to always be mindful that it's not just about the digital world. It's also about how it translates into our physical world, and what information can pass back and forth.

***TAG Cyber: There are lots of tentative plans for employees to return to the office. When they do, they may be bringing in personal devices they've been using remotely during the pandemic. Should their companies have another set of policies that they need to spell out very clearly at that point?***

**PODNAR:** Absolutely. Because remember, what's happening is you're actually having not just one device but a flow devices coming back into the office environment. And often you actually don't know that device, even if it is your corporate-issued device. Do you understand if the iOS has automatically been updated? Do you understand whether all the right patches are applied from a security software perspective? Do you understand what network that device has been on, who else has been on the network? And so as these devices, whether they're corporate-issued or they're personal devices, you really need to start thinking about how are you going to treat these things that are coming through the door that are all potentially a security threat. And then think through how you want that event to take place. Do you want people to do certain things before they come back into the office? Are you going to disable, for the time being, all USB devices until you can really get everybody patched up? Have you forgotten to disable "trusted devices" so they don't automatically connect to your network when I bring my phone back to work? There's a slew of considerations. You need the right controls. And you need to understand not just what actions you're going to take, but how you're going to respond if something does happen.

I think what I would do is challenge everyone in our audience today to not only look at the survey results, but ask themselves, “Can I go deeper? What are the issues in my organization that these questions might point to?”



**TAG Cyber:** *Yeah, but you know, all I want to do is use this thumb drive [holds one up] when I get back. It's just got a couple of gigabytes. I mean, nobody would even notice it, right?*

**PODNAR:** [Laughs] Well, it depends on your policies. For a lot of companies, they've actually disabled the ability to put in remote devices, such as a USB. And not only for devices that are coming back into the enterprise, but what might leave with that device once you stick it into the computer. Disabling those devices is really potentially important. But also keep in mind that people have a need. For you, it's your USB. How do I get this small or large file back into work? And if you don't give people a good way of doing that, if you just say, "I'm going to disable your USB," people are going say, "Oh. OK, that's cool. I'll just put all the files on Google Drive, and I'll transfer them that way." That's not the right solution. You really do need to give people a path so they can achieve what they're going to have to achieve.

**TAG Cyber:** *These policies we've been talking about – who should draft them?*

**PODNAR:** IT has to be at the table, but so does legal. If you have somebody who specializes in privacy, get them involved as well. You're going to want somebody from the business. People go, "Business? Why am I talking to the business? They don't know anything about breaches." They don't know anything potentially about breaches, but they sure know that they can go to Google Drive if their USB won't work. So you need to understand the pain points a business is going to face, and how you're going to address those. You need to have the legal perspective to understand what you can and can't tell employees to do. You need to involve HR as well, because it's a people matter. They can also help you get the word out, and they can help you with the training aspect. So look to partner with them.

**TAG Cyber:** *Any last comments about the survey?*

**PODNAR:** What's great about it is that you did create an umbrella set of questions. I think what I would do is challenge everyone in our audience today to not only look at the survey results, but ask themselves, "Can I go deeper? What are the issues in my organization that these questions might point to?" Because I suspect that just having that conversation and asking themselves the questions in your survey will get them rolling in the right direction.

# FIVE CYBER SECURITY TECHNOLOGIES YOU WILL NEED TO SUPPORT HYBRID WORK

EDWARD AMOROSO

As you develop your solution architecture to support work-from-home (WFH) initiatives, you will need to include these five security technologies to avoid any threat consequences.

With WFH comes new cyber protection *opportunities*. As one would expect, this shift has led to products from security vendors that can be quite *helpful*. To help enterprise buyers *find the right tools* amidst the marketing noise, we offer the following list of five security technologies that you will need to support hybrid work. (See our mirror companion piece on five security technologies *you will not need* in this context.)



**Zero Trust Network Access** – If ZTNA vendors had three wishes from a genie in a bottle, all three would be for WFH to continue its accelerating growth. Developed specifically to address weaknesses in virtual private networks, ZTNA supports secure access from PCs and mobiles to cloud-hosted application workloads. If you currently run a VPN (or God-help-you, a remote desktop protocol [RDP]), then it's time to check out a ZTNA vendor.

**Multi-Factor Authentication (MFA)** – Yes, you already know all about MFA, but please take a moment to ask yourself this: Are you still accessing a variety of different services using a password – or perhaps just a link to a site? Before you answer no, take a moment to reflect on how you authenticated to your last Zoom call. If things continue to evolve as they have, then MFA will soon become fully ubiquitous. This is good news for MFA vendors.

**Endpoint Detection and Response (EDR)** – There is a reason why endpoint security is considered so fundamental to zero trust: The surrounding perimeter has vanished, thus leaving your PC, mobile, or other device naked to the Internet. (And yes – this might have been true even with a perimeter, but you get the idea.) EDR solutions are therefore especially well-suited to WFH and the attendant secure access solutions for employees sitting at home in their skivvies.

**Application Security** – At the opposite end of the session spectrum from the endpoint sits the application. This device-to-app model allows security engineers to restrict their attention away from protecting every resource in the enterprise to the more humble and tractable goal of ensuring security during a zero-trust session. (One observation: Shouldn't the PC be called the starting point and the application called the endpoint? I'm just saying.)

**Cloud Security** – Just as the application must be secure for WFH, the public cloud infrastructure and associated systems must also be protected from malicious threats. For this reason, Amazon, Microsoft, Google, IBM, and VMWare are now essential components of any zero-trust architecture supporting safe and secure WFH initiatives. This obligation extends to SaaS solution providers as well.



# FIVE CYBER SECURITY TECHNOLOGIES YOU WILL NOT NEED TO SUPPORT HYBRID WORK

EDWARD AMOROSO

---

As you develop your solution architecture to support work-from-home (WFH) initiatives, you will not need these five security technologies to avoid of threat consequences.

With WFH comes new cyber protection *pitfalls*. As one would expect, this shift has led to products from security vendors that can be quite *unnecessary*. To help enterprise buyers *avoid the wrong tools* amidst the marketing noise, we offer the following list of five security technologies that you will not need to support hybrid work. (See our mirror companion piece on five security technologies you *will need* in this context.)

**Next Generation Firewalls** – The invention of next generation firewalls (NG-FWs) by Nir Zuk and others represented one of the greatest achievements in modern enterprise security. Without this innovation, our industry would have languished to protect local area networks from internet attacks. But WFH initiatives are largely orthogonal to the need to install such devices. Yes, they are necessary for secure access service edge (SASE), but mostly for branch offices.

**SD-WAN** – Related to the SASE-orientation of NG-FWs, the use of software-defined wide area network (SD-WAN) technology is designed more for branch office replacement of multi-protocol label switching (MPLS). As such, while SD-WAN will certainly be important to the enterprise, it will not be a vital component of WFH initiatives. Secure zero trust network access solutions will be more important.

**Network Access Control** – Despite the presence of one after another final nails in the coffin for network access control (NAC), the capability continues to demonstrate surprising resilience in the enterprise. This is more than likely driven by the fact that so many organizations continue to operate a perimeter-based local area network. Nevertheless, NAC will not be important for WFH initiatives.

**Cloud Access Security Broker** – This one might surprise you because cloud seems so natively related to anything considered virtual and hybrid. But CASBs are really tuned to identify cloud and SaaS usage from the enterprise. Admittedly, the API scanning mode for CASBs might help to secure cloud interfaces, but for the most part, CASB – even in the context of SASE – is not important for WFH.

**Physical Security** – This might not be as obvious as you'd think. While it will certainly be less important for an enterprise team to physically protect its data centers if everything is flying out to some public cloud, a new obligation emerges for WFH. Specifically, employees must be guided to make sure the nosy neighbor doesn't peruse corporate documents while visiting the downstairs bathroom during a barbecue. This is the new WFH physical security obligation.



# ARE COMPANIES READY FOR A RETURN TO THE OFFICE?

BY DAVID HECHLER

All the talk about hybrid work largely comes down to one big question: What will happen when workers return? Companies should already know plenty about what happened when they left. If not, they're in big trouble. But the return is what hybrid is all about. And now that many businesses are starting to bring them back, or are delaying plans to do so in deference to the Delta variant, TAG Cyber sent out a survey to ask about their views of cyber security in the hybrid environment.



Karen Painter Randall

Karen Painter Randall had interesting reactions to the results. She found many of the responses revealing, but she immediately homed in on who filled them out: IT and security professionals. "When people start asking enterprises questions about their security and best practices,"

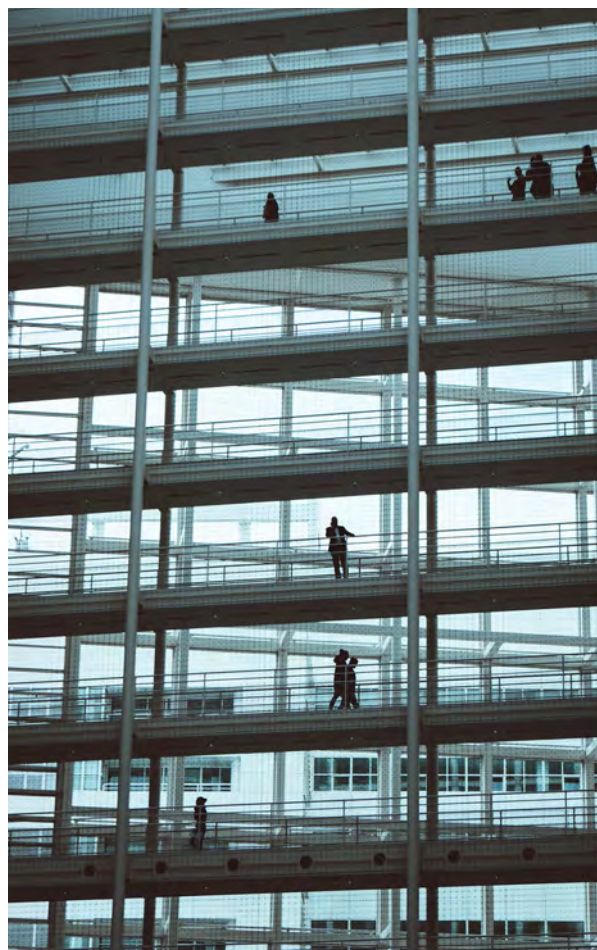
she said, "they forget about the people who are actually holding the purse strings."

In explaining what she meant, she pointed to the last question, which asked respondents whether they expected cyber security budgets to rise. Yes, they agreed: about 30 percent of them said "significantly," another 42 percent said "somewhat." "Well," said Randall, "they're not going to be able to do that unless they have the stakeholders on board, and the stakeholders understand what the mission is."

Randall is actually somewhat optimistic on that score, following the ransomware attack on Colonial Pipeline. The repercussions of that event, and the vast publicity it attracted, seem to have awakened CEOs to the dangers, she noted. At least she hopes it has.

Randall is a senior partner at the law firm Connell Foley in New Jersey, where she chairs the cyber security, data privacy, and incident response group. She's been steeped in this area for years, and has a special expertise in ransomware. Looking out on a remote workforce preparing to return to the office, she sees flashing red lights on the road ahead.

**If companies have not yet established return-to-work policies that cover devices and data protection, now is the time, Randall advised.**



What should companies be considering at this juncture? “I think it’s very important to understand where their assets are,” Randall said. Where have their employees been? Have companies “taken an inventory of their devices? Have they rolled out the rules of the game, as I call it, with regard to what is appropriate and what is not appropriate usage of work devices?”

And then she added the big one: “What’s the rule on using personal devices?” Have employers been thinking about a possible day of reckoning when devices return to the office? Randall suspects many have closed their eyes. “Not knowing makes them sleep a little better at night,” she said, “but they’re going to be in for a rude awakening when their workforce returns.” Many employees have been working remotely since March 2020, often on personal devices that could have been infected with malware during that time, she suggested.

The survey found that 48 percent of the companies allowed employees to access managed applications from personal devices when working remotely. (The actual result may have been higher, since 10 percent of the respondents were unsure of their companies’ policies.) And 69 percent acknowledged that they were concerned about employees bringing infected devices into the office. Fifty-three percent of respondents expected an uptick of security incidents in the new hybrid environment.

If companies have not yet established return-to-work policies that cover devices and data protection, now is the time, Randall advised. The survey suggested that they’re off to a slow start. Only 22 percent have finished updating or reissuing their cyber security handbooks for hybrid work. Another 43 percent said they have done so, but only in part, while 10 percent said they plan to but have not yet started.

If it were up to Randall, her first rule would be this: “You cannot use your personal device while conducting business.” She believes the risks are simply too great. Employees will use chat apps, “which are a perfect conduit for an attacker,” she said. They will fail to update and patch devices. “Microsoft is rolling out patches all the time,” she noted.

**How a company deals with employees who repeatedly engage in lax security practices is likely to pose a big challenge.**





At least on paper, there's more support behind this idea than you might think. In our survey, 38 percent of the companies said they did not plan to allow employees to use personal devices in the office going forward. Thirty-four percent took the opposite position, and 28 percent hedged their bets by answering "it depends."

What about enforcement? The concept is important, Randall acknowledged, but it's not a word companies want to use with the workforce. "You want to cooperate," she said. You want employees to "feel comfortable with the security awareness training." You want them to report to IT if they click on a sophisticated phishing email.

But the company also needs to know about bad behavior. She cited a recent example that was brought to her attention. Randall was working with a client's incident response team, and an IT employee had seen lax security practices from "some pretty key people in the organization." The chief financial officer, who was also present during this conversation, was concerned, but the IT person was "dismissive," Randall observed, even though he called the employees "repeat offenders."

Randall found it disturbing. "You really need to hold them accountable," she said. "It might be through performance reviews. It might be through a policy like three strikes and you're out. Some organizations have that," she noted, "especially health care and financial institutions." Repeat bad behavior "puts the organization at risk."

One way to mitigate risk is to purchase insurance. But cyber policies are all different, and underwriting standards are tightening quickly, "primarily because of ransomware," Randall said. Companies will want check to be sure they're covered for hybrid work. This would be a good time to sit down with an experienced broker, she suggested, and take the opportunity to ask about ransomware supplements. Our survey showed that ransomware and phishing were viewed as the two threat vectors of greatest concern (by far) in a hybrid environment.

Insurance companies are spending more time examining security practices and verifying information, so it behooves companies to make sure they're ready before they go out shopping. Multi-factor authentication is something underwriters expect to see, yet only 53 percent of our survey respondents said they use it. "If you don't have that deployed at your organization," Randall warned, "you're not going to get that insurance."



*"We have about three minutes before lunch.  
That should be enough time for our annual  
cyber security update."*





OP-ED



# WARNINGS, THREATS, AND BLURRY RED LINES

DAVID HECHLER

In July, amid what felt like a relentless surge of cyber attacks, President Biden was under great pressure to do something. There were all those attacks attributed to Russia. Then more attacks said to be from China. The United States had become an international cyber punching bag. It was time for the president to take action. And he did.

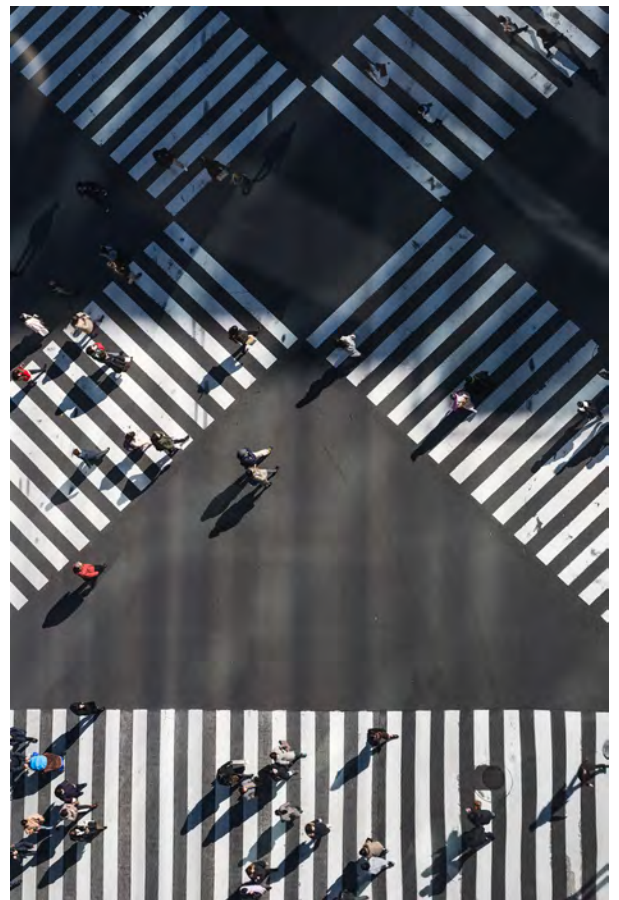
The big move was in response to China's **alleged global attacks** through a vulnerability in Microsoft's Exchange email systems. Microsoft had attributed the attacks to China back in March, and on July 19 Secretary of State Antony Blinken declared that China's Ministry of State Security "has fostered an ecosystem of criminal contract hackers who carry out both state-sponsored activities and cybercrime for their own financial gain." And for the first time the U.S. was joined in condemning China not only by the European Union but by all NATO members (though only the United Kingdom also used language tying criminal hackers to the Chinese government).

And it was not just a matter of speeches. The U.S. unsealed an **indictment** filed in May charging that four Chinese nationals worked with their government to steal confidential information from entities in a dozen countries. The defendants were accused of engaging in a sweeping campaign between 2011 and 2018 that targeted a wide range of industries, including aviation, defense, education, government, health care, biopharmaceutical, and maritime.

The indictment built on and extended U.S. efforts to establish red lines and encourage cooperation among nations to support them. It was a particularly welcome development because the U.S. response to the spate of attacks that emanated from Russia included lots of threats but no indictment. It seemed to be blurring a sense of where the lines lie. Yet, the U.S. imposed sanctions on Russia, but none on China.

This might be a good time to ask: What *are* the rules?

Cyber rules for nation states used to be fairly clear: espionage was OK, but not economic espionage. Now the rules are anybody's guess.



## THE ATTACKS FROM RUSSIA

The recent onslaught said to be from Russia began with the huge and devastating **SolarWinds** hack, which was revealed last December. What followed was a succession of cyber attacks attributed to Russian gangs, like the ransomware attack on **Colonial Pipeline** conducted by DarkSide, and several more that were the handiwork of **REvil** (short for Ransomware Evil). In the wake of these, pressure mounted on Biden to respond. But his public rejoinders amounted to warnings and threats directed at President Putin.

Harvard law professor Jack Goldsmith summed it up well in **“Empty Threats and Warnings on Cyber.”** As he pointed out, Biden has not been alone in warning the Russian Bear to back off. The Trump and Obama administrations also issued periodic threats, Goldsmith noted. But it has not been all talk. Sometimes the United States has engineered retaliatory strikes that we hear about only after the fact. But then Russia hits again. The administration fumes, fumbles for an answer, and finally threatens. Any teacher can tell you that threats without follow-through are quickly recognized for what they are: pleas for cooperation. And signs of weakness.

So, why doesn't the U.S. just hit back? Few doubt the government has the capability. Goldsmith suggested one reason is that international law limits options when the provocation isn't a conventional armed attack. The larger issue, he said, is the fear of setting off an escalating conflict. And the United States, the most digitized country on earth—and hence the most vulnerable—has the most to lose. I should add that we can't be sure what the government may be doing behind the scenes. **DarkSide** and **REvil** recently appeared to shut down their operations—at least for the time being. There's no way to know if these actions were voluntary or forced by a government. And if so, which one.

Even before the China indictment was announced, a salient issue was lost in the uproar. Where exactly are the red lines for nation states? They used to be fairly clear. Now they're hard to decipher.

## RED LINES FOR NATION STATES

The first time the United States government converted a threat into an action that established a cyber red line was in 2014, when the Department of Justice **indicted** five members of China's People's Liberation Army. (Some observers saw the indictment of people who would almost certainly never stand trial as mere bluster, but I **argue** it was, and is, much more.) In that instance, the Obama administration articulated a clear rationale. The indictment accused the PLA members of stealing confidential information, including intellectual property, from U.S. companies for the benefit of Chinese businesses that were supposedly partners of, or were litigating against, U.S. counterparts.

In the **press release** that accompanied the indictment, then-Attorney General Eric Holder explained that the Chinese government had crossed a line between political espionage, which all countries engage in, and economic espionage. As Holder put it: “Success in the global marketplace should be based solely on a company's ability to innovate and compete, not on a sponsor government's ability to spy and steal business secrets. This administration will not tolerate actions by any nation that seeks to illegally sabotage American companies and undermine the integrity of fair competition in the operation of the free market.”

Yet, the government's criticism of Russia in the wake of the SolarWinds episode seemed to walk back that understanding. Most experts agree, based on what is known so far, that Russian government employees were behind the intrusion, and that it was not for economic gain. Nonetheless, the Biden administration imposed **sanctions** on Russia for its actions. Writing in *Lawfare*, Erica Borghard **questioned why**. She praised the administration for not calling SolarWinds a “cyberattack,” going on to say: “The **distinction** between cyber espionage and cyberattack is important because espionage—including spying that takes

## If a series of ransomware attacks suddenly originate from a new country, are the leaders there now on notice that their country could be sanctioned?

place in and through cyberspace—is a routine aspect of statecraft.” And, of course, the United States engages in as much of it as any nation.

Instead of theft, the Biden administration focused on another aspect. It called the intrusion “disruptive,” Borghard noted. She wondered whether this was supposed to be a new line. In the **“Fact Sheet”** that accompanied the sanctions imposed on Russia after the discovery of the Solarwinds hack, the administration added this about it: “The scope of this compromise is a national security and public safety concern. Moreover, it places an undue burden on the mostly private sector victims who must bear the unusually high cost of mitigating this incident.” So there’s an economic cost, but it’s not the result of theft. Is *this* supposed to be a new line?

### DRAWING A NEW LINE

Beyond these questions, the public conversation has leapfrogged an important issue. In the past, nation-state attacks were those perpetrated by individuals who were employed by the nation in question. But some of the recent attacks attributed to Russia did not identify any of the military groups, like the GRU, that have been named in the past. Aside from SolarWinds, attributions for the other attacks have only meant that the perpetrators were believed to be operating out of Russia. For example, REvil claimed responsibility for an attack that affected between 800 and 1500 companies. Like the SolarWinds assault, it took advantage of a supply chain vulnerability: in this case, that of Kaseya, which sells software to help businesses manage their computer networks.

The United States seems to have no doubt that Vladimir Putin has the ability to control REvil. In blaming Russia’s president for attacks like this, Biden is also asserting that Putin also has a responsibility to do so. On July 9, the Washington Post **reported** that Biden called Putin to deliver this message. “I made it very clear to him that the United States expects when a ransomware operation is coming from his soil, even though it’s not sponsored by the state, we expect them to act if we give them enough information to act on who that is,” Biden said.

This is a new angle worth acknowledging. And it’s not just Biden who is redrawing the line. The G7 has thrown its weight behind this policy. In its **communiqué** in June following the G7 summit in Cornwall, England, paragraph 34 includes this exhortation: “We call on all states to urgently identify and disrupt ransomware criminal networks operating from within their borders, and hold those networks accountable for their actions.” It’s clear that the G7 is not speaking of networks hired by or operating under the control of states. These are independent criminal groups reporting to no one and operating out of self-interest. And the G7 seemed to make a point of saying that this is a line that applies to “all states,” not just Russia. Or not just states that don’t have extradition treaties with theirs.

We don’t know what Putin had to say to Biden over the telephone, or in their private meeting in Geneva in June, after Biden attended the G7 meeting. But this is what Putin said on the eve of the G7 summit in a **televised interview with NBC News**: “We have been accused of all kinds of things: election interference, cyber attacks and so on and so forth. And not once, not one time did they bother to produce any kind of evidence or proof. Just unfounded accusations.” This statement may be the single best justification for the time and effort that was required to present evidence to grand juries that returned all the indictments that named Russian nationals for allegedly engaging in the very acts that Putin cited.



## SO WHERE ARE THE LINES?

A final blurring of lines that was first detected a few years ago in Russia seems to have emerged full bore in China. We have generally thought of nation-state employees and gangs of cyber criminals as two distinct groups. One exception was Russia's Evgeniy Bogachev. **Indicted** by the Justice Department back in 2014, a week after the first indictment was unsealed against China's PLA, Bogachev operated the vast GameOver Zeus botnet. He and his gang used it to plant malware on the computers of businesses, steal their banking credentials, and then wire themselves money. They also surprised victims with ransomware attacks long before these were common. Bogachev never seems to leave Russia, and he's never been apprehended. Like virtually all cyber criminals in Russia, he makes sure not to victimize Russians. And he may have bought himself an extra layer of protection by moonlighting for the state. As U.S. investigators labored for years to try to track him down, they **discovered** that he was conducting espionage on the side for his government. Another Russian cyber thief named Alexsey Belan did the same thing. Belan made his name hacking Yahoo, which resulted in huge data breaches and a 2017 **indictment**.

Those dual roles took a long time to detect because they were carefully concealed. That was apparently not the case with China. The unsealed indictment details a wide array of activities and an equally diverse cast of hackers. Not the kind of operation that's easy to hide. One vestige of the old red lines in the indictment is the careful inclusion of the term that was groundbreaking when it was introduced in that first indictment in 2014. Count 2 is a conspiracy to commit "economic espionage."

It's hard to know where the lines are now. If a series of ransomware attacks suddenly originate from a new country, are the leaders there now on notice that their country could be sanctioned if they don't take swift action—even if the country's government was not involved? The statement made by the large coalition of countries that condemned China suggests it could. But none of the countries that condemned China has yet imposed penalties. Is the sanction red line only for Russia?

The U.S. has not acted to impose sanctions on China probably because the two economies are interdependent, and having been through years of tariff wars during the last administration, the current one has no desire to rekindle the conflict. And one thing we know about China's leadership: They do not issue warnings and hollow threats. If sanctioned, they will almost certainly retaliate.



# XDR: AN ALLIANCE AND A MISSION

KATIE TEITLER

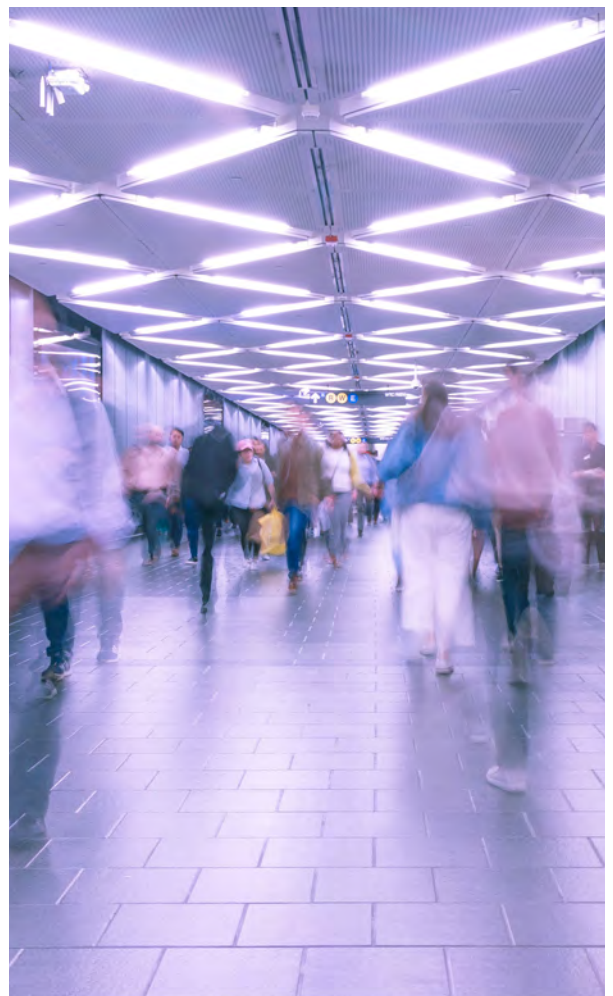
XDR — extended detection and response — is a hot cyber security category these days. It is popular with end user organizations because it (theoretically) aggregates and integrates several cyber security capabilities, giving them a holistic approach to detection and response only. TAG Cyber has advocated integration and orchestration in the past, so we're fully on board with this notion.

However, as with all things cyber, XDR is not so straightforward. The definition of XDR changes depending on with whom you are speaking. Some security professionals argue that XDR is an eXtension of EDR — endpoint detection and response — notably, the EDR and endpoint vendors. Other security pros argue that XDR is an eXtended single vendor offering, bundling endpoint and network detection and response capabilities — notably, some larger security vendors with the ability to cover edge to core. Then, of course, there are the vendor companies that are molding the term to mean whatever best benefits them. (It's akin to what we're hearing from the market about SASE. Every company now claims to be a "SASE company" if they in any way integrate cloud-based protection capabilities from distributed collection points. We also heard this same claim about zero trust a few years back, as well as plenty of other buzzwords and acronyms in preceding years. Long live the so-called hype cycle!)

From this analyst's point of view, the best definition of XDR is the middle one: a capability that eXtends from edge to core. Although time will tell what the market bears out, and I will thus adjust accordingly.

One organization that agrees with me on the edge-to-core concept is the aptly named XDR Alliance. The Alliance, formed at the beginning of August 2021, is led by founding members Exabeam, Armis, Expel, Extrahop, Google Cloud Platform, Mimecast, Netskope, and SentinelOne. It aims to bring awareness to XDR, help standardize on a definition, and gain buy-in for the idea that a true XDR capability requires integration of many components of threat detection, investigation, and response (TDIR), ranging from collecting the right data (e.g., via your endpoint and network tools) to correlation (e.g., your SIEM) and analysis (e.g., security

The goal: to deliver better threat detection, investigation, and response through XDR.



analytics). Other XDR components represented by the member companies are security analytics, identity management, email, cloud, OT/IoT, and network detection and response (NDR) as well as managed security service providers (MSSPs), managed detection and response services (MDRs) and systems integrators (SIs).

During a recent meeting with Gorka Sadowski, XDR Alliance founder and Exabeam chief strategy officer, he explained that the group was formed with the mission to “collectively and collaboratively deliver on the promise of easier and better threat detection, investigation, and response through XDR.” The group, he said, doesn’t focus on selling individual technologies (although each member company clearly sells a product that would fit into “XDR” if you’re using the edge-to-core definition). Nor does it necessarily promote buying from all the companies as a bundled solution. Instead, the idea of the XDR Alliance is to define a true XDR model that benefits enterprise end users and makes them aware of how each technology fits and plays a role within the model. It’s also an educational tool, talking about integrations that already exist within the model as well as new and future integrations based on each member companies’ continuous innovations and collaborations.

Unlike the SASE movement, the XDR Alliance is not promoting the idea that enterprises should buy into a single vendor that provides all the technological capabilities in one platform. In fact, none of the founding member companies currently offers that type of product portfolio. Thus far, from what we’ve heard at TAG, none has plans to build out or scoop up complementary tech to become the one behemoth XDR provider to rule them all.

## COLLABORATION AT THE CORE

Collaboration stands at the center of the Alliance’s plans. Sadowski said, “We are organizing so that we can explain how an open XDR approach that focuses on collaboration and integration benefits enterprises in their ongoing efforts toward better SOC operations. Tools integration and extracting value from those tools with an orchestrated approach shouldn’t be relegated to only the most mature companies with the biggest budgets. Vendors must get better at working together and at developing solutions that allow for enhanced threat detection, investigation, and response.”

Together, the Alliance has developed a three-tier model that focuses on what they consider the essential elements of the XDR stack:

**Data sources/control points:** the IT and security technology that produces IT/security telemetry, logs, and alerts that feed security decisions for SOC teams, and which implement and enforce decisions/responses that need to be performed as part of the TDIR.

**XDR engine:** the analysis engine for all collected data which allows for automated TDIR.

**Content:** pre-packaged content, such as playbooks and workflows, that allow SOC operators to triage alerts and incidents with ease.

The group is nascent and we’ve yet to see a significant amount from them, but it is certain that cyber security needs more collaboration to promote highly secure ecosystems — from both vendors and enterprise end user teams. Today, any technology vendor that tries to stand alone, cannot/will not integrate, and is not making constant improvements to their product or platform is not one this analyst would like to see remain viable.

End users, too, should be collaborating on best practices with colleagues and focusing on training and education for everything from tools optimization to skills building to indicator of compromise awareness.

The XDR Alliance appears to be in the right place to promote this effort around XDR, and we look forward to seeing how they progress over time. If you interested in learning more or becoming a member, contact the industrywide collaborative at [info@xdralliance.com](mailto:info@xdralliance.com).

# HACKING BACK AT RUSSIA IS A TERRIBLE IDEA. HERE ARE TEN REASONS WHY.

EDWARD AMOROSO

---

President Biden continues to hint that our nation will embark shortly on a retaliatory effort involving a major cyber offensive action, presumably taken by US Cyber Command, against Russian targets. This is a terrible idea – and here are ten reasons why.

- 1 Response** – If our military hacks Russian targets, then all sorts of random actors will respond with more attacks against our citizens, businesses, and other unprepared targets.
- 2 Chaos** – Everyone knows that Russia seeks to sow chaos. Offensive cyber retaliation will just escalate this process.
- 3 Defense** – Using our offense as a defense misses the point. Improving our defense is the best defense. We need to focus on fixing our vulnerabilities.
- 4 Servers** – Observers think (immaturely) that retaliation involves hitting “Russian servers” that are attacking us. The targets of US retaliation would have nothing to do with servers.
- 5 Morality** – We’ve pointed to 16 sectors as off-limits on economic and moral grounds. If we hack back, do we target these sectors in Russia? Would it include children’s hospitals?
- 6 Threat** – Russia already knows we have a world-class cyber military. Telling them we will hack back plays into a hand they’ve already considered carefully. This is not news to them.
- 7 Frustration** – We are all frustrated. I am frustrated. But this is a terrible motivation for taking highly consequential action. Everyone knows that.
- 8 Politics** – Yes, it is obvious that President Biden feels political pressure to do something. But we elected him to be a leader, not a follower.

Improving our defense  
is the best defense.  
We need to focus  
on fixing our  
vulnerabilities.





**9 Message** – By implying that hacking back at Russia will solve our cybersecurity problem, we are seriously misleading the American people. The problem will remain.

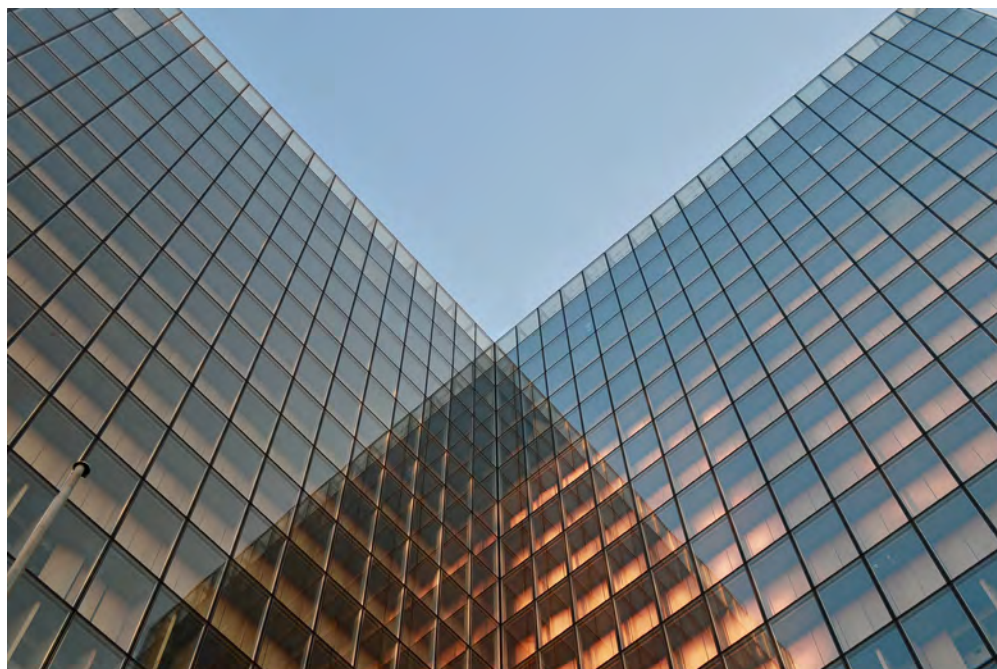
**10 Blame** – We criticized President Trump for diverting COVID blame to China. Is President Biden similarly diverting blame for our cyber weakness to Russia?

Look – the solution to our cybersecurity problem lies at home. We need to simplify our computer systems. Better fund our IT security departments. Streamline complex business processes. Write more elegant code. And massively increase the number of college grads emerging with CS degrees.

It should not be so easy to hack US systems. *Period.* This is our problem. We need to solve this at home.

Do you want to make a difference right now for the future cyber security posture of our nation? Then go help your sixth grader with her math homework.

By the way, if your response to my list is that *we need to do something* or that *we can't just sit back and let the Russians hack us* – then you just made my case.



# HIS CYBER TRAINING WAS NOT ABOUT TECH. IT WAS ABOUT PEOPLE

DAVID HECHLER

J. Keith Mularski knew that he wanted to work for the FBI when he was 16. But when he graduated from college in 1992, he was engaged to be married and the country was in a recession. Jobs were hard to find for a history major. His father, who had once worked in Pittsburgh's steel mills, had later sold furniture. And he'd noticed that a new store had just opened north of Pittsburgh. So, as Mularski told an interviewer in 2014 for the National Law Enforcement Museum's Witness to History program, his first big job was not special agent. It was furniture salesman.

Not the kind of training you'd expect would produce one of the FBI's star cyber security investigators. He wasn't even their IT guy. But it turned out that the skills he acquired and developed would prove crucial in helping him get into the FBI, and then succeed when he advanced into cyber investigations. And they're the same skills that he's counting on now as a managing director at EY, where he landed in October 2018.

What Mularski learned were people skills. It was all about building trust. "In furniture or in sales," he told the oral history interviewer, "you want to get people to give you money that they don't want to give you. And in my business [at the FBI], we get people to give us information that they don't want to give you. So I think that from a standpoint of training, it was a great base for being able to go out and talk to people and make them feel at ease."

The training didn't end there. During his first year of college, Mularski had met an FBI recruiter on campus who had given him a list of qualifications the bureau was looking for in new agents. The big one was five years of professional experience managing people. Before he applied for the FBI job, Mularski had worked his way up to become one of the furniture store's operations managers in St. Louis, and he'd done his five years. He'd also learned how to build trusting



**The career of a law enforcement star, now in the private sector, suggests the most important skills may not be what you'd expect.**

relationships with subordinates, which was an important step for a man who would later become a supervisory special agent leading teams of investigators.

## BUILDING A CYBER HUB

He made his first big splash as an agent in 2005, when he managed to infiltrate a huge international online forum for credit card scammers called **DarkMarket**. It was a testament to his ability to build relationships that the criminals he interacted with completely bought his undercover persona. (Drawing on his family heritage, he claimed to be a Polish hacker who used the handle **Master Splyntr**, which Mularski adapted from a character in the Ninja Turtles cartoons his young son loved.) He established himself so firmly at DarkMarket that the criminals themselves later asked him to take over as their administrator.

He carried on for two years in that role, scrambling to keep up with requests at all hours from members who were scattered across multiple time zones. When Mularski and his wide-ranging law enforcement partners finally shut down the market, they'd gathered sufficient evidence to bust more than 60 of its members worldwide. Officers from Brazil, France, Germany, Turkey, Ukraine, and the United Kingdom all contributed.

Mularski went on to lead some of the biggest cyber security investigations to date. Many of them were during the time that David Hickton was the U.S. attorney for the Western District of Pennsylvania, from 2010 to 2016. Hickton credits Mularski with helping to establish Pittsburgh's reputation as a jurisdiction that knew how to tackle complex cyber cases. That reputation grew as he led and trained agents in the FBI's growing Pittsburgh field office. For his part, Hickton created his office's first group of lawyers who specialized in this area. And he made it a priority. Together they were able to build a string of important cases. The partnership helped turn Pittsburgh into a cyber hub.

Two of the biggest criminal cases were filed in 2014. Hickton signed the country's first **indictment** of individuals accused of engineering cyber attacks by a nation-state. Five members of China's People's Liberation Army (PLA) were charged with planting malware to steal confidential and proprietary information from the computers of a variety of U.S. companies. Some of those companies had thought they were partners of Chinese firms. Others were locked in litigation against Chinese competitors. The 56-page indictment included a wealth of details about what, when, and how information was stolen, and it even displayed photographs of the five PLA officers allegedly responsible.

A week after the PLA indictment was unsealed, Hickton filed another that charged a Russian named Evgeniy Bogachev with stealing about \$100 million from victim companies scattered around the globe. Bogachev and his cronies allegedly launched malware attacks aided by his massive **GameOver Zeus botnet**. They stole banking credentials from companies and then wired themselves money, the **indictment** said. Bogachev surprised some victims with ransomware attacks years before they were commonly found in the cyber criminal's toolbox. Mularski and his FBI colleagues worked with law enforcement partners in a **dozen countries** to take down Bogachev's botnet and its estimated 1 million infected computers.

When I asked Hickton what Mularski's strengths were as an investigator, the former prosecutor ticked off three. "He has unbelievable positive energy. That's number one," said Hickton, now the founding director of **Pitt Cyber**, a multidisciplinary cyber security institute at the University of Pittsburgh. "Number two, he doesn't get discouraged. He doesn't sit around and start thinking about why he can't get something done. He devotes 100 percent of his energy to getting it done." And finally: "He's incredibly resourceful at building relationships."

Jimmy Kitchen, who was deputy chief of Hickton's national security/cyber crimes section, worked closely with the former agent on many cases, including the landmark PLA indictment. He called Mularski

“innovative” and “aggressive.” During his 17 years as a prosecutor—the last 14 in Pittsburgh—he estimated that he worked with at least 1,000 investigators. Mularski was “the best agent I’ve ever worked with,” said Kitchen, now a partner at Jones Day. He was also “one of the best-connected.” His relationships were wide and deep, the lawyer said, and when they needed information, he always seemed to know someone to call.

**The big difference is that he used to be on offense, trying to arrest the bad guys. Now he’s playing defense.**

## LESSONS HE IMPARTS TO COMPANIES

After he’d put in his 20 years at the FBI, Mularski was ready for a change, he said. He knew some people at EY. The company had a good reputation and was particularly strong in this area. He saw an opportunity and he took it.

How do his skills translate? It’s not as different as you might think, said Mularski, who still looks youthful at age 50. “When I was at the FBI, I woke up in the morning, I looked at what was the latest threat intelligence, and we used that to help solve cases and write reports,” he said. And now? “I wake up in the morning, I look at the latest threat intelligence, and we write reports.” And he helps clients figure out how to defend themselves against those threats. “I still talk to a lot of the same people, and partner with some of the same people,” he added.

The big difference, of course, is that he used to be on offense, trying to arrest the bad guys. Now he’s playing defense. At EY, he consults with clients as a subject matter expert on cyber threat intelligence and SecOps, he said. And he works with some clients on a regular basis. He won’t give a precise number, but it’s “dozens.” And again, that means building new relationships.

His work with them is analogous to what a football coach does, Mularski explained. Clients need to answer three basic questions. First, who are the adversaries? Some companies may be susceptible to attacks from nation-state groups, he noted, others not so much. After studying the threat landscape (which is like watching game film on the teams you’ll play), clients should ask: What tactics, techniques, and procedures are the attackers likely to use? And then: How can we craft a defense designed to match up?

Like all coaches, Mularski preaches “practice, practice, practice.” You want to have a red team that understands how it’s going to attack. And you want them to be innovative to really test the defense. And then you work with the blue team on detection—isolating and recognizing the activity. And doing it fast, and then faster, he said. You keep running those exercises, building up muscle memory. So that when the real thing happens, the company is ready.

## THE BENEFITS, AND THE LIMITS, OF TALKING TO THE FEDS

He encourages businesses to reach out to law enforcement in advance of an attack. Whether it’s the Secret Service, the FBI, or the Cybersecurity and Infrastructure Security Agency, they can help, he said. A company has a micro lens. The agencies have a macro lens. They may have information about attackers and their methods that a company wouldn’t have.

But Mularski understands that corporations are often reluctant. “I think they fear that they’re going to show up on the front page of The New York Times,” he said. “And the other thing is most companies don’t realize that the government doesn’t want your client data, or your PII [personally identifiable information].” What they’re looking for, he said, is new types of attacks, new techniques, new pieces of the puzzle.



The decision on whether to initiate contact is always up to the client. He doesn't exert pressure. He tries to educate them, he said—give them an idea of what the exchange will be like. And he can reassure them that “you can do it in a way that still maintains privilege and maintains your privacy.” But it takes time, he acknowledged. “Why do you share personal information with people? Because you know them and you trust them.” And that takes building a relationship.

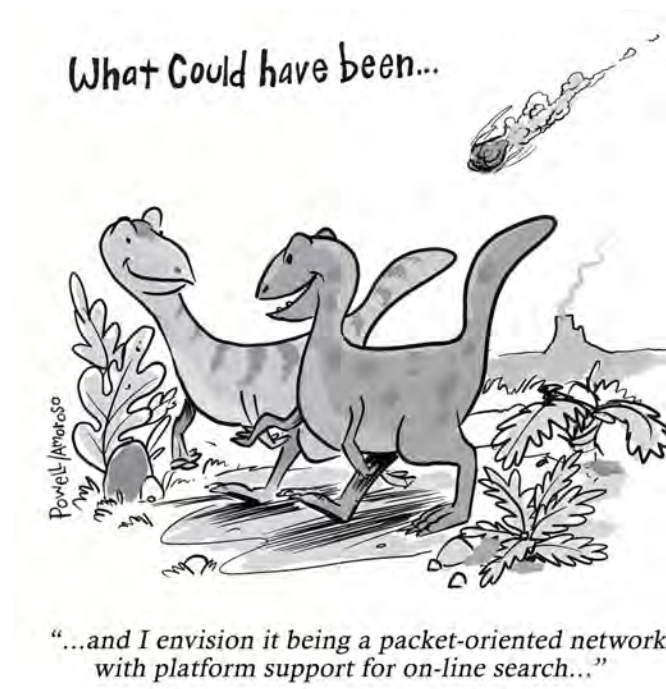
The other piece that some companies don't understand is that the feds don't come over and fix your problem. “When you have a ransomware attack,” Mularski said, “it is great to call the FBI and let them know. There's probably a field office that's working that, and they could share information.” But neither the FBI nor any of the other agencies are going to show up to unencrypt your computers, he continued, or help you with your incident response. Those are the things that companies must plan for themselves.

## LOOKING BACK

After the conversation wound down, I asked Mularski what he misses most from the old days. There were no surprises in his answer. “I miss the people and the comradery,” he said. “Over 20 years, I really developed some great friendships worldwide.” Beyond that, “I also miss feeling that your cases are making an impact and a difference on a worldwide level.”

He added that when he left, he knew “in my position at EY, I would still be able to help companies protect and defend against cyber attacks. As a result, it was a win-win situation for me.”

When I asked what he misses the least from his days at the FBI, there was no shock there either. “Hands down, the bureaucracy.”







# INTERVIEWS





Raffaele Mautone

## AN INTERVIEW WITH RAFFAELE MAUTONE, CEO, AND JULIE CULLIVAN, BOARD MEMBER, AADYA



Julie Cullivan

# SUPPORTING CYBER SECURITY FOR SMALL AND MIDSIZE BUSINESS

The challenge to reduce cyber risk has traditionally been greatest for larger businesses with high consequences for successful breaches. More recently, however, it has become clear that significant cyber threats exist for organizations of all sizes and scopes. As a result, security solutions have had to be developed that can address the unique needs of small and mid-size businesses.

The provision of such services cannot just involve either modifying or downsizing solutions that were developed for larger companies. Instead, small and mid-size companies require tailored cyber security protections that match up with their typical means for conducting business operations – often with on-going revenue growth and product or service scaling objectives.

***TAG Cyber: Tell us about AaDya. What are the types of products and services you provide customers?***

**RAFFAELE MAUTONE:** We provide smart, simple, effective cyber security software solutions for small and medium-size businesses. We believe the size of your company (or your budget) shouldn't limit your ability to combat cyber threats. That's why we've developed an all-in-one software solution to provide smart, simple, affordable, and effective cyber security protection.

Powered by Judy, our innovative AI, along with machine learning, AaDya's product provides 24/7 protection for SMBs that, without it, might lack the time, expertise, and capital to successfully implement these solutions.

***TAG Cyber: What are some emerging trends you see in cyber threats to small and mid-size businesses?***

**JULIE CULLIVAN:** Cyber threats for small and mid-size businesses are really the same as they are for larger enterprises. The differences are only the size and complexity of the attack surface, and little to no dedicated security resources. Recently, there has been an uptick in the number of ransomware attacks; however, along with it, phishing, malware, and credential stealing continue to be the biggest threats to any organization. Additionally, businesses are struggling with the fundamentals of security hygiene: vulnerability management, credential and privilege management, multi-factor authentication, and defined (and tested) incident response plans. As the old adage goes: The more things change, the more they stay the same.

Our artificial intelligence and machine learning differentiates us from our competition. Designed with small businesses in mind, this proactive AI approach manages, monitors, protects, and informs.



***TAG Cyber: Do most small and mid-size companies have dedicated security teams or even a staff member who focuses on this area?***

**MAUTONE:** Cyber security remains at the forefront of many leaders' minds as the need increases to protect their companies. However, many small businesses do not own security software due to such factors as prioritization, cost, specific expertise, and a dedicated security staff.

For too long, small and mid-size businesses have been overlooked in favor of serving the enterprise. They are left to try to build a strong security stack with point products that are often too expensive, and too complicated, for small teams to manage. And, while they have the technical expertise to manage these solutions, the service providers that support these businesses have to pass along the costs to their customers. The result is that many end up under-protected, putting their businesses, and the customers they serve, at risk.

At AaDya, we are building a partner program to bring real value to this underserved sector and to those who support it. It gives service providers, value-added resellers, and consultants an offering that is easy for them to deploy and manage, and it provides their customers with enterprise-level security in one package that even their non-technical users will enjoy using.

***TAG Cyber: How do you incorporate automation and innovation into your security platform solutions?***

**MAUTONE:** AaDya provides customers with a flexible, comprehensive solution with multiple cloud-based offerings. We are not a point product, and pride ourselves on offering a unified approach to what small businesses need.

Our artificial intelligence and machine learning differentiates us from our competition. Designed with small businesses in mind, this proactive AI approach manages, monitors, protects, and informs. It finds and mitigates issues quickly through machine learning and security automation.

***TAG Cyber: Do you have any predictions about emerging cyber threats to business infrastructure?***

**CULLIVAN:** The risk will continue to be the attack surface and what businesses can control. The reliance on large, centralized infrastructures and software services will mean that one attack could have ramifications for thousands of businesses. More and more connected devices, which are not (and in many cases cannot be) managed, will create risk for organizations. Additionally, individual online users now have access to the same tools and the ability to develop TTPS skills on a par with APT and cyber criminal organizations. The same fundamentals I spoke of earlier will remain the best way to mitigate these risks. Remember, the threat actor only needs to be right once, but your security needs to be right 100 percent of the time.





## AN INTERVIEW WITH CANDID WÜEST, V.P. OF CYBER PROTECTION RESEARCH, ACRONIS

# UNIFYING DATA PROTECTION AND CYBER SECURITY

The needs of service providers, businesses, and individuals to address cyber threats continues to increase. In many cases, different platforms and solutions are required to deal with these different requirements. While this reflects the uniqueness of the use cases for each type of user, the fact remains that many types of controls will be quite common across this range of practical applications.

One area of cyber protection that applies and scales well for service providers, business, and individuals involves continuous data protections based on foundation measures such as patch management, antimalware protection, server backup, and data recovery. All of these controls are important and relevant in virtually every practical context where data is essential to the organizational mission.


***TAG Cyber: Is ransomware the biggest threat you see to most enterprise teams and service providers?***

**ACRONIS:** Ransomware is the biggest threat for enterprises of all sizes and has the biggest impact on them. Of course, often there is a connection to other cyber attacks which enable the ransomware attack, such as phishing emails used to steal passwords, or unpatched systems penetrated to drop malware. That said, the most devastating final payload is still ransomware. Unfortunately, the entry barrier for cyber criminals is low. Ransomware is now offered as a service, with tutorials and help desks, making it accessible to a large audience. Many companies are inadequately prepared to counter this threat, so we see criminal groups acquiring millions of dollars in paid ransom, making it a very profitable attack model that is not going to stop anytime soon.

***TAG Cyber: What is the role of backup and recovery in addressing modern cyber risks?***

**ACRONIS:** Cyber attacks such as ransomware disruptions usually encrypt all data and workloads. In some cases, this data cannot be decrypted even when the victims pay the ransom demand. For this reason it is crucial to have a working and tested backup of all relevant data ready at all times. Since cybercriminals often try to delete all backups, it is also important to protect them from tampering. But having functioning backups is just one part of a cyber protection plan. Being able to recover fast and safely is just as important. The restore process should be efficient, ideally only restoring the required data, while making sure that the

In a survey conducted by Acronis in 2021, 21 percent of the respondents said that they use more than 10 different security solutions in parallel.



recovered workload is no longer in a compromised state (as from a hidden backdoor in a previous backup).

***TAG Cyber: The earliest antivirus tools did not work as well as buyers might have liked. What advances have led to more effective antimalware solutions for modern users?***

**ACRONIS:** Next-generation antivirus tools combine multiple defense layers in a defense-in-depth approach. Traditional signatures are still relevant as they are fast and accurate, but they should be combined with modern methods such as behavior-based detection. Analyzing the behavior of a threat enables the blocking of malware that has not been seen before, and can even stop the use of legitimate tools like PowerShell in a malicious context. Another important layer is the use of machine intelligence to find similarities in files or anomalies in system behavior and block it. Not to be forgotten is the integration of all of these layers with other cyber protection solutions to ensure maximum protection with minimal effort. Your antivirus solution should talk with the backup and patch management to have the big picture.

***TAG Cyber: Do managed service providers have unique needs in cyber security? How is Acronis addressing these needs?***

**ACRONIS:** Managed service providers need simple solutions that work efficiently and can be automated in many ways. In a survey conducted by Acronis in 2021, 21 percent of the respondents said that they use more than 10 different security solutions in parallel. Such highly complex environments are error-prone and cost the service providers a lot of time to manage. The trend there is to consolidate solutions, while simultaneously increasing the overall cyber protection level through integration. Of course, there are other unique features required by service providers such as multitenancy or integration into billing systems.

***TAG Cyber: How does disaster recovery factor into the cyber security equation?***

**ACRONIS:** The strategy is called “hope for the best, plan for the worst.” The likelihood of business interruption due to a cyber attack or natural disaster increases with the continued growth of digital transformation. A good incident response plan that also covers disaster recovery can mean the difference between a brief business interruption or a weeklong offline status. Or worse. The ability to quickly spin up your backups as virtual machines in the cloud or failover to a copy of the critical servers, while the compromised machines are restored, can literally save your business.



## AN INTERVIEW WITH EREZ ANTEBI, CEO, ALLOT

# PROTECTING FAMILIES FROM CYBER THREATS

During the past decade, individuals and families have increased their use and dependence on technology, software, and the internet for their personal, business, and community activities. With this increase has come a greater need to reduce the risk of cyber threats from malicious actors. These threats traverse service provider infrastructure on their inbound path to the family home and family members.

Most traditional security solutions such as antivirus have not been effective in addressing this challenge. As a result, families remain vulnerable to credential theft, account takeover, and loss of personal data. Furthermore, with the plethora of sites containing malware and other unacceptable downloads, files, and content, families struggle with a solution to the growing problem.

**TAG Cyber: What are the types of products and services you provide for your Allot customers?**


**ALLOT:** We provide network-based cyber security solutions that enable telecom carriers and other broadband providers the ability to deliver zero-touch cyber security services to their consumer and SMB customers. Allot cyber security solutions offer protection against cyber threats, including malware along with phishing and ransomware attacks. Protection covers all of an end user's devices while on the carrier's network—at home, in the office, and even off-network. And all with a simple, unified management experience. Unlike many value-added services, network-based cyber security is becoming an integral part of the carrier's offering. This has proven to be the case with numerous carriers that have achieved 30–50 percent adoption rates for network-based cyber security services aimed at consumer customers.

**TAG Cyber: What are some emerging trends you see in cyber threats to the typical consumer family?**

**ALLOT:** Consumers have always been vulnerable to cyber threats. Today, consumers face more risk than ever before. The work-from-home trend not only brings the office into the home, it also makes the home a central target of cyber crime. Larger companies are more likely targets for cyber criminals. When workers bring their devices to the home network, all the connected devices become doorways to the corporate devices in the home, making it a more interesting target.

IoT and smart homes also pose a growing threat to the consumer. Poorly secured IoT devices are often the easiest, and therefore first point of entry into the home network, for cyber attacks. As IoT device penetration grows, so does the likelihood of attacks on the home network, its devices, and its data.

## We believe that 5G and IoT will bring more frequent attacks to the consumer realm as these technologies proliferate.



Also troubling in the era of COVID 19 is the growing amount of time children at home spend staring at screens. Not only is it a problem for parents who want to protect their children from harmful content; the more browsing, downloading, and playing they do, the higher the risk of malware infection on home networks and mobile devices.

***TAG Cyber: Do families typically understand the risks that exist? Are they willing to take steps to reduce this risk?***

**ALLOT:** Our research shows that most consumers are aware that there are risks that affect their devices and data. Many have already taken some steps to try to mitigate problems they know about. But either the cost or the complexity, among other barriers, reduces the likelihood they will take real action to mitigate cyber threats. However, our global survey did reveal that 90 percent of consumers believe that their service provider should bolster cyber security in addition to offering connectivity, and they were willing to pay for the service. In addition, seven of 10 consumers indicated that they would switch to another provider if offered better security.

***TAG Cyber: How do you work with service providers to offer your solution?***

**ALLOT:** Our software solutions are installed in the service provider's network. This enables them to provide branded cyber security services to consumers and small and medium-size business customers. Through our engagement with our CSP customers, we become very close partners. This is partly as a result of our business model, which relies on revenue sharing rather than upfront solution costs. We install the solutions and customize them to match the CSP's branding and specific needs. Then, as monthly service revenues are accrued, the customer shares those revenues with Allot. To optimize revenue, Allot provides cyber marketing services designed to help the customer sell services and retain the subscribed base. We have been very successful in achieving high adoption and retention rates—because of the draw of the services, and as a result of the relationship between our cyber marketing department and our customers.

***TAG Cyber: Do you have any predictions about emerging cyber threats to families?***

**ALLOT:** We believe that 5G and IoT will bring more frequent attacks to the consumer realm as these technologies proliferate. As consumers welcome these technologies into their homes, and pockets, and wrists, and cars, the devices will bring with them more frequent and more sophisticated attacks. Without proper protection—from the CSP in the best case—consumers will be far more aware of cyber attacks, and the effects they will have on consumers' privacy and digital assets.





## AN INTERVIEW WITH RAHUL KASHYAP, CEO OF AWAKE SECURITY, ARISTA NETWORKS

# ADVANCED DATA-DRIVEN NETWORK SECURITY

The technical and operational interaction between networking and security has always been close, and experts in each area will attest to the need to cooperate when dealing with cyber threats. Founded in 2004 and headquartered in Santa Clara, California, Arista is a large public company that fully understands this interaction and has championed the delivery of world-class products in each area.

Arista specifically addresses important new issues such as cloud-grade routing, programmable switching, converged infrastructure networking, telemetry and analytics, IP storage and big data, media and entertainment support, electronic trading, and cognitive cloud computing. To this portfolio, Arista has developed a strong security solution, spearheaded by its acquisition of Awake Security.

**TAG Cyber:** *Tell us about Arista. And what acquisitions have you been involved with recently?*

**ARISTA:** We are an industry leader in data-driven cloud networking solutions for large data center and campus environments. Many of the largest cloud service providers, financial services institutions, retailers, and technology providers rely on Arista's infrastructure to provide reliable and high-performance network services. Arista invests heavily in improving business outcomes for our customers through organic innovations and acquisitions of best-of-breed solution providers. Our two most recent acquisitions were Awake Security, an AI-driven network detection and response provider, and Big Switch Networks, which delivers pervasive and programmable network observability.

**TAG Cyber:** *What are some emerging trends you see in network security?*

**ARISTA:** We see two technology trends and one business trend. Starting with the business trend, we see more and more customers that look at security as an adjective rather than a noun. They are expecting a network that, in a sense, is self-securing rather than bolting on a myriad of "security solutions" on top of the network infrastructure. In other words, customers want to see the underlying switches, routers, etc. as part of the security defenses.

On the technology front, with the rapid pace of the ongoing digital transformation, we see customers struggling to understand and secure all the unmanaged devices on the network. In many cases, north of 50 percent of devices

No discussion on threats can go very far without talking about ransomware. We are seeing trends like the use of a double tap strategy where data is both encrypted and exfiltrated.

on the network fall in the unmanaged bucket, which means no EDR agents deployed, no logs being pulled off the device, etc. These devices are everything from BYO devices to DevOps and shadow IT, as well as IoT. Of course, cloud workloads and SaaS applications also contribute to this lack of visibility. All of this contributes to a significantly larger attack surface that we already see being exploited by nation state-sponsored ransomware gangs and other threat actors.

Finally, we see a continuous increase in the amount of encrypted traffic on the network, even in east-west corridors. Traditional network security solutions rely on visibility into the clear text payload, typically achieved by TLS interception. Unfortunately, given the privacy implications and some of the changes with protocols like TLS 1.3, decryption is simply not a viable option. Therefore, we see a trend toward encrypted traffic analysis. The objective is to use data science methods to get smarter about threats buried within the encrypted traffic without ever performing decryption.

***TAG Cyber: Do most enterprise teams understand the importance of software-driven network solutions?***

**ARISTA:** I believe so. In fact, if anything, the last 18 months of “work from anywhere” have almost forced most organizations to adopt a software-driven approach. The adoption of the cloud and SaaS applications has also accelerated this trend.

Interestingly, today we find that our customers are moving one step further on this continuum by asking for a data-driven approach: What is the ground-truth data from the network telling us about the threats in the environment? Is there risky insider behavior? Are there basic hygiene issues like weak passwords that might be driving risk? They are also looking for this approach to come with broad programmability. This applies to real-time, network-state streaming, a programmable monitoring fabric, and programmable threat detection and response. For instance, we see organizations that want to evolve from traditional black box “AI-based” solutions to a system where the detection models are open and can be tweaked or adapted using a simple set of tools without the need for data scientists on staff.

***TAG Cyber: Do you have any predictions about emerging cyber threats to network infrastructure?***

**ARISTA:** Well, clearly no discussion on threats can go very far without talking about ransomware. We are seeing trends like the use of a double tap strategy where data is both encrypted and exfiltrated. This way, even if the target restores from backups, the threat actor will simply threaten to publicly release the data. The prediction here is that customers are going to get a lot more

focused on detecting the early warning signs in order to intercept and remediate before the encryption event.

We see more threats specifically looking to exploit IoT devices and other unmanaged infrastructure. Along similar lines, the lack of comprehensive visibility into the network is leading to unpatched infrastructure, from firewalls and VPN concentrators to remote access solutions. The point is that hygiene around passwords and patches is becoming “cool” again.

We also believe we will see more “hybrid” attacks—attacks that move between a customer’s on-premise and cloud-based infrastructure. For instance, we recently saw a targeted attack that used malicious browser extensions to steal the password from the organization’s cloud administrator. Those credentials were then used to login to the cloud console and compromise workloads.

Finally, we believe the mantra “every threat is an insider threat” will continue to be proven right. This is not to say that behind every threat is a malicious insider. Instead, we are seeing “innovative” ways through which external attackers are gaining legitimate insider access—whether through bribery, extortion, or tricking an unsuspecting victim.



*“Mom, if you’d like to contact me,  
I’d recommend you download my app.”*



## AN INTERVIEW WITH TUSHAR KOTHARI, CEO, ATTIVO NETWORKS

# PREVENTING AND DETECTING LATERAL MOVEMENT

When advanced attacks are initiated toward an enterprise, several familiar tactics are almost always used to gain privilege, traverse infrastructure, and advance the goals of the breach. Unfortunately, these steps are rarely addressed by existing cyber security solutions, which either try to prevent the attack (shift left) or just deal with its consequences afterward (shift right).

Founded in 2011 and headquartered in Fremont, California, Attivo Networks is a leader in bridging this defense gap for customers. With solutions that utilize visibility and mitigation into identity services, Active Directory, and deception-based processing, Attivo has become a major provider of advanced controls that can help customers avoid the negative impact of an active threat campaign.

**TAG Cyber:** *Attivo is such a prominent brand in our industry. What has been the recent evolution of the company?*

**ATTIVO:** We are best known for cyber deception technology, which provides customers with an active defense for Stage 2 post-compromise threat detection. This year, the company has extended its portfolio into the area of identity detection and response (IDR). This move is being referenced as the expansion that brings Attivo to a level where unicorn status is achievable.

With the rapid shift to remote working and accelerated cloud adoption, the concept of a perimeter and edge security has faded. Taking its place is the concept of an identity-first security posture, where security is centered on protecting credentials, privileges, cloud entitlements, and the systems that manage them.

Identity-first security is distinctly different than identity protection solutions, which include identity access management (IAM), privilege access management (PAM), and identity governance administration (IGA). Identity protection focuses on making sure that the right people can get uninterrupted access to the things they need.

Leveraging its expertise in lateral movement and privilege escalation, Attivo concentrates on prevention and detection technology. The company is uniquely positioned to provide end-to-end visibility across endpoints through Active Directory (AD), and into multi-cloud environments. When Attivo provides security professionals with unprecedented visibility, security teams can easily understand identity-based security exposures,



## The nature and scope of existing security paradigms are becoming outdated since the arrival of new identity-based threats in the public cloud.



reduce attack surfaces, and fortify the environment with concealment and deception technology for asset defense.

***TAG Cyber: What are some emerging trends you see in the detection of lateral movement in an enterprise?***

**ATTIVO:** Identity-first security has emerged as one of the top security risks and management trends for 2021. Attack surfaces have expanded dramatically over the past year as the COVID-19 pandemic forced record numbers of employees to work remotely. There's been a clear shift toward remote work, making identity a priority and demanding vendors move away from traditional LAN edge design.

Given that 57 percent of breaches involve insider threats—and employee/third-party negligence is a leading cause of those incidents—it makes sense that securing identities has made its way to the top of every CISO's to-do list. Detecting these insider threats remains a challenge for many organizations, and with more users than ever working from home, the ability to detect in-network lateral movement is only growing more important.

To make sure identities at the user, device, and domain level are secure, protecting AD is also becoming a CISO-level concern.

***TAG Cyber: Do most enterprise teams understand advanced threats, and how to detect them and prevent consequences?***

**ATTIVO:** The nature and scope of existing security paradigms are becoming outdated since the arrival of new identity-based threats in the public cloud.

Identity security is central to the cyber security threat landscape, and the ability to detect and respond to identity-based threats is essential. While many tools intend to keep networks secure, IDR gives organizations a critical new weapon in their arsenal to find and fix credential and entitlement weaknesses, and to detect live attacks on a real-time basis.

As modern cyber criminals attempt to exploit vulnerable credentials and entitlements to move laterally across networks undetected, IDR solutions play a meaningful role in stopping them. Other tools simply cannot.

***TAG Cyber: How does your platform work in the context of cloud infrastructure?***

**ATTIVO:** In a traditional setting, user accounts are the primary security focus. But in the public cloud, applications, databases, and data stores (among others) routinely have entitlements to other resources. The sheer volume of cloud identities and entitlements resulting from new concepts like non-human

identities and managed services is palpable for today's overwhelmed cloud security teams.

What might amount to hundreds of identities on a traditional network can translate into thousands in the public cloud, leaving security teams often blind to the full extent of their exposure. High-profile data breaches have underscored what identity-based attacks can do once attackers exploit misappropriated privileged credentials.

To address this challenge, Attivo Networks introduced IDEntitleX, the company's cloud infrastructure entitlement (CIEM) solution. Security teams gain actionable awareness of cloud identity and entitlement exposures so that they can see risky entitlements and drift from security policies. The solution makes identifying and reducing risk easy by providing intuitive and interactive graphical visualizations for cloud identities, roles/permissions, and resources. Defenders now gain the visibility needed to see misconfigurations and excess permissions that attackers can leverage to create attack paths and persistence within the cloud environment.

***TAG Cyber: Do you have any predictions about emerging cyber threats to modern enterprise infrastructure?***

**ATTIVO:** Next year will be the year of identity security. Businesses that want to arm themselves for an onslaught of advanced ransomware attacks must take fundamental measures to understand identity-based credential, entitlement, and Active Directory risks and attack activity.





AN INTERVIEW WITH DR. NEIL COSTIGAN,  
CEO, BEHAVIOSEC

## CONTINUOUS AUTHENTICATION FOR END USERS

One of the more familiar and common methods of authentication, other than passwords, involves the use of human attributes to validate a reported identity. While early biometrics technologies were mostly centered on voice and fingerprint capabilities, modern biometrics takes advantage of advanced methods for integrating a wide range of personal attributes into an effective authentication scheme.

BehavioSec serves at the forefront of this drive toward truly advanced biometric solutions for customers. Leveraging their work with DARPA in the early 2000s and using the most innovative techniques available, BehavioSec offers customers technology that can be used to strengthen multi-factor proofing, improve security compliance, and minimize user friction. Such objectives have become essential in the context of modern digital transformation.

***TAG Cyber: Biometrics and passwordless authentication are not new, but they're only recently gaining widespread adoption. What factors are driving this trend?***


**BEHAVIOSEC:** Consumers and the workforce have had enough of traditional forms of online security such as PINs, tokens, and passwords. Any convenience passwords had was lost long ago in a steady increase of password complexity, making them hard to remember without bringing much—or any—security uplift.

The passwordless transformation largely stems from the convenience of biometrics. While passwords have become less convenient, biometrics has become more accessible, with sensors now added to almost every device, making authentication easy and convenient. They don't need to be remembered, they are always with us, and they offer a flexibility that passwords can't match.

Thanks to our advancements in machine learning, the creation of accurate and cost-effective profiles has made continuous biometrics ready for primetime. Behavioral biometrics in particular is fast gaining popularity as more organizations see the benefits that come from continuous protection.

As we move toward a passwordless and continuous authentication future, we have the opportunity to raise the bar substantially, and biometrics allows us to do so while maintaining the convenience we have come to know and expect.

Through the convenience of biometrics, employees are empowered to be just as productive wherever and whenever they choose to work, without compromising their employer's security needs.



***TAG Cyber: What are some emerging trends you see in cyber threats to modern enterprise, and how does biometrics help to reduce the risk?***

**BEHAVIOSEC:** Security teams will need to remain vigilant in order to mitigate new challenges brought on by remote work. Enterprise attacks like ransomware, spear phishing, insider threat, and business email compromise are growing fast, and, unfortunately, there are no silver bullets to stop them.

This is complicated further as security needs collide with the access and authorization needs of a remote workforce. IT departments have been focused on authorizing the right people to access the right system at the right time, but what if an unauthorized person uses an employee's device to gain access to confidential or sensitive data?

Ensuring that enterprises can trust that employees are who they claim to be is critical. Now, with a redefinition not only of the physical workplace but the workforce itself—from office workers to distributed employees, contractors, overseas call centers, and close to 60 million gig-economy workers—that task is harder than ever.

Maybe this workplace change is permanent, forever transforming when, where, and how we work. Either way, the security benefits from continuous authentication and biometrics are here to stay. When used responsibly, biometrics can create high levels of trust between employees and employers. Trust that they are securing their devices when being used remotely, that if they lose their devices the data cannot be accessed, and that they can access their workforce applications at their convenience.

Through the convenience of biometrics, employees are empowered to be just as productive wherever and whenever they choose to work, without compromising their employer's security needs.

***TAG Cyber: How are you seeing attackers circumvent traditional authentication and commit fraud? What's new that readers should be concerned about?***

**BEHAVIOSEC:** Social engineering is still, unfortunately, one of the hardest attack vectors to defend against. Human behavior becomes the weakest link, as criminals manipulate victims into parting with money, information, or products. The easiest way for attackers to get what they want is to manipulate people into giving it to them, and our willingness to trust others is built into our DNA.

The attackers are often thorough, and prepare by collecting information about their intended targets. Many people publish enough information about themselves on social networks to facilitate this type of fraud, like a photo of a passport, driver's license, or boarding pass.



Once they have information about their targets, attackers often begin with an email or phone call that induces a sense of urgency in the victim, which leads the victim to promptly comply. Once they have a victim on the hook, the criminals use every technology available to them to make themselves more convincing—like advanced remote access tools. While technology has made some kinds of fraud more difficult to commit, it has also empowered criminals to conduct confidence tricks that are more convincing than ever before.

Luckily, continuous biometrics allows us to reverse this trend and turn human behavior from the weakest to the strongest link.

***TAG Cyber: Tell us about your platform and how it works?***

**BEHAVIOSEC:** BehavioSec offers an automated fraud and authentication platform, powered by behavioral biometrics. It is the first solution to connect behavioral biometrics to and across the entire user lifecycle, detecting attacks with superior precision while providing continuous invisible multi-factor authentication (MFA) to employees and consumers. It ensures accurate, real-time decisions across new applications to payments to existing accounts—protecting consumers and enterprises from fraud while reducing friction, supporting compliance, and giving security powerful investigative capabilities.

In contrast to static information and one-time security, our behavioral biometrics solution learns by silently analyzing how people type, swipe, and interact on their devices. It analyzes activity in the background throughout sessions to generate a continuous authentication signal that reduces both costs and false positives from legacy systems, while detecting even the most sophisticated social engineering, session hijacking, malware, or credential-stuffing attack.



AN INTERVIEW WITH PATTY WRIGHT,  
SVP AND GM OF CONSULTING, BISHOP FOX

## BRINGING AN OFFENSIVE MINDSET TO CYBER DEFENSE

The advantage between offense and defense in cyber security has almost always tipped in favor of the attackers. One of the first things learned by any individual or team with respect to cyber is that the good guys (defenders) need to fix every possible inbound path toward a valued resource while the bad guys (offenders) need only find one path in. This basic fact is one of the reasons breaches remain so common.

Bishop Fox has specialized for years in bringing an offensive mindset to playing defense. The objective is to incorporate the methods, skills, and perspective of the capable hacker into the techniques and tactics used by enterprise cyber security defenders. This approach, which includes both products and services, results in a new form of defense, one that is more flexible and malleable to the situational needs that arise during an attack.

***TAG Cyber: What cyber security solutions do you provide customers?***


**BISHOP FOX:** We offer offensive security solutions ranging from penetration testing, red teaming, and attack surface management to product, cloud, and application security assessments. Notably, our award-winning continuous attack surface testing (CAST) platform addresses the growing need to proactively secure complex and constantly changing IT environments against increasingly sophisticated attackers. We were thrilled to have CAST named “Best Emerging Technology” by SC Media earlier this year in recognition of our innovation in this space.

***TAG Cyber: How do you effectively combine professional services with platform support?***

**BISHOP FOX:** Our CAST platform combines advanced technology and automation with human expertise delivered by a team of highly skilled operators. We took what we learned from delivering offensive security services over the past 15 years and developed a proprietary engine for comprehensive asset discovery and exposure reconnaissance. This technology enables CAST to continuously discover and map ever-changing attack surfaces and identify vulnerabilities that pose real risk.

By creatively (and extensively) leveraging automation, CAST eliminates the noise and false positives that plague many tools, and reveals true exposures that are then tested and validated by our dedicated team of operators, many of whom hail from the DoD and NSA. They are emulating real-world attacks on a continuous basis for our clients, safely exploiting exposures, and then

**While the SolarWinds breach may have come as a shock, the reality is that it is the tip of the iceberg.**



conducting extensive post-exploitation activities to uncover internal pathways, systems, and data that could be susceptible to attack. The CAST operators also interact with customers via an encrypted Slack channel to provide real-time insights into findings, and to conduct on-demand retesting to validate remediation procedures.

We feel this unique combination of technology and services provides our customers with the best outcomes, and successfully addresses the challenges of securing dynamic attack surfaces in an evolving threat landscape. We're able to identify true exposures and ensure the findings are actually operationalized and acted upon to close attack windows. The continuous and collaborative nature of our delivery overcomes a lot of hurdles for our clients. For example, they no longer need to worry about missing something in between point-in-time annual pen tests, or filtering through an overwhelming volume of noise from vulnerability scanners. CAST gives them real, reliable results that are focused and actionable, as well as on-demand access to an expert team of operators.

***TAG Cyber: How does your security platform work?***

**BISHOP FOX:** The CAST platform launches with discovery, starting with the client's brand to ensure we are seeing their perimeter the same way an attacker would. The platform identifies and maps domains, subdomains, networks, cloud infrastructure, SaaS, and assets our clients often don't even know exist. This last piece is highly impactful for clients, since they can't secure what they don't know about. The targets are validated for accuracy and then run against a series of analyzers to identify exposures across five categories: misconfigurations, missing patches, sensitive information leaks, weak passwords, and insecure applications.

Our attack surface intelligence team regularly adds new analyzers based on vulnerability research and real-world findings across our client base. This allows us to continually enrich CAST and ensure we are identifying emerging threats, as well as traditionally less severe vulnerabilities that are often missed or noted as low risk, but in fact serve as steppingstones for attackers.

The exposure candidates produced by the analyzers are then processed and filtered by the CAST automation engine. Leveraging automation enables us to run more tests more quickly, so that we can accelerate identification of true exposures. It also successfully removes all those false positives, low severity exposures, and redundant data that security professionals have grown to hate. The true negatives are reported to our clients and a set of prioritized leads are sent to our team of operators for initial- and post-exploitation testing.



Our CAST operators emulate real-world attacks from persistent adversaries, leveraging the findings from the previous steps and using the same methods and tools attackers employ. They safely exploit exposures and then conduct post-exploitation activities to identify real impact and to provide insights into attack windows. Validated true positives are reported to our customers in the CAST portal, and an encrypted chat channel provides live access to our operators, where they can answer questions, provide expertise and guidance, and offer support throughout the remediation process. The operators also perform on-demand retesting to validate that exposures have been remediated.

***TAG Cyber: What are some emerging trends you see in cyber threats to your customers? Do you have any predictions about emerging global cyber threats?***

**BISHOP FOX:** Many of the threats we are seeing—and that are top of mind for our clients—fall into the following three categories we have all come to know quite well over the last 18 months.

The global pandemic caused monumental shifts in enterprise workforces, which in turn resulted in shifts in the threat landscape. Attackers quickly adapted by crafting COVID-19-themed social engineering lures purporting to provide information about vaccines and health care—which resulted in remote employees clicking on email links and visiting websites that delivered malicious code. And, of course, with so many employees working outside of traditional organizational perimeters, attackers are increasingly establishing footholds into enterprise networks through the networks of remote users, which are beyond the reach of enterprise controls. The remote access technologies deployed and expanded to support work from home are also being targeted. Finally, the pandemic has taken a toll on workers, a growing percentage of whom are unhappy with their current employers. Sadly, this has increased the likelihood of insider threats.

The ransomware ecosystem has matured significantly in recent years, evolving into a modular, decentralized model where a diverse set of specialized groups work together, each focusing on a different aspect of the ransomware attack lifecycle. For example, one group may focus on gaining initial access to an organization's network and sell that access to a criminal group. The criminal group may then deploy ransomware built via a kit sold on the dark web by a ransomware as a service (RaaS) provider.

While the SolarWinds breach may have come as a shock, the reality is that it is the tip of the iceberg. We can almost guarantee that it won't be the last time we see this type of supply chain incident, particularly as attackers set their sights on cloud providers, IaaS, and SaaS providers.





AN INTERVIEW WITH JAMES WINEBRENNER,  
CEO, ELISITY

## SUPPORTING INTELLIGENT SECURE ACCESS CONTROL

As the atomic unit for authentication and authorization, identity is being heralded by many analysts as the new enterprise perimeter. The changes in the workplace driven by the pandemic, expected to remain during the post-pandemic world, have further increased identity's relevance as the foundation of least-privilege access policy, and as the first line of defense against cyber criminals and advanced persistent threats. The sprawl of shadow IT, IoT devices, cloud applications, and other hybrid workspace trends will continue to increase.

Over time, security professionals have come to understand that "identity" doesn't only refer to users, or the person behind a keyboard. It refers to the machines and services that communicate across enterprise networks, whether they're on-premise, distributed remotely, or hosted across multiple public and private clouds. But identity in a vacuum won't tell operators their risk posture. It's only through contextualization that businesses can understand, manage, and mitigate their cyber risk.

For Elisity, it's about finding the missing link between assets and risk, where identity and behavioral context play critical roles.

***TAG Cyber: Identity has been coined by some as "the new perimeter." Why is identity alone not enough to protect corporate networks?***


**ELISITY:** It's not just identity, but behavioral intelligence around the context of that identity, that delivers the power of end-to-end protection for all the enterprise assets, regardless of location. Identities need to be mapped to authorization and then validated continuously. Contextual attributes like the time of day, the resource being accessed, device health status, risk scores, and other dynamic inputs are necessary to build and enforce a consistent adaptive policy that follows the user, the device, the application micro-service across every domain.

We could argue that access policy based on identity and context, rather than identity alone, is the new perimeter. This policy is built upon the user, device, application, and data identities, with additional contextual attributes to minimize risk. Identity is foundational to zero trust access, but identities can be compromised. Context and behavioral intelligence reinforce identities to allow for more effective risk management.

***TAG Cyber: In a hybrid work world where identity and access requirements may constantly be fluctuating, isn't it an extreme challenge to use them as control planes?***

**ELISITY:** Yes, it is. That is the reason we need to abstract the actual access from the underlying network construct. Under the zero trust premise, we must assume that all networks, hybrid or not, are untrusted. At Elisity, we are enabling a consistent policy framework and using that to build connectivity across multiple domains. We

The challenge is to make the network smarter so that it can automatically identify and apply policies, rather than treat every device as a snowflake that it must figure out and build a policy for.



are building an identity-based overlay for those access requests regardless of where the requests are coming from. Whether the requests are made on-prem or off, the policy remains the same and considers the contextual attributes and behavior intelligence mentioned earlier.

In this use case of the hybrid workspace, we care more about who or what is making the access request—the user, the device, the application—and what they are doing rather than where they are located. We are enabling ubiquitous access at scale across multiple domains, driving IT agility and efficiencies.

***TAG Cyber: What factors comprise an asset's identity?***

**ELISITY:** First, we must consider that there are different types of identities. Users, devices, applications, and data all have many distinct attributes. When it comes to user identity, it is key to ID who they are and what groups they belong to in order to enable concepts such as role-based access and inheritance. To assess the risk factor of a user, we need to see if it has authenticated with single factor or multi-factor authentication.

When it is a device making the access request, we need to see the unique identifier to understand what the device is, and then we must assess the contextual attributes like the location, health status, and more.

When it comes to application identity, it is key to get into the application layer to enable nano-segmentation. We also need to understand the app identity, regardless of which file is running and regardless of which region it's running in, to understand how that maps back into a broader policy.

***TAG Cyber: What is your Cognitive Trust™ solution all about?***

**ELISITY:** This offers an identity-driven control plane for corporate networking and remote access, without tying customers to a particular network or network security technology. Our Cognitive Trust™ platform, delivered as a cloud-based service, is deployed as an overlay on whatever WAN and/or SD-WAN infrastructure an enterprise prefers to protect data, users, devices, and applications in the datacenter, the cloud, at home, or anywhere else.

***TAG Cyber: What are some of the challenges security and operations teams will face as businesses support hybrid work and increases in SaaS applications and IoT/unmanaged devices?***

**ELISITY:** More and more unmanaged IoT devices will be connecting to corporate networks than ever before. Users will be anywhere and everywhere, interacting with SaaS applications that do not traverse the corporate network. Also, OT and IT teams face a convergence, or overlapping, of networks. Air-gapping is getting more challenging, and there's a need to further segment

air-gapped OT environments, which include multiple userless devices and legacy operating systems that are no longer supported. To secure assets effectively and minimize the attack surface, constant, complete visibility, and control across all the domains—remote, on-prem, and the cloud—are required.

When it comes to user identities and building and enforcing policies, network security operations teams usually have to translate these policies into multiple “flavors” based on the location of the assets being protected. But if we can truly abstract the policy to an asset identity level, it becomes easier for these teams to build and manage policy. The network should be smart enough to know where an asset is, and where the policy needs to be enforced, and not require a human to make that decision.

It should be an infinitely simpler undertaking to build policy for devices than for users. A user can do many different things, and we need to be careful not to artificially limit knowledge workers. But for a device, once identified, making a binary decision on whether it should be allowed on the network and determining the policy should be easier. The challenge is to make the network smarter so that it can automatically identify and apply policies, rather than treat every device as a snowflake that it must figure out and build a policy for.

The overall challenge will be to make access policy, network segmentation, and routing decisions more efficient and automated to accelerate the journey to an optimal zero trust architecture.





AN INTERVIEW WITH MARK HARRIS,  
PRINCIPAL PRODUCT MANAGER, FINITE STATE

## CONNECTED DEVICE SECURITY SOLUTIONS

Connected devices are increasingly associated with cyber risk. The sheer number of devices present in most environments combined with the number of software-defined functions, as well as a complex supply chain and easy physical access—all contribute to making these devices “low hanging fruit.” Security teams need to be able to see a greater level of detail into their device composition, but in practice this has not been an easy requirement to meet.

The Finite State platform is designed to address connected device risk. The platform was designed to give visibility into connected devices procured through a supply chain partner, or even developed locally. Such visibility enables deeper analysis of cyber risk for security engineers by exposing any exploitable vulnerabilities that might be present.

**TAG Cyber:** *What is the central problem the Finite State team solves for customers?*

**FINITE STATE:** Many device manufacturers are competing to gain market share with their latest iterations of connected devices. In that race to success, they use anything and everything to their advantage, especially third-party and open-source software to reduce development costs and time to market. Being the first to market is a coveted position, as it usually means being the market leader for a notable period of time. But where does all this code being used come from? Who wrote it? Is it being maintained? How much do you trust your vendors? Are there critical vulnerabilities in these libraries affecting the integrity or availability of a device?


The answer to this last question is almost always yes. Finite State discovers vulnerabilities in embedded products before they are ever released to customers. In addition to open-source and proprietary third-party software, Finite State identifies vulnerabilities in first-party code that is most often associated with what embedded developers refer to as user application code.

**TAG Cyber:** *How does your solution work?*

**FINITE STATE:** We analyze the final firmware binary images, uploaded by device manufacturers via API or web browser. Device manufacturers with mature product security organizations integrate Finite State into their build process, so vulnerabilities are discovered as soon as developers or their upstream software supply chains introduce them during a project. This provides the ultimate latitude for product security organizations to work with their engineering, product, and project management counterparts



## How many of us have been trained not to trust the Setup Guide downloaded from a brand new device's embedded web server?



to meet key product launch deadlines without putting their customers or product revenue at unnecessary risk.

***TAG Cyber: Do you see more emphasis on determining the components that comprise a given device or system?***

**FINITE STATE:** Yes, the executive order from President Biden set the stage for a long-needed journey to software transparency based on a software bill of materials (SBOM), which lists all of the software used in embedded devices. With an open communication channel sharing information about all of the code inside a device, organizations can start to have a joint conversation about securing embedded devices together from both the device manufacturers and their asset or device owners.

***TAG Cyber: How does your solution work with open-source components in products?***

**FINITE STATE:** We have already analyzed millions of open-source packages from all of the major sources embedded developers commonly use. Everything from plain old Linux distributions like openSUSE and Debian to newer projects like yocto and OpenEmbedded can all be analyzed by Finite State. We don't stop there; we also analyze more exotic embedded software such as real-time operating systems like VxWorks, QNX Neutrino, and FreeRTOS. Embedded manufacturers often take the same open-source software found in traditional Linux distributions and statically compile them into a single binary firmware custom built for custom chipsets only found in embedded devices.

***TAG Cyber: Do you have any predictions about emerging cyber threats?***

**FINITE STATE:** I'm expecting to see an uptick in large scale supply chain attacks. Attackers have realized they can get in undetected through trusted supply chains. Most of us have been through the required annual security training that teaches us how to recognize things like email based phishing attacks, but how many of us have been trained not to trust the Setup Guide downloaded from a brand new device's embedded web server? An attacker could strategically place a malformed PDF document that exploits a zero-day vulnerability offering up remote code execution capabilities. The truth is most device manufacturers do not scan these basic artifacts, making it easy for attackers to slip in exploits completely undetected.



## AN INTERVIEW WITH TAMER HASSAN, CEO, HUMAN SECURITY

# REDUCING THE RISK OF MALICIOUS BOTS

The earliest security attacks involved hackers manipulating or exploiting vulnerabilities. While human beings are still at the root of all attacks, automation has become the most prevalent means for engaging a malicious campaign. Typically, this is done using sophisticated bot attacks, and the security obligation to detect, mitigate, and even take down botnets has become an important part of the cyber security equation.

The techniques required to differentiate human activity from automated tasks initiated by sophisticated bots is more difficult to implement than one might expect. Automated attack tools have gotten good at mimicking the behavior of a live human, so the security defenses to manage bots must use the most advanced technologies to work in practice, as these sophisticated bot attacks can now easily bypass CAPTCHAs, WAF, CDNs and other feature-based bot protections. Bot management has come a long way from the original Turing tests used many years ago.

**TAG Cyber: Your company recently rebranded as Human. What was the motivation for the change?**

**HUMAN:** In October 2020, after a summer of social unrest, we took a hard look at how our White Ops company name no longer represented our values and who we were as a company. For these reasons, we announced plans to change it. This led us on a journey. We looked at thousands of names that would stand out and be exponentially better. We were looking for one that represented the values and the mission of the company—who we protect, a name that our employees and customers would be proud to be a part of.

In March of 2021, we launched HUMAN (short for HUMAN Security) and posted a blog, “Who We’ve Always Been: HUMAN,” along with a new website with all new branding and messaging on [www.humansecurity.com](http://www.humansecurity.com). The response from our customers, partners, employees and the community has been very positive. They all seem to want to play a role in our mission to protect the humanity of the internet by disrupting the economics of cyber crime.


**TAG Cyber: What problem are you solving for customers?**

**HUMAN:** We are a cyber security company that protects enterprises from bot attacks. We have the most advanced Human Verification Engine that verifies the humanity of over 10 trillion interactions per week, protecting applications, APIs and digital media from sophisticated bot attacks.

The key use cases we protect against are:

- Credential stuffing/account takeover
- Shopping cart fraud/inventory hoarding
- Credit card fraud
- Web scraping
- DDoS

Seventy-seven percent of all internet exposures are carried out by bots, making bot management a Top 5 priority for 90 percent of security leaders.



- Web recon
- Form fill abuse
- Analytics skewing
- Spamming
- Interface bypass/API abuse

**TAG Cyber: What are some trends in the design and deployment of automated attacks by adversaries?**

**HUMAN:** Seventy-seven percent of all internet exposures are carried out by bots, making bot management a Top 5 priority for 90 percent of security leaders. We have seen the number and severity of sophisticated bot attacks growing rapidly during the pandemic due to the dramatic shift to digital. We see every company being impacted by these attacks, and many don't know the severity as these bots act and look more human as the malware cyber criminals create lives on consumer and enterprise devices. Cyber criminals are using millions of infected devices to send billions of fake or harmful requests pointed at websites and applications.

We detect and stop bots from:

- Trying to buy tickets to a live music event. Bots grab the inventory and cyber criminals resell them at 5x+ the price while the true fans get left out.
- Testing millions of usernames and passwords to break into high-net-worth individuals' bank accounts.
- Listening to music on streaming services. Bots can create fake accounts and can influence the top-rated songs of the day. These bots also create credit card fraud and use stolen personal information creating privacy and regulatory problems.
- Impacting a delivery company where they were seeing 70 percent+ bot traffic to their site. Reducing just 1 percent of the fraud would reduce compute costs in the multi-hundreds of thousands of dollars per year plus reduce fraud to their system.

You can see an example of one major takedown, led by HUMAN, of a cyber criminal organization [here](#).

**TAG Cyber: How does the Human platform work?**

**HUMAN:** To detect sophisticated bots, our BotGuard solution collects and sends over 2,500 client-side signals indicative of "human or not" activity to the Human Verification Platform for processing, including signals from layers 4 to 7 of the OSI model. More than 350 technical, statistical and machine learning (ML) algorithms are used. Custom ML algorithms are developed for clients.



Our Human Verification Engine uses a multilayered approach that allows us to detect and prevent bot traffic with unprecedented accuracy, without compromising anyone's experience on the web. These layers consist of:

- **Technical Evidence:** We probe the device to gather data on the network, device, software, application, and user configuration to detect technical evidence of compromise.
- **Machine Learning:** We analyze thousands of data points collected across trillions of transactions to predict malicious behavior, enabling us to provide a high level of accuracy, even when there is insufficient technical evidence.
- **Global Threat Intelligence (Satori):** HUMAN's Threat Intelligence analysts proactively hunt for new threats on the Internet, attributing threats to specific botnet operators, campaigns, and other threat actors.
- **Continuous Adaptation:** HUMAN has continuously adapted over the last 10+ years, creating thousands of markers and hundreds of algorithms. Our speed to identify and build new detection mechanisms means we stay ahead of the adversary more than other solutions that are built on fixed detection mechanisms.

***TAG Cyber: Do you have any predictions about emerging cyber threats to the Internet?***

**HUMAN:** We see the level of sophistication of cyber criminals leveraging bots to attack enterprises only increasing. They are siphoning off billions of dollars in the shadows and can now easily bypass CAPTCHAs, WAF, CDNs and other feature-based bot protection.

The key prediction we see is that companies will come together in what we call "Collective Protection" to fight against this great threat to business and customers. It is impacting multiple departments within a company (cyber security, fraud prevention, performance marketing, and programmatic advertising), and each group is trying to stop the problem independently. We need to come together as departments and as companies to face this together. It is the only way we will win.





## AN INTERVIEW WITH BILL WELCH, CO-CEO, IRONNET

# SUPPORTING COLLECTIVE DEFENSE TO REDUCE CYBER RISK

Any large organization that has tried to address advanced threats by nation-states or cyber criminal groups will attest that this task cannot be accomplished alone. The sheer volume and massive scope associated with advanced persistent threats (APTs) initiated from well-funded adversaries dictates that the defenders must find ways to coordinate their defenses. This includes real-time sharing of threat information and insights.

Founded by General (Ret.) Keith Alexander, former Director of the National Security Agency, Virginia-based IronNet Inc. is pioneering the concept of Collective Defense. By combining the power and insights of multiple organizations, the commercial IronDome platform enables a new form of large-scale protection of enterprise networks. The resulting approach is seeing excellent traction in industry and is transforming how cyber defenses are operationalized.

***TAG Cyber: What are the types of products and services IronNet provides customers?***

**IRONNET:** The Collective Defense platform comprises two flagship products: IronDefense, our NDR solution that uses AI-driven behavioral analytics to detect and prioritize anomalous activity inside individual enterprise networks; and IronDome, our threat-sharing solution that facilitates a crowdsourced-like environment and analyzes threat detections across the community to identify broad attack patterns. IronDome then provides anonymized intelligence back to all community members in real time, giving all members early insight into potential incoming attacks. Automated sharing across the Collective Defense community enables faster detection of new, unknown attacks at earlier stages.

Collective Defense communities comprise organizations that share a commonality: they may be in the same industry sector, state, country, supply chain, or a tailored business ecosystem. As each Collective Defense community grows, so does the value of the shared threat data.

IronNet also provides services designed to deliver additional value. Customers can extend their SOC with IronNet's dedicated team of expert offensive and defensive cyber security operators for 24/7/365 NDR support, allowing their own SOC analysts to spend more time focusing on strategic tasks. We also offer cyber security governance, maturity and readiness services, incident response and digital forensic investigative services, and a robust set of training programs.

Most importantly, while some vendors charge a premium for expert customer success (CS) care, IronNet includes access to its CS team as part of a customer's subscription, including a dedicated customer success manager for the life of the subscription.

***TAG Cyber: What are some emerging trends you see in global cyber threats?***

**IRONNET:** Unfortunately, we are now seeing attacks on platforms and supply chains, often backed by nation-state adversaries. For example, not only was the SolarWinds supply chain attack fundamentally damaging in terms of compromising 18,000 networks, it also fueled a mindshift in the way companies think about cyber security. We can never go back to a "pre-SolarWinds" mentality, where companies defend in isolation or where the digital supply chain is not scrutinized as part of an individual company's holistic cyber security strategy. This mindshift was cemented by the Microsoft Exchange server attack, the ongoing ransomware campaigns accelerated by ransomware gangs that in many ways operate like professionalized Fortune 500 companies, and repeated attacks on U.S. agribusinesses.

Even more disturbing is that cyber criminals are eyeing the enterprise network as a stepping stone for infiltrating critical operational technology (OT) networks. In its 2020 ICS Cyber security Year in Review, Dragos reported: "Four new threat groups with the assessed motivation of targeting ICS/OT were discovered, accounting for a 36 percent increase in known groups." OT networks were once traditionally safeguarded by proprietary communication protocols and hard-wired connectivity. Now, "the abuse of valid accounts was the number one technique used by named threats" identified by Dragos. That means we have to help stop threats to critical infrastructure at the enterprise network gate before the adversary uses stolen credentials to try to take over industrial controls.

***TAG Cyber: How does information sharing reduce risk for enterprise?***

**IRONNET:** It helps reduce risk on two levels: at the organization level and at the national level. Increased visibility into the attack landscape, through the radar-like view of attacks delivered through Collective Defense, provides an early warning system that simply doesn't exist for organizations right now. It enables them to prepare and respond more quickly, before damage is done. And because the ability to take offensive action against these highly organized adversary groups is largely a government responsibility, being able to voluntarily share threat-related data in real time with the government will help them take appropriate action.

**We can never go back to a "pre-SolarWinds" mentality, where companies defend in isolation or where the digital supply chain is not scrutinized as part of an individual company's holistic cyber security strategy.**



We still encounter leaders in the private sector who have reservations about the idea of sharing data with other organizations – and even more so with the government. In a Collective Defense model, though, sharing can be done anonymously and can be correlated with what other organizations are seeing, within a secure ecosystem. As General Alexander has said before, we have to help the country understand the safety and benefits of this information sharing, and remove the political rhetoric from the conversation.

***TAG Cyber: How does the concept of a cyber security collective work?***

**IRONNET:** Customers apply our network detection and response (NDR) technology to detect anomalous behaviors on their networks, then contribute that threat data anonymously into a secure community. All the community's members, that is, IronNet customers who have elected to permit their information to be anonymously shared and cross-correlated, are then able to reap benefits from the shared attack intelligence. The collaborative aspect of Collective Defense, and the resulting prioritization of alerts based on their potential severity, help address the known problem of "alert fatigue" that plagues overwhelmed security analysts.

Our detection capabilities uncover both known and unknown cyber threats that signature-based tools often miss, giving companies a more thorough approach to network security.

***TAG Cyber: Do you have any predictions about emerging cyber threats to global infrastructure?***

**IRONNET:** As we've seen with the increase in ransomware attacks in particular, we expect that critical infrastructure will continue to be attractive and lucrative targets for adversaries. This is why it's so critical to have the sophisticated technology, like our detection capabilities in IronDefense, and a new approach like Collective Defense, to get early visibility into those malicious behaviors so action can be taken before the ransom demand is triggered.

One area IronNet has been focusing on is the commercial space industry – which is not yet considered a critical infrastructure segment, but I believe soon will be. The exponential growth that the world has seen in commercial space development – from low-earth orbit satellite communication to expanded lunar exploration and commercial space travel – is exciting stuff, but also critically vulnerable to cyber attacks. If there is a bright side, it is this: The types of attacks hitting the space industry are the same types of attacks that IronNet has experienced within other sectors, and our technology is well positioned to help protect this sector. You can't get much more "global" than that.



## AN INTERVIEW WITH ALEKSANDR YAMPOLSKIY, CEO, SECURITYSCORECARD

# USING SECURITY RATINGS TO PROTECT BUSINESS

When an enterprise team must deal with a supplier, partner, or other external entity—perhaps even a customer—it is reasonable to inspect and seek to determine their cyber security posture. For example, if a corporate function is outsourced to a commercial vendor, then understanding how that company protects data, stops attacks, and polices its infrastructure will be an important component of the local security posture assessment.

To that end, SecurityScorecard is one of the pioneers in the development of accurate security ratings. Using many relevant risk factors, the company creates a measure that reflects the security posture of a company, which helps ecosystem partners decide whether to engage in business together.

***TAG Cyber: How do security ratings work and how are they calculated?***

**SECURITYSCORECARD:** I often compare the criticality of security ratings to your car's instrument panel. How do you know how fast you're going, if you have enough fuel to get to your destination, if you need an oil change, or a variety of other indicators if you don't have the tools to tell you? Security ratings work in a similar manner. They show you an overall picture of your security posture, where your vulnerabilities lie, and ultimately what needs to be addressed.

At SecurityScorecard, we use non-intrusive, proprietary methods to assess your security posture across 10 risk categories to instantly deliver an easy-to-understand "A" through "F" rating. This includes: DNS health, IP reputation, web application security, network security, leaked information, hacker chatter, endpoint security, and patching cadence. On a near real-time basis, these ratings are updated based on objective, publicly available data that, similar to credit ratings, provides an "outside-in" view of an entity's security.


Overall, we've found companies that have an "F" rating are 7.7x more likely to suffer a cyber attack than a company with an "A."

***TAG Cyber: Are companies using ratings to support third-party or supply chain security?***

**SECURITYSCORECARD:** Absolutely. In fact, that was one of the main reasons we created the company. As a CISO myself once, I found it frustrating to go through the manual process of lengthy questionnaires and Excel spreadsheets in the course of our vendor due diligence process—especially when many of the responses were inaccurate or out of date. Thus, we created a way



Overall, we've found companies that have an "F" rating are 7.7x more likely to suffer a cyber attack than a company with an "A."



to automate the process for not only vetting third-party vendors, but also continuously monitoring their cyber health through the course of the business relationship.

With the rise in vendor relationships, organizations are exposing themselves to high-profile risks like never before. More third parties are touching corporate data, increasing risk posed to a business. Research shows that the average organization has 182 vendors connecting to its systems each week. The same survey found that 58 percent of organizations believe they have incurred a vendor-related breach.

SecurityScorecard enables companies to drive scalable and automated third-party risk management (TPRM). Leveraging our platform, organizations can instantly rate, understand, and continuously monitor the security risk of any company worldwide, non-intrusively and from an outside-in perspective. The platform identifies security issues and provides visibility into the cyber health of their entire vendor ecosystem, helping organizations make smarter TPRM decisions.

***TAG Cyber: How do changes in enterprise architectures influence security ratings?***

**SECURITYSCORECARD:** As companies change the technologies in their stack, their scores could either increase or decrease. For example, a company may replace a legacy system or upgrade virtual applications, and in turn help improve their score. Conversely, with the growth of work-from-home and hybrid workforce models that implement more SaaS applications and in-home routers, the attack surface can dramatically increase and negatively affect a score. Every technology that has the potential to connect to your enterprise technologies can provide an inherent risk.

Luckily, with over 12 million companies and entities scanned, SecurityScorecard identifies over 40 billion vulnerabilities every week, leading to the most complete and accurate ratings in the market. This allows CISOs to instantly find vulnerabilities and complicated threats. The data helps them manage all types of enterprise risks, such as operational, reputational, security, and compliance.

***TAG Cyber: How do you incorporate automation and innovation into your security platform solutions?***

**SECURITYSCORECARD:** We embrace a culture of rapid innovation and are committed to continuously updating our platform with additional signals intelligence and enhanced reporting capabilities. The goal has always been to create a platform that anticipates the needs of CISOs. Over the past seven years, we have added extensive artificial intelligence and machine



learning algorithms to discover patterns and make new predictions with greater accuracy and performance. One such enhancement is how we automate the continuous monitoring and communication of third parties.

Today, many companies are building our cyber ratings into their vendor service-level agreements (SLAs). In our solution, you can create rules-based scenarios that prompt you to alert a vendor that has fallen out of compliance. The program can automatically generate questionnaires that can be sent to them. We continuously track adherence and detect potential gaps with current security mandates.

In addition, our compliance mapping module reveals issues that pertain to the specific checkpoints of security standards—including PCI, NIST, ISO, SIG, HIPAA, and GDPR—that apply to your business.

***TAG Cyber: Do you have any predictions about emerging cyber threats?***

**SECURITYSCORECARD:** The simple truth is that threats are becoming more complex and prevalent. From an increase in ransomware attacks and phishing scams, to the recent supply-chain disruptions, we've seen that no company is immune from cyber threats. That's why it's important for every company to know their true cyber posture and take a proactive approach to securing its digital borders. If you don't know where your vulnerabilities are, you don't know which open door a cyber criminal will walk through.

Additionally, boards of directors are becoming aware of the risks associated with cyber security and are often requiring reports on an entity's cyber health. Thus, we are making it easy to create these for CISOs to share with their boards—and then have more productive conversations about cyber risk. This can help create a common language and a reporting framework that are easily understood across your organization.



## AN INTERVIEW WITH MICKEY BRESMAN, CEO, SEMPERIS

# SOLUTIONS TO OPTIMIZE SECURITY FOR ACTIVE DIRECTORY

Any competent cyber offensive actor will share (if asked privately) that Active Directory represents one of the most useful targets in any attack campaign. The information and access offered through directory services, as well as the opportunity to exploit vulnerabilities and misconfigurations, are considered essential steps in advancing privilege and supporting lateral traversal during an attack.

New Jersey-based Semperis has pioneered security and availability innovations for Active Directory. Semperis customers enjoy a level of control and protection that helps to reduce the risk of advanced cyber attacks at enterprise assets. Both security engineers and IT network experts rely on the capability, which is also beginning to emerge in modern security compliance initiatives.

***TAG Cyber: What are the types of products and services that Semperis provides customers?***

**SEMPERIS:** Semperis helps organizations protect their identity systems—the technology that controls access to all services and assets—from cyber attacks. Most organizations worldwide use Microsoft Active Directory for identity and access management. As a technology that's been around for two decades, AD was not built to withstand these attacks. Cyber criminals exploit AD weaknesses, such as risky configurations that have accumulated over time, to gain access to their victims' information systems. After they breach the system—either through on-premises AD or in the cloud—attackers can move laterally throughout the organization and drop malware.

Semperis helps organizations prevent, mitigate, and recover from these intrusions. Our Directory Service Protector product is a comprehensive AD and Azure AD threat detection and response platform. It helps organizations uncover risky configurations, detect attacks, automate remediation, and conduct post-attack forensics to prevent repeat attacks. For organizations with hybrid identity environments, DSP provides a single view of changes across on-premises AD and Azure AD. It also tracks Azure AD indicators such as changes to role assignments, group memberships, and user attributes.

Our Active Directory Forest Recovery (ADFR) product helps businesses quickly recover AD to a known-secure state within minutes or hours (rather than days or weeks) after an attack. This allows the company to get back to business without worrying about being hit with the same malware a second time. This year, we also

**We're seeing more cases, such as the SolarWinds attack, that start by infiltrating on-premises Active Directory, then move to the cloud—or vice versa.**



introduced a free security assessment tool, Purple Knight, which has been used by thousands of organizations to scan their environments for indicators of exposure or compromise.

***TAG Cyber: Why did you decide to develop and release a free security tool?***

**SEMPERIS:** From our work in helping customers shore up their Active Directory security defenses in post-breach situations (incident response), we saw that many don't have a good understanding of the AD exposures that adversaries are able to use against them. We wanted to give security teams that don't have deep AD expertise a way to understand their AD security posture—and then close any existing gaps so that adversaries won't use those against them.

Drawing on the deep expertise of our in-house directory services and security experts, we built this standalone utility that helps organizations identify and address common security gaps in AD that proliferate over time due to a lack of knowledge, resources, or focus. Purple Knight generates a graphical report with an overall security score, individual scores in five categories, and prioritized guidance so that teams can start fixing the problems.

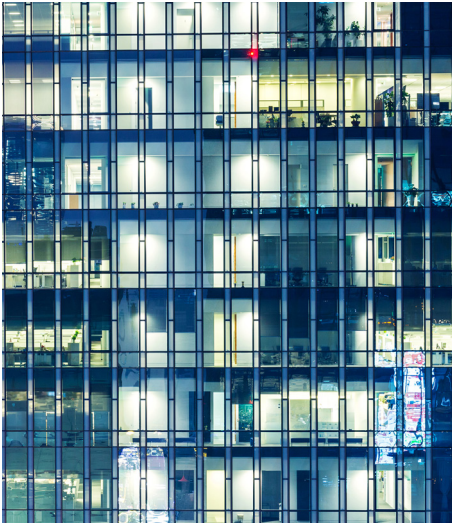
The overwhelming response from the community told us that the product tapped an unmet need. Since its release in March 2021, thousands of IT and security professionals have downloaded the tool. We didn't expect this response, but it's a welcome surprise as organizations are now able to make a direct connection between attacks they see in the wild and the security weak spots in Active Directory.

***TAG Cyber: What are some emerging trends you see in cyber threats Active Directory?***

**SEMPERIS:** Defending against cyber attacks that target hybrid identity systems is a serious challenge for many organizations. We're seeing more cases, such as the SolarWinds attack, that start by infiltrating on-premises Active Directory, then move to the cloud—or vice versa. Securing on-premises Active Directory is difficult on its own, but securing a hybrid identity system that includes Azure Active Directory brings additional complexity.

Azure AD provides a different stack of protocols, requiring a very different management approach. For example, in some configurations, when I make changes to identities in the cloud, that action affects my overall security posture in the on-premises data center and in various cloud applications. With a hybrid scenario, the potential attack surface expands for an adversary. Organizations now need to think about what changes are made to identity systems in each environment, and how the connectivity between the two can create an entry point for adversaries.





***TAG Cyber: Do you tend to work with IT operations teams – or have security teams adopted responsibility in this area?***

**SEMPERIS:** Because the importance of protecting the core identity store from cyber attacks is gaining awareness, we are seeing a shift in how organizations are structuring their IT and security teams to improve their overall security posture. Cyber attacks like the Colonial Pipeline breach put the security weaknesses of Active Directory in the spotlight. Turning a blind eye to the role of identity protection in the context of overall security strategy is extremely risky. So we're seeing companies start to transition the responsibility for identity protection to the security team. And even with organizations where identity remains with the operational team, we see more security awareness among IT professionals, and increased collaboration between the security and IT teams. Creating an environment where security is the shared responsibility of the identity and SOC teams will help organizations defend against current attacks.

***TAG Cyber: How do you incorporate automation and innovation into your security platform solutions?***

**SEMPERIS:** We have a dedicated team of security researchers who are experts in uncovering tactics that cyber attackers could use—or are already using—to breach organizations' directory services. Our bench strength in security research allows us to develop indicators of security exposure or compromise even before attackers have used them, and to quickly produce indicators in response to emerging threats. As an example, we released an indicator for the PrintNightmare vulnerability in the Windows Print Spooler service about six days after the flaw was uncovered.

***TAG Cyber: Do you have any predictions about emerging cyber threats to directory services?***

**SEMPERIS:** Cyber criminals will continue to target Active Directory, Azure Active Directory, and other IDPs because they are soft targets that many organizations are failing to address. Purple Knight users have reported an average overall security score of 61 percent, which is a barely passing grade. Many of the uncovered security weaknesses came as a complete surprise to users. Problems like account ownership are low-hanging fruit for adversaries.

They aren't looking for new attack paths because the old tried-and-true tactics still work. So for the foreseeable future, we will continue to see cyber criminals exploiting well-known gaps in Active Directory. But all is not lost: Companies can significantly harden their defenses against these escalating attacks by implementing solutions that evaluate overall security posture, continuously monitor for malicious activity, and quickly recover AD to a known-secure state after an attack.



AN INTERVIEW WITH JAMES WILDE,  
GLOBAL HEAD OF SECURITY STRATEGY, SPHERE

## SECURITY AND COMPLIANCE ENHANCEMENTS TO PERMISSIONS

Identity and access management has emerged as a foundational aspect of both security and compliance in the modern enterprise. This reflects the criticality of identities as a primary control in protecting data, especially with the perimeter dissolving and companies relying on zero-trust network access for its critical applications. Permissions and credentials must be properly managed for this to work.

New Jersey-based SPHERE is pioneering advanced platform solutions that help enterprise teams improve their identity and access management for both security and compliance. This is done by focusing the platform on how to assist teams in cleaning up and improving the management of their permissions. It's for legacy applications in the data center as well as public cloud and SaaS.

**TAG Cyber: Tell us about your company. What are the types of products and services you provide customers?**

**SPHERE:** We are an 11-year-old cyber security company focusing on attaining and maintaining an evergreen state around access governance. The company's cyber hygiene solutions lower an organization's risk posture by focusing on zero trust and implementing a least-privileged access state for all end user and privileged entitlements. Through a combination of software, SPHEREboard (an end-to-end workflow to understand the state of your environment), and a team of SPHERExperts providing world class thought leadership, operational efficiencies are gained. In addition, automation brings more depth and breadth to address ongoing reporting and remediation needs. We have the necessary visibility and remediation workflows in place to reduce the risk of breach, and minimize the cyber attack surface of an organization's IT environment.

**TAG Cyber: What are some emerging trends you see in cyber threats to businesses?**

**SPHERE:** The concept of zero trust now extends well past the scope of how devices are connected and how authentication is configured. The expeditious move to the cloud, accelerated by the new remote work requirements, has raised awareness of the importance of managing security in a non-traditional perimeterless world. Zero trust is also expanding past the application scope, and companies are looking to enforce access control policies across all their data repositories, storage landscape, platforms, and systems.

You can have strong zero-trust controls deployed across your environment, but if you're not applying the underlying logical access controls to your data and resources, you are not protecting them.

Also, considering the very public threat of ransomware, the federal government's raised awareness of cyber threats, and the requirements driven by internal audit functions, companies are increasingly looking to improve their overall coverage of access management. To do so, businesses are proactively looking to remove erroneous access that exists, while standardizing permissions so that these can be managed more holistically, just as a handful of more sensitive systems are. The push to be granular in handling access to all data, systems, and platforms is a trend that will continue to expand in the short and long term.

***TAG Cyber: Do most companies have dedicated security teams or even a staff member who focuses on their permissions?***

**SPHERE:** Most enterprise organizations have built dedicated teams that center around identity and access management as a whole. The sophistication and comprehensiveness of their roles and responsibilities vary, with companies in more regulated verticals spending significantly more time and energy on these requirements. Also, most companies tend to have a good grasp of their most sensitive systems, like financial reporting applications, but struggle to understand the permissions landscape in areas that are more complex, such as unstructured data repositories.

There is a need to have expertise in how permissions are applied, where to look for major risks, such as open and excessive access, and most importantly, how to standardize access and onboard it into the company's IAM workflows. Finally, special attention must be applied to privileged access to ensure that accounts that have the "keys to the kingdom" are understood, pruned where necessary, and governed by the IAM systems and company policies.

***TAG Cyber: How do you incorporate automation and innovation into your security platform solutions?***

**SPHERE:** Organizations need to cast a much wider net than they were previously required to. This means they must have the necessary visibility into permissions across every asset, the ability to track KRIs related to inappropriate access, and have a method to remediate issues as they are found. And most importantly, they must manage ongoing access requirements through vetted workflows. For this to work effectively, it cannot be done manually. Automation is key, and breadth and depth are essential. Also, once all the issues are identified, organizations cannot wait to make the necessary changes to remove inappropriate access. This must be done quickly, but in a controlled manner, to ensure there is no disruption to business critical systems.

Having performed assessments and remediations of poorly managed permissions for well over a decade, SPHEREboard automates all the heavy lifting. The solution also takes all the "lessons



learned” from manual approaches and provides an end-to-end platform to handle nearly every edge case and nuance in the source systems permissions, inconsistencies in referential data feeds, heavy integration requirements with downstream requirements, etc. The result is the ability to resolve thousands of access control issues daily in a repeatable and predictable fashion.

***TAG Cyber: Do you have any predictions about emerging cyber threats to business infrastructure?***

**SPHERE:** Cyber threats will continue to grow and attract significant attention from governments and industry alike. Massive investments from governments to bolster cyber security defenses underpin the partnerships being formed between government and industry to strengthen their capabilities to detect and respond to attacks. The heavily cloud-focused future will inevitably drive security investments in cloud-centric areas, forcing organizations to concentrate heavily on supply-chain risks as the broader adoption of cloud and consumption increases.

Recent data shows that 51 percent of data breaches in the past 12 months were caused by a third party. Organizations will need to gain assurances that third parties have the right security controls in place. Also, where shared responsibilities exist, firms must gain assurance that configurations and controls are delivering the protection needed. This is an area on which SPHERE focuses heavily, having introduced our cloud module that provides visibility and insight into how data is being protected and shared within cloud services.

“The connected home” is another area that extends the corporate attack surface, and organizations need to rethink their cyber security approach. Zero trust is one approach, and is an objective at the core of most security strategies. Secure access service edge (SASE), identity and entitlement management, and data security are some of the fundamentals that organizations will need to focus on to make zero-trust initiatives effective. You can have strong zero-trust controls deployed across your environment, but if you’re not applying the underlying logical access controls to your data and resources, you are not protecting them. Strong access controls must be defined and enforced consistently across the environment. These controls should be continuously monitored and maintained to ensure that strong cyber hygiene is being applied.

Finally, embedding security in the software development lifecycle is critical. With the adoption of modern application architectures and development methodologies, embedding security into these processes is key to realizing the value cloud offers. Embedding integrated security controls into DevOps processes should be a major focus for organizations, in addition to education and awareness of security best practices for engineers and developers.





## AN INTERVIEW WITH SURESH VASUDEVAN, CEO, SYSDIG

# ADVANCED DEVOPS SECURITY CONTROLS

Modern application hosting no longer involves monolithic software hosted in private data centers inside the corporate firewall. Instead, applications are now hosted using a scattering of containers, including front-end interfaces and back-end databases. These are orchestrated using tools such as Kubernetes, and are tightly integrated into the DevOps software lifecycle.

Sysdig is developing advanced solutions to assist DevOps and security teams in the task of securing these new software application architectures. This is done using a combination of visibility, monitoring, and mitigation tasks—all designed to be easily adopted and supported by software developers, hosting teams, and security engineers. In essence, these components help transform DevOps into DevSecOps.

**TAG Cyber:** *Tell us about Sysdig. What are the types of products and services you provide for DevOps customers?*

**SYSDIG:** We provide a platform for security and visibility that allows our customers to confidently run containers, Kubernetes, and cloud. The Sysdig Secure DevOps Platform provides cloud security to manage configuration risk. This includes identities, entitlements, access levels, passwords, and infrastructure as code security. For containers, the platform secures the build process, detects threat, captures a detailed record for investigation, and continuously validates compliance. DevOps teams are able to maximize performance and availability by monitoring and troubleshooting cloud infrastructure and services.


Unlike other security offerings, we are a SaaS-first platform and built on an open-source stack. We have a strong presence in financial services and telco, as our product scales to meet the needs of the largest organizations.

**TAG Cyber:** *What are some emerging trends you see in software development and cloud hosting?*

**SYSDIG:** Kubernetes and containers are quickly moving from emerging to the mainstream, as organizations realize they need to redesign their software and processes to get the agility benefits from cloud. As they transform development processes, most organizations are adopting secure DevOps workflows.

There are several aspects to these workflows. Teams often think first of reducing risk by shifting security left and fixing vulnerabilities in images. However, runtime security is becoming even

What we believe works best for customers is having the security team involved early, providing policy as the guardrails for developers.



more important following the latest supply-chain attacks. Organizations recognize they will never be able to prevent all threats because new vulnerabilities are always being discovered, and teams typically do not fix them all. Therefore, it's crucial to have runtime visibility and detection of both anomalous behavior and new vulnerability.

Within secure DevOps, another trend is policy as code, which can be applied to Kubernetes and cloud infrastructure as code as well. Using automation to integrate security into the DevOps workflow results in improved efficiency and reliability, which also can reduce security risk. Secure DevOps also increases the pool of resources available to assist the core security teams. Team members typically ensure that vulnerability and configuration issues are addressed, define network security policies within container environments, and triage security alerts.

One final trend to mention is the move to use open-source software as part of the modern development stack, including security tools. The Biden administration's executive order highlighted the criticality of transparency in enhancing software supply-chain security. Commercial offerings typically act as a black box that lacks the transparency that is critical to trust. Open source has the advantage that anyone in the community can inspect the code and run their own vulnerability tests at any time. There is a global team of researchers using and testing the open-source code, increasing test coverage.

***TAG Cyber: Do most modern developers understand the need to protect their containers and orchestration?***

**SYSDIG:** Absolutely. Developers do not want to be responsible for a security breach, and they understand the need to address vulnerabilities in images. However, they may not always know exactly what they need to do. What we believe works best for customers is having the security team involved early, providing policy as the guardrails for developers. This policy can be implemented using cloud native controls, such as the Kubernetes admissions controller, to enforce the policy and act as a reminder to developers. Beyond fixing vulnerabilities, Kubernetes configurations are quite liberal by default. For example, containers run as root, which is not necessary in most cases. Developers need guidance on the level of risk their organization is willing to take, as addressing configuration issues takes time.

***TAG Cyber: Do you tend to work more with developers, security engineers, or both?***

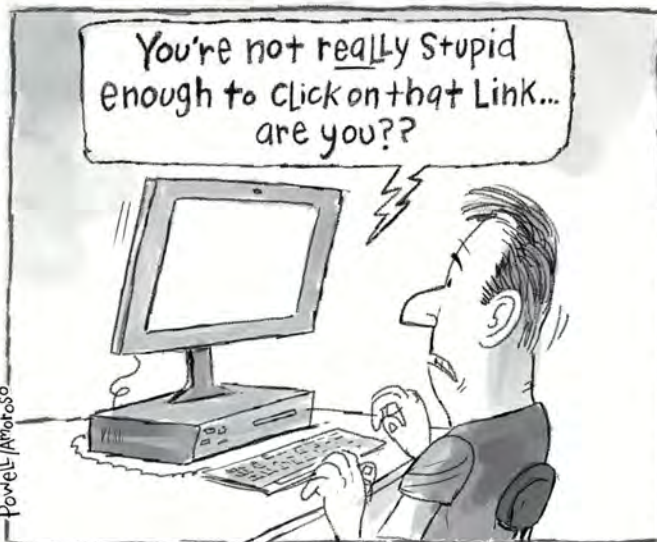
**SYSDIG:** We work with DevOps teams, platform engineering teams, and security teams. Many times the investigations into

tool selections are led by architects—both cloud and security architects. In the past, the DevOps and platform teams would pull the security teams into container security discussions, but in the last year we have seen more and more security teams engaging early in the process of selecting tools for container environments.

**TAG Cyber: Do you have any predictions about emerging cyber threats to DevOps?**

**SYSDIG:** One emerging threat is a result of managing permissions across multi-cloud, multi-account deployments. Teams are using an ever-increasing set of services in the cloud. Managing the complex permission structure across these deployments adds risk of misconfigurations. A second emerging threat is lateral movement in the cloud. The increased use of multi-tenant applications deployed in the cloud will reveal the need for stronger isolation and segmentation inside VPCs.

### Future Anti-Phishing Security





AN INTERVIEW WITH ALLAN ALFORD,  
CISO & CTO, TRUSTMAPP

# CYBER SECURITY PERFORMANCE MANAGEMENT FOR ENTERPRISE

Given the investments made in cyber security tools by enterprise teams, it is surprising that more attention has not been paid to managing the performance of security controls, systems, and processes. If it were, the resulting improvement would be welcomed by practitioner-level security staff as well as by management teams, including the senior-most leadership from the board of directors.

TrustMAPP is focused on providing cyber security performance management through consistent delivery of security metrics, key performance indicators (KPIs), and other qualitative and quantitative information. The company focuses on communicating with boards, executives, and operations teams, with emphasis on trending, risk assessments, risk investment reviews, and other important security considerations.

***TAG Cyber: What are the types of products and services you provide customers?***

**TRUSTMAPP:** We sell just one thing: a SaaS solution that helps CISOs and their teams manage and improve the performance of their cyber security infrastructure. The platform is scalable, so we can address the needs of any size organization. We sell directly to organizations for their own use, as well as to a variety of service providers (MSP, MSSP, vCISO, CPA firms) that use TrustMAPP to manage their clients' needs.


***TAG Cyber: How does cyber security performance management work?***

**TRUSTMAPP:** We like to talk about the five main areas where CISOs need help, and how we address those needs:

- Consistent messaging – provide industry benchmarks, consistent metrics, KPIs, and KRIs
- Business narrative – communicate with boards, executive leadership, audit, and operations using business metrics
- Trending – trend improvements in security and privacy posture over time
- Risk appetite – answer “how much is enough?” in terms of investment related to risks
- Prioritize – Prioritize human capital, capital investment, identify outsourceable areas, and reduce overlapping solutions



In just an hour or two, you can know where you stand, and what you need to improve to be more resilient—if and when a ransomware attack comes.



What our software does is centralize and automate all the steps needed to deliver those results:

- **Assess:** We automate all the steps of an assessment. Our software is pre-loaded with frameworks supporting more than 50 regulations and standards (such as the NIST CSF, HIPAA, CMMC, etc.). It also lets assessment proctors automatically assign responses to employees, send emails with those assignments, collect responses, and show percentage complete.
- **Report:** We offer more than a dozen analytics/dashboards that let the CISO track all aspects of cyber security performance management, from assessment, to perceived control gaps, to remediation planning and implementation. We also have an automated report builder that produces customizable, editable Word and PowerPoint documents, so security teams can add their narrative to complement the reported scores and analytics.
- **Prioritize:** Our software comes with more than 60,000 remediation recommendations, with budget estimates, so CISOs can prioritize which control gaps are most urgent, balanced against costs (both up-front and on-going), and justify those investment priorities to the board.
- **Remediate:** We automate the assignment of remediation tasks to the IT and security staffs, and track progress in real-time, as the assessment is updated and maturity scores rise.

***TAG Cyber: Do most companies have security teams, or even a staff member who can focus on this area?***

**TRUSTMAPP:** Large organizations all have CISOs, and that really is the job title we're most focused on serving. But we think CISOs and their staffs have been underserved by the current, mostly manual, approaches. They use lots of spreadsheets, or use a legacy GRC platform, which just makes their job that much harder (and probably contributes to the high turnover that we see in that role).

Small and mid-size orgs mostly don't have a dedicated, full-time CISO, but it's clear they need that kind of help. That's why we're seeing the rise of virtual CISOs (vCISO), also sometimes called fractional CISOs. We're also witnessing many CPA firms getting into cyber security consulting, beyond their roots in SOC. We've made sure TrustMAPP is a platform that these kinds of advisers can use to support all their clients, so they can standardize and streamline how they do assessments.

***TAG Cyber: How might a team use cyber security performance management to address issues such as ransomware?***

**TRUSTMAPP:** Whatever tools the security team uses, they need to think about what security controls specifically protect against (and help recover from) a ransomware attack. In fact, we recently launched a new framework completely focused on ransomware. It's a short, 33-question subset of the NIST CSF, so it's rooted in an industry standard, but it really simplifies and accelerates assessing your ransomware readiness. In just an hour or two, you can know where you stand, and what you need to improve to be more resilient—if and when a ransomware attack comes.

***TAG Cyber: Do you have any predictions about emerging cyber threats to business infrastructure?***

**TRUSTMAPP:** I don't think we've even come close to "peak ransomware," because it's so lucrative and so many organizations are poorly prepared. So I expect that we'll continue to see new ways for attackers to get into the network to compromise machines. It's why we chose ransomware to be our first threat-specific framework, so our customers can get straight to the truth of how prepared they really are.

The recent focus on third-party security is also expanding to every industry, so I expect we'll see more focus on that. For example, we're getting a lot of interest from companies in the U.S. defense industrial base, driven by the CMMC standard. A lot of these manufacturers are small businesses that really need help figuring out if they comply with CMMC, and what they need to do to comply. If they don't, they can't bid on projects! Traditional GRC tools are too big for small businesses, so we're trying to make TrustMAPP an affordable way for them to become compliant (and then further their cyber maturity).







# ANALYST REPORTS

# CYBER INSURABILITY AS A POSTURE INDEX

EDWARD AMOROSO

---

Representing the cyber insurability of an organization as a dynamic, real-time index, based on contextual posture, introduces a new way to establish policy terms for cyber insurance. The resulting index method suggests a new type of insurance coverage driven by real-time security posture assessment based on enterprise visibility.

## INTRODUCTION

Cyber insurance involves transferring risk from one organization to another. At the instant of the transfer, both parties should understand all relevant terms, including the amount of risk involved. Such understanding is usually attempted through due diligence, document review, technical discussion, and other forms of business communication. The process is imperfect, but generally results in reasonable comfort levels for both parties.

Unfortunately, cyber posture is an unpredictable attribute, and can shift wildly from one instant to the next. Unlike traditional analog systems with more predictable continuity, cyber security relies on software, which can include Trojans and other spurious functions that can take an organization's perceived risk from zero-to-sixty in a millisecond. It goes without saying that this calls into question the validity of manual due diligence for security.

This paper describes an approach to due diligence where cyber insurability is expressed as a real-time index based on applicable contextual information. The security posture of an organization thus becomes the output of a function that takes into account any relevant information collected in the traditional manner, but that also integrates live telemetry from enterprise visibility tools. Cyber insurability is thus a posture index that will change over time.

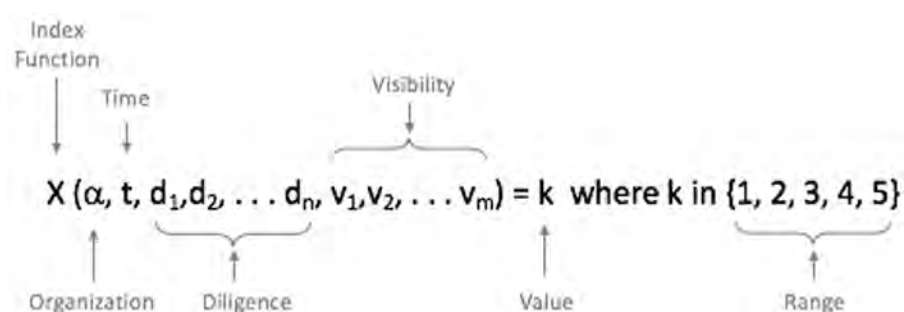
## DEFINING THE INDEX

The cyber insurability index for an organization is created from two sources: (1)



Due diligence information collected manually before the index value is computed, and (2) enterprise visibility information collected continually before, during, and after the index value is created. The index function can be expressed quantitatively using an arbitrary numeric scale, qualitatively using locally meaningful language, or as a pass/fail grade with respect to a threshold.

Expressed more formally, the quantitative index  $X$  for an organization  $\alpha$  at time  $t$  can be a function whose domain includes the cross product of the sets of data  $d_1$  through  $d_n$  collected during due diligence, along with sets of visibility information  $v_1$  through  $v_m$  collected in real-time by enterprise tools at time  $t$ . Its domain can be a set of arbitrary numeric values ordered from, say, 1 through 5 (low to high). For this example, we would express the index as follows:



The organization and time inputs to the index are self-explanatory in the sense that any organization should be able to utilize the index at any time. The diligence inputs would likely remain the same for intervals; that is, between diligence processes which would be performed before any insurance is written, and perhaps at various times during renewals, the values might change. But for the most part, the diligence information would not change significantly.

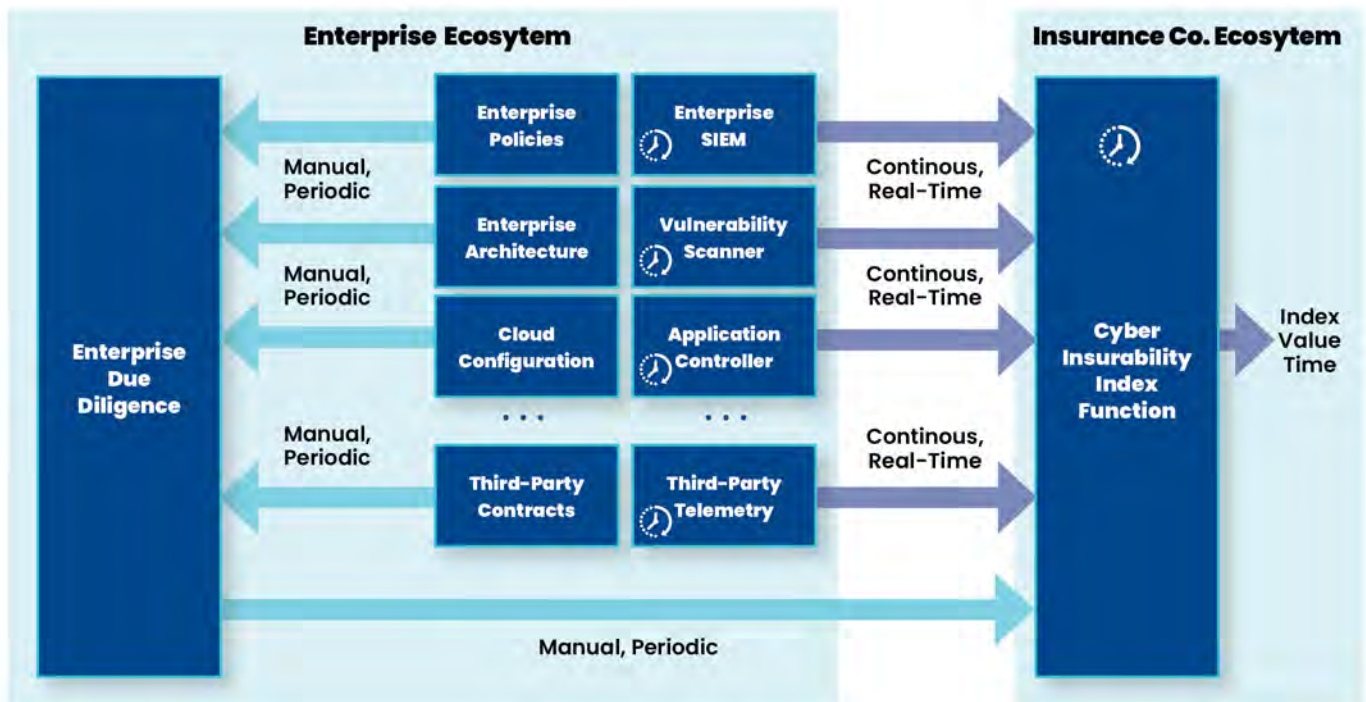
The visibility information, in contrast, might change considerably, and the time input would ensure that it is accurately portrayed in the calculation of the range value. The advantage here is that as collected data about an enterprise shows a reduction in risk, perhaps through some new protection scheme or improved security, the corresponding insurability would be adjusted. If this is done continually, then insurability would be an evolving function of time.

## BUILDING CYBER INSURABILITY TOOLS

To implement an index such as described above, information would need to be ingested from a collection of applicable sources, as with a security information and event management (SIEM) system, or similar system that creates big data representation of collected security telemetry. To organize the required data collection, we can identify two primary sources:

- *Due Diligence* – This includes the policy, architecture, contracts, and other documentation that can be reviewed by underwriters and other insurance company representatives to determine risk on a non-real-time, periodic basis, including just before initial policy terms are established.
- *Live Telemetry* – This includes the real-time telemetry and log information that can be ingested automatically via a standard protocol and used as the basis for an on-going, continuous view of enterprise security posture.

Given these collection sources, an insurance company or designate could set up a so-called *Cyber Insurability Index Function (CI2F)* that takes data from an enterprise and produces an index value for the enterprise. This index value would change with time if the ingested continuous data from the enterprise should change.



The functionality of a CI2F clearly requires open interfaces, standard security information transfer, and agreements to properly protect collected information. But none of these are insurmountable problems. For example, most security solutions include application programming interfaces (APIs) to support external interaction, and workable standards such as pre-defined json templates provide solutions for data exchange.

The problem of sharing live security information with an insurance indexing system does require considerable due diligence to ensure that compromise or leakage does not occur. Security teams would need confidence in the security operation of such a system, and compliance managers would need to agree that such sharing does not degrade the trust and assurance in a given enterprise.

## NEXT STEPS

The ideas represented here require agreement on standard means for calculating real-time insurability, including a standard index range. The 1-through-5 example listed above is simply representational and would require a more fine-tuned scale. Commercial vendors would also have to agree to provide the necessary information for the C2IF through an industry standard information sharing protocol. Finally, the compliance community would have to provide relief to Chief Information Security Officers (CISOs) who might be reluctant to share vulnerability information with an external source.

# MAPPING CVE RECORDS TO THE ATT&CK FRAMEWORK

DR. EDWARD G. AMOROSO

DR. PAULO SHAKARIAN

---

The enterprise security benefit of mapping common vulnerabilities and exposures (CVEs) to the offensive tactics included in the MITRE ATT&CK framework is explained. On-going mapping work at CYR3CON is used to exemplify the process and its usefulness for cyber practitioners.

## INTRODUCTION

One of the most useful methods in modern cybersecurity risk management involves keeping an accurate and detailed record of the threats, vulnerabilities, and attack methods that are applicable to the enterprise application, computing, and networking environments. Within an organization, this is performed in the context of a *vulnerability management* (VM) program, usually in conjunction with a locally supported cyber risk registry.

To assist with this important security task, which is especially challenging if only because of the enormous number of potential vulnerabilities and attack methods, research teams have tried to create frameworks and public repositories that can serve as a base for enterprise protection efforts. The MITRE organization has been particularly helpful in this regard, publishing useful models that are applied in practice today around the world.

Two especially meaningful such resources from the MITRE team are the *Common Vulnerabilities and Exposures* (CVE) list of known vulnerabilities,<sup>1</sup> and the *MITRE ATT&CK* framework,<sup>2</sup> which lists and organizes known tactics and techniques used by offensive cyber attackers. Both of these frameworks are well-known globally and are used frequently by cyber security practitioners and commercial vendors to help guide their day-to-day work.

The relationship between the CVE list and the ATT&CK framework is less well-known, however, which is unfortunate since the two resources can and should be used

in coordination. In this report, we outline how such a mapping might be done by practitioners and vendors. We also offer a case study from CYR3CON<sup>3</sup>, a commercial security vendor, which uses this type of mapping to help prioritize which vulnerabilities should be addressed in a given security program.

## COMMON VULNERABILITIES AND EXPOSURES (CVE)

The CVE Program was created by MITRE in 1999 to help identify, define, and organize publicly disclosed cyber security vulnerabilities. Designated partner organizations agree to publish CVE records to ensure reasonably consistent descriptions of the vulnerabilities that are relevant to practitioners. The approach helps security teams coordinate how they should prioritize vulnerabilities for mitigation. The CVE database is free for use and download.<sup>4</sup>

The primary contribution of CVE is the standardization of cyber vulnerability and exposure descriptions. Having common CVE identifiers eases the problem of dealing with multiple sources (e.g., security information and event management (SIEM) platform, endpoint security) all referring to the same security issue, but with different descriptions and terminology. CVE normalizes these disparate references, which improves the sharing of security data across platforms, tools, and services.

Interestingly, the way CVE works is that it links together existing cyber vulnerability databases. That is, CVE records contain standard identifier information along with a brief description to related vulnerability advisories. A separate database called the US National Vulnerability Database (NVD) is used to provide more detailed information such as mitigation guidance, priority scoring, and other useful data. Below is a sample CVE record related to the recent SolarWinds incident.

CVE-ID	
<b>CVE-2021-3109</b>	<a href="#">Learn more at National Vulnerability Database (NVD)</a>
• CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information	
Description	
The custom menu item options page in SolarWinds Orion Platform before 2020.2.5 allows Reverse Tabnabbing in the context of an administrator account.	
References	
<b>Note:</b> References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.	
• CONFIRM: <a href="https://documentation.solarwinds.com/en/Success_Center/orionplatform/Content/Release_Notes/Orion_Platform_2020-2-5_release_notes.htm">https://documentation.solarwinds.com/en/Success_Center/orionplatform/Content/Release_Notes/Orion_Platform_2020-2-5_release_notes.htm</a>	
• MISC: <a href="https://support.solarwinds.com/SuccessCenter/s/">https://support.solarwinds.com/SuccessCenter/s/</a>	
Assigning CNA	
MITRE Corporation	
Date Record Created	
20210107	Disclaimer: The <a href="#">record creation date</a> may reflect when the CVE ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.
Phase (Legacy)	
Assigned (20210107)	
Votes (Legacy)	
Comments (Legacy)	

Figure 1. CVE Record Related to SolarWinds Incident

As one might expect, considerable debate has occurred about the respective pros and cons of exposing vulnerabilities so publicly. Hackers and nation state actors, for example, gain access to the same cyber security exposure data as the defenders, and this can have consequences. The general consensus, however, has been that sharing this data produces more benefits than risks – and the process has thus continued to grow in application and use.

## MITRE ATT&CK

According to MITRE, ATT&CK is a *globally accessible knowledge base of adversary tactics and techniques* based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community.<sup>6</sup> The framework includes over five hundred techniques, and each is associated with one or more of fourteen tactics, which correspond to different phases of an adversary attack.





analysts to determine whether various patterns are associated with certain behaviors or threat groups. For example, an analyst can map network data from a SIEM to ATT&CK techniques, and to then create a chart showing which threat actors use those techniques. This method can provide a decision maker with insights into which threat actors may be conducting initial reconnaissance on the enterprise.

One area where different ATT&CK elements often differ is in their mapping to the physical world. For example, ATT&CK technique T1200 (Hardware Additions) involves an adversary introducing “computer accessories, computers, or networking hardware into a system or network that can be used as a vector to gain access.” This has clear physical-world implications, whereas T1068 (Exploitation for Privilege Escalation) does not involve the physical world.

The screenshot shows the MITRE ATT&CK framework interface. At the top, there is a navigation bar with 'MITRE ATT&CK' on the left and 'Metrics', 'Tactics', 'Techniques', 'Mitigations', 'Groups', 'Software', 'Resources', 'Blog', and 'Contribute' on the right. Below the navigation bar, there are tabs for 'layouts', 'show sub-techniques', and 'hide sub-techniques'. The main content area is a grid of 15 columns representing different categories of techniques: Reconnaissance (10), Resource Development (7), Initial Access (9), Execution (12), Persistence (19), Privilege Escalation (13), Defense Evasion (39), Credential Access (15), Discovery (27), Lateral Movement (9), Collection (17), Command and Control (16), Exfiltration (9), and Impact (13). Each column contains a list of specific techniques with their IDs and names, such as 'Active Scanning (T1046)', 'Abuse Infrastructure (T1190)', 'Drive-by Compromise (T1200)', etc.

Figure 3. Screenshot of ATT&CK Listing Techniques Used and Associated Tactics

## ALIGNING ATT&CK WITH CVEs

In contrast to the ATT&CK framework, the Common Vulnerability Enumeration (CVE) system was created to identify, define, and catalog publicly disclosed cybersecurity vulnerabilities. As of the time of this writing, there are over 150,000 CVEs each associated with one or more pieces of software enumerated by a related taxonomy called the Common Platform Enumeration (CPE) system. In Q1 of 2021 there were about 4,419 published CVEs and an additional 9,455 reserved CVEs.

Today, there has been much work to map patterns of behavior from system logs and network traffic to the MITRE ATT&CK framework. Additionally, an increasing number of reports have been written about attacks that directly reference ATT&CK technique numbers. This is a good trend for defenders because a common taxonomy helps us analyze adversary actions using automated techniques spanning from database query visualization to advanced artificial intelligence.

There are some practical limitations to the use of ATT&CK, however. For example, mapping system log data and network traffic data to ATT&CK techniques will only cover a subset of the techniques. For example, tactic T1588.005 (Obtain Capabilities) deals with an attacker obtaining an exploit, which

occurs prior to even launching an attack. For this reason, the tactic cannot be directly associated with observables in system logs or network traffic.

Additionally, certain vulnerabilities can enable multiple techniques. For example, MITRE identifies many techniques as requiring privilege escalation in the ATT&CK framework and also identifies privilege escalation provided by certain vulnerabilities in the CVE framework. There are other examples of techniques directly enabled by vulnerabilities such as T1498 (Network Denial of Service) and T1212 (Exploitation for Credential Access).

## CONSIDERATIONS IN ALIGNING CVEs AND ATT&CK TECHNIQUES

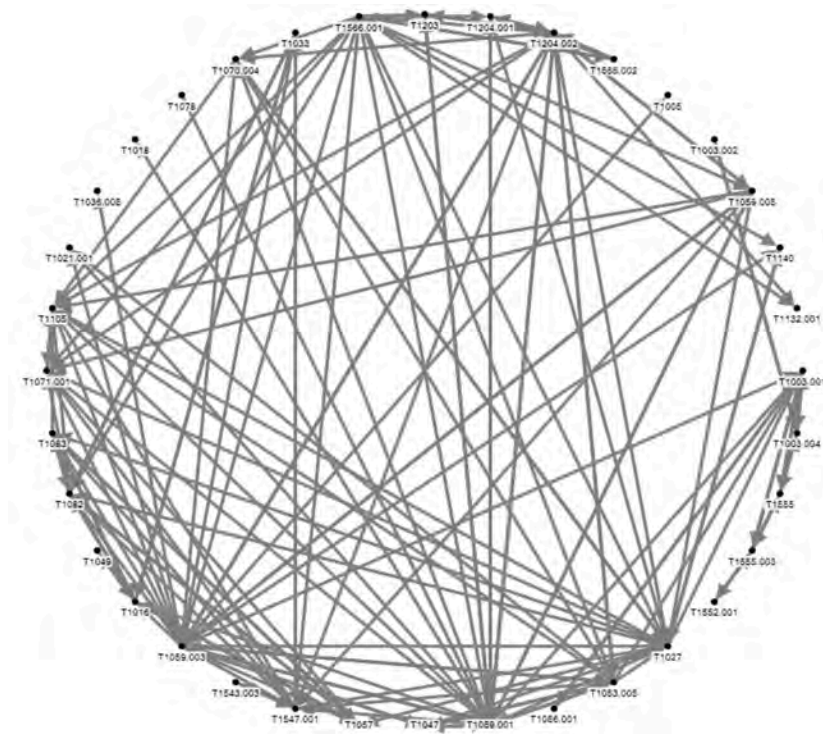
Our discussion above focused on alignment of CVEs with ATT&CK techniques. In this section, we identify three practical considerations (identified in our own case study mapping work) that must be kept in mind when aligning the two paradigms.

- **Not All MITRE ATT&CK Techniques Should Align to CVEs** : Most MITRE ATT&CK techniques will have nothing to do with vulnerabilities. As part of the CYR3CON mapping (described below), the number of ATT&CK techniques associated with vulnerabilities was found to be roughly 25%. As techniques are chained together, however, it is possible to disrupt attacks involving non-vulnerability related techniques through remediation of CVEs. Thus, while most techniques will not be directly related to vulnerabilities, they remain relevant to the overall analysis.
- **NIST/MITRE information about CVEs is not sufficient to align with ATT&CK** : While the CVE standard contains metadata about vulnerabilities (such as software applicability), it does not contain all the information needed to provide the greatest insight into the relationship. An example is that often the CVE number for the vulnerability will be registered, but the standard information from NIST will not be available. Similarly, vulnerabilities might allow for the execution of techniques not enumerated in the CVE system, but that *are* classified in ATT&CK. In these cases, multi-sourced intelligence helps ensure useful alignment.
- **Manual analysis for alignment will not scale** : The CYR3CON mapping included data from vulnerability scans of tens of thousands of vulnerabilities, and each of these vulnerabilities was available for mapping to several of the hundreds of ATT&CK techniques. With thousands of new vulnerability disclosures each month, manual methods for alignment will not scale. Data science and machine learning methods become very important in such alignments as a result. Alerting the data owner of access or edit attempts.

## CASE STUDY: USING CYR3CON INTELLIGENCE TO GENERATE ATTACK SEQUENCES

We've discussed how mapping ATT&CK techniques to CVEs can help vulnerability management teams disrupt sequences of techniques taken by attackers. Now, we take a step back to look at how such sequences can be generated in the context of a case study mapping at CYR3CON with the goal of generating attack sequences for improved intelligence.

Specifically, CYR3CON conducted a pilot involving analysis of over 700 security reports that each described adversarial techniques. The analysis associated those reports with the corresponding techniques. Using information about the techniques, such as applicable MITRE ATT&CK, computing platform, and required privileges, CYR3CON created a directed graph where two ATT&CK techniques are linked together with an arrow if the use of one was reported to proceed another. A subset of the resulting graph is shown in Figure 4 below.



**Figure 4. MITRE AAT&CK Directed Graph Mapping Visualization**

Such mapped information enables various analytic approaches. For example, if ATT&CK techniques are observed by the SOC, or if they are available to an attacker due to an un-mitigated vulnerability, the relationships shown in the above visualization can be instantiated to that situation, representing what hackers previously had available to them. In addition, upon instantiation for a specific situation, the above representation can be unrolled to produce a list of possible sequences that an attacker can use. These, in turn, can further be analyzed through automated means for disruption.

#### *Disrupting Attack Sequences*

The CYR3CON mapping of relationships among ATT&CK techniques provided insights, based on historical reporting, into which ATT&CK techniques normally proceeded each other and/or used in tandem with each other. The resulting construct is what data scientists refer to as a graph, which is not the type that show the relationship between an X and Y variable, but rather a depiction of relationships.

As mentioned above, relationships can be unrolled, which means that potential attacker patterns can be observed in an automated way. With this level of understanding, one can look at how such patterns can be disrupted. Further, by mapping CVEs to ATT&CK techniques, analysts can understand which CVEs can play a potential role in an ATT&CK chain. As part of the CYR3CON mapping effort, attacker sequences were unrolled and examined to determine which vulnerabilities can be remediated to disrupt such attack chains. The below figure shows an example from our experiment.



### **Example output from CYR3CON attack sequence disruption experiment:**

The following sequences can be disrupted by remediating CVE-2017-10271:

T1059.001-PowerShell, T1203-Exploitation for Client Execution, T1204.002-Malicious File, T1053.005-Scheduled Task

T1059.001-PowerShell, T1203-Exploitation for Client Execution, T1204.002-Malicious File, T1059.003-Windows Command Shell, T1047-Windows Management Instrumentation, T1053.005-Scheduled Task

T1059.001-PowerShell, T1203-Exploitation for Client Execution, T1204.002-Malicious File, T1059.005-Visual Basic, T1059.003-Windows Command Shell, T1053.005-Scheduled Task

### **Figure 5. Example Output from CYR3CON Mapping**

Note that the attacker had multiple sequences available to him in this case that could potentially involve exploitation of the above-named CVE. A defender, for example, can also identify all potential attacker sequences available based on a vulnerability scan and work to remediate vulnerabilities that are involved with attack sequences they wish to disrupt. Using techniques like identification of predicted exploits can narrow such a list further.

## **HOLISTIC ATTACK DISRUPTION: OPS AND VM**

Throughout this article, we've looked at both the MITRE ATT&CK and CVE frameworks, discussed how CVEs could map to ATT&CK techniques, shown how attacker sequences could be derived, and outlined how such sequences can inform a vulnerability management program to strategically remediate CVEs to disrupt attacker activities. However, the disruption of attacker sequences can also require vulnerability remediation – and this exposes a strength in the ATT&CK taxonomy – namely, that one can map CVEs along with operational data to ATT&CK techniques. By looking at what is available to an attacker, security teams can examine a variety of options to disrupt a given attack sequence.

Suppose, for example, that foreign hackers are suspected of launching attacks against a domestic enterprise. Using ATT&CK, analysts can map all sequences of techniques known to be used by these attackers. They can look at how to disrupt the sequences based on a full arsenal of security tools. For example, patching certain vulnerabilities might deny a portion of these sequences, with some vulnerabilities be non-remediated due to dependencies with legacy software. In these systems, analysts can resort to disrupting different portions of the attack sequence, such as taking steps to avoid privilege escalation through additional authentication techniques, blocking ports, or even isolating systems.

Ultimately, the defensive goal is to stop attackers before their attacks can start. Whether the defensive action deals with patching vulnerabilities or taking a more SOC-oriented action becomes a secondary management concern, because in either way the threat can be blocked. This holistic approach to cyber security leads to a better unity of effort across enterprise teams, and results in a more proactive, threat-centric, automated approach.

<sup>1</sup> Information on the CVE program is available here: <https://cve.mitre.org/>.

<sup>2</sup> Information on the MITRE ATT&CK program is available here: <https://attack.mitre.org/>.

<sup>3</sup> Founded by Dr. Paulo Shakarian, Arizona-based CYR3CON uses machine learning to derive useful cyber threat and vulnerability intelligence from hacker networks to help enterprise teams properly prioritize their security controls.

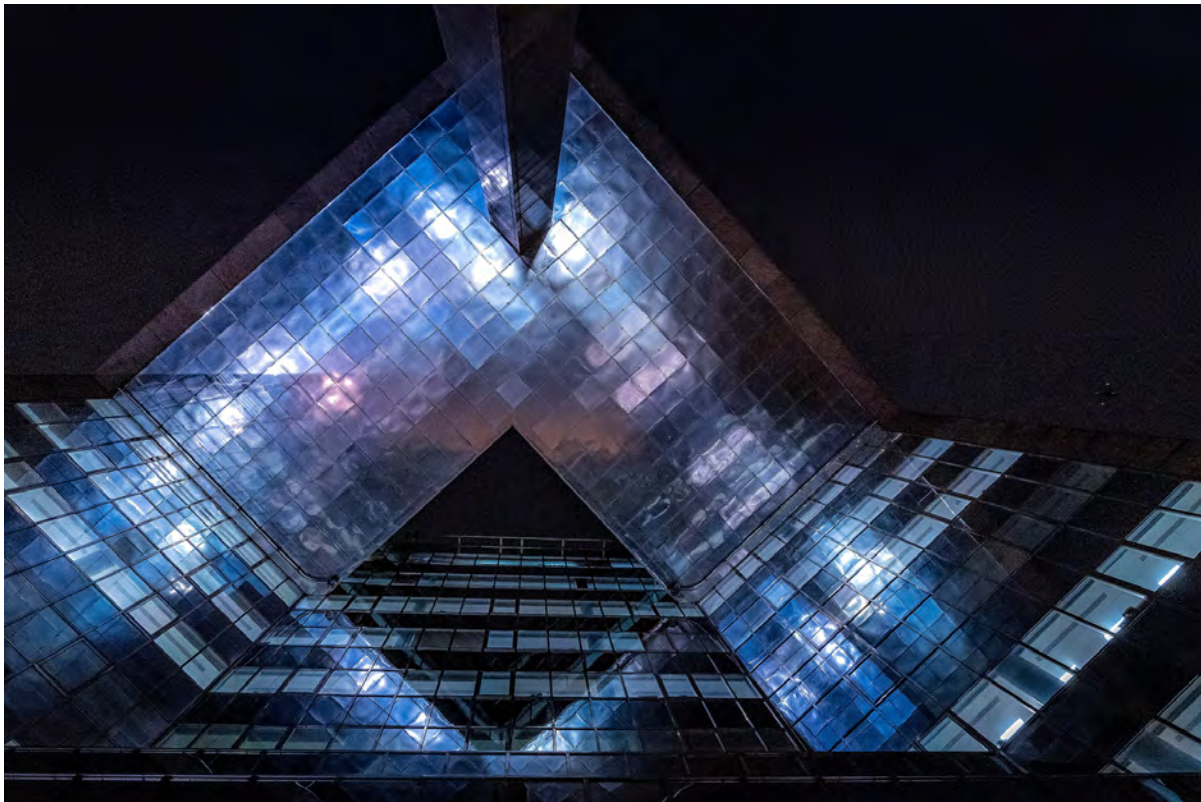
<sup>4</sup> Download of the CVE database is available here: <https://cve.mitre.org/data/downloads/index.html>.

<sup>6</sup> These two sentence quotes from MITRE are taken from the heading on this website: <https://attack.mitre.org/>.

<sup>7</sup> Here is a typical report outlining the results of such MITRE testing of endpoint security products: <https://www.mitre.org/news/press-releases/mitre-releases-results-of-evaluations-of-21-cybersecurity-products>.

<sup>8</sup> Many salient aspects of threat modeling, including attack trees, were invented by this author and are referenced in [https://en.wikipedia.org/wiki/Threat\\_model](https://en.wikipedia.org/wiki/Threat_model).

<sup>9</sup> First introduced in this early 1993 computer security textbook by the author: <https://www.amazon.com/Fundamentals-Computer-Security-Technology-Amoroso/dp/0131089293>.





# NEXT-GENERATION VULNERABILITY ASSESSMENT AND PATCH MANAGEMENT: AN OVERVIEW OF ACRONIS CYBER PROTECT

EDWARD AMOROSO

---

Vulnerability assessment and patch management are foundational cyber security tasks that have evolved toward next-generation coverage of multicloud infrastructure, data center virtualization, and zero-trust architectures. The Acronis Cyber Protect Cloud platform is shown to effectively implement these important controls.

## INTRODUCTION

Despite the changes that have occurred over the years in cyber security, many traditional protection approaches have remained as important and as effective as ever. Two complementary examples are vulnerability assessment and patch management. As organizations continue to shift toward virtualization, zero trust, and multicloud infrastructure, proper attention to vulnerabilities and patches helps to ensure consistency with cyber risk objectives.

In this report, we review the best current approaches to this combined activity, which we dub VA/PM – and prepend the moniker “next generation” to highlight the evolution of these capabilities to handle multicloud infrastructure, virtualization, zero trust, and many other attributes of modern enterprise networks. The Acronis<sup>1</sup> Cyber Protect Cloud platform is shown to effectively implement this next-generation vulnerability assessment and patch management (NG-VA/PM) approach, especially for service providers.

## IMPORTANCE OF VA/PM

Keeping track of vulnerabilities and patches is hardly the most exciting aspect of modern cybersecurity, but it could arguably be viewed as one of the most important tasks in an IT risk program. Security breaches often result from exploitation of vulnerabilities that could have been removed, or from patches that were not applied. So the combined task to address these issues has a clear implication for cyber risk.

As such, every team responsible for security, regardless of size or sector, must have some means of tracking and prioritizing vulnerabilities, and of ensuring the timely application of patches. The ability to ensure high-integrity support with fail-safe operation is also highly desirable. For example, according to one research survey, 88% of companies claim that they would apply patches more quickly if they had the option to un-patch if necessary.<sup>2</sup>

It is worth mentioning that VA/PM is particularly important for managed service providers, because of their scope. That is, as nearly all SMBs rely on service providers to assist in operating and protecting infrastructure, software, and services, their overall cyber risk can be significantly reduced if the service provider handles this task properly. This is one of the great benefits, in fact, of working with a capable service provider.

## CHALLENGES OF VA/PM

One major challenge for VA/PM involves the existence of known and unknown vulnerabilities. It is reasonable to assume that a large VA/PM program would have good coverage of known, reported vulnerabilities – but it is not reasonable to expect that this will extend to unknown, zero-day problems. In most cases, teams become aware of zero-day exploits only after they have been used in an actual campaign.

An additional coverage challenge, which is arguably more intense, involves the existence of known and unknown assets in an organization. That is, most nontrivial organizations have an incomplete understanding of their asset inventory. As a result, for any vulnerability, it might be unclear whether it actually applies to the local environment. These two unknowns, vulnerabilities and assets, can be represented in a conceptual matrix (see Figure 1).

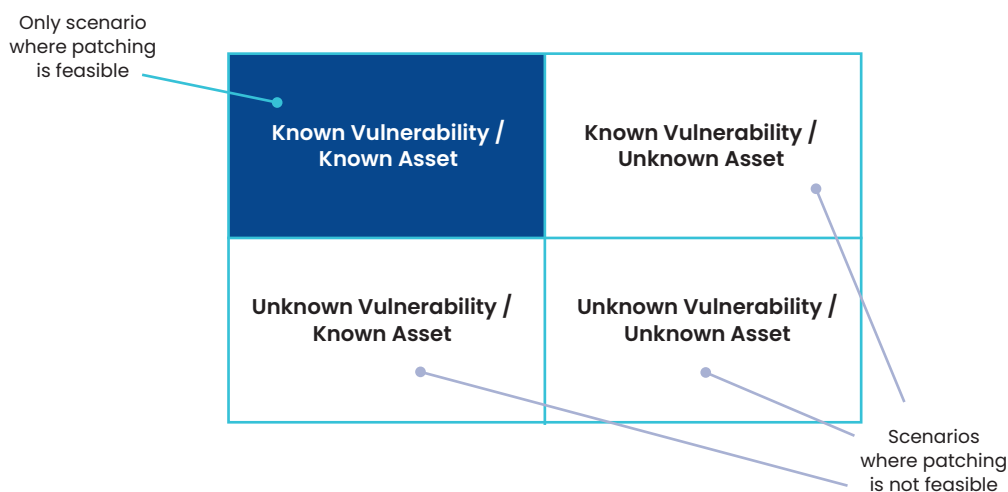


Figure 1. Matrix of Vulnerability/Asset Scenarios



The matrix highlights how important it is for vulnerabilities to become well-known quickly, and for assets to also become known accurately and quickly. These next-generation requirements help to explain how NG-VA/PM has come to be – namely, to ensure that organizations wanting to maintain more accurate and complete coverage of vulnerabilities and patches have sufficient means to achieve this critical security objective.

## MODERN NG-VA/PM REQUIREMENTS

The cyber security community well understands the vulnerability management challenge and its adjacent tasks of prioritizing and patching (including for non-Windows products). NG-VA/PM is all about making these familiar processes more intelligent, manageable, automated, and complete. The specific types of next-generation continuous security functions that are required in this area include the following:

- *Vulnerability Assessments* – Teams responsible for security must have the ability to collect, catalog, and manage an accurate list of applicable vulnerabilities. This is best done using global threat monitoring and alerting from multiple sources.
- *Prioritized Patching* – Security teams must use analytics and threat intelligence to determine which patches to prioritize. This analysis requires accurate asset management and inventory and good external threat intelligence.
- *Forensic Analysis* – NG-VA/PM programs must support future analysis and investigations by archiving vulnerability-related data and associated patches. This allows for more accurate case analysis.
- *Fail-Safe Patching* – NG-VA/PM programs must support the ability to roll back patches if necessary and to ensure high-integrity patch application.
- *VA/PM Compliance* – As with all aspects of modern cybersecurity, NG-VA/PM includes the obligation to support compliance goals. This often involves the automatic generation of reports for external auditors and regulators.

As suggested above, the progression to next-generation capability for VA/PM includes driving intelligence, automation, and completeness. It also, however, involves extending applicable techniques, tools, and processes to handle the modern transition to new infrastructure such as public cloud, mobile networks, and perimeterless zero-trust environments. In the next section, we use the commercial Acronis platform to illustrate how this can be done in practice.

## CASE STUDY: ACRONIS CYBER PROTECT CLOUD PLATFORM SUPPORT FOR NG-VA/PM

The Acronis Cyber Protect Cloud commercial platform is designed specifically to enable MSPs to provide next-generation vulnerability management and patching support for enterprise customers of all sizes around the world. As such, it serves as an excellent use case to demonstrate how NG-VA/PM requirements might be implemented in a live production environment, where a cyberthreat might have significant consequences.

Cyber Protect Cloud includes a range of capabilities that directly address anti-malware, patching, virus scanning, backup, vulnerability assessment, sensitive data protection, and application controls. MSPs can rely on these capabilities to address safety, security, authenticity, privacy, and accessibility requirements among their SMB customers in the context of processes for backup and recovery, security management, and anti-malware (see Figure 2).



**Figure 2. Acronis Cyber Protect Cloud**

The primary advantage of combining these functions into a commercial platform is that it helps to streamline the complexity of many different processes and functions. The many challenges inherent in the coordination, combination, and integration of the various processes shown in Figure 2 should be obvious. Coordinating backups with anti-malware, for example, is one of the great difficulties in dealing with advanced ransomware attacks.

The implication for managed security service provider teams is that an integrated commercial platform such as Acronis Cyber Protect will likely simplify and streamline the overall NG-VA/PM infrastructure and associated processes for enterprise customers. This is an essential task, especially in organizations with considerable size and scope. Attention to simplification will continue to grow as a requirement in emerging compliance environments.

## **ACTION PLAN**

MSPs are advised to take immediate action toward implementing a modern NG-VA/PM program using a suitable commercial platform and associated set of processes – such as with the Acronis solution. This can be achieved by following a simple four-step management plan. Each of the four high-level steps must obviously be decomposed into more granular tasks, but the overall approach should be as follows:

### *Step 1: Inventory of Existing VA/PM Approaches*

The head of security and his/her team should create an accurate inventory of existing approaches to identifying, documenting, assessing, prioritizing, and closing vulnerabilities. In larger firms, this is likely to include many disparate approaches, tools, and processes.

### *Step 2: Development of NG-VA/PM Requirements*

Once the inventory has been established, the security team should create a set of NG-VA/PM requirements along the lines of the functions discussed in this report. The requirements should combine the best elements of approaches identified in the inventory.

### *Step 3: Commercial Platform Scan and Review*

The next step involves scanning and reviewing available platforms such as Acronis Cyber Protect Cloud for suitability in the customers' environments. TAG Cyber analysts can assist with this task, which must take into account nonfunctional considerations such as license terms and cost.

### *Step 4: Begin Gradual Transition and Integration*

The final management step involves transition and integration of the newly selected platform into the local NG-VA/PM ecosystem. The good news is that the types of tasks included in this area are highly conducive to a smooth transition.

<sup>1</sup> Switzerland-based Acronis GmbH (<https://www.acronis.com/en-us/>) supported and participated in the preparation of this technical report.

<sup>2</sup> 0patch Survey Report, 2018. <https://0patch.com/>



# SELF-PROTECTION DATA AS A MEANS FOR BUSINESS RESILIENCY

KATIE TEITLER

---

Enterprise resiliency, a cornerstone of sustainability, has a new partner: Self-protecting data. With cloud usage at ubiquitous levels, and cyber criminals leveraging vulnerable infrastructures to target valuable data, organizations need greater control over how their data is accessed and used. Traditional security and privacy technologies — especially those built for on-premises networks — do not go far enough to prevent tampering and ensure end-to-end data file confidentiality, availability, and integrity.

## INTRODUCTION

Data has been called the “crown jewels” of organizations, meaning, data is the foundation upon which organizations plan, produce, profit, and prosper. As such, many data protection mechanisms have been developed over the years, from kludgy DLP to fussy encryption to zero trust-based access controls. All these protection capabilities (and more) have a place in the data lifecycle, but none of them (as standalone controls) fulfills end-to-end data protection and control, from creation to network traversal and storage and, finally, through secure data disposal or destruction. Furthermore, any visibility into how and when data is used throughout the numerous stages relies on the technologies implemented to protect it, not the data itself. When those technologies are circumvented, or they don't function as intended, the data itself remains largely vulnerable.

Encryption is the best mechanism by which organizations can shroud data from unauthorized and malicious individuals, whether that data is stored on a network, traversing a network, or traveling between networks. Encryption allows data



owners to obfuscate data, rendering it unreadable to unauthorized individuals and systems. However, encryption is neither resilient to reverse engineering (in fact, many legitimate security technologies must decrypt data in order to protect it) nor straightforward to manage. To wit, attackers generally do not attempt to defeat encryption – instead, they steal the passwords, other authentication credentials, and basically exploit the complexities of key management or authentication management or privilege management systems.

What's more, data is the life blood of a business. How valuable is your business if no one can read your data, analyze it, update it, sort it, process it, share it, etc.? These functions are part and parcel of working life. Thus, the very existence of data implies the expectation of access and handling. Though data can be encrypted during many stages of the data lifecycle, it cannot be used (processed, updated, etc.) in an encrypted form. Simply leaving it unencrypted creates a vulnerability. As a result, even when organizations have rigorous encryption practices, data ends up going through oscillating stages of encryption–decryption–encryption–decryption. Therefore, other layers of protection and governance must be applied over the top.

Furthermore, the increased dependency on traversing disparate supply chain networks and the abundant use of cloud networks necessitates another level of data protection. Though the major cloud providers are very good at protecting their infrastructure, the Shared Responsibility Model means that organizations must assure the security and privacy of any data and data files placed into cloud environments as well as the access controls and configurations that allow authorized users to access the environments, including data in files.

In 2020, cloud misconfigurations were cited as the attack vector that caused the exposure of 33.4 billion records. It should come as no surprise, then, that utilities to directly protect data and files must be a business priority in 2021 and beyond. In this report, we explore how companies can create and utilize data that can defend itself to ensure that it's tamperproof and resilient to the cleverest of cyber attackers but accessible and usable by intended users.

## WHY TRADITIONAL DATA PROTECTION AND ACCESS CONTROLS AREN'T ENOUGH

The prevalence of cloud usage and the vulnerabilities associated with it, as described in the introduction, are evidence that new mechanisms for protecting and controlling cloud data files are needed. A few other prime use cases also bubble to the top:

- **Data migration:** Many companies are reducing the amount of on-premises infrastructure they manage and thus must develop a strategy for secure migration of data files to the cloud. The biggest risk is transmission to and retrieval from the cloud. Protecting data in transit can be accomplished through encrypted connections (HTTPS, TLS, FTPS, etc.) and encryption of the data, itself. Yet, as data transits the TCP/IP comms layer, node2node2node, “securing” multiple, sometimes disparate channels is complicated. Companies should also implement robust network security and endpoint controls to ensure those vectors cannot be attacked in the process. While this layered approach is assumed “trusted,” it fails to include any data self-reporting, meaning, if a savvy attacker is able to exploit any stage in the migration process, operations team may not know that an attack is happen at the data layer until the exploit has already succeeded.
- **Data creation in cloud (including software development):** More and more, data is created in cloud environments. Data in use – which includes writing, testing, and deploying code – cannot be encrypted. Most businesses therefore use access controls to try to protect software and data files. But when those controls are compromised or entrusted to others, the data remains highly vulnerable to tampering if they are not self-controlling and do not have a self-awareness or self-reporting mechanism.

- **More sensitive data in the cloud:** As with data and data files created in cloud environments, the addition of more highly sensitive data requires organizations to have end-to-end processes for protecting and controlling data files, whether they are in use, at rest, or in transit. No stage can be ignored and policy enforcement should be autonomous.
- **Backup, recovery, and resiliency:** Ransomware is a top-line business threat. As demonstrated with the Colonial Pipeline attack, as well as many others, ransomware can bring a business and its customer eco-system to its knees if they are not adequately prepared. While we at TAG Cyber advocate for proactive cyber security, it would be foolhardy to ignore the fact that some cyber attacks will be successful. Therefore, we believe that a part of a proactive cyber security program is building and maintaining a robust backup and recovery process. Doing so ensures resiliency in the event of a cyber attack. It is not enough, though, to simply backup data for recovery purposes. While a novice may go after data files on users' devices or corporate/cloud servers, savvy cyber criminals understand that it is more devastating to tamper with all instances of data files, including backups. If backups are not properly protected — and standalone encryption may not be an option given its useless in a ransomware scenario — organizations would be wise to develop alternatives which utilize data that can defend itself.
- **Privacy and compliance:** The GDPR and the CCPA ushered in a wave of privacy regulations worldwide. In their wake, and because of the persistent frequency of data breaches coupled with a burgeoning “big brother,” citizens are demanding greater privacy protection from not only governing bodies but also the organizations within which they work. In turn, businesses have begun to realize the competitive advantages of provable data privacy. *Demonstrating* data privacy when asked or required is a necessity, and manual, traditional efforts not only do not scale but cannot be trusted in today's digital world.

## THE IMPACT OF DATA THAT CANNOT DEFEND ITSELF IN THIS GLOBAL, DATA-CENTRIC FRONTIER

When security pros think of data management, it's generally in the form of data protection, a “shift left” mindset. Resiliency is a less-considered aspect of security programs, though arguably a more important one. Far too often, organizations do not realize the criticality of resiliency until a breach occurs and (either or both) data and systems that house said data are unavailable or unreliable.

Resiliency is truly the cornerstone of operational sustainability and should be considered a top priority of security teams. When a breach occurs, corporate brand attrition leads to loss of shareholder value, and the regulations intended to preserve enterprise security don't go far enough in their efforts nor do they combat the core problem: data resiliency.

While certain data protections, such as those mentioned above, are a good start, they are wrappers, of sorts, that hover around the data. In contrast, data that protects itself by means of embedded controls does not rely on third-party mechanisms, either for protection or for reporting on the status of the data, and therefore supplies a hardened security and privacy layer. It is this hardening that allows companies to mitigate data compromise and remain resilient when another system vulnerability — such as a cloud misconfiguration or stolen credentials — is exploited.

**“Resiliency is truly the cornerstone of operational sustainability and should be considered a top priority of security teams.”**

## DETECTING AND PREVENTING DATA MISUSE AND ABUSE

As is consistent with zero trust principles, data protection and privacy controls must be independent of the environment or network in order to prevent data misuse and abuse. Modern business requirements simply won't allow for network-based controls alone, as they have proven exploitable. Today, companies need policy and control throughout the OSI stack, however, very few (effective) security technologies exist at layer 2, the data layer.

Nonetheless, the data layer has taken on new importance, especially in the last year as businesses shifted to work-from-home and now to hybrid work operating environments. Employees, customers, and systems all need fortified data access, but in such a way that doesn't hinder productivity. Yet, preventing unauthorized access to and use of data is a top-line business requirement for any company that wants to stay out of the breach headlines. But protecting the networks on which the data reside, transport mechanisms, or even the access and permissions to the data isn't enough; far too many breaches have occurred when these controls were in place.

Self-protecting data that is decisioning and controlling at layer 2 conform to the principles of zero trust and preserve privacy and enforce security, wherever the data is – at rest, in transit, or in use. What's more, an intelligent approach to data protection and privacy incorporates self-awareness and self-protection and allows businesses to immediately identify – or prevent entirely – when code is changed without authorization, when malicious code is inserted, and prevent any sort of tampering, thereby assuring the integrity of the data. This fulfills the need for data, and more importantly, business resilience.

### Data That Stands Up for Itself

The Last Line of Defense

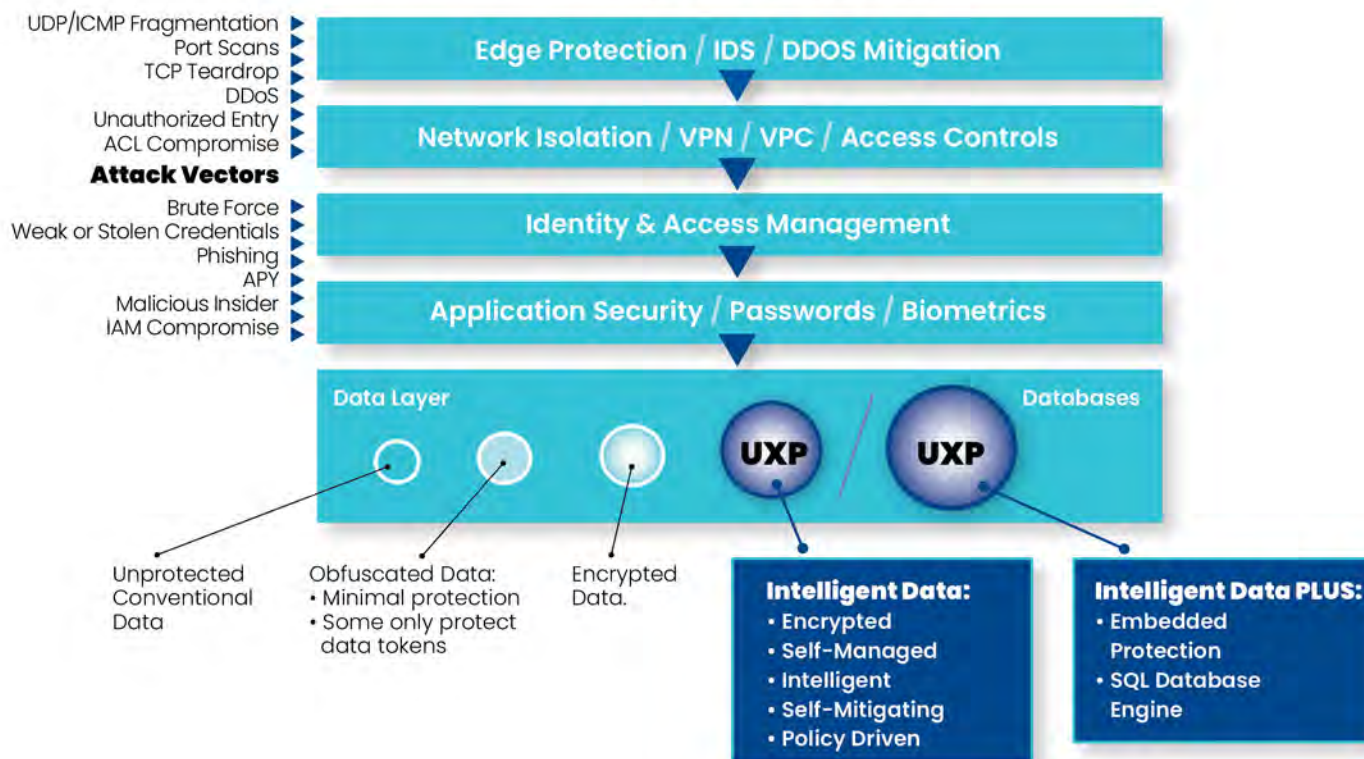


Figure 1. Smart Data vs. The New Standard for “Intelligent Data”

## HOW DO YOU MAKE DATA INTELLIGENT?

What, exactly, should be the new standard for “intelligent” data? There are many solutions today that embed “intelligence” into data-files. But that definition of intelligence is essentially information relating to rules, encryption keys and in some cases, authentication credentials. This standard for “intelligence” built into data-file does not translate into self-protecting data and does not empower the data to decision and control enforcement of security and privacy policies? The new standard for intelligent data uses an embedded decisioning and control engine which identifies, authenticates, and governs what a user can do with the data file. Decisioning and control functions are exclusively the purview of the embedded engine, while execution of the functions is carried out by the application. This intelligence capability assures the integrity of data and affords data resiliency even when other parts of an organization’s digital systems have been compromised.

The embedded “intelligence” instructs and controls the application to carry out both proactive and reactive processes. This intelligence capability assures the integrity of data and affords data resiliency even when other parts of an organization’s digital systems have been compromised.

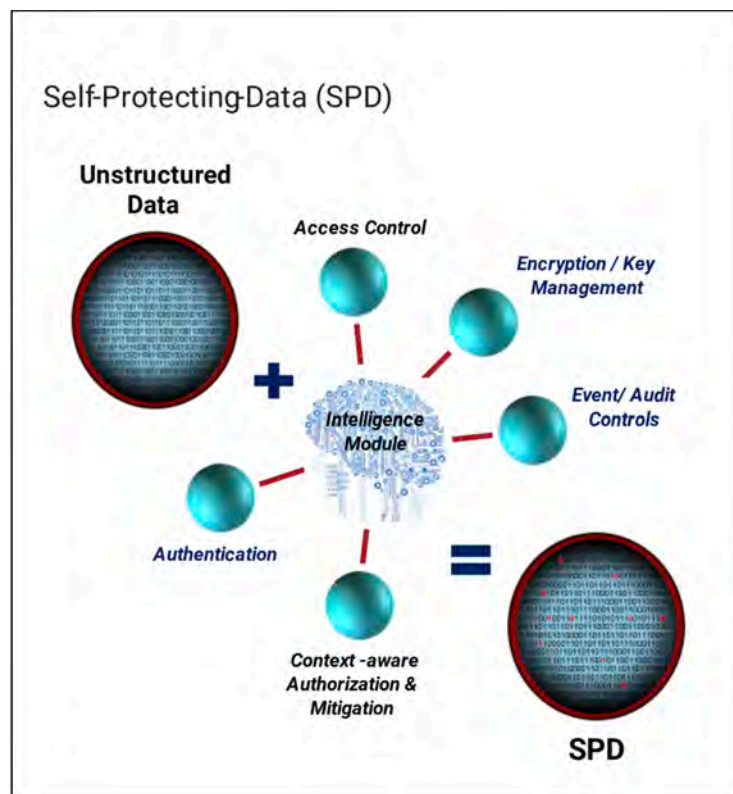


Figure 2. Data Self-Protection Intelligence Module

Some examples of these proactive and reactive processes are given below.

- Self-protecting “digital identities” are utilized to control selective access to sensitive information within the data-files
- Track who is attempting access, to what information, when, from where, how
- Enforce stepped-up authentication credentials
- Inform and/or alert the data-file owner of key events
- Self-shred



## WHAT IS SELF-PROTECTING DATA?

In the last few years, terms like “self-healing” and “self-protecting” have cropped up in cyber security marketing materials. It’s easy to dismiss these terms as hype, hyperbole, or outright exaggeration. However, when combined with credible and demonstrable technological capabilities, they become powerful mechanisms for protection and privacy.

So, what is “self-protecting data,” practically speaking?

- **Data that can defend itself:** As opposed to solutions that put security information “in” data or protections around data, self-protecting data has intelligent software code written directly into it that beacons back to data owners, giving them insight into how the data or data file is being used, accessed, and by whom. This embedded defense includes important protection techniques like encryption, but unlike traditional encryption where keys must be managed, self-protecting data stores the (cloaked) keys inside the data file so they cannot be intercepted by an attacker.
- **Data that can authenticate itself and its users:** The embedded programmable code supports zero trust and allows only authorized users access to data and data files. Further, authentication protocols are independent of the underlying infrastructure of the networking environment, mitigating the possibility of an attacker hijacking or hiding in easily spoofed network protocols.
- **Data that can enforce policy and take mitigative action in real-time:** Because the code is part of the data/data file, not a protective layer around it, it provides an intelligent decisioning and controlling service at the data-layer to alleviate suspicious attempts to access information in the data-file, in real time, wherever the data is, and at whatever stage of the data lifecycle it’s in. Policy enforcement and remediation at the data layer result in governance policies that follow data, wherever it goes. Examples of actions self-protecting data can take include:
  - ◇ Alerting the data owner of access or edit attempts
  - ◇ Providing only partial access to non-sensitive data files
  - ◇ Denying access
  - ◇ Requiring step-up authentication for access
  - ◇ Shredding the data (in extreme cases)
- **Data that can track events, end-to-end, and assure its providence:** From who the data owner is to how data files are being shared and stored, self-protecting data keeps records all throughout the data lifecycle and ensures data integrity.

## EVALUATING DATA PRIVACY AND PROTECTION PLATFORMS

The total number of data records compromised in 2020 grew by 141% over the previous year. Correspondingly, the number of cloud breaches also continues to rise, due often to misconfiguration, inappropriate data access, and misuse (i.e., mis-delivery). As businesses shift more of their data to cloud environments – or create it there – the need to implement strong controls around data and data files is essential. Encryption, alone, can be difficult to manage and expensive, not to mention that circumventing encryption doesn’t require special talents or techniques.

Today, a thorough data protection and privacy program incorporates not only a multi-layered approach -- including data-layer policies, transport-layer controls, and strict data access governance and reporting – but also a more granular approach. For example, how does one control selective access to important information within a file without at the same time compromising the PII in that file? Further, a data security strategy must incorporate elements of real-time visibility and reporting so that

data owners can adjust policies and controls when necessary.

When evaluating business applications for provable data privacy, the following questions will help determine which type of tool your organization needs:

1. *Risks* – How is your company currently assessing data risk?
  - a. *How are you measuring your data risk?*
  - b. *How much data do you have?*
    - *Where is it located?*
    - *How is it protected?*
    - *Who has access to it?*
  - c. *How long would it take your organization to identify a data breach and quantify the scope?*
  - d. *How are you creating and maintaining a data audit trail?*
  - e. *What are the impacts to your business if certain types of data are lost, stolen, irreparably modified or unavailable?*
2. *Assets* – What tools and techniques for data security and privacy do you maintain?
  - a. *How many tools/techniques do you need to use?*
  - b. *Which data access technologies and processes are implemented?*
  - c. *What data file access policies do you maintain?*
    - *How easy/hard are they to maintain?*
    - *How frequently do they need to be updated?*
    - *Do you have one place for central management of data file access -policies or do you need disparate systems for different data types and locations?*
  - d. *What systems do you have for backup and recovery?*
3. *Compliance* – Which regulatory requirements are your organization subject to?
  - a. *How are you meeting compliance requirements?*
  - b. *How are you auditing compliance requirements?*
  - c. *Are there additional industry standards (e.g., ISO 27701) that are required or desired?*

## CONCLUSION

Given the amount of data in use at enterprises today, the requirements for such use, and the mandates imposed by regulatory bodies as well as employees, partners, and customers, enterprises must look for ways beyond encryption and access controls to protect data and ensure its resiliency. Self-protecting data is a new approach to data protection and resiliency that will enable organizations to safeguard the privacy of its stakeholders, its investments, and cloud deployments. By implementing a self-protecting data program, enterprises and SMBs alike will be better prepared for and able to recover from technological, security, and environmental disruptions, irrespective of the infrastructure in use.



# UNDERSTANDING COMPROMISE INTELLIGENCE

EDWARD AMOROSO

---

Compromise intelligence offers cyber defenders a means to utilize cyber threat information about malicious actor behavior to discover and contextualize compromises. The Prevailion commercial offering is shown to implement this compromise intelligence platform concept.

## INTRODUCTION

The role of threat intelligence in the context of cyber security has become well-established. This is true for all sectors, and in all security operational contexts, regardless of size, scale, or scope. Collecting, integrating, and interpreting intelligence to improve the accuracy and coverage of any security control is now an accepted best-practice – one that has contributed to making threat intelligence a vibrant component of the commercial cyber security marketplace.

Cyber threat intelligence products can be roughly categorized into two basic types: Intelligence designed to provide input that helps defenders prevent future attacks from ever occurring, and intelligence designed to provide insights that help to explain attacks that have already occurred. Certainly, a security operations team will need the ability to support both functions, but their application and usage are different.

In this report, we introduce the notion of compromise intelligence, which focuses more on the prevention of attacks. The purpose is to derive insights from sources such as hacker networks to alert defenders to brewing issues before they can develop into serious breaches with long dwell times. The approach is shown to be helpful to enterprise protection as well as supply chain risk management. The Prevailion platform<sup>1</sup> is used to illustrate the approach in practice.

## USING INTELLIGENCE TO ADDRESS KILL CHAIN

Perhaps the most serious concern regarding modern cyber threats involves the stealth nature of an advanced targeted campaign. Where the original goal of cyber security was to prevent attacks, modern security teams have shifted their focus to the right (so to speak) and adjusted their emphasis to finding attacks that have occurred and creating response plans. By some estimates, attacks now have dwell times of over 200 days before being detected.

Cyber offensive models, such as from Lockheed Martin<sup>2</sup> or as part of the NIST Cybersecurity Framework (CSF)<sup>3</sup>, offer useful frameworks for addressing how defenders deal with the process followed during offensive cyber campaigns. If the kill chain is represented horizontally, then it become easier to visualize how increasing emphasis on proactive prevention is viewed as a so-called shift-left and increasing emphasis on reactive response is viewed as a shift-right.

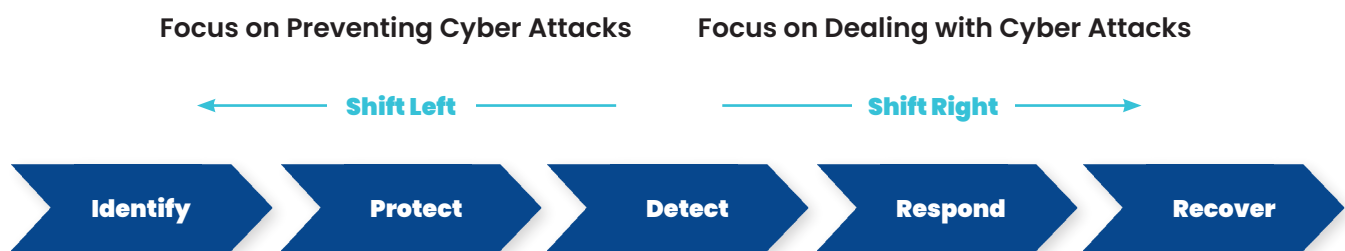


Figure 1. Shifting Cyber Defenses Left and Right

The role of intelligence in the overall defensive process is important regardless of whether the emphasis shifts left or right. It is true, however, that the proactive benefits of preventing attacks far outweigh the reactive process of dealing with damage that has occurred. (Remember the familiar advice about an ounce of prevention.) As such, intelligence is most valuable when it helps to stop attacks before they can ever occur.

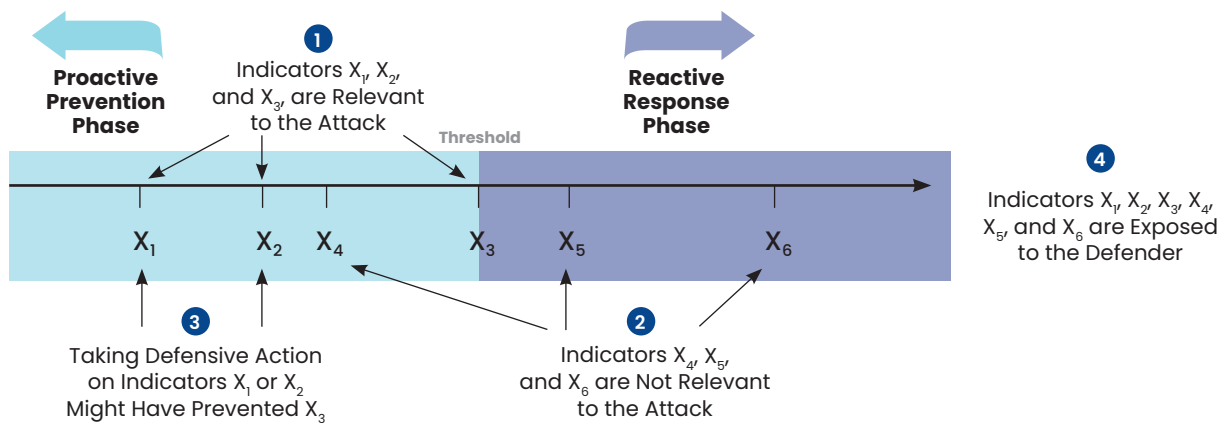
## DERIVING INTELLIGENCE TO PREVENT ATTACKS

To illustrate the use of threat intelligence as a preventive measure, it helps to review the purpose of so-called indicators of compromise (IOC). Long used by the most capable military intelligence teams, IOC focus allows a defender to seek evidence that something is amiss before it can brew into an actual breach. In this sense, the intelligence gathering and derivation process becomes more active and preventive.

Suppose, for example, that a security operations center (SOC) team optimizes its review process for alerts and alarms to focus on clear evidence that a compromise has actually occurred. This SOC team will certainly benefit from greatly reduced false positive alarms and will avoid any response activity that might not be needed. By analogy, this is like sending fire trucks only when there is absolute confirmation that a real fire is on-going.

In contrast, however, if that SOC team adopted an IOC focus, then they would direct their energies toward detection of evidence, perhaps false, that some compromise might be underway. Obviously, this creates more up-front work, because many IOCs might turn out to be unrelated to any attack, but the argument can be made that prevention will ultimately reduce the response burden sufficiently to warrant the earlier investment of time and energy.





**Figure 2. Advantage of Early Indicator Approach**

As shown in Figure 2, the theory of IOC focus in an enterprise SOC is that a malicious attack that might expose indicators x1, x2, and x3 to the defenders could conceivably be prevented if the SOC team had taken some preventive action after indicators x1 or x2. As shown in Figure 2, however, indicators x4, x5, and x6 might be totally unrelated to the compromise. This mixing of indicators greatly complicates cyber defense.

One of the great advances associated with compromise intelligence (as will be illustrated in the Prevailion case study below) is that where IOCs can serve as building blocks for enterprise teams, a good compromise intelligence platform can provide more meaningful evidence of compromise (EOC) to defenders. This is a more complete and actionable view and might include valuable evidence such as hash values for files or IP address ownership attestation.

It is worth emphasizing that the cyber risks being experienced by enterprise teams today would seem to warrant this focus on compromise intelligence. With businesses, government agencies, critical infrastructure, and citizens having their data and systems compromised repeatedly, something must be done to change the risk equation. In the next section, we will examine a commercial solution using a clever intelligence method that is showing promise in this context.

## CASE STUDY: PREVAILION COMPROMISE INTELLIGENCE

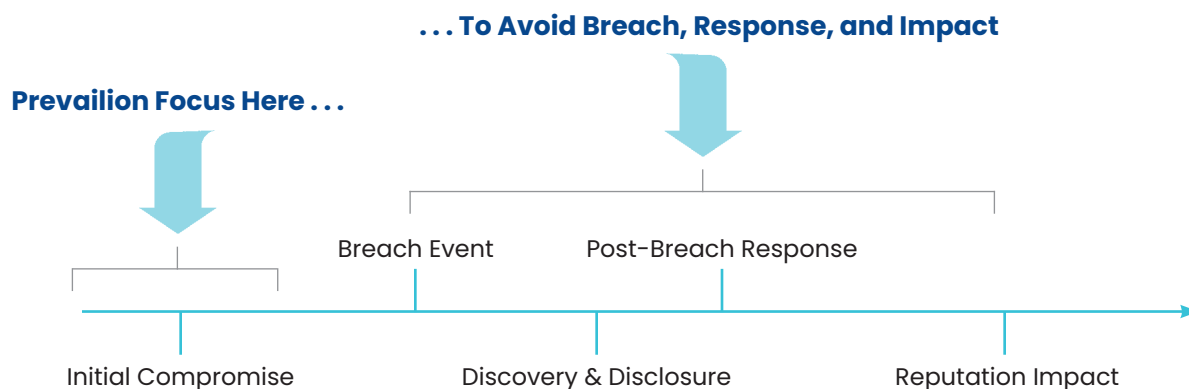
A promising technique that is becoming part of the standard process for deriving useful threat intelligence for cyber defense involves the active penetration by experts of hacker networks. By networks, we do not mean their computing network, as in a local area network. Instead, we mean the virtual communication networks used by hackers to exchange ideas, tools, and potential indicators or evidence of compromise.

Founded in 2017, Texas-based cybersecurity firm, Prevailion, offers a commercial solution called APEX that follows this approach to collecting and deriving intelligence. Specifically, the APEX platform provides its customers with insights into attacker networks, which helps to provide confirmation of new, on-going, and prior cyber threats already having infected and active within a targeted organization. APEX includes many features consistent with the goal of compromise intelligence, including the following innovations:

- *Compromise Monitoring* – The APEX platform is designed to provide continuous monitoring for evidence of compromise whether for a supply chain partner or targeting the actual enterprise. This intelligence is collected directly from adversary behavior.

- *Compromise Analysis* – The APEX platform includes historical data that can be used to analyze compromises including detailed information about previous cyber infections that are searchable based on company name or IP address.

- *Compromise-Based Decision Making* – The objective of the APEX platform is to assist an enterprise with prioritization and decision-making regarding making the best design choices and investments for prevention, detection, and response.



**Figure 3. Prevalion Focus**

The key insight into how the APEX platform supports compromise intelligence is its approach to data collection. To effectively support the goal, while spying on the attacker communications itself outside of a target’s network, APEX collects data about a customer’s network and which malware is being used, and this is correlated with the threat group behind the malware, whether the attack is active elsewhere within partners, and sometimes what the attack generally seeks to accomplish in terms of gain to the malicious actor.

## **ACTION PLAN**

The TAG Cyber analyst team recommends that enterprise teams create an action plan regarding compromise intelligence. Such a plan should be driven by the security team but can include management coordination with adjacent groups such as IT operations or the privacy team. The recommended high-level step in the plan are as follows:

*Step 1: Inventory* – The enterprise team should take an inventory of the applicable internal, partner, supplier, and customer infrastructure or networks that are applicable in the context of compromise intelligence. This is easier said than done and the exercise has excellent side benefits for other aspects of the enterprise security program.

*Step 2: Vendor Review* – A set of compromise intelligence requirements should be shared with a set of suitable vendors (including the Prevalion platform outlined above). The requirements should include the goal of gaining insights into hacker networks to gain insights. TAG Cyber can always help buyers in the determination of optimal commercial vendor selection.

*Step 3: Implementation* – The implementation of compromise intelligence is generally quite easy without the need for complex software or system deployment. Starting a proof of concept (POC) with a capable commercial vendor should be simple enough to initiate in a matter of days or weeks.





**DISTINGUISHED  
VENDORS**



## DISTINGUISHED VENDORS

Q 4 2 0 2 1

**W**orking with cyber security vendors is our passion. It's what we do every day. Following is a list of the Distinguished Vendors we've worked with this past three months. They are the cream of the crop in their area – and we can vouch for their expertise. While we never create quadrants or waves that rank and sort vendors (which is ridiculous), we are 100% eager to celebrate good technology and solutions when we find them. And the vendors below certainly have met that criteria.



AaDya provides smart, simple, effective and affordable cybersecurity protection for small and midsize businesses. The Detroit-based company's all-in-one cybersecurity platform, Marzo4, is powered by Judy, an AI-driven virtual assistant. The platform offers endpoint and anti-phishing protection, along with password management and single-sign-on, with the goal of making cybersecurity protection accessible to companies of all sizes.



Allot is a global provider of leading innovative network intelligence and security solutions for service providers and enterprises worldwide. Its platform combines network-based security with home router and endpoint security to provide a unified security service for the mass market that's capable of protecting consumer IoT devices in the home, on mobile networks, and on public Wi-Fi.



Cloud adoption continues but concerns over secure usage remain. The confidential cloud provided by Anjuna facilitates the move to secure cloud by leveraging the hardware-grade secure enclaves available by the major cloud providers. Anjuna's confidential cloud helps secure all applications, databases, AI platforms, and custom and packaged code.



Arista Networks is an industry leader in data-driven client-to-cloud networking for large data centers, campuses, and other routing environments. The Santa Clara-based company's platforms deliver availability, agility, automation, analytics, and security through CloudVision and Arista EOS, an advanced network operating system. Its customers include global Fortune 500 companies in cloud services, finance, and other large public enterprises.



# TAG CYBER DISTINGUISHED VENDORS

2 0 2 1



When it comes to deception, Attivo Networks knows its stuff. For several years, the team at Attivo has been so generous to invest many hours helping us understand this important aspect of cyber security. Their advice is especially appreciated because it comes from a deep understanding of the practical issues that arise supporting deception in enterprise.



Avanade was founded as a joint venture between Microsoft and Accenture. The company's solutions include artificial intelligence, business analytics, cloud, application services, digital transformation, modern workplace, security services, technology, and managed services. Avanade helps clients transform business and drive competitive advantage through digital innovation.



BehavioSec is a behavioral biometrics company that provides continuous authentication for end users based on their interactions with the web and mobile apps. Its platform, which is used by numerous Forbes Global 2000 companies, uses deep authentication to continuously verify user identity, with zero friction and more than 99% accuracy across millions of users and billions of transactions.



The insider threat to enterprise has risen from a minor issue a decade ago to possibly the number one concern amongst the chief information security officers we deal with at TAG Cyber. Code42 has been a wonderful partner to help us understand the best ways to mitigate this significant concern. We are grateful for their kind assistance.



Deduce uses collective intelligence to protect businesses and their customers from unauthorized account access, data leakage, and identity fraud. Its platform and developer-friendly tools combine aggregate historical user data, identity risk intelligence, and proactive alerting to deliver a robust identity and authentication solution – empowering businesses to do their part to keep their users and communities safe.



Email is one of humans' most-used tools – for work and even for personal business. Yet, many email-focused security solutions aren't sufficient to stop the prevalence of attacks that start with email. Egress provides human-layer, intelligent email security to stop phishing attacks and business email compromise.

# TAG CYBER DISTINGUISHED VENDORS

2 0 2 1



Elisity helps companies redefine security and access in a world of cloud, mobility, and connected devices.

Its platform, Elisity Cognitive Trust, combines zero-trust network access and an AI-enabled software-defined perimeter, allowing enterprises to proactively protect their data and assets while ensuring secure access to any application or device, by any user, from anywhere.



With its acquisition of Signal Sciences, Fastly is vying to become the world's leading edge security provider, offering secure content delivery API security, and a cutting-edge web application firewall. The company's mission is to provide real-time visibility and protection via cloud-native solutions.



Truly iconic companies in cyber security are far-between, but HP stands out in its determination to provide a suite of products that not only support cyber security, but that actually play a key role in reducing risk to an organization. The TAG Cyber team is so grateful to HP for its kind support of our program and we appreciate the partnership.



HUMAN is dedicated to keeping enterprises safe from bot attacks. By installing a single line of code on a client's website, HUMAN reveals the differences between human and bot traffic patterns, and the company's advanced Human Verification Engine protects applications, APIs, and digital media from bot attacks, preventing losses and improving the digital experience for real humans.



DNS data offers insights into attacker domains and infrastructure. But many enterprises don't leverage DNS because traditional tools are too noisy and complicated. HYAS offers a next-gen protective DNS (PDNS) platform that helps security teams reduce the attack surface by identifying and blocking known maliciousness.



IronNet merges industry-leading cybersecurity products with unrivaled service to deliver real-time defense that spans the private and public sectors, globally. When organizations collaborate to detect, share intelligence, and stop threats together, they form a collective defense community. IronNet's Collective Defense platform — built on its IronDome and IronDefense products — enables organizations to reap the full benefits of this approach.

# TAG CYBER DISTINGUISHED VENDORS

2 0 2 1

## opentext™

OpenText™ Security Suite, powered by OpenText™ EnCase™ – industry-leading cyber forensics technology – provides 360° visibility into data-centric threats across endpoints and servers.

With a long history in enterprise information management, OpenText offers forensic-grade security solutions which help security teams make faster decisions and rapidly remediate threats.

## P R E V A I L I O N

Prevailion reduces companies' mean time to detect and mean time to respond. Prevailion's Compromise Intelligence™ tool, beacons out and collects data on attacker TTPs as well as target victims. Unprecedented insight into attacker networks gives security teams the ability to identify and prevent cyber compromise.



The Randori platform was designed to think and act like the attacker groups executing ransomware attacks. The platform identifies attack targets and illuminates where and how attackers will strike. Randori allows enterprises to find vulnerabilities, prioritize remediation, and close points of entry before they're exploited.



Protection of data is one of the most essential aspects of enterprise security, and the team at Sertainty has pioneered the idea of embedding intelligence into the data. This creative introduction of smart control into data has been one of the more interesting areas covered by our TAG Cyber analysts. Thanks to Sertainty for their continued support.



Shift5 protects operational technology from cyber compromise. Led by former military cyber experts, the company allows critical infrastructure companies to operate without significant cyber risk. Through data capture, visualization, analytics, and alerts, the Shift5 platform helps operators find and detect events and prevent cyber incidents.



Sphere is a woman-owned company that is redefining how organizations achieve controls across their environment. Its automation platform, SPHEREboard, provides an innovative approach that starts with collection and incorporates remediation of a client's most critical data, privileged accounts, and on-premises Messaging and Office 365 assets, while simplifying reporting and automating remediation to immediately reduce risk.

# TAG CYBER DISTINGUISHED VENDORS

2 0 2 1



Sysdig is a software-as-a-service platform built on an open-source stack. Its Secure DevOps Platform provides security that lets clients confidently run containers, Kubernetes, and cloud services – allowing them to secure their build pipeline, detect and respond to runtime threats, continuously validate compliance, and monitor and troubleshoot cloud infrastructure and services.



The use of a threat intelligence platform in enterprise has become a requirement for optimal cyber security protection. ThreatQuotient provides a world-class solution in this area, and they were so kind to invest the time and effort to help the TAG Cyber analysts understand how a threat-centric approach to operations can significantly improve posture.



The TrustMAPP team drives a new discipline called security performance management that we embraced fully at TAG Cyber in our program this past year. With the goal of offering continuous, automated assessment of posture, TrustMAPP provides an essential component of the modern enterprise security program. We are appreciative of their assistance and support.



Application protection is imperative for organizations of all sizes. Virsec provides runtime workload protection at all layers. With full visibility into workloads and a patented mapping technology, companies can get a handle on what's running in their environments and prevent known and unknown bad from executing.





