TAG Cyber Security Annual

1st QUARTER 2021

MARKET OUTLOOK & INDUSTRY INSIGHTS

WELCOME TO THE FIRST 2021 TAG CYBER SECURITY ANNUAL – 1ST QUARTER EDITION

If you've been following us for a few years, you know that it has been our process to publish an Annual each September. While our readers always provided positive comments on the content, we received one consistent piece of criticism: It's just too darn big! At over 400 pages, the Annual became a tome, which, when printed might look good on a coffee table, was less suited to how people consume content today. Thus, we moved to a more digestible Quarterly.

In addition to paring down the amount of content included in this cyber security report, publishing a quarterly report gives us the opportunity to focus on current cyber events. And, boy! Is there ever a lot to talk about as we open 2021. As this is being written, the world is dealing with the aftermath of the cyber attacks on FireEye and SolarWinds. Yes, the world. Cyber security is no longer a domain exclusive to our little community. It has become much bigger than that.

We suspect you, the cyber security practitioner reading this, are keenly aware. You've likely been saying the same thing for the duration of your career; cyber security is more than a "computer problem" or a "malware incident" that means the CEO or sales team can't access their email. Cyber attacks can adversely affect national security, individuals' livelihoods, companies' abilities to generate revenue from our hard-earned intellectual property, and more.

If you think this is hyperbolic, just look at the extent of the SolarWinds attack and how it has permeated throughout the global business community. At the time of this writing, not only were 18,000 SolarWinds Orion customers affected, but the method of execution—inserting malicious code into a software update pushed to SolarWinds customers—means that all those customers' customers may be potentially impacted. At the time of this writing, Microsoft, a SolarWinds customer, has identified more than 40 customers targeted via their compromised systems and has indicated that their source code may have been compromised as a result of the attack..

The attack on the U.S. Federal Government is potentially even more damaging. While specifics haven't been made public, the Department of Homeland Security and the State, Commerce, and Treasury Departments are suspected victims. Allegedly, so are the National Nuclear Security Administration, the U.S.'s nuclear weapons agency, and the Energy Department.

Continued

Mr. President, uh... Let's pick a different password. 'No_Malarkey' seems a tad obvious.
Powell/Amoroso

We do not yet know the full extent of this attack. We might not know for years. *What we do know* is that it won't be the last, the biggest, or the most consequential attack we're going to see.

That is why we do what we do.

To summarize a recently published article on the TAG Cyber website, enterprise security is one of the most difficult aspects of running a business. Cyber criminals have the advantage, and the continued use of perimeter controls and siloed approaches to cyber defense aren't working. While the vendor community is diligently building products, enterprises don't have the holistic, comprehensive security architectures required to prevent targeted, persistent attacks. Point products which support specific use cases aren't going to cut it in 2021 and beyond. Zero trust isn't a buzzword anymore; it's a necessity.

The articles, reports, and advice included in this Quarterly are reflective of the work we do day-to-day with enterprise security teams and cyber security vendors. But it's also not exhaustive (exhausting, perhaps, but not exhaustive). The security teams with which we consult are on a perpetual hunt for processes and technologies which allow them to reduce architectural complexity, manual efforts, and practices that don't allow them to quickly and accurately identify potential—relevant—security incidents.

We're helping enterprises review their portfolios to reduce product overlap and shelfware. We're helping them mine through marketing buzz and useless "trends" and "best product" rankings to find the right solutions for their environments. And they're asking for strategies that allow them to move faster and be more in-tune with overarching business goals.

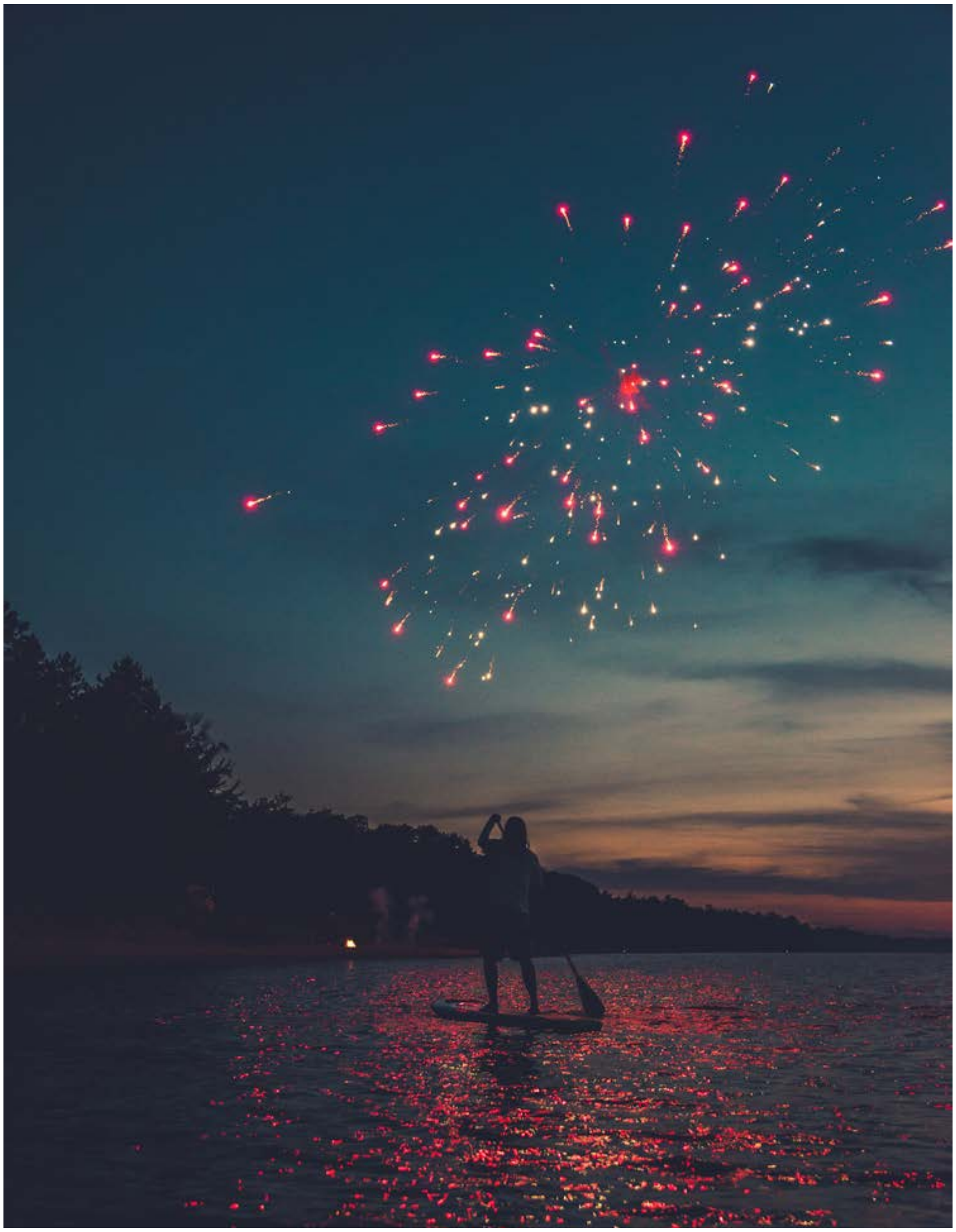
Yes, we've been saying similar things in cyber security for at least the past 10 years. But the rubber is really starting to hit the road in 2021 and cyber security is no longer just a media headline; it's a business impacting discipline in the same vein as finance or sales. It's been a long time coming.

Maybe it's the continuation of the COVID-19 crisis which has accelerated cyber security in a way no other event has, or maybe it's the political turmoil in the U.S., which affects the entire world in some way, shape, or form—but the needs of and pressures on enterprise security teams have never been more dire. I suspect we'll be saying the same a year from now. Nonetheless, organizations must adopt a serious and determined approach to cyber defense.

We humbly hope that the information provided in the following pages and the TAG Cyber 54 Controls are useful. We're constantly evolving and revising as the needs of enterprises change and as we see how environmental pressures affect security teams' abilities to defend their organizations. But we seek your guidance, too. In the words of a not-so-effective security campaign: if you see something, say something. In other words, get in touch. Let us know how you see and experience cyber security in 2021.

Despite the grim tone of this introduction, the growing team at TAG Cyber is incredibly excited about 2021! There is plenty of work to be done, for certain, but every day we see the skills, talent, and creativity in both enterprise teams and security vendors as they improve the industry. We've yet to encounter a security pro on either side who isn't motivated to make gains for the good guys. If you have read this far, you're probably pretty motivated to strengthen defenses against cyber criminals, too, and we look forward to continuing the conversation throughout 2021.

Stay safe, healthy, and secure – and we hope you enjoy our Q1 2021 TAG Cyber Security Quarterly.



FEATURED PHOTOGRAPER
Max Bender / Unsplash

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

TAG Cyber LLC
P.O. Box 260, Sparta, New Jersey 07871

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.

January 22, 2021

TAG Cyber Security Annual

1st QUARTER 2021

CONTENTS

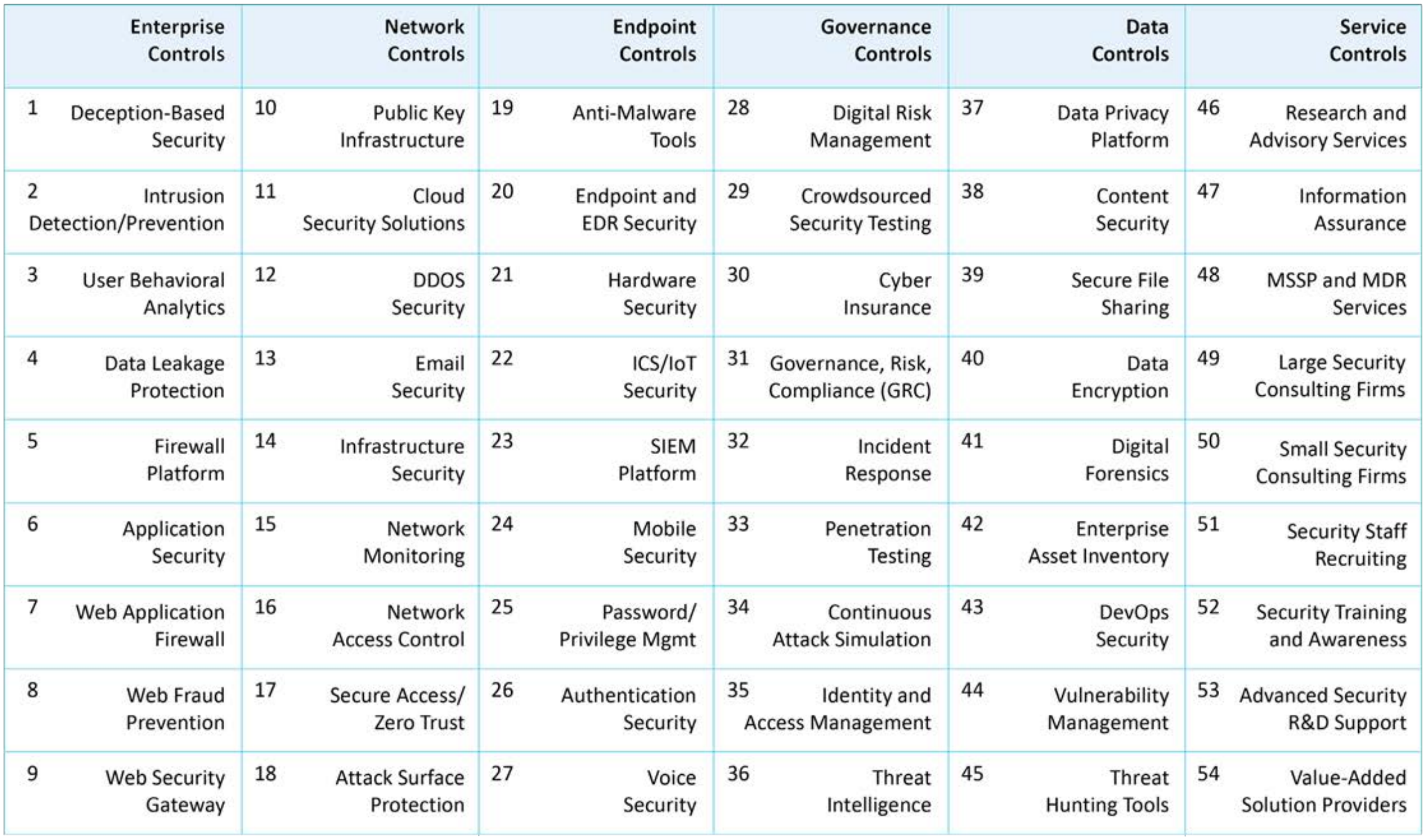
OVERVIEW OF THE TAG CYBER CONTROLS FOR 2021

Each year, our expert industry analysts review and update a list of what we refer to as the TAG Cyber Controls. Our list is best interpreted as those areas in which a Chief Information Security Officer (CISO) must include focus in their enterprise security program. The TAG Cyber Controls represent our best answer to the following question that we hear almost every day from CISOs and their teams: *What elements should I include specifically in my enterprise security program?*

We understand that many might choose to answer this question in terms of existing security frameworks. For example, we have the comprehensive NIST Cybersecurity Framework (CSF) and its detailed security requirements in NIST 800-53 (rev 5). We also have the smaller and more accessible Center for Internet Security (CIS) Controls, which boils things down to twenty functional recommendations to reduce enterprise security risk.

These frameworks, and those in between – including Payment Card Industry (PCI) Data Security Standard (DSS), Health Insurance Portability and Accountability Act (HIPAA), and others – play a key role in helping security teams develop protection programs. Even the privacy-oriented frameworks such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) introduce useful ideas that can help enterprise teams ensure proper coverage.

Continued



Enterprise Controls	Network Controls	Endpoint Controls	Governance Controls	Data Controls	Service Controls
1 Deception-Based Security	10 Public Key Infrastructure	19 Anti-Malware Tools	28 Digital Risk Management	37 Data Privacy Platform	46 Research and Advisory Services
2 Intrusion Detection/Prevention	11 Cloud Security Solutions	20 Endpoint and EDR Security	29 Crowdsourced Security Testing	38 Content Security	47 Information Assurance
3 User Behavioral Analytics	12 DDOS Security	21 Hardware Security	30 Cyber Insurance	39 Secure File Sharing	48 MSSP and MDR Services
4 Data Leakage Protection	13 Email Security	22 ICS/IoT Security	31 Governance, Risk, Compliance (GRC)	40 Data Encryption	49 Large Security Consulting Firms
5 Firewall Platform	14 Infrastructure Security	23 SIEM Platform	32 Incident Response	41 Digital Forensics	50 Small Security Consulting Firms
6 Application Security	15 Network Monitoring	24 Mobile Security	33 Penetration Testing	42 Enterprise Asset Inventory	51 Security Staff Recruiting
7 Web Application Firewall	16 Network Access Control	25 Password/ Privilege Mgmt	34 Continuous Attack Simulation	43 DevOps Security	52 Security Training and Awareness
8 Web Fraud Prevention	17 Secure Access/ Zero Trust	26 Authentication Security	35 Identity and Access Management	44 Vulnerability Management	53 Advanced Security R&D Support
9 Web Security Gateway	18 Attack Surface Protection	27 Voice Security	36 Threat Intelligence	45 Threat Hunting Tools	54 Value-Added Solution Providers

Figure 1. TAG Cyber Controls for 2021

Our belief at TAG Cyber, however, is that none of these frameworks are sufficient for our industry research and analysis, and none match our collective experience running security programs, managing enterprise protection, and coaching CISOs across every sector. Instead, the frameworks always include something important *just slightly off* in their coverage. What industry CISOs, for example, actually use the many pages of documentation in NIST as a practical guide?

THE CONTROLS

We developed the TAG Cyber controls based on practical experience. The framework includes familiar areas such as firewall platforms and multi-factor authentication, but it also includes newer strategies such as deception platforms and managed detection and response (MDR) vendors. Furthermore, the framework provides our subscription customers direct linkage to categorized lists of commercial vendors, rather than pages of detailed sub-requirements.

The TAG Cyber Controls are presented to support visual inspection at a glance, which explains why many refer to it as the Periodic Table of Security. CISO-led teams now use the fifty-four controls as a checklist to determine the completeness and accuracy of their program. Consultants can also use the framework to help clients assess the appropriateness of their security program without having to deal with the academic and often impractical requirements in other compliance criteria.

Readers of previous versions of this TAG Cyber report should note that some changes have been made to the framework for 2021. We expect this to continue as we monitor the industry, review new trends, and work with CISO-led teams. The changes are subtle, but important – because they help to ensure that our control structure is complete and accurate. We work hard to ensure no gaps in our treatment, so that your program can avoid exploitable seams.

The six categories used to organize the fifty-four controls – namely, enterprise, network, endpoint, governance, data, and service – were created to help enterprise teams differentiate between the various entries. Admittedly, the categorization is not perfect, and any security expert perusing the structure will find one or two examples quickly that might not exactly match up with their listed category. We therefore don't make too big a deal of the categories, and just use them as a presentation device versus something more substantive.

To review our control details visit: **www.tag-cyber.com/advisory/controls**

GOVERNMENT

A PROPOSED BIDEN DOCTRINE FOR CYBER

EDWARD AMOROSO

This article first appeared on the TAG Cyber website in late November 2020 as the results of the 2020 election were becoming clear. The advice and guidance remain 100% relevant today in early 2021.

The **first** mistake the US federal government has made in cyber security since 2000 has been its mistaken belief that the best defense is a good *offense*. The truth instead is that the best defense is a good *defense*. The problem is that preventing attacks is much harder than breaking into systems – hence the twisted emphasis.

Asking your adversary to stop hacking is like asking the clouds to stop raining.

It's time to leave cyber offense to US Cyber Command and to refocus 100% of our collective energies on improving our nation's defenses through distribution, virtualization, and simplification. This is best done *locally* versus nationally, for the same reasons that we like our elections to be local and distributed. When it comes to cyber defense – we must think local.

The **second** mistake we have made in cyber has been our over-reliance on the effectiveness of information sharing. Certainly, good threat intelligence is important – and excellent commercial platforms exist. But this belief that a big-group-hug with our international allies will stop cyber threats is both immature and incorrect.

I worry that the Biden team, likely stocked with Obama veterans who will believe in friendly collaboration like religion will mistakenly emphasize cyber alliances as effective cyber defense. Unfortunately, this is like setting up a neighborhood watch to prevent leaks in everyone's roofs. It's much better to just fix the damn roofs.

The **third** and most serious mistake we've made as a nation in cyber involves our private requests (Obama) and public cajoling (Trump) that the Russians and Chinese should please stop attacking our infrastructure. Asking your adversary to stop hacking is like asking the clouds to stop raining. This approach does not work.

It amazes me that more experts in our field do not see the folly in this strategy. Imagine the misguided CISO wandering into the board room to explain that the new risk reduction plan is to plead with the fraudsters to stop hacking. Any CISO taking this approach would be out of work quickly. And yet, we do this every day on a national level.

My advice instead to the incoming administration would be to create a new strategy – a *Biden Doctrine for Cyber*, if you will. Such a strategy would boldly establish the following goal: To implement a massively distributed cyber defense using our *existing* localized teams that is so effective as to render attacks from adversaries obsolete. Here's how to do it:

First, we should immediately retire any new investment in overlay security programs such as Einstein 2. This centralized monitoring system was conceived twenty years ago and has been about as useful to our risk posture as a Styrofoam shield in a gun fight. Leave it running for now, but don’t waste any more money trying to fix it.

The goal instead should be to step away from any large, centralized systems of monitoring or mitigation – and to replace such efforts with massively distributed protection initiatives. A mosaic of distinct and diverse security schemes should emerge, which will greatly complicate attacks from adversaries. We need distributed-micro, not centralized-macro.

Second, we should identify the top public and private organizations considered part of our critical infrastructure and reallocate in prorated grants the majority of money budgeted for CISA for detection and prevention of cyber threats. Let the recipients use the cash to hire new staff, buy new tools, and upgrade their protections. This is a better use of the money.

Consider this: The CISOs of our major public and private institutions have reached the point where they have more hands-on experience with cyber defense than their DHS counterparts. Energy companies, telecoms, civilian agencies, cloud providers, and the like – have become the new collective cyber front. That’s where the money should go.

I know many of you will gasp at the suggestion that we take such a step. But the goal must be a distributed defense versus a centralized one. We already have the localized components of such a decentralized set-up in our public agencies and larger private companies. So, the goal should be to improve them – and this is done by sending money. It is honestly that simple.

One more thing: You might gasp at the idea of sending money to the big greedy energy or cloud companies – demanding that they take more of their earnings and allocate them to cyber. Well, they are not doing this, so you can cut off your nose to spite your face, or you can do what needs to be done to reduce risk. It’s a simple choice.

And third, we should dramatically accelerate and rejuvenate a massive national program of cyber security service for your people. The formula is easy: Four years of university in return for five years of cyber-related service at a designated public or private organization. DHS can help coordinate all the logistics. This will inject fresh ideas into our cyber defenses.

Here's the math: If this program includes *twenty thousand* fresh graduates each year, then after four years – each of the top two thousand public and private organizations could see ten new cyber-trained employees arrive *each year*. Funding would be easy to obtain, and many youngsters would remain in their jobs after the five-year commitment.

By following these three strategies – de-emphasizing centralized DHS monitoring, improving local defenses through cash grants, and injecting youngsters into the work mix – we create the conditions necessary for the distributed parts of our national infrastructure to properly protect themselves. It's micro-protection versus macro-protection.

Here's one more observation: Virtually every cyber security lead for every major organization of consequence knows exactly how to protect their infrastructure more effectively. The reason they do not do this is three-fold: They don't have enough budgeted cash, they don't have the right people, and their infrastructure is too complex.

My proposal addresses the first two of these problems by allocating DHS cyber budget to the places where the money can be better used, and by directing a national program for youth in cyber. The third problem of simplification would have to be addressed in conjunction with the IT and CIO leaders across critical infrastructure.

Here are our choices: Scenario one is that the United States decides to toss more money at some new centralized Son-of-Einstein. Scenario two is that Biden adjusts the plan as per the points made above to strengthen *existing local programs.* Which do you think would inject more fear and uncertainty into our adversaries? I think the answer is pretty obvious.

Regarding effectiveness of this approach, recognize that attacks target local entry points. Adversaries find weaknesses in some soft spot and then use this access to laterally traverse to other assets. By strengthening soft spots and minimizing trusted cascade (called zero trust in our industry), we create the best chances for a workable national defense.

By the way, I would not expect any of this to result in staff reductions at CISA. But it will require that existing staff be deployed where they are truly needed. Instead of sitting in a cubicle in Northern Virginia writing CDM documents that no one will read, they should be assigned to live teams to help reduce risk where it truly resides. These will be better jobs.

Let me know what you think of all this. I know it can be jarring to hear that our national cyber defense isn't working and should be scrapped. But recognizing and admitting to a problem is the first step in fixing it.

TRUMP TWITTER HACK SHOWS PASSWORD POLICIES YET AGAIN LACKING

KATIE TEITLER

This article was written after President Trump's Twitter account was compromised by a cyber security researcher to demonstrate how lack of two-factor authentication can lead to breach – but before his account was permanently suspended in January 2021.

Victor Gevers must have a 197-point IQ and a better-than-15% guess rate on President Trump's password because, guess what? Gevers claims he was able to access Trump's Twitter account by accurately guessing Trump's highly complex and long password: "maga2020!"

At least he used the exclamation point.

By now you've surely read the news, and given that we're less than two weeks out from the U.S. Presidential election, you surely have some opinion on Trump. And not just if you're a U.S. citizen.

But this isn't a political post. We at TAG Cyber have opinions, but we'll only publicly share the ones about cyber security.

Let me iterate the problems we all know so well:

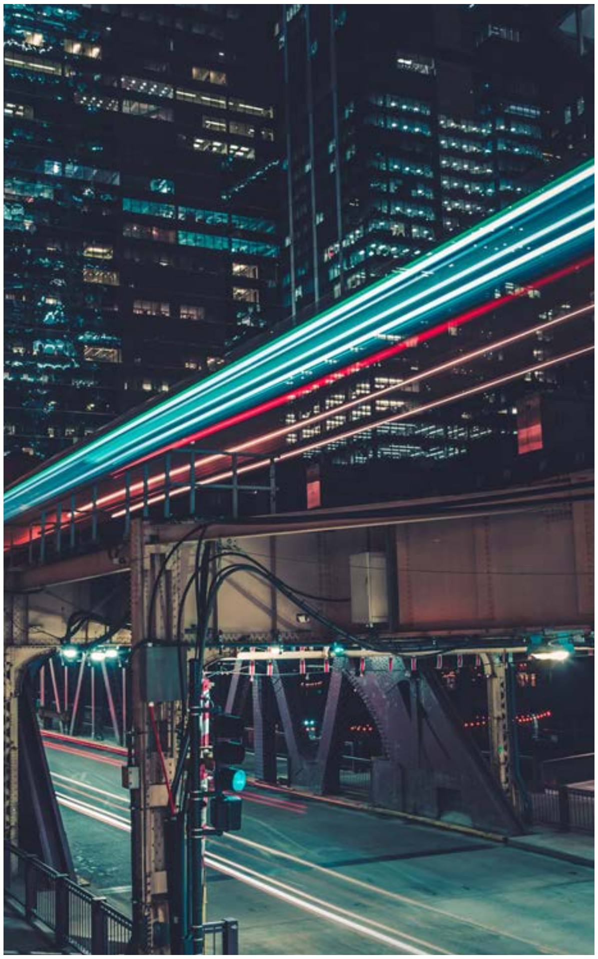
- The account was "protected" by an easy-to-guess, insufficiently long (sorry, NIST), human-devised password
- The account did not have two- or multi-factor authentication turned on

Now, I bet you're going to expect me to chastise the President.

Nope, not going to happen here.

Instead, let's look at the platform provider: Twitter, which has been compromised numerous times over the years, promised to implement stricter access controls for political figures after last month's breach. Why only political figures deserve better security is anyone's guess.

> …if companies expect to secure customers'/consumers' accounts, 2FA/MFA must be turned on by default.



But the promise apparently didn't turn into action. Although Twitter is denying claims of a breach, stating there is "no evidence," I think most people's money is on the validity of Gevers' claim.

Even if this is a security researcher seeking the limelight, the facts are this: I was able to just minutes ago log into Twitter and change my password to "asdfgh2020!" (Yes, I changed it again—before finishing this sentence—to an auto-generated, excessively long, new password for which a second factor of authentication is required.) I am not a political figure. I am not even famous among industry analysts. I'm barely even recognizable in the security industry. But, come on, Twitter. This shouldn't be allowed and you know it.

Also, I use 2FA because everyone should. All cyber security guidance says the same thing—I haven't seen much dissent among our community. But, as anyone using Twitter knows, 2FA is a "feature," not a requirement. Maybe Twitter isn't your bank account, your mortage account, or your health care provider, but if companies expect to secure customers'/consumers' accounts, 2FA/MFA must be turned on *by default*. If a user wants to turn off 2FA/MFA, they should be required to acknowledge they are reducing the security of their account(s).

Also…forced long passwords for the win.

I know, I know: Users don't like long passwords. Users don't like friction. The business wants convenience. Twitter and others like it want more users so that they can sell our data. I get it. But the reality is, if businesses expect to reduce breaches, especially stupid ones like this where the password is way too obvious and there isn't an additional authentication factor, they're going to have to step up their game. Maybe Twitter doesn't care. They won't lose users over this.

What if your company is a bank, or a mortgage lender, or a health care company, though? Will you lose customers? Revenue? Damage your brand? Will you negatively impact people's lives? This is a moral and ethical question just as much as it is a business and security question.

The least companies can do for their account holders is require strong passwords and 2FA/MFA by default. We know there are other, potentially better, options than username/password, but this should be the minimum viable requirement.

A TALE OF TWO SECURITY EXECUTIVES

EDWARD AMOROSO

This article first appeared on the TAG Cyber website in late November 2020 to a great deal of discussion and debate. We include it here as a useful guide to the types of considerations important in selecting or removing security executives.

You can learn much about an organization by comparing the executives who are being hired with those who are being fired. This has been a valid assessment technique for as long as modern organizations have existed. To that end, let's have a brief look at two very different types of cyber security executives passing in opposite directions through the revolving door of the departing Trump Administration.

> Despite a healthy resume of excellent positions … the word "cybersecurity" isn't even hinted.

To start, you might *not* have noticed that the outgoing President recently hired a Chief Information Security Officer (CISO) for our nation. Way back on November 4th (seems like a long time ago), articles began to appear that Camilo Sandoval had been quietly appointed to one of our nation's top cyber security positions in October. The previous CISO, Grant Schneider, has quit the job during summer to join Venable's advisory team.

Like perhaps some of you, I'd never heard of Camilo Sandoval, despite four decades in the industry with my tentacles reaching into and around most nooks and crannies of our nation's cyber community. So, I checked LinkedIn and found him to possess a nice resume that was certainly impressive. But it was also a background that would also make him patently unqualified for the CISO position in any large organization – much less *our country.*

Let me explain: When hiring a CISO, and TAG Cyber has been involved in this process many times, the background of the candidate must include extensive experience in senior positions that involve selection of cyber security technology, management of policy and compliance initiatives, leadership of security teams, and immersion in the massive security community. As far as I can tell, Sandoval's resume would be tossed in any reasonable search process.

Despite a healthy resume of excellent positions advising the VA in technical matters, serving as a chief of staff at a bank, and spending time in the 90s as an intelligence analyst, the word "cybersecurity" isn't even hinted on his LinkedIn resume. There is, however, the one position that jumps off the page: He spent over a year as the guy directing voter contact operations for Donald J. Trump for President, Inc. This is important work but has nothing to do with cyber.

I would ask that you set aside the partisanship for a moment and ask yourself: Is this a valid background for a cyber security executive for America? Take me for example: Would I make a better choice? I've spent forty years in this area, and no one called me. Take Charles Blauner, or Jim Routh, or Phil Venables. Would any of these fine executives have been better choices? Did anyone in Washington call them? Answer: No.

Now let's glance across the turnstile at someone Donald Trump just fired-by-tweet (I still can't get used to that process). Christopher Krebs spent the last couple of years as the Director of the Cybersecurity and Infrastructure Security Agency (CISA), in our Department of Homeland Security (DHS). Unlike Sandoval, Krebs does have the word "cybersecurity" all over his resume, including time spent at Microsoft directing cyber policy.

I can personally attest to his fine approach to the job, and his immersion in our complex community. (He and I sat together for dinner at February's RSA conference – the last event I attended before the pandemic.) Despite partisan correlation between his government and commercial appointments (worked for Bush, left for industry during Obama, and returned to government under Trump), I can report that his approach has been anything but partisan.

Now – again setting aside the bias, have a second look at the background of this executive, and ask yourself if he looks like someone worth keeping in our government. I believe that you will come to the same conclusion as me: This is *exactly* the type of person who should be making decisions about cyber security for our nation. His background could serve as a template for the academic, industry, and government experience required for a senior position in cyber.

Here's another thing: I've watched the many sad eulogies about Krebs on TV these past few hours, and I can't help but laugh. Krebs told the truth and got fired. As his punishment, he will now follow the path of prior fine executives like Andy Ozment who left DHS for a CISO position at Goldman Sachs. If you do the typical salary math on this type of transition, you will measure something like a twenty X increase in annual compensation. Really.

So, I guess the good news in all of this is that while our nation has inherited a nakedly partisan vote solicitor as our temporary CISO, and while an experienced and capable security executive, now cleaning out his desk in DC, and who will probably be shopping for a brownstone in Tribeca pretty soon – we can at least come to one conclusion that might help you feel a bit better: Telling the truth can be a lucrative decision.

BUSINESS

HOW IS YOUR CYBER SECURITY SALES PROCESS?

KATIE TEITLER

Sales has been around since the dawn of tradesmanship. Even before the term was codified, heck, probably before humans' early ancestors spoke a language anyone alive today would recognize, humans have been selling wares. Looking at more recent history, pre-1990s or so, sales were conducted in person or over the phone. In person—even door-to-door—sales were considered the best and most reliable method. If you could look someone in the eye and shake their hand, your chances of making a sale were greatly increased.

> **The startup SaaS culture has turned sales into metrics rather than relationships.**

When email and the internet started to become ubiquitous, salespeople held on to tried and true methods, dialing for dollars, as it were, and racking up thousands of dollars in travel fees and air miles to visit prospects in cities wide and far. By the early 2000s, the digital realm changed sales for good. LinkedIn was launched in 2002 and suddenly businesspeople had a new way to connect. It wasn't long before savvy salespeople saw an opportunity and started trying to connect with new, prospective clients, then move them to the next phase, a.k.a., the one-on-one, in-person meeting where the relationship was fully developed.

As time went on, and other platforms made it easier for salespeople to find their "financial buyer" via a quick internet search, the number of unsolicited cyber sales pitches increased exponentially. Executives were inundated with the one-two punch of email-followed-by-phone-message—*always under 30 seconds!*—in an effort to reach new prospects. As it became easier for salespeople to identify and connect with potential buyers, buyers found new ways to filter out the noise. Thus, it grew even more imperative for salespeople to connect with a greater number of people every day. It didn't matter how you got through. Just get through. Just get someone to take a call. Just get someone to sit through a demo. Just get them to know you.

SALES DIGITAL TRANSFORMATION

Consequently, over the last few decades, sales has evolved from a highly personalized profession to a high velocity numbers game. Especially in light of COVID, without any in-person meetings or industry events, and as the economy has presented numerous sales challenges, enterprise buyers have reported a massive uptick in digital solicitations. But because cyber security product sales, for many (not all), has become high volume, high velocity outreach, product seekers and budget holders have become the causalities of a spray and pray sales approach.

TAG Cyber's enterprise clients note this all the time: *I'm receiving more LinkedIn messages where the person has no idea what my job title is or what my responsibilities are. I got two emails today where the note read, "Dear %FirstName%."* I, myself, have receive several messages in the last few weeks asking if I am interested in buying networking equipment, phishing prevention software, video conferencing software, and lead generation lists. I'm a cyber security industry analyst. I need none of these things (OK, maybe technically I need the phishing [spam] prevention but it's not my network, not my budget, not my decision).

Quite simply, this spray and pray approach doesn't work for end users, practitioners, implementers…i.e., buyers. Good salespeople know this, but they can feel trapped by arbitrary metrics required by management teams pushing employees to hit their quotas. Somehow, a good portion of sales has become like the 1980s perfume sales reps in the mall who would ask if you wanted a spritz of their new perfume, and even when you said no, would spray it in your direction anyway. *Maybe the shopper will catch a whiff and realize they really do want to buy this perfume.* Today, the sales process has changed, and many salespeople have lost sight of the need to educate themselves on prospects—the individuals they're contacting—before reaching out. And spritzing.

The art of taking the time to get to know a prospect has been lost, and it has been precipitated by our overreliance on technology and the rush, rush, rush world we live in. As a result, nearly every time we talk to an enterprise security client about vendor product selection, we hear the same things: *It's hard to find a salesperson who will listen to what we need. Vendors have canned product pitches, and they all focus on the same "differentiators" as their competitors. We went through multiple sales calls and an entire demo then found out their product is incompatible with our environment. On the first call, the vendor said they could do X, but when we were ready to purchase, they said they'd be building that capability custom and we wouldn't have it until 4 weeks after we deploy.*

But we know that there are good cyber salespeople out there who believe in their products and have just lost their way. The startup SaaS culture has turned sales into metrics rather than relationships. And it's hurting both sides of the equation.

Because, as analysts, we sit at the intersection of vendors and buyers, we recommend cyber security salespeople return to the "old-fashioned" mentality of a personalized sales approach but combined with the advantages of modern technology. If done correctly, the result will be more conversations, more opportunities, and more (possibly higher value) sales. One challenge, in certain cases, will be convincing sales managers to adjust metrics to reflect the time and effort it takes to get to the first meeting—more reflective of a pre-2000s sales cycle where "hitting the number" is more important than number of new contacts added to the CRM.

DO YOUR HOMEWORK

For those with true sales persuasive powers (or enough trust of their sales leadership), we recommend getting back to sales basics. Selling your cyber security solution is about *people and their needs*. And no two companies have the exact same needs, so throw out the corporate pitch deck and start your meetings with conversations. Before you're given the permission for a conversation, though, you'll need to do your homework on the person whom you're trying to convince to make time in their schedule. This convincing will require more time than stalking the surface of someone's LinkedIn profile. For instance, my profile says that I am a cyber security analyst. Job titles in security can be tricky, but it's well worth a salesperson's time to a) visit my company's website to see what the company does and the context of my work as an employee and, b) look at my LinkedIn activity. Literally two minutes is all it would take someone to figure out that I am a research analyst, not the person who monitors network/cloud technologies and investigates alerts and security issues.

Many security executives intentionally have sparse social media profiles, but a quick Google search will often provide greater context about the person's offline activity and interests. For instance, before Ed (TAG Cyber's CEO, founder, and lead analyst) founded TAG Cyber, he did a ton of presenting and speaking as AT&T's Chief Security Officer. His presentations were varied—Ed could/can speak eloquently on any security topic—but often his presentations reflected what his internal team was currently working on. Even if this isn't the case for other CSOs/CISOs, it's at least an opening for a conversation. And it shows the CSO/CISO that the salesperson bothered to minimally look into the individual rather than simply spamming them because of their job title.

For large, publicly traded companies, salespeople should peek at the Annual Report/10K, other investor information, and company press releases to see what security tidbits they can glean. As cyber security has become a top-line business risk, security initiatives have made their way into these public documents and can give hints about the company's approach to security. And again, if it doesn't give the salesperson specific information about the prospect, referencing business goals in the context of security will at least demonstrates effort to learn and listen. That said, don't half @$s it. Do your homework with honest intentions and you're more likely to gain the connection.

If you're a salesperson doing more speaking than listening on your first few calls, you're headed down the wrong path.

AFTER THE CONNECTION

If the salesperson has done a bit of background investigation and catches the eye or ear of a potential buyer, the next step is…more research! This time, though, in the form of listening. Use the 80/20 rule: listen 80% of the time; speak 20% of the time. If you're a salesperson doing more speaking than listening on your first few calls, you're headed down the wrong path. Don't make it about your groundbreaking, fully automated, cloud-based, zero latency, environment-agnostic powered by artificial intelligence solution.

Go in with the intention of fact finding. A good salesperson must understand the buyer's/enterprise's:

- **Business requirements:** How will the technology be used? In what context? What are the intended outcomes? What are the KPIs the tool will be measured against? Who will be responsible for the day-to-day management/operation of technology? How much professional service support will they need? Are there additional stakeholders involved in the decision (who are not involved in current discussions)?
- **Architectural requirements:** What networks/data/apps/OSs/languages does it need to support? Does the company run legacy tech, or does it operate in the cloud only? Will the company need help migrating from on-prem to cloud? What are the company's plans for scaling?
- **Implementation requirements:** Can the company support network changes? Can the company support integrations themselves? What is their timeframe for implementation? What is their timeline for results/reports/data?

The main thing for salespeople to remember is that there are humans on the other end of the phone/keyboard/screen who need to solve real problems for their businesses. For them, buying a product is about a need, not your quota. While it's a conundrum—the more product you push, the more you get paid, the better your job security—the irony is that the more you listen, the quicker and easier it will be to find the right buyers and the less time you will spend time sending blind emails.

For example, on a recent call with a major enterprise, the security program owners were complaining that they were about to enter the POC stage with a security vendor and it became clear the vendor was unaware that the company was still running a large chunk of its infrastructure on Linux/Unix.

To the enterprise, it was obvious—it's what they dealt with every day. The vendor, on the other hand, was thinking about its cloud-friendly tech and missed a major foundational element that made the product incompatible with the enterprise's environment.

Because the vendor didn't take the time to learn about the business's requirements, discussions were halted in their tracks after months of conversations. This was wasted time for everyone; the salesperson would have been better served gathering requirements in the first calls and moving on to a more viable prospect with real sales potential, and the enterprise would have been better off evaluating a different vendor.

MORE THAN ENOUGH PROSPECTS TO FILL YOUR FUNNEL

The reality of today's cyber security landscape is that there are more than enough enterprise buyers. The trick is finding the right match. And salespeople won't do that with vanilla emails or messages that aren't suited to the buyer and don't touch on a pain point.

Every day I log on to social media and see end user friends and colleagues complaining about the inappropriate and off-target messages they're receiving from product salespeople. Yet, they all need to buy products to run their companies! In fairness, and salespeople know this, there is some recalcitrance around the idea of "sales." The spray and pray method used by few (but too many) salespeople has soured the soup for potential buyers—they've come to expect a smash and grab approach rather than someone who takes the time to get to know them and their security technology needs.

Technology has made it possible for people to reach farther and wider than ever before. And as such, there's been a loss of personalization in how we interact. However, technology has also given us the tools to learn more about people—or any subject—from anywhere and at any time. While digital transformation has largely made sales a numbers game, it also has the potential to bring it back around and create opportunities for customization. One very successful salesperson I know recently said to me, "Sales has gone way too far into metrics and away from actually being human and solving real needs. So, anything I can do to correct that is top of my list. It's easier for me to work on a problem when they know I'm not just trying to shove software down their throats."

Though sales culture won't change overnight, I firmly believe we have a huge opportunity—as most of us still sit at home, working in isolation—to start connecting better with others. In a sales context, this will result in less time spent on emails that are inevitably filtered directly into spam, never read, and only count toward arbitrary metrics goals. A personalized approach to connecting will, in fact, lead to quicker, larger deals that end in bigger paychecks and President's Club awards…when we can all travel and see each other in person again.

THE HOSPITALS' *OTHER* INVISIBLE ENEMY

DAVID HECHLER

When we think about hospitals under attack, we immediately focus on the pandemic and health care workers. But they have another battle on their hands at the moment. There's a growing wave of ransomware attacks that, like COVID-19, seems to be intensifying. With no sign of a flattening curve.

The medical troops, of course, have community, professional, and government support behind them. And knowledgeable experts like Dr. Anthony Fauci, director of the National Institute of Allergy and Infectious Diseases, to advise them.

What about the brigade fighting the cyber war? Not so much.

As if their jobs weren't hard enough, employees are buckling under a wave of cyber attacks.

They do have support, of course. Like all of the industries victimized by the explosion of attacks in which criminals lock up a company's data and demand payment in exchange for the key, hospitals can turn to lawyers, law enforcement, and cyber security vendors for help. The hospitals also have John Riggi.

Riggi is their Anthony Fauci. He's not a doctor. He's the senior adviser for cyber security and risk at the American Hospital Association (AHA). For nearly three years he's been guiding member hospitals through the unpredictable weather of this turbulent world. His 25 years in the FBI, including a lengthy stint focused on cyber crimes, have given him a solid grounding. His communication skills are equally clear in presentations at conferences and in the articles he writes.

But unlike Dr. Fauci, there's no clear formula he can offer. In cyber security, there's nothing comparable to: "Follow the science." Updating and patching software won't protect a hospital when an employee opens an email and clicks on a link. Managing these risks is more of an art than a science.

He's had plenty of practice plying that art. When hospitals are under attack, they call. And he counsels. Not just AHA members, he emphasized. "We provide that to any hospital," Riggi said. "Simply as a public service, to help guide them through the event."

He can help them get in touch with government agencies. He's often a "sounding board." He offers an outside perspective, based on lots of experience. But he doesn't tell them what to do.

Like the FBI, the hospital association "highly discourages the payment of a ransom," Riggi noted. He ticked off some of the reasons. It rewards and encourages the attackers. It funds the criminal organizations that perpetrate them. And there's no guarantee that the encrypted data will be decrypted after the payment is made.

It's not a coincidence that the AHA's policy aligns with the FBI's. "I actually helped write the FBI policy," Riggi said. But the decision is not up to the AHA. "We would never want to come out and say that the hospital should pay or not pay. That has to be left to an individual decision for the hospital, based on the circumstances."

A PROBLEM THAT ONLY GROWS

Ransomware has been the bane of the industry for some time. Verizon's Data Breach Investigations Report found that more than 70 percent of malware attacks on health care organizations in 2018 and 2019 were ransomware.

Early in the pandemic, it seemed as though the hospitals had caught a break. Cyber criminals recognized the desperate need for medical care. In March, some said they would seek other targets.

Did they keep their word? "They did not," Riggi said. "The proclamation was noble, but their actions have not been. The attacks soon continued."

In September, the hospital chain Universal Health Services (UHS) was hit. More than 250 hospitals and clinics in the United States were crippled by the attack. With digital data unavailable, employees were forced to rely on paper backups.

There aren't great statistics in this area, Riggi said. Some hospitals would just as soon keep these things quiet. But from September 1 to November 10, U.S. hospitals reported 104 breaches, he said. Not all of them were ransomware attacks, he added, but many of them were.

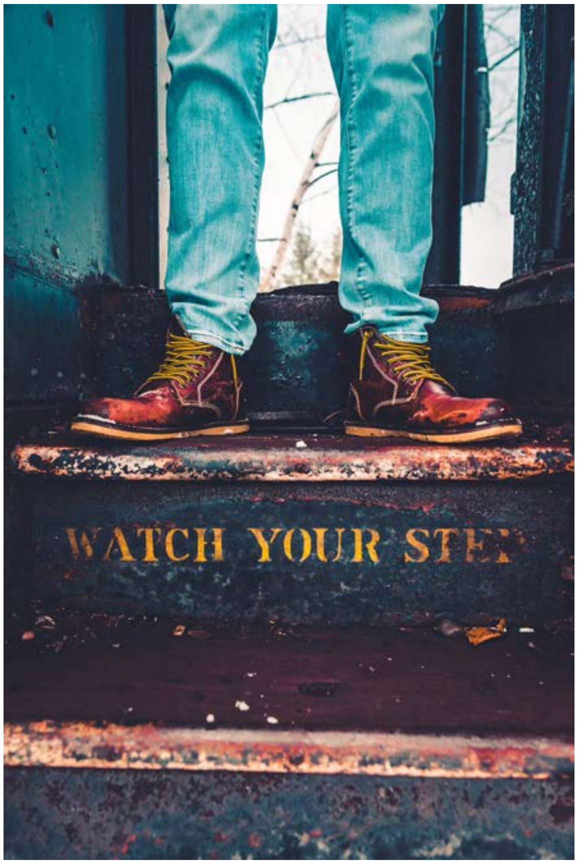
The onslaught seemed to come to a head in October. There was the threat of another wave of attacks. "Hundreds of hospitals" were being targeted by criminals believed to be based in Moscow and St. Petersburg, according to The New York Times. They were said to be the same group that had earlier attacked the UHS chain.

DEFENDING FORWARD

But the news wasn't all bad. The Russians had suffered a big setback themselves in September. They were associated with Trickbot, a giant botnet used to launch ransomware attacks that drew intense attention as the U.S. election approach. The authorities feared ransomware might be used to disrupt or even sabotage the vote.

But public and private defenders emerged to thwart the effort. Apparently working independently, the United States Cyber Command hacked into the botnet's infrastructure in an effort to disable it, and Microsoft Corporation managed to secure federal court orders to take down a vast number of Trickbot servers. Together they succeeded in putting it out of commission—at least temporarily.

Riggi was heartened by these efforts. He'd already seen real improvement in the sharing of threat information among government agencies. The increased frequency and greater specificity of the intelligence, and the coordination among the FBI, Homeland Security, Health and Human Services, and the National Security Agency underscored their determination to assist hospitals before, during, and after attacks, he said. But the actions of Cyber Command took it to another level.



He applauded the government's willingness to "defend forward," using the phrase that Paul Nakasone, NSA director and commander of the U.S. Cyber Command, used to describe the strategy in a recent article (in which he acknowledged it originated with the Department of Defense). The election was the apparent justification for the aggressive actions in September. Could protecting hospitals justify future action by Cyber Command?

"In my opinion, yes it would," Riggi said. "Because there is a threat with real physical impact, physical harm resulting. And I think it was even acknowledged that the collateral benefit of going after the Trickbot botnet was that it would also help slow down the spread of ransomware, which we know is heavily targeting hospitals at the moment."

LOOKING BEYOND HEALTH CARE

The hospitals' experience offers lessons for other industries, Riggi continued. He recommends that they establish a relationship and develop a rapport with the FBI and other government agencies, like the Cybersecurity and Infrastructure Security Agency, prior to an attack. All companies would be wise to do likewise, he said. You don't want to start the process as you fumble for advice in a crisis.

And now more than ever, Riggi said, all industries are vulnerable. The Covid pandemic that forced a mass exodus from the office has made us all more dependent on technology, he noted. "Technology is great, digitization is great, our use of artificial intelligence is great. But within those advancements," he said, "there is embedded risk, which may expand the attack surface for the adversaries."

And the risks aren't limited to business failures, he warned. There can be safety risks as well. Not only to your employees. They can also endanger your clients, he added.

TOP FIVE IDEAS FOR YOUR 2021 ENTERPRISE SECURITY PROGRAM

EDWARD AMOROSO

This article was written in late 2020 with the goal of helping enterprise security teams advance their 2021 initiatives. Use this as a guide to check your own plan or to create one now. It's not too late!

Thanks to frameworks like PCI-DSS, most enterprise security programs have evolved to a familiar common baseline. Such resemblance has its advantages – especially when considering partnerships and third-party arrangements. We can thus agree that most security teams by now have learned to perform the basics reasonably well. Suggestions for improvement must therefore go beyond obvious methods.

As a result, the best guidance an analyst can offer CISO-led teams will include ideas that transcend conventional frameworks. The hope is that by introducing new concepts – or reinforcing old ones– we can help enterprise security teams gain some advantage over their adversary. This is especially important in 2021, where we all know that nation-state and criminal offensive actors will be at the top of their game.

Perhaps you might break up your massive compliance initiatives into smaller pieces, perhaps aligned with the micro-segments and distributed workloads you are moving to cloud.

In this article, we provide our top five ideas for enterprise security teams to consider for incorporation into their programs. The ideas stem from the myriad hours (and hours) (and more hours) spent by the TAG Cyber team in 2020 working with commercial vendors, enterprise security professionals, and government agencies. The ideas thus emerge from the trenches versus some ivory tower. We hope they are helpful to you.

IDEA 1: LOCALIZE YOUR SECURITY COMPLIANCE

As enterprise infrastructure has tended to grow more complex, the associated enterprise security compliance obligation has also increased in complexity. It is not uncommon for a company or agency to have a massive team of experts who focus their time and energy on compliance – full-time. This has also become *big* business for GRC tool vendors who provide big tools to help teams get their arms around this *big* problem.

Here is our idea: Perhaps you might consider focusing on a divide-and-conquer approach to security compliance. Think *small and local* in your compliance work, versus large and overarching. Just as books are divided into chapters and plays are divided into scenes and acts, perhaps you might break up your massive compliance initiatives into smaller pieces, perhaps aligned with the micro-segments and distributed workloads you are moving to cloud.

You will need to translate this idea into a proper implementation for your compliance work – and we know that not every situation will warrant this type of strategy. But we are quite certain that good opportunities will arise for you to accomplish large compliance objectives through orchestration of many smaller ones, operated locally – perhaps by your BISOs, to reach the type of completeness that is required by most auditors and assessors.

IDEA 2: CROWDSOURCE YOUR SECURITY TESTING

The most familiar and canonical unit of cyber defense has always been testing. This began with early security functional tests for operating systems ("Does the system generate logs for this event or that?"), and has evolved to include expert penetration testing performed by well-meaning hackers ("We gained access to your payment processing system and here's how we did it!"). Testing remains an essential component of every enterprise security program.

One area, however, where you might not be taking enough advantage of the available benefit involves crowdsourcing portions of your test activity. Evolved from early bug bounty programs, modern crowdsourcing provides a diverse perspective on your vulnerabilities, and can be quite cost-effective. Sufficient commercial support exists today for this function that it seems inexcusable to not be taking advantage of this control.

The foundation justification is that a diversity of techniques, tactics, backgrounds, expertise levels, and motivations will help uncover unforeseen exploitable vulnerabilities in your infrastructure. It's been our experience as analysts and consultants that every team that has engaged in such crowdsourcing finds something critical that requires fixing. It might be a good idea in 2021 to fill this hole in your program, if it exists.

IDEA 3: SIMPLIFY YOUR SECURITY DASHBOARD

One disadvantage to serving as a TAG Cyber consultant to senior executive teams and corporate boards is the massive onslaught of dashboards one becomes subjected to. Every company seems to have dozens of dashboards for reporting data to leadership, and the design goal appears to be 100% coverage of every square inch on the PowerPoint screen. Unused real estate on the screen seems almost illegal.

Our idea is that perhaps this approach is wrong – and while we cannot comment intelligently on areas such as real estate, human resources, and finance, we can comment on enterprise cyber security. And we can report that the dashboards being used are too complex. This might result from commercial dashboard vendors competing based on reporting features, or it could stem from CISOs wanting to maintain dashboard parity with their peers.

That said, we strongly recommend simplifying your enterprise security dashboard in 2021. Find the three or four main points that you'd like to make and focus on these in your reporting. And yes – we truly mean *three or four* main points.

Why the hell is this Google Mesh Wi-Fi not working?
The answer to Your Question is "42"
Powell/Amoroso

This might involve recruiting, or it might involve security analytics, or it might involve compliance. But remember: For your dashboard, keep it simple. Simplify your dashboard.

IDEA 4: EXPOSE COMPLEXITY TO EXECUTIVES

The biggest mistake we see on a day-to-day basis in the communications between CISOs and other executives is the over-simplification used to convey security concepts to non-security leaders. In the best case, this involves a bit too much baby-talk ("Security is really just people doing the right thing") and in the worst case, it involves embarrassing condescension during briefings ("A firewall is like a big door into our company").

Here is our suggestion: Though you might sometimes suspect otherwise, the truth is that senior executives and board directors really *are* intelligent people. In most cases, they have survived decades of business problems, corporate conundrums, and significant issues. They can understand complex topics – and there is no reason under the sun why cyber security issues should be no different. They do not require oversimplification.

To that end, we strongly recommend that you really let it fly during briefings in 2021. Go ahead and mention your new micro-segmented orchestration – and go ahead and reference how you use machine –learning-based tools to discover new variants – and do not hold back one iota in referencing NIST 8000-53 rev 5 (let 'em look it up). The result is that executives will come to respect the complexity of what we do for a living – and this will be good for your budget.

IDEA 5: EXPAND YOUR SECURITY INTERNSHIPS

It is commonly reported (including from the ad board on the C-Train to Brooklyn) that a skills shortage exists in cyber security. While it is tempting to reject such commentary as marketing for retained search or excuses from failed CISOs, we must grudgingly agree that the claim is mostly true. It has in fact been quite difficult for enterprise security teams to find good talent in cyber security, especially for technical positions.

To that end, we would like to remind enterprise and government teams that young people studying computer science at the university level are like sponges when exposed to good technology from capable mentors. We thus recommend that you consider increasing the intensity, scale, coverage, and investment in your internship program in 2021. This is especially true for larger companies with more leeway in their budget.

But please do not place these interns in virtual cubicles doing busy work. Challenge them to solve real problems. Have them simplify that dashboard we referenced earlier in this article. Have them prototype cloud workload compliance tools we also mentioned above. When we give interns bad jobs, they get the wrong idea about what we do. Use 2021 to put real creative energy into your internship program – and you will help us all.

WHAT IS LEADERSHIP?

KATIE TEITLER

Leadership. It's a misunderstood word. In corporations all over the world, people use the term to connote a certain job title, like "CISO" or "CTO" or "CEO." We see it all over company websites: About Us: Leadership Team.

But the anointment of a title does not equal leadership. In truth, one of the main problems with the word "leadership" is that it implies a certain set of skills or personal attributes, yet I would bet everyone reading this short rant knows of some person who has risen through the ranks to a "leadership" position without the possession of any leadership skills whatsoever. After nearly three decades as a codified discipline, cyber security practitioners still talk about how CISOs typically come into the role—that is, some very technically skilled practitioner takes on more and more responsibility until he/she/they are the security expert in the company. As the resident expert, they are promoted to a VP or C-level position and are deemed a "leader," someone who may even have a proverbial "seat at the table," who reports into boards, and has numbers of employees working for them.

Too often, though, these same people have received no leadership, never mind basic management, training. Their acquired—and very valuable skills—are focused on security and technology. But the lack of experience with and training in leadership can be detrimental to the organization.

Cyber security is a business risk. Straight up, no chaser. It has become a critical business risk which can impact the productivity of entire organizations, jeopardize people's identities, and cost companies significant ARR. In more extreme situations, cyber security risk threatens lives.

This is not meant to be hyperbolic, but we are seeing in real life how lack of leadership costs lives.

While people are not dying every day from a data breach of PII, the impacts of such a breach are significant. At present. we're watching a former CISO face potential jailtime and half a million dollars in fines for allegedly covering up a breach and failing to report the breach properly. This is not playtime.

We need leaders who can make tough calls when a security incident is in question, but who can execute with humility and respect.

And as such, we need leaders in security. We need people who are more than technicians. One hundred percent we need experts who can reverse engineer malware, analyze packets, and properly implement encryption/access controls/pick-your-functional-area-of-interest. But we need leaders who learn, understand, and practice communication skills. We need leaders who learn, understand, and practice empathy. We need leaders who do what's right rather than what's popular or that which gains them speaking invitations. We need leaders who can make tough calls when a security incident is in question, but who can execute with humility and respect.

These are the so-called "soft skills," yet I posit that this is a misnomer. These "soft skills" are, in fact, extremely hard to acquire. And it takes training and practice and the ability to look outside oneself. A true leader isn't someone who seeks glory and tries to be a hero. How far will that get you in the aftermath of a breach? A true leader doesn't conceal information to save face, because they're afraid of repercussions, or because they want to orchestrate the response at a personal level rather than doing what's right.

Being a leader is hard work, and in security, covering up information or holding back information about vulnerabilities or exploits has substantive impacts on people's lives. Perhaps not in the same way as Covid-19, but without a doubt cyber breaches of confidentiality, availability, and integrity have downstream effects on people's abilities to work, earn money, obtain credit to rent or buy a home, take out a loan to attend college, and many other real-life situations.

So if you're a CISO or want to be a CISO, I implore you to work just as hard on becoming a better listener, better communicator, and better conduit for empowering those around you. These are just some of the attributes that make the best leaders—and we have some great examples in the security community! But do not, for one second, think that a title makes you a leader. Your actions can harm people and threaten their livelihood; it is leaders' responsibilities to be truthful and to make difficult decisions, but do it with an understanding that the role is in service of a larger picture—one that dwarfs whether you left your RDP exposed to the internet or didn't encrypt your customers' credit card information.

THE INDEX OF CYBERSECURITY

MATTHEW AMOROSO

What does it mean to "measure" something in cyber security? Well, if you really want to know, I would suggest you pick up a copy of "How to Measure Anything in Cybersecurity Risk," written by Douglas W. Hubbard and Richard Seiersen.[1] Inside you will find a foreword written by Dan Geer, who, as many of you may know, also has some things to say about measuring risk. Coincidentally, Dan is also the subject of our discussion here.

Back in 2011, Geer teamed up with Mukul Pareek, current SVP – Technology Control Modeling and Analytics, at Wells Fargo. The pair set out to create an index that measures the state of the cyber security industry. They collected data by surveying a number of experts in the field each month and applying those numbers to an ongoing index.

Many of you reading this may be skeptical about the possibility of an all-telling index giving you a sense of where we're at as a community just from a glance. I don't blame you. It was my first reaction as well. However, I implore you to, for just a moment, put aside the cynicism that makes you all such good security practitioners in the first place and imagine how nice it would be if we did have such an index.

In 2019, the project became the inspiration for a course taught at NYU, where a group of graduate students began to analyze the historical data more closely and determine what, if anything, we could learn from the index. As a previous member of this group of students, the course concluded that the index in its current state was not measuring the state of our industry.

We matched the chart up against significant security events such as the Equifax and Target breaches. Unfortunately, the chart did not show any meaningful representation, or prediction of events such as these. While this in and of itself does not prove or disprove anything about the index, it also makes a compelling argument that the index is not entirely useful. Upon further inspection of the data and inner workings of the index however, we noticed that maybe we were looking at the wrong chart altogether.

Everyone, and I mean everyone, in this industry is apparently incredibly pessimistic.

The chart is based on the survey that is filled out by experts each month, where questions are answered on, essentially, a 1-5 scale and weighted to have equal pressure. When you look at only this data, before it is turned into a chart, it becomes very clear what was bogging down our chart's accuracy.

Everyone, and I mean everyone, in this industry is apparently incredibly pessimistic. Participants were significantly more likely to say a given area of security has "gotten worse" or "gotten much worse" than they were to say anything has gotten better. This meant that our index as it was was flawed, since it gave every answer the same weight and power over our chart. Due to this, it was impossible for our chart to ever say anything has really gotten better since the default feeling from experts was on the negative side of neutral.

Once we readjusted the weights in the data, the chart suddenly took shape. We tried again, matching the data against historical events, and wouldn't you know it, we actually got some matches.

Since this course in 2019, TAG Cyber has teamed up with NYU, Dan, and Mukul to reinvigorate the project and push it to new heights. Currently, an internal team at TAG Cyber, led by Andy McCool – EVP Cyber Security Analytics, is overseeing the creation of a brand new website and operational process for the index. It is our hope that at some point in 2021 we will be launching a brand new home for the index with a shiny coat of paint and some fancy new functionality.

Currently, you can view the historical index at **wp.nyu.edu** or if you just google "NYU CCS Index" you should see it.

If you are interested in becoming a participant in the monthly survey, please reach out to us! You can do so by sending an email to: **contactus@tag-cyber.com**

[1] https://www.amazon.com/How-Measure-Anything-Cybersecurity-Risk-ebook/dp/B01J4XYM16

ACME
SMART
MIRROR
Send us 10 bitCoin Now or we will Post an image of Your Body on Facebook.
Powell/Amoroso

THE UBER DATA BREACH AND ITS IMPLICATIONS FOR THE CISO

KATIE TEITLER

Businesses and individuals in charge of cyber security, especially, have an obligation, a legal one, to protect data assets.

As the criminal charges against former Uber CISO, Joe Sullivan, hit mainstream media, there is, understandably, a sense of outrage among the security community, with some voices defending the position of CISO and some siding with the prosecution, based on the published details of the case. I've seen the barrage of social media posts decrying why it's unfair for Sullivan to potentially be facing jail time. The arguments range from, "security is hard," to "there's no way he was the only one who knew about the breach but he might have been scared to go against his superiors," to "what does this mean for future breaches?" On the other side of the argument, people seem relieved: "I'm glad the private sector is holding the integrity thing down," and, "If you do what Joe Sullivan was indicted for and conceal incident info, even at the behest of your superiors, you not only destroy your career, you destroy the ability of your employer to use insurance resources to help resolve it."

As an analyst who speaks with enterprise CISOs daily, I can tell you that 1. security practitioners are scared for their careers, but 2. security practitioners on the end user side are more likely to be condemning of Sullivan's actions than those who consider themselves part of the hacker community.

Let's dive in and look at what happened before we get to personal commentary: The attack against Uber happened in November 2016. Compromised data included the names, email addresses, and phone numbers of approximately 50 million riders, and the personal information of approximately 7 million drivers, along with driver's license information of about 600,000 U.S. drivers. This information was readily reported among the press, but only after a new CEO stepped in in 2017 and took responsibility for the breach; that's when Sullivan was fired. At the time of the breach, one year before it was exposed, Uber chose to cover up the incident, all the while negotiating with U.S. federal regulators on separate claims over non-compliance with data security disclosures and the handling of consumer data. Based on this information, one can assume that a culture of irresponsibility toward the security and privacy of customer and employee data was knit into the fabric of the company under previous management.

The breach wasn't an isolated incident and Sullivan wasn't the only one to know about it. Not a chance.

DUTY TO PROTECT

This is all bad enough: Businesses and individuals in charge of cyber security, especially, have an obligation, a legal one, to protect data assets. It could be argued that security practitioners also have a moral and ethical obligation as well—but that's much, much more subjective. Opinions aside, the job of security practitioners is asset protection. Practitioners are obligated to take due care and must be able to demonstrate reasonable implementation of measures that protect their employers' systems—even third-party systems like GitHub on which data is stored—networks, data, and applications. There are myriad laws and regulations requiring due care. Does this mean breaches won't happen? Of course not. Does it mean security executives won't be fired when a largescale breach does happen? No. Is that right? That's debatable.

The case against Sullivan isn't about whether a breach happened under his watch. That shouldn't be the subject of debate on this topic.

The facts are this: Uber was breached. In 2017 when Kalanick was ousted and a new CISO was hired, the new CEO was told about the breach (again, flying in the face of the argument that anyone other than Kalanick and Sullivan knew about it), and Sullivan was fired. An investigation was instigated, and it was discovered that in efforts to "contain" the breach, Sullivan paid the attackers after they approached Uber saying they had illegally accessed the GitHub repository used by Uber engineers. They claimed to have found AWS credentials and used them to access private data (which should have been encrypted, but, technicalities…) on Uber's AWS cloud.

FAILURE TO REPORT AND AN ATTEMPT AT A COVER UP

So far, this is typical attacker fare. Getting attacked may be embarrassing, but Uber would have been far from the first or worst to suffer a breach like this. Why, then, the controversy? Instead of declaring a breach, as required by law, Sullivan paid the attackers—allegedly after they contacted Uber saying they had access to a treasure trove of data. He called it a bug bounty, even though the payout was 10X larger than any known bounty paid by Uber. It would not have been illegal for Sullivan to pay the $100,000 in exchange for safe return of the data and details about the exploit (theoretically to learn from the incident and prevent future breaches), despite the exorbitant fee and despite the fact that the attackers approached Uber instead of being hired by Uber to find and/or exploit vulnerabilities.

Sullivan isn't potentially facing jail time and $500,000 in fines because of a bug bounty program. The charges against him are 1. for attempting to cover up the breach and the claw back of information by requiring the attackers to sign a non-disclosure agreement (a.k.a., a gag order) about the breach, and 2. for obstruction of justice; he failed to report the breach to the proper authorities, including the 57 million people whose records had been breached.

WHO'S RESPONSIBLE FOR WHAT?

Reasonably, the security community is crying foul here: Is the CISO personally obligated or even empowered to report a breach to the public or law enforcement? Possibly not. Does the CISO have an obligation to inform company executives? 100%. Absolutely. The head of Uber's legal team at the time said she wasn't informed of the extent of the breach. Possible? Yes. Unlikely? Well, considering that the company was already under legal scrutiny for associated data handling matters…sounds like willful negligence. Is the speculation? Yep. But if that's the case, how did Uber's Board of Directors have enough suspicion to hire outside legal counsel to investigate, at which time the breach was discovered?

So is Sullivan a bit of a fall guy? Potentially. But he made some bad, bad decisions, likely aided and abetted by some terrible decisions by fellow executives. Based on conversations with current and former CISOs, including TAG Cyber's CEO—the former 17-year CISO of AT&T—it's unthinkable that Sullivan acted autonomously throughout the entire kerfuffle. Yet, he paid the cyber criminals, as the CISO—a position he'd held since 2010. Not his first rodeo. Even if Sullivan's actions were indisputably honest, there was a breach, he was CISO at the time. He knew the rules of the game.

AFFIRMATIVE OBLIGATION TO PROTECT AND NOTIFY

The moral of this story, then, is this: The job of a CISO is a big one: it's stressful, it's time-consuming, it's hard. CISOs are responsible for everything that happens on their team, which means they are ultimately answerable for the entirety of the security team's actions—even if a mistake was made at the sysadmin level. That's the job. Anyone who accepts a job as CISO yet thinks they're abdicated of responsibility when there's a compromise of the assets they're obligated to protect is not suited to the role. Individuals who want to take on the title and (considerable) pay of a CISO but don't want the responsibility should probably continue to dream about riding a unicorn bounding through poppy fields in The Land of Oz.

Treat every incident like your job depends on it, because it does.

Cyber security is a business-critical risk. Over the last 30 years (yes, 30) security practitioners have fought to earn a seat at the table. They have fought to be taken seriously. They have fought for the handsome compensation by arguing all the intricacies and difficulties and pressures of defending an entire enterprise while attackers need identify just one, small vulnerability. And it's all true! Why, then, would anyone who has fought this hard think it's OK for a CISO to conceal a breach by forcing criminals into non-disclosure and blatantly disregarding legal mandates? Were Sullivan's hands tied by his internal organization? Maybe to an extent. But it's time to grow up and accept the job or look for another one where the stakes aren't so high.

WHERE DO WE GO FROM HERE?

In the meantime, any security practitioner who feels they are being put in an untenable position or are being ignored when they are trying to do the right thing by reporting a security incident—and goodness knows corporations can make it hard on individuals who are perceived as bucking the system—the advice is this: always create an audit trail. Document, document, document. If the CEO/legal team/HR team/risk team etc. is not taking your advice seriously, if they ignore your guidance or dismiss your concerns, put it in writing. Formally submit your concerns. Treat every incident like your job depends on it, because it does. Can you still be fired? Yes. Can you get another job? Yes. If you've done your job with honesty and integrity, a good future employer will see that. If you've covered your tracks and cross the line into criminality, you could also be personally facing federal charges. Don't be that person.

And for goodness sake, implement security measures to restrict access to systems and data, architect for zero trust, continuously monitor, review configurations, conduct regular testing, inventory your assets, encrypt, and just generally harden security controls across your environments. Do these things before a beach. Practice good cyber security hygiene. A breach might still occur under your watch, but at least you'll know you put honest effort into the job and will be able to demonstrate due care when the time comes.

CYBER CORPS GRADUATES TO ENTERPRISE SOLUTION

SHAWN HOPKINS

TAG Cyber Corps small business threat and vulnerability reporting solution is now being requested by large enterprises to manage their 3rd party supply chains. The program started two years ago with the intent of providing internship opportunities to university students while supplying much needed cyber security information to the small business community. With the expansion of student participation and technology improvements, the service is ready for larger deployments.

The educational aspect of the program revolves around real-world business scenarios that are common cyber security decisions made every day.

The primary customer of Cyber Corps is the small business owner using a combination of cloud services as their network. The service is a customizable security information portal which provides monthly threat intelligence on the business's internet assets. Research interns provide information on the latest OS versions, recorded vulnerabilities, attack vectors, and business news for each cloud service being used. Additionally, domain adjacency review is performed on all registered adjacent domains similar to those of the customer. Any suspicious domain is reported to bring awareness to the customer and help protect their reputation.

Domain accessibility is another area of concern, and it usually gets overlooked by a small business that does not have the resources to fully monitor their network. Continuous monitoring of configured URLs report and alert the business when there is an outage and the duration. Finally, Cyber Corps provides security tips to the business to help with awareness and education of its employees.

The Cyber Corps workforce is primarily university interns. Through a grant partnership between TAG Cyber and universities, students interested in cyber security are paid for their research that populates the information portal. The twelve-month internship is a part-time, remote work/learning environment. Interns spend approximately ten hours per month on the program. Forty percent of students' time is paid research, with the remaining hours spent on course work and lectures. The educational aspect of the program revolves around real-world business scenarios that are common cyber security decisions made every day. Successful completion of the internship provides the student with one year of experience as a security researcher along with 2 course credits towards their university degree. University partners adopt Cyber Corps to augment an existing concentration in cyber security or to start a program where none exists. TAG Cyber is committed to attracting young talent to cyber security and addressing the skilled worker shortage.

WHAT'S NEW

This past year has brought about major changes in the service. In March 2020, TAG Cyber launched our personal online security information portal for each customer. This allows for 24-hour access to alerts and reporting as soon as the information is updated. The intern pool has expanded to a greater number of universities and students. Now, a cohort of 5 students from each institution is engaged all at once under a grant given to the university from TAG Cyber. This structure creates a more cohesive learning environment and a built-in support system for the students involved.

The latest adoption of the portal service is for large enterprises looking for a simple, effective solution to manage 3rd party vendors or satellite franchise offices. Typically, tier 2 and lower suppliers do not handle sensitive or personal information but still pose a cyber risk. A large majority of these vendors do not have a dedicated security team to properly monitor their network, let alone answer technical questions standard on cyber security surveys. As a result, the enterprise is stuck with governance over the supply chain but without a way to monitor or audit the integrity of its suppliers. This is the gap that Cyber Corps is addressing. It is also bringing awareness to external vulnerabilities to which large enterprises are subject but which might not be readily apparent.

Metrics and reporting

When an enterprise requires its supply chain to subscribe to the Cyber Corps service, aggregate metrics are relayed back to their security team. Knowing which vendors are receiving monthly threat intelligence regarding their own environment allows the enterprise to ensure that suppliers are aware of the cyber threats and attack vectors facing their systems. As such, Cyber Corps lowers threats to the larger entity (as well as the supplier) via relevant information and potential threat mitigation solutions.

For the first time, the enterprise will also gain visibility into the aggregate threat from cloud services their suppliers or satellite offices consume. For instance, if a number of the enterprise's suppliers are using a questionable cloud service, Cyber Corps provides visibility into the service, which helps them identify and potentially remediate areas of vulnerability from a previously unknown attack vector. Other relevant information shared about the collective usage of the supply chain will enable the enterprise to assist smaller companies with advice on mitigating risky usage and/or configurations; Cyber Corps gives enterprises the ability to govern monitoring and audit compliance for its small partners in a way that was previously untenable.

The Cyber Corps program is a win-win situation for all parties involved. The small business community is able to receive cost effective, simple advice for their cyber security needs. Universities and students are able to obtain real-world experience and augment cyber programs. Large enterprises have a way to monitor their 3rd party suppliers. Finally, TAG is able to advance its mission of democratizing cyber security information while also training the next generation of security professionals.

INTERVIEWS

AN INTERVIEW WITH BRETT GALLOWAY, CEO, ATTACKIQ

PERFORMANCE DATA THROUGH AUTOMATED SECURITY CONTROL TESTING

It's a blessing and curse that security practitioners have a plethora of security tools at their disposal. These robust tools all produce plentiful data that security and ops teams can slice and dice innumerable ways. But the problem is that all these tools produce plentiful data that can be sliced and diced innumerable ways. For most enterprises, more data just creates more noise; they're lacking the context and applicability that affords true understanding of the tech stack and the actions they must take to effectively protect the business from cyber threats.

We spoke with Brett Galloway, CEO at AttackIQ, about how enterprise security teams can make actionable, data-driven decisions about their deployed security controls. We focused on the challenges security teams face when trying to manage hybrid, disparate environments, where the pitfalls are, and how AttackIQ can help strengthen controls and improve business operations at scale.

TAG Cyber: The average enterprise has 75 security products deployed across environments. At first glance, this seems like a great, layered strategy, but how does it complicate security teams' abilities to identify, detect, protect, respond, and recover from incidents?

ATTACKIQ: Chief Information Security Officers (CISOs) have hundreds of regulations to meet and manage dozens of security controls from nearly as many vendors. Each of these security technologies performs a valuable function, from monitoring and detection to security segmentation, to drive down cyber security risk. A security stack of best-in-class technologies should provide an organization with defense-in-depth (as you indicate), but absent a baseline against which to align their defenses, security teams can go from one compliance responsibility to another without ever improving effectiveness, caught in a web of administrivia as teams and technologies proliferate. The result of such complexity is an increase in activity without a commensurate increase in effectiveness.

The core issue is this: while CISOs are responsible for operating a set of security controls to protect vulnerable systems, they have no inherent way to know if those controls are working. Verizon estimates that 82% of breaches should have been stopped by existing controls but weren't. Why? Security controls fail, and when they do, they fail silently. The only way to ensure effectiveness across the security stack is by actively testing your security against known threats. When you generate real performance data about your security control performance, that provides a path to minimize complexity, gain control over the security stack, and manage your teams for effectiveness.

TAG Cyber: What are enterprises missing in their current strategies that lead to compromise?

ATTACKIQ: Adversaries penetrate networks all the time. The good news is that after a decade of investment, CISOs have robust security controls in place. The question is whether those security controls are working. If they are not working, penetrations are not detected or prevented—or they are detected later than they should be—and that increases the risk to the business and the cost of remediation. Chief information security officers therefore need a means to measure the effectiveness of the valuable security controls (composed of people, processes, and technologies) that they have acquired and developed.

At AttackIQ, our Security Optimization Platform generates performance data through automated security control testing. By deploying assessments and adversary emulations against security controls at scale and in the production environment, the Security Optimization Platform emulates adversary behavior—tactics, techniques, and procedures—to determine whether your security controls are detecting and preventing attacks as intended.

With robust performance data, CISOs and security leaders can make measurable improvements in team performance. They can find ways to improve information flows and communications processes. They can quantify their security technologies' effectiveness. Armed with real insights, they can then take a strategic step back and make data-driven recommendations to the board about what to do (or not) from an investment standpoint.

TAG Cyber: AttackIQ's platform tests security controls in production. Why there? Can't that potentially disrupt operations and cause continuity problems?

ATTACKIQ: We test security controls in production because security controls fail in production. That's where the adversary operates, so that's where our testing platform needs to operate to generate real data. We have designed our software to test in production safely and at scale, and every assessment and adversary emulation we design goes through rigorous lab testing by our team before we release it into the platform to assure quality operations.

TAG Cyber: You highlight your platform's compatibility with MITRE ATT&CK®. Why the MITRE framework and not other, equally respected frameworks?

ATTACKIQ: Published in 2015, MITRE ATT&CK is an all-source, globally vetted "periodic table" of insights about adversary tactics, techniques, and behaviors. In just a few short years it has become the global standard for incorporating threat knowledge and understanding adversary behavior. The MITRE Corporation, a federally funded non-profit research and development organization working in the public interest, published the ATT&CK framework to help defenders all over the world to understand and focus on the threats that matter most. It gives the cyber security community a baseline for threat-informed analysis, and that baseline has been adopted by institutions across the globe from the U.S. Cybersecurity and Infrastructure Security Agency (CISA) to the Australian prime minister's office to critical infrastructure owners and operators all over the globe. It has led to a transformation in security effectiveness and it serves as a foundation of our strategy as a company.

Absent a baseline against which to align their defenses, security teams can go from one compliance responsibility to another without ever improving effectiveness.

TAG Cyber: What are some of the new attack behaviors that enterprises should be on the lookout for?

ATTACKIQ: Today as we are speaking, the story of the SolarWinds supply chain attack on U.S. government agencies and private companies continues to unfold as security teams work to address the risks that the malware has introduced. The first big take-away from the story is that advanced nation-state actors have the financial resources, personnel, and time to invest in novel methods of intrusion; they will constantly work to find new ways to break in. This particular intrusion reveals for all to see how they can use components in the commercial supply chain to strike at our most important organizations. We should assume that other nation-states will invest in this method going forward.

As we think about what has happened, to my mind the question is: what are some principles for organizations to adopt going forward? First, it is not a question of "if" but "when" an intruder will break past. While the methods of initial intrusion may vary—whether ransomware released through a phishing email, or a Trojan horse supply chain attack—advanced nation-state adversaries will inevitably break through at some point. Strategically, security leaders should therefore operate under the assumption of breach and plan for what will happen next.

The good news is, we know how adversaries will operate once they break in. The MITRE ATT&CK framework provides a catalogue for understanding adversaries' approaches, and in the period following the SolarWinds attack government and private sector organizations used ATT&CK to describe the intruder's behavior inside the network.

Second, we have the technologies to detect and prevent lateral movement across the network, as occurred in the case of SolarWinds, but organizations need to adopt those technologies to prevent breaches from spreading. Government agencies and private companies need to invest in advanced defensive technologies to detect attackers and prevent them from moving laterally.

Third, once best-in-class security technologies have been adopted, organizations need to exercise their defenses to make sure they work for a post-breach scenario. We should never assume that the best personnel, the best processes, and the best technologies will always work as intended. We need to adopt and then test security technologies to ensure security effectiveness.

Going forward, organizations will face a constant requirement to optimize their security controls and detection capabilities with updated indications of compromise and adversarial tactics, techniques, and procedures using ATT&CK. From our standpoint at AttackIQ, our platform provides a fully automated way to rapidly exercise security controls' detection and prevention rules—continuously validating that cyber defenses are optimally tuned to stop intruders.

Our new AI based mobile app helps you keep track of your meetings and tasks.
Great. Let's pick a time for a demo.
OK. I'LL just make a little note here.
Powell Jamotoso

AN INTERVIEW WITH LENNY ZELTSER, CISO, AXONIUS

ACCURATE SECURITY POSTURE ASSESSMENT THROUGH ASSET MANAGEMENT

When security and IT operations staff think about asset inventory, often the first thing that comes to mind is, "you cannot measure that which you cannot see." When they think about asset *management*, it's not just which assets are present, but which servers/hosts/apps/devices are talking to which others, which have vulnerabilities, applied policies, and more. Effectively, combined, inventory and control of assets is 100% about understanding the current state of asset risk so further action can be taken.

The key, then, is operationalizing asset inventory and management information. In a typical enterprise, this information is fed into third-party remediation tools. However, a different and highly valuable use case for asset intelligence is vulnerability testing—pen testing, red teaming, threat hunting, and other forms of vulnerability assessment—for the purpose of system hardening. We recently spoke with Lenny Zeltser, CISO, at Axonius about the role that cybersecurity asset management plays in today's enterprises

TAG Cyber: The idea of continuous testing is widely accepted, but the reality of it is hard. Automated vulnerability scans can fulfill the "continuous" part but can be incomplete, while pen tests and red teaming go deeper but are limited in scope. How can asset management streamline assessments?

AXONIUS: The notion of continuous security monitoring has gained prominence in security discussions because enterprises recognize the limitations of point-in-time visibility. Instead, we want ongoing validation of our security controls, and rapid notification of the relevant gaps. Vulnerability scanners and penetration tests provide some insights, but they're just one set of signals needed to assess and maintain the company's security posture.

To achieve broad, actionable insights into security gaps, organizations are turning to multiple sources of information pertaining to security posture. Our ongoing assessments should examine data from vulnerability scanners, security agent management consoles, infrastructure management tools, user identity management software, and so on. Modern asset management solutions can gather, clean, and correlate all this information, so the organizations can act on it right away, without waiting for annual or quarterly assessment checkpoints.

TAG Cyber: Asset management inventories the assets in a company's digital ecosystem, identifies vulnerabilities and coverage gaps, and validates policies. Isn't there a significant overlap with vulnerability scanning?

AXONIUS: Vulnerability scanners offer insights into many weaknesses that might need to be addressed, but they're insufficient for a broad, comprehensive view into the gaps. For example, most organizations are unable to scan all systems—be they workstations in remote offices or people's homes, or cloud workloads that exist for moments before they're decommissioned. Even knowing what to scan requires a comprehensive list of its IT assets, which has been out of reach for many enterprises.

I prefer to take a broader view at assessing security measures and identifying security gaps. I've found it useful to rely on asset management as a way of bringing together relevant details from a diverse set of data sources. Vulnerability scanning is just one of them.

> Modern asset management solutions can gather, clean, and correlate all this information, so the organizations can act on it right away, without waiting for annual or quarterly assessment checkpoints.

TAG Cyber: How are some of the new and updated cyber security regulations impacting companies' testing needs and thus more thorough, reliable asset management?

AXONIUS: Laws, regulations—and customer contracts, by the way—are placing security practices under greater scrutiny nowadays. Companies find themselves having to demonstrate the effectiveness of their security programs with a greater frequency and to a larger set of stakeholders. This is causing a shift from annual security reviews to ongoing security assessments. Achieving and demonstrating compliance on a continuous basis is too costly and impractical without comprehensive and up-to-date visibility into the state of the company's IT assets.

TAG Cyber: There are a lot of asset inventory platforms on the market. What makes some better than others?

AXONIUS: An asset management system must accommodate the rapid pace of change and the diverse nature of assets that characterizes today's business and IT practices. Organizations are finding that CMDB alone isn't sufficient anymore. Neither is network or vulnerability scanning. NAC can help, but that's not enough either.

A modern asset management system should be able to tap into multiple sources of asset data. It needs to aggregate the relevant details, normalize the data. And it should provide a convenient way of identifying changes, confirming that the right security measures are in place, and assist with automatically remediating gaps. Not all asset management systems can act as such a nexus of security and IT data flows in today's enterprises.

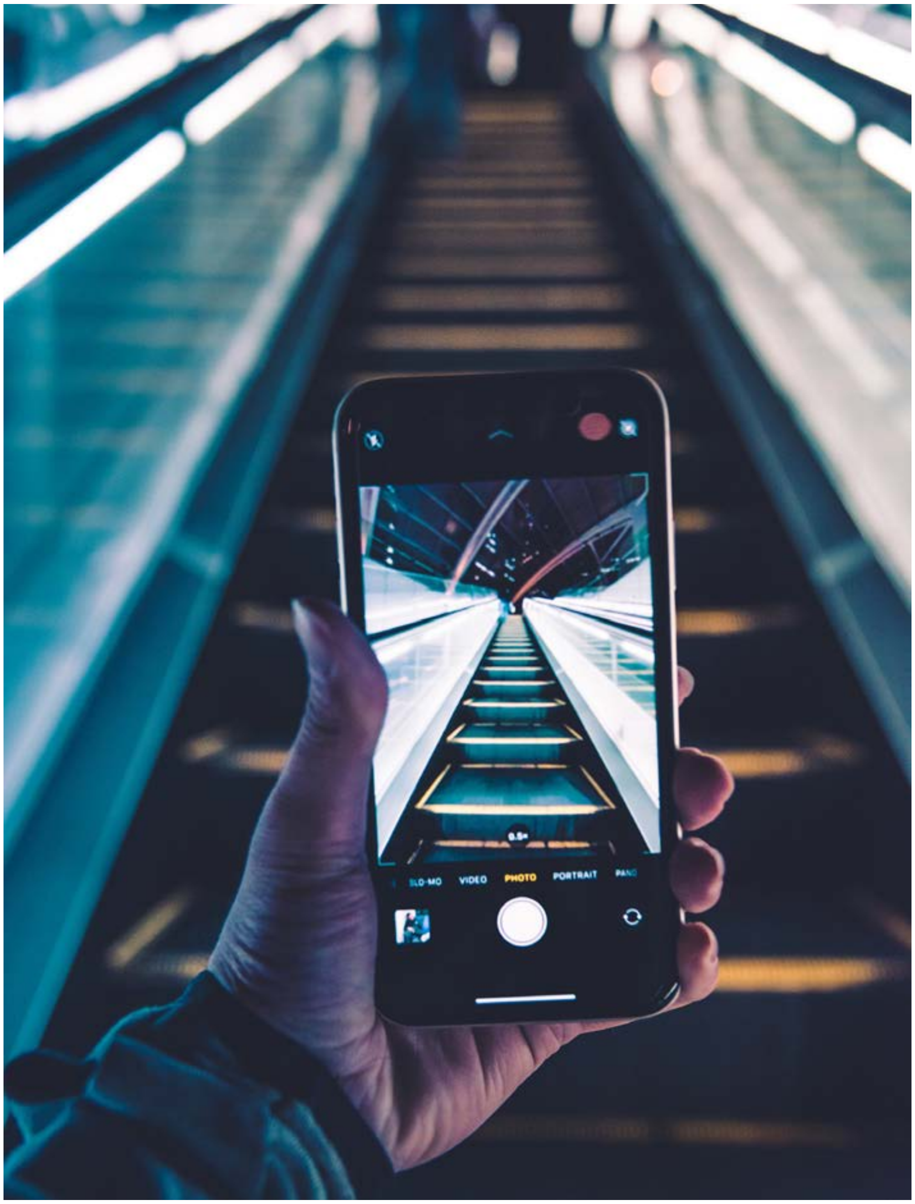
TAG Cyber: What can we expect to see from Axonius as we move through 2021?

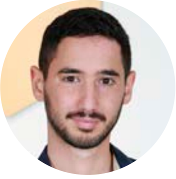
AXONIUS: Driven by customers' need for better cyber security management tools, we're growing rapidly, which increases the pace at which we can propel the industry. I caught up with our product team to ask what I can share here. They were comfortable highlighting a few things:

Axonius will continue to integrate with more and more IT data sources, normalizing and correlating the data to turn it into useful, actionable information. This will allow customers to reduce their mean time to inventory by capturing key details from a broader range of systems and applications.

Also, we will be building a wider range of response actions that our customers can automatically take when the assets (such as devices, virtual machines, and user accounts), don't meet the appropriate security criteria.

In addition, we'll be placing greater focus on aiding customers' efforts to demonstrate compliance with frameworks and standards, such as CIS Benchmarks. This will empower a broad set of stakeholders—both operations and government folks—to benefit from our asset management platform.





AN INTERVIEW WITH DOR KNAFO, CO-FOUNDER AND CEO, AXIS SECURITY

SECURE REMOTE ACCESS FOR THE ENTERPRISE

Over the past several years, the security industry has seen a shift in focus within the control plane, that is, moving away from the network layer and up to the application layer. The reasons are these: networks are big, vast, and ever changing. Most companies use hybrid environments, consisting of on-prem, cloud, multi-cloud, virtual, and containers. And modern networks are not static places. While networks remain vital in the security equation, it's applications that have become the critical resources upon which businesses depend. And they're where all the sensitive data and information reside.

As a result, enterprises are realizing the need for application-centric security, with strict access controls at the center. Axis Security was founded to help companies bridge the gap between users and private applications. We spoke with Dor Knafo, co-founder and CEO at Axis Security, about the state of application security and the modern enterprise.

TAG Cyber: Dor, what is the main problem Axis is trying to solve?

AXIS: We are solving the problem of secure remote access for the enterprise. The challenge of providing secure access is not specific to any one industry, rather it is a key capability for any organization that relies on remote employees and numerous third parties to support their daily operation. In the current environment, this is not a "nice to have" capability; it is foundational to business continuity.

If we learned anything in enterprise IT this year, it is that VPNs are not the future of enterprise access. IT and security teams require a more secure and scalable approach, and employees and partners would certainly welcome a better user experience. This is the problem that Axis is solving today.

TAG Cyber: What do you mean when you say, "agentless-first" approach to application access?

AXIS: Our agentless first approach means that we are about simplicity for customers. We offer a path for them to immediately transform their access solution. Agentless-first eliminates the need to make network changes or add agents to endpoints. It is the quickest, easiest way to deploy secure remote access. The best use cases for agentless secure access are third-party supply chain partners, vendors, contractors, and remote employees while addressing insider risks.

There are, however, some use cases that require an agent, and Axis provides that as well. These include access to custom apps, specialized platforms, TCP, or UDP apps, even VOIP. Secure access to SaaS apps and access to locallyhosted thick client apps are the other primary use cases that require agents.

TAG Cyber: We saw a wholesale shift to work from home in 2020, and an uptick in cloud migration, both of which necessitated better access controls to applications. What trends are you seeing now, at the start of 2021? What has changed, if anything?

AXIS: From the standpoint of enterprise access, everything has changed. In early 2019, before we had written a line of code, we met with nearly 50 CIO/CISOs to discuss the problem of remote enterprise access. The stories we heard were remarkably similar.

Across the board, regardless of industry, these executives realized that current VPN infrastructure was a struggle to maintain, that it was not a great user experience, and it was risky to bring people onto the network. Despite knowing this, not one had the appetite or desire to rip and replace. The message was clear: VPNs were considered "good enough" and other priorities were considered more important.

Not anymore. When COVID-19 hit and suddenly every employee required remote access and the weaknesses of legacy approaches became too big to ignore. They were difficult to deploy and scale, requiring new hardware and licensing. Businesses were forced to ration access, the last thing any IT leader ever wants to do. It is the opposite of what digital transformation is supposed to be about.

The move away from VPNs is a massive, multi-year shift that we believe began in earnest in 2020, out of necessity. In its place, we are seeing the emergence of zero trust access solutions.

Businesses were forced to ration access, the last thing any IT leader ever wants to do. It is the opposite of what digital transformation is supposed to be about.

TAG Cyber: Axis is a relative newcomer to the scene and bigger players are in the zero trust application access space. What are some of the advantages you and your team can offer to enterprises?

AXIS: Number one is focus. We are all about delivering secure remote access to enterprise applications, that's it. Number two, Axis is easy to deploy, manage, and scale. Axis Application Access Cloud is a true zero trust access platform that delivers immediate ROI along with a significant reduction of risk for the organization.

As an agentless solution, we are operational in minutes, eliminating time-consuming network changes, the need to deploy agents on endpoints, and concerns over use of personal devices.

Axis' Application Isolation Technology keeps users separate from the network and the application, greatly reducing the threat surface and eliminating the possibility of a potentially hostile partner/user from gaining access to other network systems. Continuous security monitoring is a critical component of any zero trust solution, and Axis Adaptive Access Technology continuously assesses risk and restricts access. Every user request validated, authenticated, and based on that individual's policy settings. Users are no longer free to roam the network. Axis is delivering an application level solution—policy, visibility, and control. All users, insiders and outsiders, are treated the same with zero trust.

We believe that this approach is the future of enterprise access.

TAG Cyber: A lot of companies are still reliant on VPNs. What's the benefit, and how hard is it, to move toward a new control like Axis?

AXIS: The benefit of moving to Axis is a more secure, scalable platform with zero trust access for all, employees and third parties alike. Our original use cases were focused on third-party access and M&A scenarios. Both required rapid onboarding of new users so we designed an agentless, cloud-based platform that requires no network changes or any deployment of agents on endpoints. As it turns out, enabling access on any device, from any location in minutes is a great capability to have when all employees suddenly require remote application access.

Beyond the rapid deployment is a commitment to zero trust access. The Application Access Cloud sits between users, the network, and the applications, greatly reducing the threat surface. Unlike VPNs which have a binary authorization decision when the user first tries to access the application, Axis Adaptive Access Technology continuously assesses risk and restricts access. Every user request is validated, authenticated, and based on that individual's policy settings. A centralized application and user-focused management console gives tremendous insights to customers.

Employees, third parties, contractors—everyone is treated the same with zero trust. The benefits are immediate, with a scalable, secure platform for zero trust access that delivers a better end user experience at a lower cost than maintaining a legacy VPN infrastructure.

AN INTERVIEW WITH CARSON SWEET, CO-FOUNDER AND CEO, CLOUDPASSAGE

SECURING THE CLOUD CONTROL PLANE

Businesses have been steadily adopting cloud over the past decade. For enterprise security teams, the idea of outsourcing any amount of security control is a scary prospect. As providers' security postures have improved, and even become best-in-industry, in some cases, enterprises have grown more comfortable working inside others' environments. However, the shared security model can still be tricky; there is no one-size-fits-all; requirements change between SaaS, IaaS, and PaaS; and no one but the enterprise can determine which data and applications are most sensitive and in need of the strongest protection.

If this weren't enough, visibility into cloud providers' environments have been a challenge. Yet, companies remain obligated to know what's going on in their cloud instances, how secure their data and apps are, and the current state of compliance at all times. We spoke with Carson Sweet, co-founder and CEO at CloudPassage, about cloud security and compliance and why the ability to streamline across workflows is imperative.

TAG Cyber: We've seen steady migration to the cloud over the last decade, but the last year has had more rapid adoption than any other period, due to work-from-home. What challenges are enterprises up against when migrating to cloud so quickly?

CLOUDPASSAGE: With this shift to work-from-home, you have more people sharing data and using applications outside the safety of the corporate data center. Many security teams have had to rethink their strategy overnight. So I think the biggest challenge is just the pace of change coupled with an overreliance on legacy security tools and strategies that don't keep up.

The faster a company moves to the cloud, and the more resources they use, the less likely IT security is able to keep track of what's even out there, let alone know how secure it is. Not without the right tools and automation strategies. Automated cloud security posture management tools can help alleviate some of the struggle and help security teams wrap their heads around what's happening to their environments so they can regroup and strategize. Because, as we've seen in the past, once a company moves to the cloud, they're not going back. It's only going to grow bigger, faster, from here on out.

TAG Cyber: Why do you think the shared security model remains difficult for enterprises?

CLOUDPASSAGE: There's a lot of nuance to the shared security model. That line between "who owns what" is a little different for each cloud provider and even every product they offer. Assumptions get made. And while service level agreements might be similar between cloud providers, assumptions of like-for-like protection

The vast majority of the time, cloud security issues are due to misconfiguration. That's why it's important to have automated cloud inventory and configuration assessments that automatically scale.

aren't always valid. And then there's the introduction of the cloud control plane. The vast majority of the time, cloud security issues are due to misconfiguration. That's why it's important to have automated cloud inventory and configuration assessments that automatically scale with new cloud resources. Having the right security controls in play helps cover those blind spots, eliminate assumptions, and provide a clear picture of not just what's in your cloud environment, but whether it's properly configured based on the best practices for the specific cloud vendor.

TAG Cyber: Halo, your flagship product, is classified as a unified cloud security and compliance platform What does that mean practically, and how does the category benefit enterprise users?

CLOUDPASSAGE: Unified cloud security means we secure all of your cloud assets—servers, containers, and cloud infrastructure services and resources—using a single platform. Halo provides a unified view of assets, vulnerabilities, exposures, compliance, threat indicators—basically the overall cloud security posture in a single view. In addition, we automate not only the discovery, inventory, and monitoring process, but deliver results from our analytics engine directly into the tools and workflows that operations and DevOps teams use, along with remediation advice so that issues can be resolved in a timely fashion. And all of this is unified across all your cloud service providers. It's the same platform, policies, rules, API, and micro-agents, no matter where you're running.

TAG Cyber: How does DevOps create obstacles in security and compliance?

CLOUDPASSAGE: To be fair, I think security teams inadvertently create as many obstacles for DevOps as the inverse. Both sides of the discussion need to accept that fast, secure delivery is the new reality. It's the world that our enterprises compete in now; security can't be a bottleneck to speed, and speed can't exist at the cost of security. The old adage is, "you can be fast, or you can be secure." We need to wipe that away. In a DevOps environment, you need to be both.

Security needs to be an integral part of the DevOps process, and it needs to work in a way that's natural to the CI/CD deployment cycle. The idea of shifting left is that you get potential vulnerabilities and security issues in front of the developers as early as possible. When those issues get fixed during the initial build, you end up with compliance, secure code, and DevOps becomes a force multiplier for security.

TAG Cyber: Security and privacy compliance mandates are continually increasing. What should be enterprises' top concerns, for established regulations or new ones that are forthcoming?

CLOUDPASSAGE: They need to keep up. That's a full-time job for a team of people. Continuous compliance is critically important for any organization with compliance concerns. And let's face it—that's every organization now. With an automated tool like Halo, that process of keeping up with new mandates happens much more organically.

Here at CloudPassage, we have an excellent security research team that keeps abreast of new regulations, CVEs, and breaches, and works very hard at setting up the policies and rules within Halo to check our customers' environments for compliance. While it's important for any security team to stay abreast of changing regulations, we maintain and regularly update our libraries of policies and rules as mandates change. We can then alert security and DevOps teams of new findings as they arise, so if someone misses an update, the tool will let them know. That saves the company from those last-minute fire drills before the audit that chew up valuable development time. And that's what we mean by continuous compliance. Your team can fix issues before they become security events or audit failings. It just makes everyone's job a little easier, and gives them some breathing room without sacrificing security, compliance, or delivery schedules.

How do I detect fake news?
If something makes perfect sense to you, then it's fake.
That makes perfect sense to me.
Powell/Amoroso

AN INTERVIEW WITH KAILASH AMBWANI, CEO, CONSTELLA INTELLIGENCE

ENHANCING THE ABILITY TO INVESTIGATE CYBER CRIME

Phishing attacks, especially those that result in stolen credentials and personally identifiable information (PII), are often cited as the initial attack vector that allows threat actors to infiltrate networks, commit fraud, and successfully execute a breach. Thus, many security solutions are built to protect the endpoints at which sensitive information can be obtained. These solutions are necessary.

Just as necessary, however, are methods to unearth stolen or leaked credentials after at attack has occurred. It's naïve to believe that security teams and tools can prevent all attacks, therefore, finding the tidbits that allow security teams to track down stolen or leaked information, and the threat actors perpetrating such attacks, is an important element in restoring defenses and avoiding future attacks.

Constella Intelligence helps enterprises make compromised data obsolete by providing data and adversary intelligence. We spoke with Kailash Ambwani, CEO at Constella Intelligence about this next-gen threat intelligence space and how businesses can use it to combat cyber crime.

TAG Cyber: Most threat intelligence is broader based than adversary and data intelligence. Why did Constella choose to home in on this area? What is the scope of the problem for enterprises?

CONSTELLA INTELLIGENCE: Conducting complex investigations can be arduous due to the evasive tactics of adversaries. Our platforms allow investigators to explore and analyze breach datasets to focus investigations instead of searching for a needle in a haystack. We have spent years verifying and curating billions of identity records and relevant intelligence so that organizations can increase effectiveness and unmask identities of adversaries.

TAG Cyber: What can adversary intelligence provide that traditional threat intelligence can't?

CONSTELLA INTELLIGENCE: Constella products enhance investigations of financial crimes, cyber crimes, human smuggling and trafficking, and transnational gang activity. Our investigative platform leverages over 25 billion deduplicated and curated identity records that contain over 100 billion attributes with 16 million identified malicious actors and over 9 billion validated passwords. This data is collected from deep/dark web and black markets; surface web and data spills; hacker and malicious forums; cryptocurrency transactions and passive DNS; and automated crawling of public and private websites. This intelligence can expose hidden activities and real identities of malicious actors to reveal intent and activity.

By unmasking cyber criminals, organizations can take action to know the adversary and prevent future attacks and exploitations instead of playing whack-a-mole.

TAG Cyber: What identity-based attack trends have you seen in the last year?

CONSTELLA INTELLIGENCE: Constella continues to observe a returning trend of big company breaches like Twitter, Google, and the SolarWinds supply chain attack. Threat actors, organized crime, and nation-sponsored attacks around the world have resulted in a continued surge of stolen data being sold on the black market. This information includes personally identifiable information (PII), such as email addresses, full names, birthdates, phone numbers, IP addresses, social media IDs and profiles, driver information, relationship status, and more. Constella monitors the surface, social, deep, and dark web to detect exposed credentials and stolen data and help consumers and companies manage the risk.

TAG Cyber: Why is adversary attribution important? Some people argue that it's too hard and, in the end, not all that useful in preventing attacks.

CONSTELLA INTELLIGENCE: Conducting complex cyber crime investigations is difficult mainly due to multiple layers of purposeful misdirection created by threat actors. Pseudo names, anonymity tools, cryptocurrencies, and other evasive tactics make identity attribution difficult and time consuming.

Breach data provides context to threat actors, revealing their real identities, cohorts, and criminal rings by following digital footprints to solve cases faster and more accurately than ever before. By unmasking cyber criminals, organizations can take action to know the adversary and prevent future attacks and exploitations instead of playing whack-a-mole.

TAG Cyber: Constella Intelligence just raised a round of capital. Congratulations! How will you use that funding to build out your product suite and help intelligence analysts and investigators get better at their jobs?

CONSTELLA INTELLIGENCE: This funding will allow us to invest in additional capabilities to help our customers better address the rising tide of digital risks to their businesses and employees. This month we're excited to announce an upgrade to one of our existing products. Hunter, which builds upon the product formerly known as IDHunt Core, provides a better user experience and new features specifically requested by customers to speed investigations of threat actors. We look forward to empowering those on the cyber frontlines with better anticipation of emerging threats, proactive analysis, and adversary identification — so they can act before any harm is inflicted.

AN INTERVIEW WITH ALAN SALDICH, CMO, CORELIGHT

IDENTIFYING THE RIGHT DATA FOR INCIDENT RESPONSE AND THREAT HUNTING

It had been said that the network is the "ground truth" of an organization's security posture. Analysis of what is communicating on the network will tell the security team what is needs to know about normal operations, expected patterns, and therefore which communications and behaviors indicate anomalies. However, "network" today means something very different than it did 20 years ago, and security and operations teams must approach gaining network visibility with fresh eyes.

Corelight, a network detection and response (NDR) vendor out of San Francisco, was born out of the popular open source network monitoring tool Zeek. Built on Zeek, and also integrated with Suricata, an open source intrusion detection engine, Corelight Sensors allow enterprises to collect comprehensive insight about their networks and stream it to SIEMS so analysts can respond more efficiently to alerts and also proactively hunt for threats. We spoke with Alan Saldich, CMO at Corelight, about how they are helping SOC operators and threat hunters become better defenders.

TAG Cyber: Many commercial products tout their ability to gain holistic network visibility. Why would an enterprise use a separate tool like Corelight for visibility?

CORELIGHT: Corelight is purpose-built for security operations, not a force-fit of a network performance monitoring (NPM) product applied to security challenges. Unlike most network visibility tools that provide information that's primarily useful to diagnose network or application performance, but which offer scant detail even though detail is what security operators need, Corelight's underlying open source technologies (Zeek and Suricata) have been honed over decades to provide incident responders and threat hunters with the exact data they need to do their jobs faster and more effectively.

TAG Cyber: How and where is Corelight deployed in a company's network?

CORELIGHT: Corelight Sensors can be deployed out-of-band, anywhere a copy of network traffic is available (via packet broker, TAP, span port, native cloud mirror, etc.). Generally speaking, they are deployed to cover "north/south" traffic at an egress point of the enterprise network, a connection to the outside world. But, they can also be deployed to monitor "east/west" traffic inside an organization, or in front of high-value enclaves (e.g., sensitive sites or data locations, compute infrastructure), applications, locations (e.g., data centers, military bases), or specific infrastructure (e.g., nuclear weapons labs).

TAG Cyber: How does the increased encryption at the network traffic level (which is positive for security!) impact your ability to see what's traversing the network?

CORELIGHT: Corelight reliably identifies, parses, and generates actionable security insights around key encrypted traffic protocols such as SSH, TLS/SSL, and RDP without breaking and inspecting traffic. While of course encryption reduces the observable traffic footprint, there are still powerful insights to be gleaned around the encrypted connection, such as the open source JA3 hashing function that allows security analysts to fingerprint and blacklist/whitelist TLS connections.

Corelight's Encrypted Traffic Collection, or ETC, preloaded on all Corelight Sensors provides more than a dozen insights about underlying behavior in encrypted traffic which might be an indication of something malicious, such as the presence of keystores over an SSH connection. The ETC was developed based on deep partnerships with several of Corelight's very large commercial and government customers that allowed our research team to look at their live network traffic, and to work cooperatively with their own security teams to validate suspected malicious activity detected within their encrypted traffic.

TAG Cyber: The Corelight team started in academia. How does this influence the decisions you make and the products you build?

CORELIGHT: It has had a huge influence. Corelight is a "mission-driven" organization. And while like many companies we have a written mission — "To protect the (inter)connected world"— our heritage started at Lawrence Berkeley National Laboratory (LBNL), which is part of the US Department. of Energy (DOE). The DOE oversees the national lab network which includes both scientific labs like LBNL, but also the US government's nuclear weapons complex (like Los Alamos, Sandia, Oak Ridge, etc.). Zeek has been in production use for more than 20 years to help defend the DOE network (ESNet) from nation-state attackers, and arguably there's no more critical network to protect than the one underlying our nuclear weapons.

Trying to "detect bad guys" as a primary defensive approach simply does not work. There is too much unusual behavior and too many unknown devices.

From the beginning, Zeek was first honed by the requirements of the DOE, then by other government agencies and large research universities around the country. Generally those requirements were things like: massive bandwidth (ESNet is usually the highest bandwidth network in the world at any time); many uncontrolled users (visiting scholars and researchers); massive international and national collaboration across many disciplines; lots of BYOD; no defined physical perimeter at many sites; lots of experimental content, new applications, unknown data types, odd behavior, etc. With requirements like these, traditional perimeter-based security approaches are largely insufficient. Likewise, trying to "detect bad guys" as a primary defensive approach simply does not work. There is too much unusual behavior and too many unknown devices, so the approach of Zeek to offer "neutral" information about network traffic has been essential to helping SOCs to understand whether something on the network indicates malicious or benign traffic.

TAG Cyber: How did the sudden work-from-home movement affect companies' abilities to rapidly identify anomalies on their networks?

CORELIGHT: Corelight Sensors can be invaluable in detecting improper traffic, attacks, or other indicators of compromise from individuals working from home, whether they are outsiders or employees doing things they shouldn't be doing. Deploying sensors at ingress/egress points to an organization's network is a simple first step toward providing visibility to aid in efforts to improve security during this time, such as insight around remote work driven SSH connections through Corelight's aforementioned Encrypted Traffic Collection.

While we don't offer commercial solutions in home network monitoring, we have launched a program called Corelight@ home that allows people to download a trial copy of our Software Sensor that can run on any Linux machine, including a Raspberry Pi. This program allows engineers, incident responders, and threat hunters to experiment with a fully functional Corelight Sensor in order to understand their capabilities and get more familiar with the data they produce. Primarily this is an internal sales tactic we're using during the pandemic to keep prospective accounts engaged when in-person selling isn't possible, and also in cases where POCs have been delayed due to datacenter access restrictions or other issues.

AN INTERVIEW WITH CARY WRIGHT, VP PRODUCT, ENDACE

ENTERPRISE SCALE PACKET CAPTURE AT HIGH SPEED

When looking for evidence of anomalies or incidents, network packet capture provides a clear picture of what's happening on the network, when, and how, and allows enterprise security teams to investigate incidents before they become breaches. Packet capture is also a critical element in managing network performance; ensuring the network is always available—and free from malware or other performance-impacting issues—prevents costly and damaging interruptions.

Endace, an open network analytics security platform provider based in New Zealand, has reinvented network packet capture to fit modern computing environments. We spoke with Cary Wright, VP Product, at Endace about network monitoring, analysis, and recording, and how it's helping security and network operators detect and investigate cyber threats.

TAG Cyber: Cary, please tell us a little about Endace and your flagship product, EndaceProbe.

ENDACE: The EndaceProbe platform is the only enterprise scale packet capture solution on the market. Customers told us they need to capture weeks of network traffic at many key locations across their global networks, and when a threat emerges their SOC, analysts need answers fast.

EndaceProbes can be deployed as a globally distributed packet capture fabric providing weeks or months of recorded network traffic that can be searched in seconds. Horizontal scaling means that search times remain fast as you scale up the deployment. Specialized high-density EndaceProbe capture hardware means that it's now economically viable to record weeks or months of network traffic at up to 100G and beyond. Scale, speed, and accuracy are key attributes of the EndaceProbe solution.

TAG Cyber: How is packet capture and analysis impacted by increasing amounts of encrypted network traffic?

ENDACE: A majority of traffic on the network is now encrypted, which is good for data privacy but terrible for cyber security. Many attacks are now encrypted using the same TLS encryption that all our web applications use. This can make it difficult for security tools that inspect payloads to detect threats. The customers we work with typically monitor decrypted traffic streams where possible. There are several ways to do this, the most common is to deploy a TLS proxy or break-and-inspect device that terminates, inspects, and re-encrypts all TLS. This provides a full view of all threats traversing the network, and any downstream impacts such as sensitive data exfiltration or credential theft.

TAG Cyber: You refer to your solution as a "platform." What do you mean by that, and what are the benefits of a platform approach?

ENDACE: Endace has almost 20 years' experience in capturing and recording network traffic accurately at high speeds, and on very large, geographically distributed networks. We realized early on that being able to provide this accurate historical packet data was critical to helping customers protect the security and performance of their networks.

SecOps and NetOps teams need access to the data so that they can reconstruct events to see exactly what's happening on their network. And security and performance monitoring tools need to be able to analyze the data to look for cyber threats and performance issues.

...attackers are using polymorphism to defeat signature-based security monitoring tools, and fileless malware is also on the rise.

By creating a platform that specializes in capturing and recording traffic and making it easily available to the teams and tools that need access to it, we could provide a shared, reliable source of truth about precisely what happens on the network and give customers visibility.

So we built a platform that it makes it easy for analysts to find the precise packet data they need quickly. It enables quick search and integrates with their security and performance monitoring tools to gives them one-click access from alerts directly to the related packet data. And customers can host solutions that need to analyze packet data—such as IDS tools, AI tools, NPM and APM solutions, and others—on the same hardware platform that is capturing the traffic and access that traffic in real-time, or "playback" traffic to look for historical issues.

The benefits of this are that customers can consolidate hardware and deploy security and performance monitoring tools far more quickly—as virtualized software applications—without having to roll out function-specific hardware appliances. It puts reliable network evidence at the fingertips of the security, network operations, and IT teams that need it, which dramatically accelerates incident investigation and response and gives team certainty.

TAG Cyber: What are some of the typical challenges security and forensic analysts have when trying to analyze or reconstruct security incidents?

ENDACE: Attackers have become very skilled at covering their tracks. The good ones go to great lengths to delete log entries and temporary files and remove any evidence that they were there. There may have been a firewall alert, but your investigation turned up nothing because system logs were deleted. These attackers can lay dormant in your infrastructure for months or years, collecting intelligence and waiting for the right time to execute their final attack.

Recorded network history cannot be altered by an attacker. When you have network packet evidence at your fingertips you can see everything that occurred before, during, and after any security alert. That makes it a supremely reliable source of evidence for reconstructing attacks and validating threats.

TAG Cyber: What are some of the craftier techniques attackers are using nowadays to get around network security tools?

ENDACE: The use of zero-day attacks is becoming more common, especially during the period after a CVE is announced but before patches or detection rules are yet available. This is a very vulnerable time for any organization as the race to exploit these vulnerabilities is already underway.

Having a record of all traffic is a great way to reduce risk during this vulnerable period. Once detection rules are available, you can re-scan old traffic for any signs of executed exploits. You can also threat hunt across the recorded traffic using IoCs from your threat intelligence and investigate any downstream threat activities such as lateral movement, payload downloads, data exfiltration, etc.

Another approach is using common internet protocols such as DNS, which is typically not blocked and often not carefully scrutinized, to hide low-and-slow data exfiltration or command-and-control traffic. With access to full packet data, it's easier to detect and investigate these sorts of attacks quickly and accurately to see exactly what's going on.

And lastly, attackers are using polymorphism to defeat signature-based security monitoring tools, and fileless malware is also on the rise. AI-based monitoring tools can help here by detecting behavioral anomalies. But analysts need to be able to validate the alerts that these tools raise. Again, packet data provides an extremely powerful source of evidence that allows analysts to quickly and definitively confirm the scope of threats these tools detect or identify and flag false positives.

AN INTERVIEW WITH SAM CROWTHER, CEO & FOUNDER, KASADA

DISINCENTIVIZING BOT OPERATORS

A bot can be good or bad, productive or destructive. Good bots help with search engine indexing, monitoring a website for performance issues, or providing customer service through pre-programmed communication, a.k.a., "chatbots." In security, humans are pre-programmed to think of bots as bad, and they certainly can be when used for malicious activity such as data stealing or scraping, DDoS attacks, and content abuse.

In recent years, the cyber security community has seen an uptick in companies committed to stopping malicious bot attacks to prevent automated criminal activity. One such company, Kasada, a global bot protection company founded in 2015, is helping security teams prevent malicious use of automation that can damage a company's brand, compromise customer accounts, and overload systems to render them useless. We spoke with Sam Crowther, CEO & Founder, at Kasada about their differentiated approach to protecting web and mobile apps and APIs from bad bots, and how this approach helps businesses increase revenue.

TAG Cyber: Your value proposition goes beyond the typical, "we stop bad bot traffic." What's the complete message and how do enterprises benefit from this holistic approach?

KASADA: When most people think of a bot, they think of stealing customer accounts or scraping data, when the reality is that bot activity is much broader than that. Any non-human process that interacts with an online application is technically a bot. Since we look at the bot problem through that lens, we're able to help our customers solve a wide array of problems, which includes stopping bad bot traffic as well as other web application security use cases such as web application firewalling and application DDoS in a way that's different from heuristic signature-based approaches.

It's one thing to stop bad bots today, but we're even more interested in how we make sure that we stop them in the future as the adversaries inevitably retool to continue to be successful in their automated attacks. We solve this by dissecting why someone would be using a bot in the first place. The answer is: it's economical. Not only are we stopping them from a technical perspective, but we're striking back by taxing them to remove the financial motivation they have in carrying out their attacks. By focusing on the economics, we disincentivize a bot operator to retool and try again. As a result, our customers are not just protected from today's automated attacks, but also from what adversaries will do next.

TAG Cyber: Many security technologies look for the anomalous or "bad" behavior, but Kasada is designed around zero trust principles. How and why is this beneficial?

Kasada: Instead of examining the behaviour of a bot, we are looking for the presence of

The people we're typically up against are creative, smart, competitive, and financially motivated. We know that we need to attack the problem with this mindset.

automation itself. By assuming everyone is guilty until proven innocent, we can prevent bots that we have never seen before. Most solutions approach the problem the other way around by requiring an arduous set of learning and rules that assume innocence until proven guilty. Because we don't rely on such backend rules and we make it prove that it is in fact good before we let it through, we have an adaptable and sustainable long-term solution. This quick, yet flexible decision making is highly beneficial to our customers because there's no longer a window of opportunity for an attack to succeed and it is much easier to configure and manage.

With Kasada, you don't need to configure or manage rules, and every time a web or mobile app is updated, you don't need to re-learn what's good and what's bad—that all becomes irrelevant. Organizations often face a type of bot attack that no other company faces, or ones that haven't been seen before. But for us, that's fine because we don't care about what the bot is doing; we just care that it's a bot.

TAG Cyber: What are some of the more prevalent bot attacks enterprises need to be concerned with?

KASADA: Enterprises need to be concerned with how bots and bot operators are evolving. It's not necessarily about any specific bot attack; it's more about the bots that mimic human behaviours or abusing legitimate human functionality, which can be very difficult to detect.

Due to this, we focus more on the tools and techniques they're using to try to mimic human behaviour than actually trying to figure out the attack itself. A practical example of this would be a hotel website. What bots used to do is directly query a hotel for given dates and scrape the price, which is super easy to detect because no human does that. A human might come in from Google, go on the homepage and click around for a bit, enter dates and then go, and then they'll click around again. Bots will do their best to behave as humans do to evade defences. How do you distinguish that? You can't unless you've got the level of visibility that we have. In essence, the bots are getting even better at mimicking human behavior aimed at bypassing the defenses put in place.

TAG Cyber: Have your researchers assessed any new types of fraud schemes emerging? How are attacker tools used to conduct fraud changing?

KASADA: The fraud schemes themselves are generally the same at their core, but the techniques to commit the fraud schemes are evolving. A good example is registering fake accounts and subsequently brute-forcing gift card codes. Our researchers see the massive scale at which fraudsters are starting to operate, thanks to automation. As a result, a fraud scheme that may not have previously been very profitable is now unbelievably lucrative.

What is changing is the plethora of free tools, and they are getting more sophisticated with the communities that support them. An example is a library that helps make Puppeteer look exactly like Chrome, which makes the presence of bots especially difficult to detect. Libraries like this are very actively maintained by people who have a lot of money at stake should they run into issues, yet it's free and simple to use. You can go to Google, download it, and within about two minutes, you can bypass most bot detection solutions on the market. There are a number of these tools that are gaining some serious traction and support in these communities.

Part of our researchers' jobs is to know what the fraudsters are doing with these tools and understand exactly how they work—this helps us stay ahead.

TAG Cyber: There is a misconception that bad bots are the real problem, but you've stated that it's the humans behind the bots that are the real issue. Can you enumerate for our readers?

KASADA: The people we're typically up against are creative, smart, competitive, and financially motivated. We know that we need to attack the problem with this mindset. We need to undermine why they're doing what they're doing and disincentivize them. One way is by frustrating the bot operator. This can be a very effective and valid way to win. We do this by ensuring that it's as difficult as possible for them to understand what we're doing in our code, which is necessary to fight back.

Carding is a great example. Let's assume 1% of credit cards bought on the dark web will work, and the criminals will plan to sell them for a few bucks each. If they buy 1 million credit cards for $10,000, and 1% will actually work, and they are $3 each, then that equals $30,000 total. If we introduce enough compute costs in the carding attack, that $30,000 all of a sudden goes away. Since a card only has value for a week once it's been compromised and we can drag out the length of the attack to stall their retooling efforts, then there's no value in carrying out the attack anymore.

A solution that enables you to do all these things to frustrate and disincentivize an attacker is absolutely key to success in defending against malicious automation.

AN INTERVIEW WITH C. REED,
CHIEF MOBILITY OFFICER, NOWSECURE

ASSESSING MOBILE APP RISK ACROSS THE ENTERPRISE

Enterprise reliance on applications cannot be overstated. Applications run everything from internal systems to customer-facing resources.

In today's environment, workforce and supply chain mobilization have become critical, enabling remote, geographically dispersed employees, partners, and suppliers to tap into systems—even if they were initially developed for internal use only—that have been transformed into mobile apps.

And we cannot forget the necessity of customer-facing mobile apps. From financial services to healthcare to retail, every consumer expects a mobile, seamless—and secure—method of engaging and transacting with businesses. Yet, while innumerable application security testing tools exist in the market, few are hyper focused on ensuring the security and privacy of mobile applications. Nonetheless, a mobile app with vulnerabilities or one that leaks data can be ruinous. We spoke with Brian C. Reed, Chief Mobility Officer at NowSecure about why companies gloss over targeted mobile app security testing, rolling it into more general web application testing, and why doing so inadvertently increases cyber risk.

TAG Cyber: Brian, can you frame the scope of the mobile application risk problem?

NOWSECURE: Mobile apps have driven tremendous gains in revenue, customer engagement, employee productivity—creating new markets and disrupting existing markets. In fact, today mobile apps drive over 70% of all digital time and traffic… but the attackers are following.

Major mobile app breaches include AirCanada, British Airways, UnderArmour, Walgreens, Dave Banking, Samsung, Facebook, True Secure Messaging, Firefox, Twitter, Mercedes-Benz, 7-Eleven, Quest Diagnostics, Equifax, Western Union, and Priceline.

Mobile app risk spans apps an organization builds, apps they download and even apps employees bring to work on BYOD. Every mobile app and every mobile user running those apps extend the enterprise attack surface.

Alarmingly, we have tested millions of apps in the public app stores and internally developed for years and still 85% have security vulnerabilities and 70% leak private data that could violate GDPR/CCPA.

Some executives are beginning to understand the inherent mobile risks they have accepted through their mobilization and digital transformation efforts. These enterprise risks are real, wide ranging, and already present. Regulatory fines, brand damage, and revenue loss from mobile must all be factored into existing enterprise risk management programs.

But many Chief Security, Risk and Audit Officers aren't aware of how pervasive the mobile app risk problem is across their enterprise. Leaders need to evaluate cyber risk across the entire mobile application development and mobile app procurement supply chain. A rigorous, consistent mobile application security testing and monitoring program can identify risks before they impact an organization's assets and reputation.

TAG Cyber: Mobile was a primary security topic of conversation circa 2008-2010. Yet, as businesses transformed and mobile apps became commoditized, the industry didn't keep that hyper focus on mobile apps. Why, and what problems does it cause?

NOWSECURE: Yes, back in those days of Blackberry dominance when executive iPads and commodity Android devices invaded the enterprise, the focus was device-level security and MDM—with little attention paid to the mobile apps. Some in regulated industries did recognize app-level security issues and deployed containerized solutions.

Mobile app developers grew by the thousands, filling the app stores with millions of mobile apps, but with few security standards and no real official certification. Developers of mobile app sprinted ahead focusing on delivering new and exciting mobile app experiences, not underlying security and privacy. In the pressure to deliver for the business, teams race forward and scale their dev throughput, but traditional security teams don't have the tools and processes to keep up. Today, thousands of businesses and millions of users take advantage of millions of mobile apps in app stores and millions more custom developed for internal use, assuming they are safe and secure with no real visibility into the real risks.

TAG Cyber: Why is conventional application security testing insufficient for mobile apps?

NOWSECURE: There are two key issues: differences in web vs. mobile architecture and traditional approaches to security testing.

From an architecture perspective, web developers can focus on features because web apps run in a more protected environment where 98% of code lives behind a firewall and a web browser provides secure container and SSL connectivity. Mobile apps live in a completely unprotected environment on a mobile device that is easily reversable where attackers can uncover intellectual property (IP), find vulnerabilities, and harvest personal data. What's more, mobile app developers have to know how to write secure code for everything including

Mobile apps live in a completely unprotected environment on a mobile device that is easily reversable where attackers can uncover IP, find vulnerabilities, and harvest personal data.

secure data storage and transmission. In our real-world testing, some 80% of vulnerabilities and privacy leakage are found with insecure data storage or transmission.

From a testing perspective, a lot of organizations use web-style source code scanning on mobile apps that generate high false positive rates and only covers 20% of the actual mobile attack surface. But the 80% of common vulnerabilities noted above are only found through dynamic and interactive security testing, not static source code testing. To make up for this, some organizations use costly manual pen testing to dynamically and interactively test a running mobile app, but high cost means they can only afford for most important apps once or twice a year.

TAG Cyber: Tell us a little about the NowSecure Mobile App Security Solutions.

NOWSECURE: NowSecure provides a full suite of mobile app security software and services to help organizations create and scale their mobile app security program. Built on a decade of experience testing millions of mobile apps, the NowSecure suite includes NowSecure Platform for fully automated mobile app security testing and continuous monitoring of mobile supply chain risk, NowSecure Workstation for analyst-driven mobile pen testing productivity, NowSecure Training Services Courseware for developer and security analyst skills advancement, and NowSecure Pen Testing Services for expert mobile app certification.

Our holistic, standards-based approach ensures that organizations can tap into our expertise and technology to form their mobile appsec program, improve productivity, ensure full test coverage, automate for fast feedback loops, up-skill their dev and security teams, and shift left for DevSecOps scenarios—all leveraging our decade of experience and our world-renowned security experts.

Our customers have reported impressive results, from collapsing release cycles from annually or quarterly to monthly or weekly, to slashing mobile pen testing costs by 90%, to growing mobile app revenue by 10X. Some of our DevSecOps customers report build-to-release times of less than 3 hours. Others are running more than 90 mobile app pipelines at scale to meet their global business needs.

TAG Cyber: We've talked about the need for automated and continuous testing for years—and the NowSecure solutions offer that capability. Why do you think a lot of companies still haven't moved toward automated, continuous testing?

NOWSECURE: Automated, continuous security testing certainly is the pinnacle of efficiency and scale… and it can be challenging but rewarding. It starts with executive sponsorship to accelerate the business through product innovation, which eventually leads to a DevSecOps approach.

Start small with one team, one mission, pick the tools, and design the process with incremental goals leveraging purpose-driven, collaboration-minded members from each of Dev+Sec+Ops. Assemble an integrated toolchain for all stakeholders, automating each manual task. Leverage tools to do the grunt work and focus human work on development, creativity, and optimization. Leverage standards like OWASP MASVS and NIAP. Track the right metrics to drive continuous improvement.

The speed gained by this shift to DevSecOps with automated, continuous mobile app security testing can drive substantial topline impact on revenue gained and competitive advantage that more than pay for the journey—all while reducing overall business risk. Every organization we talk to that achieves this will say it was challenging, but they were committed and iterative and eventually achieved their goals.

Charlie, my personal wants and needs...
I wonder...
...can only be met at their deepest level...
...whether it would be better...
...by a wonderfully attentive man like you!
to use Azure or AWS to host our app.
Powell/Amato ©

AN INTERVIEW WITH MICKEY BRESMAN, CEO, SEMPERIS

REMOVING ACHILLES' HEEL FROM ACTIVE DIRECTORY

For a time, the network was core to security control. As the concept of a network has changed, and as companies' digital ecosystems have become highly distributed and dynamic, enterprises have had to evolve their concept of the control plane. Identity has thus emerged as "the new perimeter," with directory services at the center. Active Directory, in particular, as the most widely used service, has become the battleground for both control over access to network resources and attackers who want to exploit the people and resources governed by it.

With the ever-expanding ecosystem of remote workers, cloud services, and devices, securing Active Directory is a business-critical imperative. Semperis helps enterprise security and identity management teams monitor and protect AD and respond to and recover from incidents when necessary. We spoke with Mickey Bresman, CEO at Semperis, about how the attack landscape is changing and how AD has become such a critical element in cyber security.

TAG Cyber: Semperis calls Active Directory the "Achilles' heel" of enterprise security. Most of our readers likely understand why that is, but can you explain why native AD controls are not sufficient to prevent AD compromise?

SEMPERIS: Microsoft Active Directory was built before cloud computing, nation-state cyber warfare, ransomware, and other modern threats that organizations are grappling with right now. Simply put, Active Directory was built for a different era, and it isn't equipped to handle today's challenges. Yet, Active Directory is still a foundational piece of infrastructure for 90% of organizations, and it's not going anywhere. Securing Active Directory is difficult given its constant flux, the sheer number of settings, and increasingly sophisticated threat landscape. The hard truth is that Active Directory is a soft target for attackers because its default configuration is easy to exploit, and the system is rarely properly secured. Hacking tools, like BloodHound, PowerSploit, and MimiKatz, make it easy for attackers to takeover Active Directory and cause harm to government agencies and enterprises. And with the recent theft of FireEye's automated pen testing tools, even less sophisticated attackers can be just as dangerous as sophisticated adversaries with years of red team experience.

When Active Directory is compromised, you must assume that all resources that depend on it have also been compromised. So, it's extra critical that defenders anticipate the adversaries' advances and be able to thwart off attacks at every stage of the cyber kill chain. To be clear, this goes beyond the traditional monitoring tools, as they often lack the Active Directory-centric security that's required to catch more sophisticated identity attacks. By modifying Active Directory, attackers can get access to anything in the network. Therefore, specific security provisions must be in place to monitor for and prevent unsanctioned changes within Active Directory, as well the ability to return to a known secure state, should a change find its way past prevention efforts.

At Semperis, we've delivered first-of-its-kind solutions to address the entire lifecycle of a directory attack—from finding and fixing security vulnerabilities, intercepting privilege escalation and persistence, and quickly responding to ransomware and other data integrity emergencies.

TAG Cyber: We've now been in a predominantly remote work situation for almost a year. How have attacks changed in the last 11+ months, and what do you see on the horizon?

SEMPERIS: In 2020, cyber security programs put special focus on defending their identity infrastructures, particularly as COVID-19 accelerated the adoption of remote workers, cloud services, and devices. And it's become clear just how opportunistic attackers are, compromising targeted networks several months before deploying the ransomware, waiting to monetize their attacks until they see the best financial gain. Bad actors even launched phishing, malware, and other attacks that exploited public concern over COVID-19. Nothing is off-limits, not even the most vulnerable.

The best way to predict the future is to study the past. The SolarWinds supply chain attack recently took the world by storm, triggering flashbacks to the 2017 NotPetya attack. In 2021, we, unfortunately, expect to see more of the same. The good news is that organizations are waking up to the fact that identity is the first and last line of defense.

TAG Cyber: Optimally, enterprises can prevent attacks, but we know some compromise is inevitable, which is why Semperis offers Active Directory Forest Recovery. How is this platform different from traditional recovery tools?

SEMPERIS: Surprisingly or not, Active Directory is at the center of most IT operations. But it's not an uncommon scenario to see organizations prepare for ransomware recovery and totally miss the fact that they can't access any of their network resources without Active Directory. So, if your organizational recovery plan starts with logging in to the recovery server and Active

Directory is unavailable, this plan will not work. If Active Directory is down, business stops. Period. It's impossible to stop every attack, especially as remote workforces rapidly expand the attack surface. But you can control how resilient you are. Your business depends on it. Widespread attacks exploiting Active Directory have crippled businesses in recent years. Take the most destructive attack to date, for example, NotPetya, which wrought $10 billion in total damages in 2017. Like many high-profile companies impacted by NotPetya, the world's largest shipping firm, Maersk, spent over a week manually recovering its Active Directory.

So, to answer the question directly, the requirements for Active Directory recovery have changed. Believe it or not, many organizations still rely on recovery methods built for natural disasters and operational mistakes; they're not optimized for cyber disasters. So, when a ransomware or wiper attack takes out the domain controllers, traditional recovery processes drag on for days or even weeks and risk malware re-infection in the process.

Semperis introduced a fully automated forest recovery solution to avoid human errors, cut downtime by 90% or more, and eliminate the risk of malware re-infection. Essentially, we've empowered organizations to think "cyber-first" and modernize Active Directory disaster recovery, core to any business continuity strategy, to stand up against today's threats.

TAG Cyber: Do you have any metrics on your customers' mean time to recover versus industry norms?

SEMPERIS: The industry norm for recovering Active Directory ranges from a few days to weeks for mid-market and large enterprises. Microsoft provides a lengthy technical guide that details the 28-step multi-threaded manual process required to recover an Active Directory forest. Or, many organizations use third-party Active Directory backup tools that rely on bare-metal recovery. But unfortunately, recovery from system state or bare-metal backups can re-introduce the infection all over again.

Semperis introduced something totally different—the first backup and recovery solution purpose-built to recover Active Directory from cyber disasters like ransomware and wiper attacks, all automated. From real-world scenarios and lab tests, Semperis customers report shortening recovery time of the entire Active Directory forest by 90%. Essentially, Semperis enables customers to measure recovery time in minutes instead of days or weeks, even for the largest and most complex Active Directory environments in the world.

> It's universally understood that Active Directory is a prime target for attackers attempting to steal credentials and deploy ransomware across the network.

TAG Cyber: Semepris was recently named the fourth fastest growing company in the Tri-State area in Deloitte's 2020 technology Fast 500™. To what do you attribute your success?

SEMPERIS: Several factors, the first being the experts and talent that Semperis has attracted, including the world's foremost Microsoft identity MVPs. It all comes down to the people at the end of the day, and I can't say enough about the depth of knowledge at Semperis. Another factor is the urgent need for threat mitigation and rapid response to directory attacks, and Semperis has risen to the occasion to help customers thwart off the bad guys. It's universally understood that Active Directory is a prime target for attackers attempting to steal credentials and deploy ransomware across the network. Simply put, if Active Directory isn't secure, nothing is.

Semperis is on a mission to help organizations combat the deluge of escalating attacks targeting Active Directory, which is especially important for healthcare providers, pharmaceuticals, manufacturers, and others on the frontline. Think about hospitals that can't access their systems to save a life or cities that get held hostage—it's what drives Semperis to help organizations take back control.

ANALYST REPORTS

TAG CYBER

Advice on Security Selection for SOC Analysts and DevOpsTeams

Platform advice is offered for SOC analysts and DevOps teams addressing security risks. A patchwork of locally integrated, developed and open source point security solutions is shown to be suboptimal. Instead, an end-to-end commercial security platform is shown to be a better option, and guidance is offered on how to make this selection decision properly.

Prepared by

Katherine Teitler
Senior Analyst, TAG Cyber
kteitler@tag-cyber.com

Edward Amoroso
Chief Executive Officer, TAG Cyber
eamoroso@tag-cyber.com

Introduction

Until recently, commercial security platforms offering true end-to-end support for enterprise teams were rare. As a result, enterprise security teams often had few unified options when trying to secure their overall environments. The protection challenge increased once organizations began moving portions of their data to the cloud, and as application developers, following DevOps, needed to ensure that their process was agile, scalable, and secure.

Because enterprise security portfolio managers have had meager end-to-end options for so long, the normal integration process has involved stitching together many disparate off-the-shelf security point products. This patchwork design and integration process has been especially complex in security operation center (SOC) and DevOps ecosystems, because analysts and developers tend to lean not only toward multiple point solutions, but also toward inclusion of home-grown tools.

Additionally, regardless of whether a team uses commercial or open source tools, they must train experts to operate the resulting platform. This is true even if the organization chooses to hire a managed security services provider (MSSP) to implement and manage their protection. Whether managed or in-house, dealing with a patchwork of point solutions will be complex and will require more work to support than a holistic end-to-end platform.

This TAG Cyber analyst note outlines how piecing together an assortment of different point solutions, including both commercial and open source tools, is thus sub-optimal for SOC and DevOps teams seeking to minimize risk. We argue in this note that security portfolio managers should instead be working with their expert SOC analysts and software developers to identify and use commercial platforms that employ a more holistic, end-to-end cyber security focus.

Security Challenges for SOC Analysts and DevOps Teams

We all know that modern continuous build/deploy cycles allow software developers to meet the demands of their customers in a quick, scalable way without the excessive manual oversight of pre-continuous integration/continuous development (CI/CD) lifecycles. Furthermore, CI/CD approaches to building software and applications allow developers to make use of multi-cloud services and containers, which can speed up delivery and lower costs.

Despite these obvious benefits of Agile software development, several challenges still exist. For example, developers often use tools to manage CI/CD pipelines that do not properly incorporate cyber security functionality. It is not uncommon for commercial CI/CD support capabilities to lack support for security governance and mechanisms for integration with third-party security tooling. This is particularly true when security tools are developed locally.

This problem extends to the SOC, where security analysts also often select and use tools that lack visibility, monitoring, and control. When security analysts practice this type of do-it-yourself security, they create complex platforms that can result in exposed vulnerabilities. Like software developers who might create patchwork protection, analysts often create support environments that are suboptimal from a security perspective.

> “When security analysts practice this type of do-it-yourself security, they create complex platforms that can result in exposed vulnerabilities”

In both cases, we see the root problem stemming from this patchwork approach to piecing together point solutions, combined with locally developed tools. The confidence and expertise typically found in expert development and SOC analysis environments are welcome, but also enable these groups to dive into building complex systems. Should these experts switch jobs or leave their companies, what’s left is a complicated infrastructure often with high levels of risk.

Open Source and Locally Developed Tools

Both developers and security analysts are responsible for the management of the IT and security technologies that aid them in dealing with security events and incidents. Within any one organization, this infrastructure will combine systems located in on-premises networks, public cloud, private cloud, hybrid cloud, or multi-cloud. They employ unique dashboards and data streams from various vendors, and they must be used to monitor and analyze networks, servers, applications, and endpoints communicating across their infrastructure.

The ability for such platforms to gain uniform visibility, establish baselines, and identify anomalies is often further challenged because many tool outputs are non-standard and alert volumes can become massive. Security teams must also contend with the fact that a significant portion of the alerts investigated may be false positives. Developers and analysts understand that these problems cannot be fixed through improved manual processes.

Unfortunately, many expert developers and experienced SOC analysts try to address these shortcomings by locally building their own tools or utilizing open source utilities. Certainly, open source usage carries many wonderful benefits, but for security, it's been our observation that the application of open source tools can be uneven. Worse, the use of open source often leaves support gaps that are exacerbated when experts move to other jobs.

Similarly, when software developers and SOC analysts create and use their own home-grown tools, unpredictable results can emerge. With the use of open source, it is certainly admirable that such experts have the initiative and expertise to create their own tooling—but with open source and locally-built proprietary tools, the result is forever obligation to support these utilities and to keep up with evolving technologies.

Support for Cloud

One challenge that emerges for home-grown security platforms involves ongoing support for cloud. As organizations adopt more cloud infrastructure, security analysts are feeling pressure to gain the same visibility and control over these environments as they have with internal networks. Because of the nature of cloud access, however, they cannot merely adapt on-premises tools or adjust tools built for one cloud to extend ubiquitously across multi-cloud.

Thus, the desire for cross-infrastructure security tooling is high on many SOC analyst and DevOps team wish lists. The decision to try to connect together the various off-the-shelf security tools from their cloud security providers, to build their own security point products, or to integrate security point products to stretch across their premise and multi-cloud infrastructure can result in a severe operational challenge. This suggests the need for end-to-end solutions to simply use and support.

Use of Metrics

An additional challenge of patchwork security involves the establishment of meaningful metrics. Security analysts and DevOps teams need platforms and tools that collect, correlate, combine, and provide actionable data about their environment. To date, security information and event management (SIEM) and aggregated log management systems have been the tools of choice for such internal telemetry. These are commercially provided and often premises-oriented.

However, while these SIEMs have been good at collecting simple data about network events such as failed login attempts or the number of malware variants handled in a given period, they have also had to evolve to meet changing enterprise demand. Teams have learned, for example, that quantity-based metrics often drive initiatives to reduce the numbers of security events or false positives, which may be useless to identify which assets to prioritize for remediation.

So, just amassing data on what's happening in an environment is insufficient. Instead, security platforms for SOC and DevOps environments must contextualize collected data from across their infrastructure to support meaningful investigation, and to support action by executives, incident responders, and forensic experts. Since this security insight might not be available from premises-based SIEM or log management tools, teams often turn to patchwork design.

Staffing Pressures

A third challenge introduced by patchwork security design using point solutions, open source tools, and proprietary software involves support for staffing. Everyone knows that a successful enterprise security program requires the right people to operate smoothly, and the lack of skilled security staff, as well as insufficient talent pipelines in our industry, compound the technology challenges mentioned above.

The main issue is that enterprise teams must select and hire staff to focus on the key security challenges supporting the organization. This involves protection of data, investigation of incidents, and developing insights for management. If experts spend their time supporting tool development and updating patchwork platforms, then this diverts their attention and can lead to dissatisfaction in their day-to-day work.

Commercial Security Platform Options

To address these security challenges for SOC analysts and DevOps teams, two types of commercial platforms are available—some with greater focus on supporting cloud-hosted data and applications, and which should be considered especially when the organization is running hybrid or cloud-only environments. The first type of platform is an all-in-one proprietary technology, built from the ground up. The second type integrates different industry-leading security modules into a platform. Before digging into recommended requirements, it helps to look at the pros and cons of each.

Regardless of the type of platform, when migrating one's data and applications to the cloud, it's important to look for platforms that didn't emerge from former on-premises solutions and were recently adapted to the cloud. A cloud-native focus is a huge benefit for cloud-first users, as they can feel confident that these providers understand the idiosyncrasies of cloud environments.

> "A cloud-native focus is a huge benefit for cloud-first users, as they can feel confident that these providers understand the idiosyncrasies of cloud environments"

Proprietary Platform Option

In this first case, vendors build their platforms to include native capabilities to cover the entire spectrum of use cases and requirements. This can include support for intrusion prevention, email security, network monitoring, and even data encryption. Usually these vendors must employ a capable team of marketing and technology experts to ensure that the right capabilities are being included.

One advantage of this approach is that a common design and development process may be applied to the platform. In addition, the buyer will deal with far fewer security vendors, which can ease the procurement and support process. This is especially true if the vendor offers a larger range of IT products such as development platforms or runs its own data center.

However, several serious disadvantages must be factored into the selection process. The first one is related to working with just one vendor. Choosing an all-in-one proprietary platform might not lend well to all customers, as some might be wary of vendor lock-in when using a vendor-specific platform. Binding one's organization to a single provider, regardless of capability, could prove problematic if requirements change, if infrastructure changes, if the provider or technology is acquired, or if there is a switch in the vendor's management personnel.

Second, recognize that few vendors will have the in-house talent to create world-class solutions in so many different areas of cyber security. Larger vendors will obviously have a deeper talent bench than smaller ones. However, even in the case of a more extensive organization, in-house developed platforms are usually created through acquisition. Larger vendors often research and buy smaller security players and then integrate these smaller players' products into their offerings. However, with acquisition, true integration of the acquired technology often takes longer to accomplish due to several factors such as competing development priorities, people integration and knowledge transfer.

Lastly, even if the acquisition process is smooth, the underlying functionality for all the merged products may be designed to different standards (as it was built by different engineering teams), using different processes, and employing different underlying utilities. Open interfaces will help ease these complexities, but the overall integration will rarely result in a uniform design. Rather, the resultant platform might look like a collage of different software—so buyers should be careful to inspect.

In the end, enterprise buyers who decide to select a proprietary security platform to address the needs of their SOC analysts and DevOps teams will have to balance the convenience of dealing with a common vendor, with the challenges that emerge to support a complex integration of acquired company solutions. Working with analysts such as TAG Cyber can help teams make this decision properly.

Integrated Platform Option

In the second case, security vendors develop commercial platforms that are specifically designed to consolidate myriad security modules via an extensive integration ecosystem. These companies generally focus on trying to extend their platform offering by partnering with best-of-breed IT security vendors in adjacent areas. Open solution designs and APIs enable this type of integration by supporting a common means for interconnection.

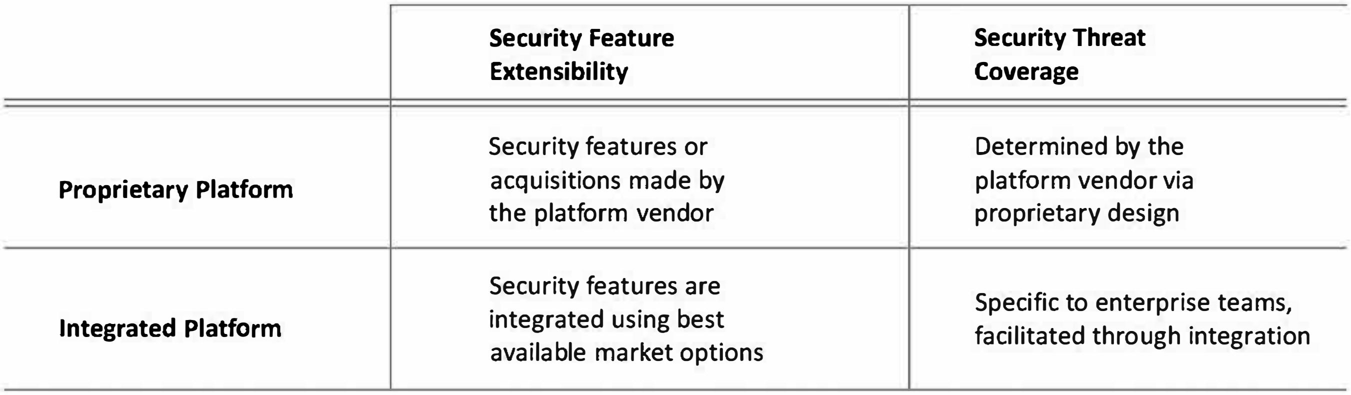
One challenge with this approach is that enterprise teams must typically choose the best security capabilities based on availability and business needs. Unlike pre-built platforms where the integration decisions are made by the vendor, this option does come with the expectation that the enterprise team—including SOC analysts and DevOps teams—play a more active role in how their platform is integrated, deployed, and used. While an API-based approach offers flexibility and the ability to change or upgrade when needed or desired, several integrated platforms are now offering pre-integrated solutions, which customers can choose, to turn on or off, based on their business needs.

Many advantages exist for this security integration platform option, including the obvious benefit of making available to buyers the market's leading security solutions. Vendor lock-in not an issue with an integration platform; if a new and/or better security solution becomes available, it can easily be integrated into the platform. With cyber threats and architectures changing so dramatically, especially in SOC and DevOps environments, this is a major advantage, that helps enterprises protect their environment as their needs evolve over time.

In addition, the security integration platform approach has the benefit of making available those solution offerings that are cloud-compatible, so the resulting platform will be easily deployed into multi-cloud operations. Integration, by its very definition, orchestrates data and outputs from chosen, best-of-breed, deployed technologies and allows for uniform and consistent visibility and control. Visibility and protection across premises, public cloud, private cloud, and hybrid cloud can thus be ensured more smoothly.

The integrated platform approach also aligns well with companies' DevOps programs which require rapid and easy deployment. As opposed to proprietary options, which often rely on third-party hardware and require network changes, the "plug and play" approach of integrated platforms may be attractive to fast-moving and rapidly-scaling organizations.

Ultimately, buyers will have to measure the respective pros and cons of a proprietary versus integrated platform. Attention should be placed on how each approach might address security operations, and in particular, how each will ease the temptation for SOC analysts and DevOps teams to develop patchwork solutions. As suggested above, working with industry analysts such as TAG Cyber will help with this selection process.



	Security Feature Extensibility	**Security Threat Coverage**
Proprietary Platform	Security features or acquisitions made by the platform vendor	Determined by the platform vendor via proprietary design
Integrated Platform	Security features are integrated using best available market options	Specific to enterprise teams, facilitated through integration

Figure 1. Comparing Proprietary and Integrated Platform Options

Developing an Action Plan

Developing an action plan for platform selection in SOC and DevOps environments is best done by first creating a prioritized list of relevant functional and operational requirements. Certainly, as for any platform selection, some obvious criteria elements will apply. These include the need to minimize costs, maximize investment return, simplify platform deployment, and reduce as much friction in the acquisition and operational processes as possible.

For security requirements, however, guidance can be offered that will be more specific to the combined SOC analyst and DevOps team objectives to reduce risk. While these requirements will obviously differ from one enterprise environment to another, we can list below some of the more common choices being made today by the best enterprise security teams working to reduce risk across their enterprise.

Multi-Cloud Focus

A primary requirement for any security platform, and especially one that targets expert SOC analysts and DevOps teams, is that it must deal smoothly with multiple cloud environments. This includes public clouds, private cloud, and hybrid cloud solutions being used in the enterprise. Such multi-cloud coverage should seamlessly optimize and integrate any native security capabilities offered by the hosting provider.

Threat Prevention

An additional platform requirement should include support for preventive controls that can help stop breaches and attacks before they occur. An advantage of the platform integration option is that such extensibility is easily obtained by just snapping in the desired prevention vendor. Proprietary platform providers would have to be reviewed to ensure that they incorporate sufficient coverage in this area, and potential customers should ask how the provider allows for adding or replacing integrations.

Threat Detection and Response

A third requirement for security platforms in this area includes support for threat detection and response. A clear trend in the security industry involves the familiar shift-right focus that comes from the recognition that advanced persistent threats (APTs) and other types of breaches and exploits are probably not going to be prevented in most environments. Detection and response must therefore be in place to minimize the consequences.

Continuous Security Compliance

The fourth requirement for SOC analysts and DevOps teams to include in their security platform selection is the need for compliance support that is continuous and ongoing. Point-in-time compliance data that comes from periodic reviews and spot-checks are increasingly insufficient to address the governance and risk obligations that come from auditors, regulators, managers, and executive teams.

Protection of Critical Workloads

The final requirement worth noting here is that platforms must include the capability for the enterprise team to protect its most critical workloads. Too often, platforms are optimized to a threat that might not be the main focus for a buyer. Platforms should allow users to tailor the protections toward the highest priority assets, applications, systems, and other resources supporting the organizational mission.

About TAG Cyber

TAG Cyber is a trusted cyber security research analyst firm, providing unbiased industry insights and recommendations to security solution providers and Fortune 100 enterprises. Founded in 2016 by Dr. Edward Amoroso, former SVP/CSO of AT&T, the company bucks the trend of pay-for-play research by offering in-depth research, market analysis, consulting, and personalized content based on hundreds of engagements with clients and non-clients alike—all from a former practitioner perspective.

TAG CYBER

Introducing MFAz: Multi-factor Authorization

Readers are introduced to multi-factor authorization, a complement to the better-known multi-factor authentication, which has become a cyber security best practice. Justification for the emergence of the category and adoption of the technology is made.

Prepared by

Katherine Teitler
Senior Analyst, TAG Cyber
katie@tag-cyber.com

Introduction

Identity and access management (IAM), once relegated to IT's domain, has squarely become a cyber security risk. As such, over the last decade, cyber security teams have gained increasing control over IAM in an effort to mitigate cyber risk from unauthorized access, fraudulent identities, and inappropriate use of permissions. Yet, despite its name, identity and access management encompasses more than just identity and access; central to strong IAM are authorization, directory management, and user management.

Because end user identities and overly permissive access are the low-hanging fruits of cyber security, the industry has spent considerable time and effort addressing ways to better verify identities (both human and machine), limit access permissions (especially on privileged accounts), and tighten up directory services management. As identity is, unfortunately, one of the easier attributes for threat actors to usurp, one of the prevailing strategies in improving IAM is the implementation of multi-factor authentication (MFA)—requiring the user or entity requesting access to prove they are who they say they are.

MFA is today an industry best practice and, when implemented correctly, a demonstrable method for preventing unauthorized access to networks, systems, files, and applications. It has become so prevalent that even non-technical device users understand what MFA is and its importance for security and privacy. However, MFA, by its current definition and set of technical controls, leaves out an important component of IAM: authorization.

Authorization is, of course, the mechanism by which a user or entity is permitted access to a system. It is also the process of providing instruction for a transaction. While authorization is part and parcel of IAM, when it comes to transaction instructions and approvals, IAM isn't always sufficient to ensure validity of the transaction. In other words, when system A is authorized to transact with system B, and all requirements for secure connectivity have been met, there is today no second factor to ensure validity. In the same way that MFA is used to double check, if you will, a user's/device's identity, authorization needs an additional factor to guarantee that false transaction requests are not completed.

In this report, we introduce the concept of multi-factor authorization (MFAz) as a complement to IAM, and explain its use in high risk transactions, such as requests for personal records and the transfer of money or sensitive documents between parties.

What is MFAz?

Traditional authorization is well-known to cyber security practitioners. The process works by establishing connections between the requesting device—OAuth or some other authorization protocol—and the authorization and resource servers. This transaction is heavy in terms of necessary infrastructure to support the transaction, and also introduces multiple points along the verification path than can be exploited by attackers.

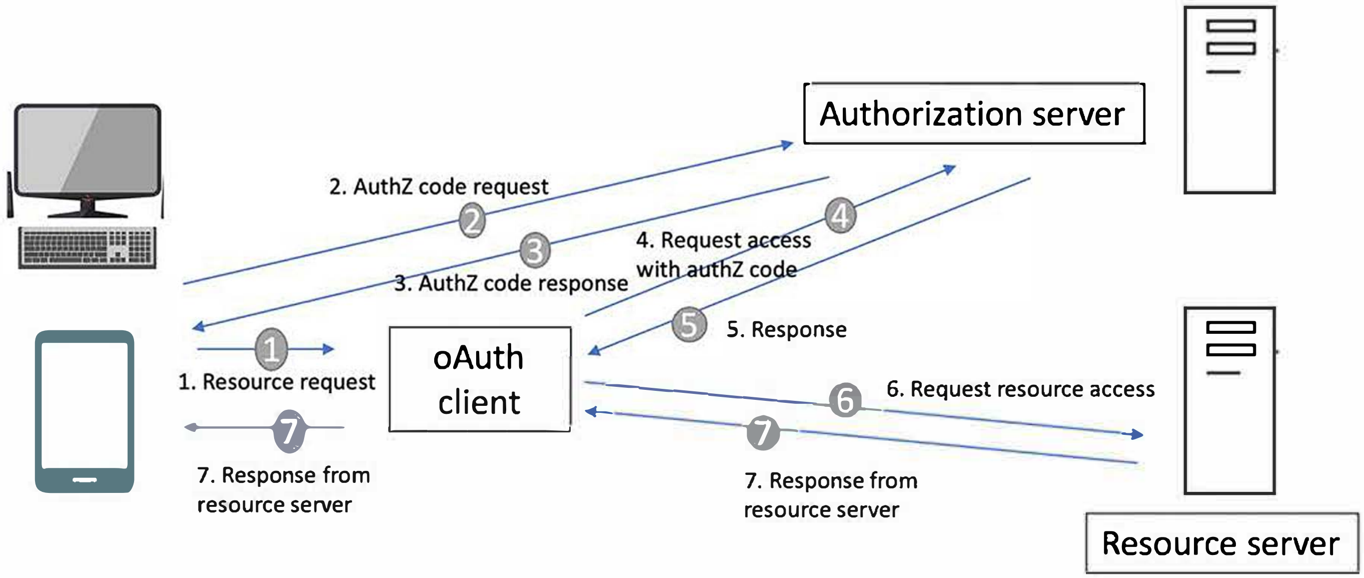

Authorization server
2. AuthZ code request
3. AuthZ code response
4. Request access with authZ code
5. Response
1. Resource request
oAuth client
6. Request resource access
7. Response from resource server
7. Response from resource server
Resource server

Figure 1. Traditional Authorization

And though traditional authorization is effective for system to system transaction requests, it is only effective once a human has initiated the request. For example, let's say Sally is applying for a mortgage on a new home. Sally must interact with her agent and the bank/lender to request the transmission of multiple, sensitive financial documents and approvals between entities. In a traditional scenario, Sally, will call, email, or use an online portal/application to request the transaction. If Sally's bank is using MFA for authentication, there is some level of confidence that Sally is who she says is. Although, security practitioner know that certain forms of MFA are more easily hacked or spoofed than others.

What authentication-based MFA does not double check, however, is the authorization piece. The bank's systems may be set up to ask Sally if she's "sure" she wants the transaction to occur, but all of that verification is done on the system to which Sally, or "Sally" is authenticated. There is no mechanism by which the system can externally verify Sally's authorization for the transaction to occur—no parallel second-factor of authorization, and thus no way to ensure the prevention of fraudulent transactions.

How does it work?

In contrast, MFAz—multi-factor authorization—provides an off-system functionality by which the bank can authenticate Sally's authorization to digitally transfer sensitive documents to her agent. It is a third-party mechanism through which the bank can positively affirm that Sally is making the specific request (since they can't see or hear her in person) and the process in which Sally can have confidence that the bank won't execute transactions on her behalf without explicit and cross-checked approval.

One might argue that MFA is confirmation enough, since traditional MFA is meant to ensure Sally is who Sally says she is. However, numerous breaches involving stolen identities have shown us that MFA isn't always a foolproof way to prevent fraud. One reason for this is that traditional authentication-based methods rely on the channel being secure once identity is established. Many channels are subject to interception and hijack (such as man-in-the-middle (MitM)). Chat, email, text, and requests passing through third parties are examples

When dealing with the digital transfer of hypersensitive information and/or funds, it is especially important to corroborate that the request, itself, is proven legitimate, as well as the identity of the person making the request.

Like with multi-factor authentication, when an authorization request for a digital transfer is received by an institution, the institution sends a request back to the user/customer for a one-time code. Unlike MFA, with MFAz, the code is generated through an application on the user's device—computer, tablet, or smartphone. The code is generated locally, thus it doesn't have to traverse servers, thereby reducing the risk of interception. The details of the transaction are embedded in the code and securely shared with the institution after the user/customer approves the transaction. Optimally, each code should include a time restriction and be single use, decreasing the window of opportunity for exploit should a threat actor somehow intercept transmission.

Every action—from request by the customer to the institution and back—should be encrypted and digitally signed.

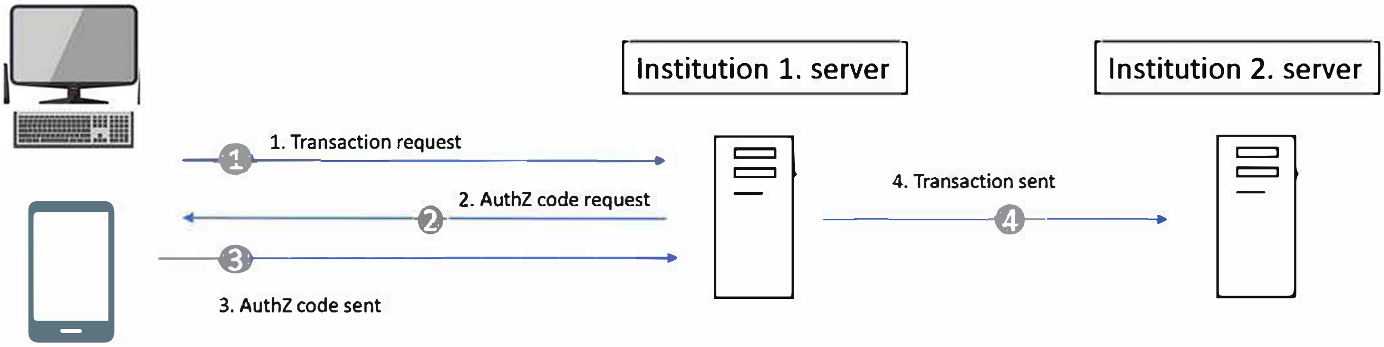


Figure 2. Multi-factor authorization architecture

Why is MFAz necessary?

The Federal Trade Commission (FTC) reports that the Consumer Sentinel Network, a secure online database that stores consumer complaints, received over 3.2 million reports in 2019. Complaints of fraud comprised 53% of all reports and identity theft comprised an additional 20% of reports. Twenty-three percent of complaints reported monetary losses. Median individual losses reported were highest in the categories of foreign money offers and counterfeit check scams, mortgage foreclosure relief and debt management, and business and job opportunities. Wire transfers of funds were the most frequently reported method of fraud, totaling an aggregate loss of $493 million USD.[i] Furthermore, since Sentinel was launched in 2001, number of fraud and identity thefts has increased every year except for a slight dip in 2017.

It's easy to see the correlation between online activity and fraud; steadily since 2001, mobile devices have become more powerful and functional and are now the non-work device of choice for conducing all types of online activity. As consumers have adapted their lives to a mobile world, greater numbers of transactions occur digitally. Today, it's almost expected that people can manage their lives from their mobile devices, from anywhere. This digital transformation has thus increased the digital attack surface. And with consumer device security lagging behind corporate security—where certain controls can be enforced regardless of consumer preference—adversaries have the opportunity to exploit insecure devices, people's trusting nature, busyness, stress, and more.

Authentication—verifying that Sally is who she says she is—was the first effort to reduce stolen identities and limit unauthorized transactions. Though AuthN usage has improved over the years, it is still not ubiquitous across logins and methods for AuthN MFA continue to focus on "frictionless" experiences. In other words, the lower the annoyance factor to consumers, the more likely they are to use MFA.

SMS text codes are the most popular method of MFA today, but server-/app-generated credentials are vulnerable (as illustrated above) and we've seen numerous instances of attackers exploiting SMS and thus identity to commit fraud.[ii] Challenge questions, another mechanism (which are, fortunately, seeing a decline in usage) are also easily exploited by attackers who can easily uncover personal information via social networks and online databases like Appllo.io, instantcheckmate.com, Spokeo.com, and others.

Further, MFA doesn't yet have the ubiquity it needs to adequately protect people's identities; MFA is often "opt-in" rather than set by default, which has led to countless account compromises.[iii] While MFA adoption increases every year, consumers are less likely to opt in when they cannot see the tangible benefits of doing so. A consumer might not worry if their email address is leaked online—almost everyone's email address is available somewhere on the web. However, especially when it comes to consumer-initiated financial transactions, the pain threshold is much lower. The prospect of having money lost or stolen from accounts; being denied a mortgage, a government issued ID, or healthcare; not being able to establish a line of credit or file taxes—these are scenarios that would immediately negatively impact people's lives and continue to do so for years to come. It's easy to explain that importance of implementing hardened authorization controls for these types of transactions.

MFAz augments MFA by putting authorization control into the hands of the data subject and account holder—the consumer or customer—providing assurance that fraud cannot be so easily perpetrated.

Benefits

Multi-factor authorization has the benefit of low user friction: there are no passwords to remember, no challenge questions to answer, and there is no delay in the transaction process. When an institution is using MFAz for client transactions, once the MFAz app is installed on the user's device (which can be embedded in the institution's mobile app or offered via an app store), as soon as the user requests a transaction, all they need to do is supply the generated code to the authorizing entity.

This puts the user in control of their transactions and avoids reliance on less-secure methods and channels of verification. From the business point of view, the company increases security for the authorization of transactions, thereby reducing liability and the potential for unsatisfactory customer experiences.

More tangibly, perhaps, businesses can immediately reduce capital expenditures (CapEx) for infrastructure used to support the verification of transaction requests. Authorization codes initiated via an app and generated client-side scale more easily because of the distributed model, and they work across channels without any development on the business side. All details of the customer's identity and authorization request are contained within the app, not the organization's servers or databases, thus the management burden on the business are reduced, saving already-stretched security teams time and effort.

Use Cases

Financial

The most obvious use case for MFAz is around financial services—instances when a consumer needs to transfer personal, sensitive information and/or money to/from accounts. Even small money transfers often require sharing information beyond bank details or account numbers. Social Security Numbers, residential addresses (including past residences), and employment information might be part of those transactions. Unauthorized access to this level of knowledge could result in life-altering fraud for individual for many years. An exploited individual could lose money, be denied loans or credit, see credit scores plummet, have their identity stolen, incur tax debt as a result of a fraudulently filed return, or even lose job opportunities if background checks return tampered or inaccurate reports.

Fraud and identity theft also take an emotional toll on individuals. The FTC's report on the aftereffects of identity theft[iv] shows that victims commonly experience severe distress, frustration or annoyance, rage or anger, insecurity about personal or family members' finances, a sense of powerlessness/helplessness, feelings of betrayal, and a loss of ability to trust.

Given the severity of detrimental repercussions resulting from identity theft, financial institutions must consider how to add extra layers of security to the information request process. One such action includes adding a second factor of verification on information access, sharing requests, and transaction confirmations through multi-factor authorization.

Customer service

It's no secret that the number of consumers buying and researching products and services online has grown exponentially since the turn of the century. Since 2000, the number of online shoppers has doubled.[v] With the COVID pandemic reshaping our world starting in early 2020, data suggests that U.S. e-commerce advanced more than 30% in the first half of the year alone,[vi] more than doubling previous years' trends.

In addition to e-commerce, more businesses offer online experiences than ever before; from healthcare to banking to hospitality, it's not just the exchange of money for goods and services that requires secure, private interactions. Many companies use live online chat for customer service or have built their own proprietary portals through which customers and staff can exchange information about appointments, account information, or other related needs. For these communications, customer service professionals often need permission to access customer accounts, which can include sensitive information like account numbers, financial data, and PII. Today, many businesses will require a one-time authorization code to gain permission and further conversations, and these are typically sent via text or email, which, as previously mentioned, can be hijacked or spoofed by attackers.

The use of a client-side generated authorization code for authorization ensures that attackers cannot MitM the transaction and usurp the session. Even if the attacker has gained access to the consumer's email or text, they cannot generate an MFAz authorization code and therefore cannot authorize the customer service agent to access the target records.

Government IDs

Similarly, agencies which allow consumers to apply for or renew government identification online must consider the positive benefits of adding MFAz to their processes. Ironically, to obtain state/federal issued identity documents, an individual must present alternative forms of identity verification. Many of these entities allow consumers to simply upload photos or scans of these documents online, but if a fraudster already has access to these documents, or can intercept the traffic between the browser and the institution's server, there is only a small chance that that transaction will be flagged as compromised. Instead, government agencies could implement secure transfer between entities using a multi-factor authorization system that must be approved by the consumer (after they're authenticated using traditional MFA), thereby increasing security controls for access and diminishing the probability of fraud.

Health records

Another prominent use case is for access to health records. HIPAA limits access and unauthorized sharing of patients' health records, however, the language around use is somewhat permissive[vii]:

- *Only you or your personal representative has the right to access your records.*
- *A health care provider or health plan may send copies of your records to another provider or health plan only as needed for treatment or payment or with your permission.*
- *The Privacy Rule does not require the health care provider or health plan to share information with other providers or plans.*
- *HIPAA gives you important rights to access your medical record and to keep your information private.*

Patients must sign off on the transfer of their records between health provider(s) and insurer and amongst providers, for instance. In most cases, patients are asked to sign off on a blanket sharing request for almost all of their data versus only the relevant parts. This is due to the complexity of managing entitlements, but opens up another layer of vulnerability. In addition, unless the permission is granted in person, current practices typically require only an acknowledgement on a web page or in a web form—without any second factor of verification—for that transfer to occur. Once again, if a cyber criminal has illicitly accessed a patient's account by stealing credentials or intercepting web traffic, they can illegally authorize a transfer.

While this scenario may seem far-fetched and high-effort on the part of the attacker, it is important to remember that health records command a higher price on the dark web than other types of records and are thus quite attractive to malicious individuals.

Device manufacturers

The final use case we will note in this report is for device manufacturers to embed the technology or include it as a free option in app stores. Authenticators such as those from Google, Microsoft, and Authy have become popular due to the ease with which they offer enhanced MFA. Adding MFAz as another layer would encourage adoption and, when used, significantly reduce the risk of fraud. Given that fraud is continually increasing—with no signs of a slowdown in the future—this feature would be an attractive consumer benefit which also aids corporations when they opt in.

The consequences of dealing with fraud, stolen identities, and breached documents are not relegated to consumers, alone. The financial impact of consumer identity theft to businesses is in the double-digit millions of dollars. In addition to immediate financial losses, business fraud can devalue a company, result in legal/compliance issues, ruin a company's reputation or internal culture, and in extreme cases, land executives in jail. Then, of course, there's the cost of a data breach; the most recent Ponemon Institute *Cost of a Data Breach Report 2020*[viii] calculates the average cost to business as $3.86 million USD. This cost could be untenable for a small- or medium-sized business and cause material impact to a larger one.

These are not mere line item expenses and, as such, businesses must take a hard look at how to reduce the risk of unauthorized access of sensitive information pertaining to the access and transfer of private, personal documents.

Another option, needless to say, is for the adoption and offer of MFAz technologies on a business-by-business case. However, a piecemeal approach will be slower and the coverage spottier than if it is offered ubiquitously, like with Google Authenticator et. al.

Conclusion

Multi-factor authorization is not yet a well-known concept, nor has it seen widespread adoption. Nonetheless, MFAz is an important technology which has the potential to drastically reduce fraud, identity theft, and data breaches pertaining to document and information transfer. MFAz puts controls over personal information into the hands of the consumer and does it in such a way that security is increased without creating appreciable friction.

Both businesses and consumers will benefit from the enhanced security afforded by a second factor of authorization for transfer requests. While some security experts may argue that MFAz is unnecessary if both authentication and access controls are configured correctly, we have not reached a point where those controls are hardened enough or deployed correctly enough to prevent the mis-sending or unauthorized access to and transfer of documents.

As more personal and business transactions occur online, and as greater numbers of individuals work from home, potentially on unsecured devices and over insecure internet connections, it is imperative that authorization controls are adapted. MFAz has the capability to be this new control used by both consumers and businesses.

[i] https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-2019/consumer_sentinel_network_data_book_2019.pdf

[ii] https://www.wired.co.uk/article/sms-hack-text-twitter-j3ws3r; https://www.forbes.com/sites/zakdoffman/2019/11/03/chinese-hackers-just-gave-us-all-a-reason-to-stop-sending-sms-messages/#15f5a7278c12

[iii] https://www.tag-cyber.com/advisory/articles/trump-twitter-hack-shows-password-policies-yet-again-lacking

[iv] https://www.ftc.gov/system/files/documents/public_comments/2017/10/00004-141444.pdf

[v] https://www.pewresearch.org/internet/2008/02/13/part-1-trends-in-online-shopping/#:~:text=Today%2C%20e%2Dcommerce%20accounts%20for,from%200.8%25%20in%20early%202000.&text=As%20noted%2C%20the%20number%20of,has%20doubled%20since%20mid%2D2000.

[vi] https://www.emarketer.com/content/us-ecommerce-growth-jumps-more-than-30-accelerating-online-shopping-shift-by-nearly-2-years

[vii] https://www.hhs.gov/hipaa/for-individuals/medical-records/index.html

[viii] https://www.ibm.com/security/data-breach

TAG CYBER

Developing an RFP for Attack Surface Management

This TAG Cyber analyst report provides guidance on the requirements necessary to properly solicit good attack surface management proposals from commercial vendors.

Prepared by

Edward Amoroso
Lead Analyst, TAG Cyber
eamoroso@tag-cyber.com

Introduction

In this report, we focus on a new area of enterprise cyber security called *attack surface management (ASM)*. While this category is still somewhat evolving, commercial ASM solutions are typically designed to address the zero trust nature of modern, de-perimeterized enterprise IT and network infrastructure. They typically include the functionality required to discover and manage risks to the *external* attack surface of an organization.

ASM solutions have become especially attractive to enterprise teams in recent years as organizations have experienced accelerated IT and network infrastructure sprawl beyond their traditional firewall boundaries. This expansion includes dramatic increases in computing dependencies on cloud-hosted services, social media networks, SaaS-based applications, third-party service support, and public internet-based systems.

The good news is that excellent commercial vendors exist to support this important new ASM security control[1]. Enterprise buyers can either research locally or engage an expert team to assist in developing a suitable shortlist of suitable providers of ASM solutions[2]. To assist in this process, we offer a set of recommended requirements below to serve as a base for enterprise *request for proposal (RFP)* documents.

ASM Framework

An attack surface management framework was created by TAG Cyber to develop RFP requirements in a manner that would simplify tailoring by an enterprise. The framework model is sufficiently general to cover most aspects of ASM protection, but also specific enough to differentiate ASM from other types of enterprise security solutions from commercial vendors. The salient aspects of the framework are illustrated in Figure 1.

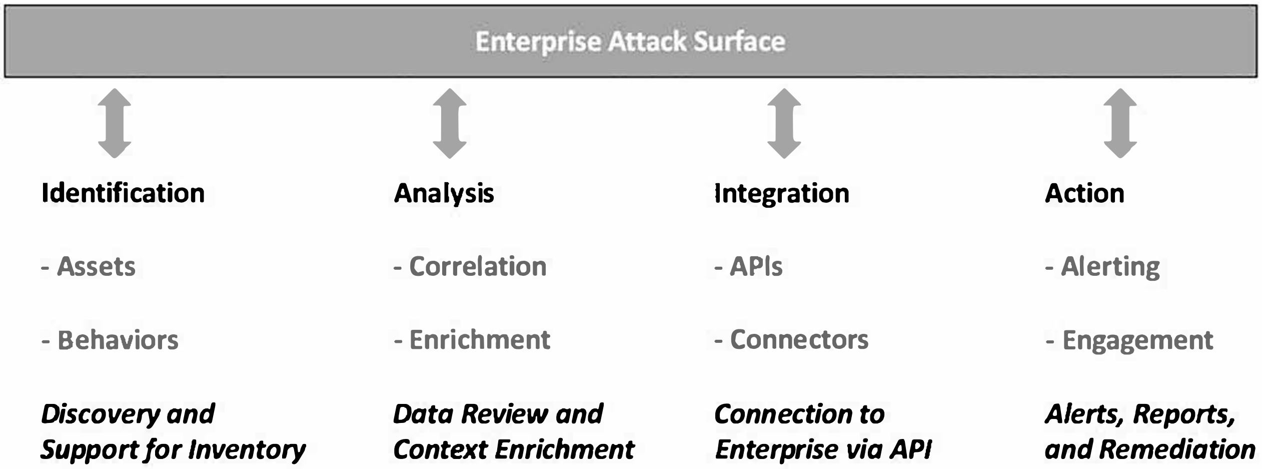

Enterprise Attack Surface
Identification
- Assets
- Behaviors
Discovery and Support for Inventory
Analysis
- Correlation
- Enrichment
Data Review and Context Enrichment
Integration
- APIs
- Connectors
Connection to Enterprise via API
Action
- Alerting
- Engagement
Alerts, Reports, and Remediation

Figure 1. Framework for ASM Enterprise Protection

[1] TAG Cyber benefited considerably from guidance and review from the commercial technical and marketing team at Expanse during the writing of this document. That said, the set of requirements included here should generalize to any ASM RFP under development by an enterprise team.

[2] TAG Cyber provides this type of commercial vendor research and advisory service for enterprise security teams. Information can be obtained at https://www.tag-cyber.com/.

The four components of enterprise attack surface management include identification, analysis, integration, and action based on discovered assets and behaviors. Analysis is performed using correlative and enrichment algorithms, with integration to the enterprise via APIs and connectors to tools such as SIEMs and service management tools. Actions are focused on alerting the enterprise and engaging proper remediation.

Draft RFP Requirements

The draft ASM request for proposal (RFP) is written below in a formal enough manner for cut-and-paste by source selection teams[3]. Nevertheless, enterprise team are advised to ensure legal, policy, regulatory, contractual, and procurement review by experts with attention to coverage, treatment, and wording. These requirements represent best-effort suggestions from TAG Cyber based on the framework model in Figure 1.

Section 1 – Identification

The ASM offering shall support identification and inventory of ACME global attack surface assets via the following:

1.1 Discovery
Automated discovery of ACME assets publicly exposed to the Internet.

1.2 Inventory
Inventory of ACME virtual and network assets that are publicly exposed to the Internet.

1.3 Visibility
Visibility into ACME virtual and network assets including public cloud (including Azure, GCP, and AWS), ISP networks (including AT&T, Verizon, and Comcast), shadow and rogue IT services not being monitored by ACME, networks of subsidiaries, joint ventures, suppliers, and other entities supporting ACME, and applicable IPv4 address space.

1.4 Independence
No input, deployment, agents, or software installations from ACME during deployment or use.

Section 2 – Analysis

The ASM offering shall support analysis of discovered and managed ACME attack surface assets and behaviors via the following:

2.1 Accuracy
Attribution on a broad range of information (versus just using registration records).

2.2 Alerting
Alerting on asset appearance and disappearance via email, API-based notification, and SIEM integration.

2.3 Update
Update and refresh of all data and notifications on at least a daily basis.

[3] The platform being considered for purchase is referred to as the "ASM offering" and the procuring enterprise is referred to as "ACME."

2.4 Sprawl
Visibility into asset sprawl including certificate issuers, domain registrars, and cloud providers.

2.5 Stale IP
Identification of stale IP registration including IP registration records that should be updated to reflect ownership by a different organization so that registration information can be kept current.

2.6 Expiration
Forecast of asset expiration to include certificate and domain registration expirations.

Section 3 – Asset Coverage

The ASM offering shall include coverage of attack surface assets as follows:

3.1 Coverage
Inclusion IP ranges, domains, certificates, HTTP services, video services, databases, email, file transfer, and remote access services.

3.2 Validation
Protocol validation versus just detection of open ports.

3.3 Devices
Inclusion of multiple device types including building control systems, data storage devices, embedded systems, network infrastructure, collaboration devices, and VPN devices.

3.4 Cryptography
Identification of cryptographic weaknesses such as expiration, self-signed certificates, short public keys, long expirations, wildcard and domain validated certificates.

3.5 Prioritization
Prioritization of risks based on flexible severity levels in order to triage issues based on ACME security policies and best practices.

Section 4 – Behavior Coverage

The ASM offering shall include coverage of attack surface behaviors as follows:

4.1 Communications
Detection of communications to and from ACME's network to meet customizable risk or compliance criteria.

4.2 Flows
Detection of inbound flow to exposures on ACME perimeter, outbound flows from ACME servers, inbound and outbound connections to TOR, evidence of cryptographic mining, and outbound flows to devices with self-signed certificates.

4.3 Enrichment
Context enrichment of flow alerts with active scan data.

4.4 Filtering
Filtering out of low importance behaviors such as broad Internet scanning.

4.5 Policy
Assurance that network communications policies are being consistently applied across all parts of the ACME network and that monitoring is comprehensive.

Section 5 – Integration

The ASM offering shall support integration of attack surface-related information with ACME systems and tools as follows:

5.1 Exports
Exports of all discovered assets, risks, and behaviors to ACME via structured format such as CSV.

5.2 APIs
Support for RESTFUL APIs to ensure data is consumable by ACME for correlation with internal, on-premise data sources for context and remediation.

5.3 SIEM
Integration with ACME SIEM via connectors to support correlation, triage, alerting, visualizing, and data enrichment.

5.4 Service Management
Integration with ACME service management tool via connectors to support more rapid opening, tracking, and verifying closure of tickets.

5.5 Hunt and Response
Integration with ACME threat hunting and incident response tools via connectors to support defensive threat hunt and incident response producing actionable leads based on indicators of compromise (IOC).

5.6 Scanner
Integration with ACME scan tools via connectors to increase scan coverage and accuracy by including external attack surface data.

5.7 Cloud Accounts
Integration with corporate controlled cloud accounts including shadow environments.

5.8 Threat Feeds
Ability to ingest custom datasets and threat feeds to enhance coverage and improve alerting.

5.9 Custom Integration
Integration of ACME-defined services, devices, or infrastructure through engineering and development support.

Section 6 – Action

The ASM offering shall support attack surface-related actions including reporting, remediation, and engagement as follows:

6.1 Reports
Alerting on asset appearances and disappearances to triage new issues on ACME's attack surface as they are detected to reduce the time window for remediation if necessary.

6.2 Progress
Remediation progress tracked through risk statuses and notes to visualize ACME's progress toward reducing the attack surface.

6.3 Briefs
Support for executive briefings, peer benchmark reports, and operational reports to help ensure ACME understanding and awareness of Internet-facing risks and closure of audit issues.

6.4 Removal
Support to remove assets when needed including rapid update of ownership changes for any asset attribution problems.

6.5 Divested Assets
Assurance that ACME has properly divested that might remain comingled with ACME.

6.6 M&A Targets
Insight into M&A target external attack surface.

6.7 Suppliers
Insight into select ACME supplier target external attack surface.

6.8 Joint Ventures
Insight into select ACME joint venture target external attack surface.

6.9 Engagement
Dedicated engagement manager support to partner with ACME to operationalize data for immediate time-to-value with quick wins and long-term integration to support process improvement.

TAG CYBER

Using Continuous Security Testing to Support Digital Transformation

This TAG Cyber analyst report makes the case that continuous security testing is an essential component of enterprise digital transformation. Its primary value comes from the enablement of business process automation through the prevention of disruptive cyber threats.

Prepared by

Edward Amoroso
Lead Analyst, TAG Cyber
eamoroso@tag-cyber.com

Introduction

Corporate executives are now focused on *digital transformation* to integrate technology into all aspects of their business. This objective might seem obvious and even redundant with modern organizational practice, but the fact is that many businesses continue to operate using legacy methods that are manual, slow, and error prone. Digital transformation seeks to improve these areas through automation.

Success at digital transformation requires nurturing a culture that encourages employees to challenge the status quo. Enterprise teams must be guided to explore new ways to use technology – and that if failures occur, they are accepted as lessons learned that move the organization toward its goal. The result is that long-standing business approaches are replaced by new methods introduced in an agile and continuous manner.

One aspect of digital transformation involves renewed attention to *cyber security*. Where businesses might previously have tried to avoid exploits in a non-technical manner, perhaps by training employees or imposing penalties if they violate security policies, digital transformation instead highlights the need for security platforms that can prevent disruptive cyber attacks via combination of human and automated support.

This paper explains how enterprise teams can integrate a new cyber security method called *continuous security* testing into digital transformation. Our advice is framed in the context of hours of research into and ongoing conversations with commercial security vendors and enterprises building and using various forms security testing, respectively.

General Questions on Digital Transformation

What is digital transformation, exactly, and how is it supported in a typical enterprise?
TAG Cyber researchers have found through interviews and discussions with technology, business, IT, and security leaders[1] that digital transformation is real in the enterprise, but often not uniformly supported. In fact, TAG Cyber's research suggests that digital transformation initiatives fall into two distinct categories:

- *Cultural Transformation:* Some digital transformation programs are led by teams of strong executives, usually including the CIO, who drive change based on cultural transformation with an aggressive plan to enable deep improvement in how technology can reduce cycle times, remove friction for users, and increase security.
- *Transactional Focus:* Other digital transformation programs, in contrast, are not designed to drive cultural change, but instead address automated enhancements in a more transactional manner, with review and acceptance of each proposal on a case-by-case basis.

[1] TAG Cyber is a New York-based research and advisory firm founded by Dr. Edward Amoroso, retired SVP/CSO of AT&T, that works with hundreds of companies each year – including commercial vendors, enterprise teams, and government agencies – to advise on their cyber security initiatives, platform features, go-to-market approaches, and other aspects of their IT, technology, and security program. Detailed information is gathered from this work and used to inform TAG Cyber customers privately. Information on digital transformation initiatives has been gathered and interpreted based on this on-going work.

The key difference between these two approaches to digital transformation programs is the decision (or not) to make *cultural changes regarding use of technology*. One large bank, for example, explained to the TAG Cyber analysts that they have empowered all of their IT team members to make changes to any process that will introduce digital technology to reduce cost or cycle time, even if this requires a short-term investment.

In contrast, when digital transformation is addressed more transactionally, team members will generally feel less empowered to fully embrace all possibilities to take full advantage of digital technology. The transactional approach does reduce the risk of poorly executed digital transformation execution cascading across the enterprise, which is why many management teams select this approach.

What research has been published on the success rates for digital transformation initiatives?
Several excellent research compendiums are available that help modern business managers and executives understand the opportunities and potential pitfalls of digital transformation initiatives. One of the better research studies on this topic was published by McKinsey and it includes statistics that are sobering with respect to digital transformation projects[2]. The research includes the following startling findings:

- *Overall Industry Success* – Less than 30% of digital transformation initiatives are described as successful by their managers.
- *Digital Industry Success* – The rate of reported success in industries such as technology and telecommunications does not exceed 26%.
- *Traditional Industry Success* – The rate of reported success in automotive, oil and gas, and infrastructure is between 4 and 11%.
- *Company Size Success* – Organizations with fewer than 100 employees are almost three times as likely to report success than companies with more than 50,000 employees.

Do enterprise buyers select commercial vendors based on their ability to support digital transformation?
They should – but this may not be uniformly true. The challenge, especially for enterprise security solutions, is that the senior executives often driving digital transformation initiatives are not the same as the engineers and practitioners making decisions about technology and security. This is especially true for new protections such as crowdsourced security testing which are likely to be curated by experts well-steeped in the details of the technology.

[2] The McKinsey 2018 research report on the success and failure of enterprise digital transformation initiatives is available for download at https://www.mckinsey.com/business-functions/organization/our-insights/unlocking-success-in-digital-transformations#. TAG Cyber often supports McKinsey under a consulting subcontract, did not participate in the study cited above.

This observation might seem inconsistent with the significant emphasis of many commercial vendor pitches regarding support for digital transformation. Informal surveys by TAG Cyber analysts suggests that over 30% of marketing materials presented to typical analysts include some mention of how the solution will advance digital transformation objectives[3]. Clearly, technology and security vendors seek to make the case that they support this corporate goal.

A key observation, however, is that few commercial vendors truly understand the practical challenges of digital transformation, especially in the area of cyber security. This can create a disconnect between the vendor's message and the actual needs of the enterprise. TAG Cyber analysts and consultants have observed two strategies that can help enterprise buyers determine how a security platform might actually assist in their digital transformation work:

- *Threat Avoidance:* Enterprise buyers should seek to understand how a given security platform will help to avoid threats that can be disruptive to digital transformation initiatives. Such prevention might be the most powerful means for security teams to demonstrate support for digital transformation from their selected security solution.
- *Cultural Change*: Enterprise buyers should demand information on how a given cyber security platform will help to guide the cultural changes required to trust the transition to automation required for digital transformation. This is also essential for security teams to convey to executive teams.

Who are the enterprise advocates for digital transformation – and does this include the security executives?
The primary advocates for digital transformation within an organization will always include the senior leaders, but this tends to imply varying degrees of digital savviness. The McKinsey study showed that roughly a third of surveyed companies designated an individual as Chief Digital Officer (CDO) to work with the CIO and CISO and this decision did improve success rates. Many organizations also engage consultants to assist with their digital transformation work .

TAG Cyber's research suggests that it is difficult to find CDOs who also have cyber security responsibility. In nearly one hundred interactions with enterprise teams, including consultation, coaching, and strategic support, TAG Cyber has not encountered a single case where the CISO reported into the CDO (or the reverse). Instead, the CDO – should one exist – is always in a separate organization from the security team.

[3] TAG Cyber analysts interview and review roughly 600 cyber security vendors and commercial providers of cyber security solutions each year. This on-going work provides unparalleled visibility and insight into the current methods being used in the cyber security industry to market commercial products and services.

[4] A 2015 published report from McKinsey provides a reasonable overview of the Chief Digital Officer (CDO) position. It is worth noting that cyber security is barely mentioned in the report which is available at https://www.mckinsey.com/business-functions/organization/our-insights/transformer-in-chief-the-new-chief-digital-officer.

[5] As one data point, TAG Cyber has a vibrant enterprise consulting business, but has never been engaged specifically to support the security aspects of a digital transformation initiative. Instead, security advancement is presented always in the context of specific objectives being driven by the leadership team, CISO organization, or Board of Directors – and this rarely, if ever, is connected to digital transformation KPIs.

Digital Transformation and Security

Does digital transformation normally include attention to cyber security?
In virtually every live engagement that TAG Cyber analysts have observed, coached, or served, the digital transformation initiative is initiated at the senior-most leadership level – often the CEO or CIO. Guidance is then passed down to the applicable business units, including the security team. This guidance is usually reinforced through key performance indicator (KPI) objectives, executive bonus and salary direction, and corporate strategy plans.

The result is that the primary sponsors for digital transformation will rarely be the enterprise security team leaders, including the CISO. This is important for enterprise security teams to understand, because digital transformation does not typically Of course, originate with their CISO but instead serves as an inherited initiative. This does not diminish the typical CISOs' willingness and eagerness to drive automation, but it does help place the initiative in context.

Of course, CISOs can be effective accelerators of digital transformation, and security should be at the forefront of all enterprise-wide initiatives. Furthermore, security must be embedded from the beginning into all digital transformation programs. The CISO has the great challenge of bridging the gap between the larger initiatives and the day-to-day work activities of an enterprise team, including for crowdsourced security.

Is the market converging on a common security solution for digital transformation?
No. Unlike companies like Salesforce who have become synonymous with customer relationship management (CRM), or even Trustwave (in their early days) who became synonymous with PCI-DSS compliance, no present enterprise cyber security vendor – or even segment – has become the industry leader in supporting digital transformation. As evidence, CDOs typically do not engage directly with security vendors.

Convergence for securing digital transformation has not occurred to date because the initiatives associated with digital transformation are so broad. Not only is this unlikely to change, it is also true that no general IT platforms or tools have converged to become synonymous with driving digital transformation. The situation is similar to initiatives focused on improving quality or improving net promotion scores. These require broad emphasis for success.

Have any security solution market segments properly aligned collectively to drive digital transformation success?
Not yet. Instead, many of the more capable enterprise cyber security vendors have individually published white papers and other material to map their solution to the tenets of digital transformation. Some common examples of enterprise cyber security vendors who have mapped their capabilities to digital transformation include the following:

- *Synack* – The TAG Cyber team spoke at length with Synack about how the specifics of *crowdsourced security* testing enables digital transformation.
- *Fortinet* – The Fortinet team maps digital transformation to their security-driven network (including SD-WAN) solutions.[6]
- *Imperva* – The Imperva team maps digital transformation to their data and web application security solutions.[7]
- *Netskope* – The Netskope team maps digital transformation to "security transformation" in the context of marketing CASB solutions.[8]

Strategy for Crowdsourced Security Testing in Digital Transformation

Why should enterprise teams seek commercial security vendors who are focused on digital transformation?
Clearly, enterprise customers of commercial cyber security solutions include senior executive teams who are most likely being encouraged (or driven) to embrace a digital transformation strategy to reduce cost, improve customer satisfaction, and enhance product quality. Since these initiatives inevitably find their way from CIOs and CDOs to the CISO-led management team, digital transformation is clearly a visible issue in their day-to-day work.

Cyber vendors now recognize, however, that the lower level, more technical decision-making staff in charge of enterprise security will probably not be swayed by digital transformation messaging. In fact, the TAG Cyber team has observed that digital transformation emphasis on marketing collateral from a security testing or vulnerability management vendor are mostly viewed neutrally or even negatively by working-level staff.[9]

This also implies that security vendors should be encouraged by enterprise buyers to focus on two aspects of the digital transformation. First, they should offer platforms that truly help avoid disruptive attacks and increase trust in the automation being used to drive digital transformation – and second, they should offer learning collateral to help these enterprise experts communicate their support for digital transformation to the executive team.[10]

What is crowdsourced security testing and why is it important to digital transformation?
The process of crowdsourced security testing is a relatively new area of cyber protection for enterprise teams. It involves leveraging teams of vetted hackers targeting unstructured security testing efforts at a company's visible assets. The hackers are incentivized through bounty-based rewards to detect vulnerabilities which can then be reported to customers for their response and mitigation.

[6] The Fortinet report is available at https://www.fortinet.com/blog/industry-trends/simplifying-digital-transformation-with-security-driven-networking.
[7] The Imperva report is available at https://www.imperva.com/blog/secure-your-digital-transformation/.
[8] The Netskope report is available at https://www.netskope.com/es/blog/netskope-doubles-down-on-security-transformation.
[9] During the course of this research, the author raised this point to three working-level enterprise security practitioners (all three at least one level down from the CISO), asking this: "If a crowdsourced security vendor approached you with a message related to digital transformation, how would you react?" Two said neutral, and one said negatively. It is important to note that none of these practitioners (all current TAG Cyber consulting clients) would have final budget say on this type of spend, but all would have technical input to the decision. None of the participants agreed to have their comments attributed in this report. Industries included telecom, technology, and package delivery.
[10] This TAG Cyber note, developed in conjunction with Synack, represents exactly the type of learning collateral that will improve communication between security teams and executives regarding digital transformation.

Crowdsourced security testing is particularly well-suited to digital transformation because it targets exactly those digital assets deemed critical for success. These include internet-visible services and capabilities that extend an organization's footprint to its external ecosystem. The testing is also especially useful to digital transformation because it provides increased trust that hackers will not identify and exploit vulnerabilities to produce disruptive outcomes.

How does crowdsourced security testing directly support digital transformation initiatives?
The core enablement message from enterprise security teams to the business units and other leaders of the organization regarding the contribution of crowdsourced security testing to digital transformation should be designed around the following simple logic:

Enablement Messaging:
1. *Digital Transformation* automates critical processes
2. *Crowdsourced Security Testing* secures the systems supporting critical processes
3. *Crowdsourced Security* Testing is thus essential to *Digital Transformation*

How does crowdsourced security testing map to the important digital assets of an organization? Can a strategic framework be established?
The mapping should start with the blanket observation that cyber security threats are disruptive and even existential to digital transformation initiatives. That is, even if the digital transformation program is well-conceived, properly managed, and proceeding toward clearly defined goals, an intense cyber attack can subvert the entire process. This alone should justify the connection between cyber security and digital transformation.

The specific mapping from crowdsourced security testing must therefore include a risk-based assessment. It should clearly espouse that security risks exist to critical resources involved in digital transformation. Here is the logic behind the mapping to be used within the enterprise:

Risk Avoidance Messaging
1. The enterprise is focused on *Digital Transformation* initiatives
2. Security risk from exposed vulnerabilities can cause *Digital Transformation* to fail
3. *Crowdsourced Security Testing* is thus essential to *Digital Transformation*

DISTINGUISHED VENDORS

TAG CYBER

DISTINGUISHED VENDORS

1Q 2021

Working with commercial cyber security vendors is our passion at TAG Cyber. It's what we do every day – and during the course of a given year, we meet some really good ones. The vendors we connect with range from larger well-known companies, selling to a massive customer base, to smaller start-ups which might be transitioning from stealth to an early adopter stage.

A key consideration in evaluating vendors is their *purpose for- eing*. We've found in our many years of experience as practitioners and now analysts that average security solutions are a dime-a-dozen. What differentiates great solutions from average ones, however, is the driving force behind their creation. It's not an easy thing to preprogram: Solutions either comes from the founder's gut or they don't.

In all cases, however, when we meet a good vendor, we ask to dig in deeper. Typically, this involves multiple deep dive sessions with their technology team. This can include architecture reviews, product demos, and design discussions.

A small subset of the great vendors we meet choose to become part of our research and advisory program. This involves an agreement to let us inside their technology so that we can develop advisory notes in their area, create video content, and produce webinars – all with the direct participation of the vendor. This allows us to work with — and learn from — these world-class experts. It's great fun.

Part of the engagement is a detailed interview with these select Distinguished Vendors, and we include excerpted versions of these interviews in this volume for your enjoyment. We find these interviews to be quite enlightening, often providing color commentary not found in standard marketing material on vendors' websites, and worth the time to read an absorb. The advice and guidance from these experts can help with your own planning and day-to-day work in cyber security.

Below is a list of the 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.

TAG CYBER DISTINGUISHED VENDORS

1Q 2021

accurics™

Accurics enables self-healing cloud native infrastructure by codifying security throughout the software development lifecycle. The company's products programmatically detect, monitor, and mitigate risks in Infrastructure as Code to reduce customers' attack surfaces and prevent cloud posture drift before infrastructure is provisioned.

AGARI©

Through applied science, the Agari Identity Graph™ delivers business context to every email risk decision. Agari ensures outbound email from the enterprise cannot be spoofed, increasing deliverability and preserving brand integrity, and protects the workforce from devastating inbound BEC, VEC, spearphishing, and account takeover-based attacks.

ATTACKIQ

AttackIQ, the leading vendor of breach and attack simulation solutions, built the first Security Optimization Platform for continuous security control validation. AttackIQ is trusted by leading organizations worldwide to plan security improvements and verify that cyber defenses work as expected, aligned with the MITRE ATT&CK framework.

avanade

Avanade was founded as a joint venture between Microsoft Corporation and Accenture LLP. 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.

axis security

Axis Security simply and securely connects users to any application through one centrally managed service. The Axis Application Access Cloud replaces disparate and complicated secure access technologies such as VPNs, VDI and inline cloud access security broker services using a single zero trust platform.

AXONIUS

Axonius is the cybersecurity asset management platform that gives organizations a comprehensive asset inventory, uncovers security solution coverage gaps, and automatically validates and enforces security policies. By seamlessly integrating with nearly 300 security and management solutions, Axonius is deployed in minutes, improving cyber hygiene immediately.

CloudPassage

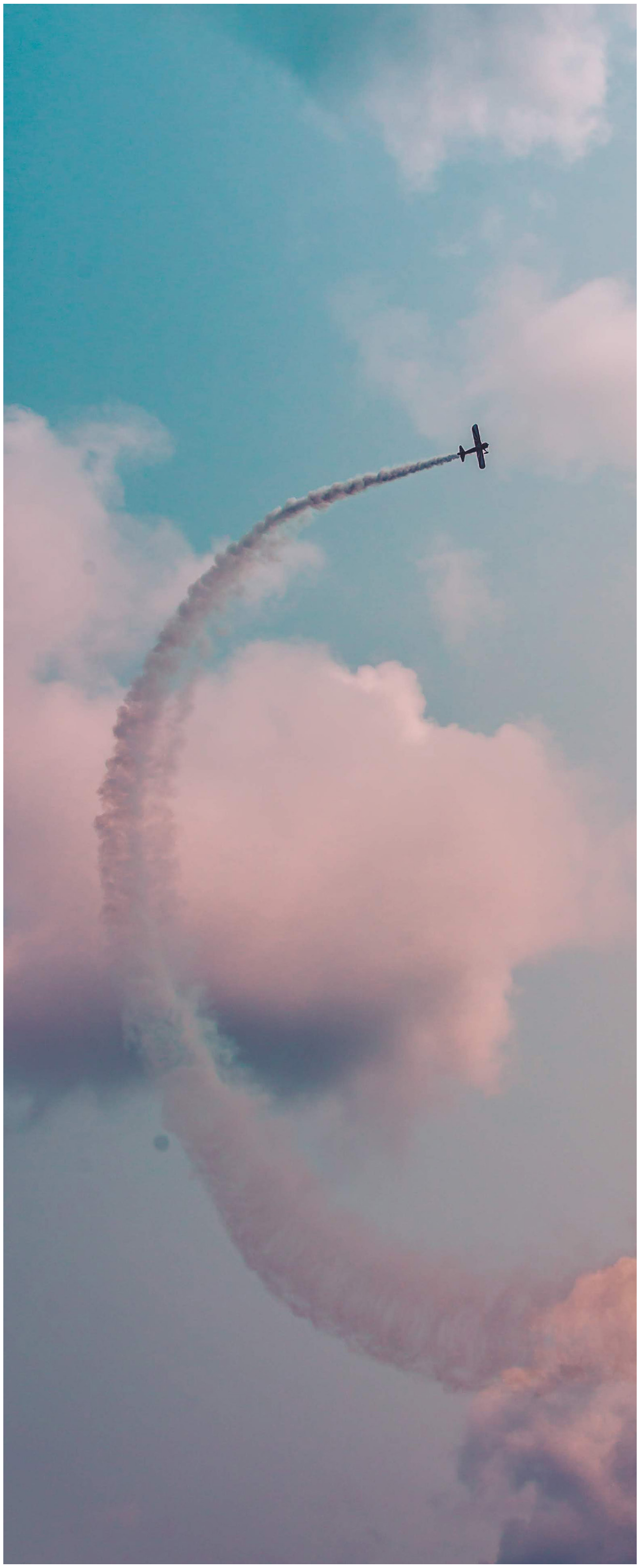
CloudPassage's Software-as-a-Service product is CloudPassage Halo, a unified cloud security platform that automates security and compliance controls across servers, containers, and IaaS resources in any public, private, hybrid, and multi-cloud environment. Halo's extensive automation capabilities streamline and accelerate.

Constella INTELLIGENCE

Constella Intelligence is a leading digital risk provider. Its solutions are powered by a combination of proprietary data, technology, and human expertise—including the largest breach data collection, with over 100 billion attributes and 45 billion curated identity records spanning 125 countries and 53 languages.

corelight

Corelight gives defenders unparalleled insight into networks to help protect the world's most critical organizations. Based in San Francisco, Corelight is an open-core security company founded by the creators of Zeek, the widely-used network security technology.



TAG CYBER DISTINGUISHED VENDORS

1Q 2021

Eclypsium helps organizations manage and protect devices for their distributed workforce, data centers, and networks, down to the firmware and level. The Eclypsium platform provides security capabilities ranging from basic device health and patching at scale to protection from the most persistent and stealthiest threats.

Endace's EndaceProbe Analytics Platform records a 100% accurate record of network activity, while simultaneously hosting third-party network security and performance solutions. The ability to integrate accurate network history into these solutions enables rapid investigation and resolution of network security and performance issues.

Kasada provides the only online traffic integrity solution that accurately detects and defends against bot attacks across web, mobile and API channels. Kasada restores trust in the internet by foiling even the stealthiest cyber threats, from credential abuse to data scraping.

NowSecure are the experts in mobile app security testing and services. Their platform provides comprehensive mobile app testing for security, compliance, and privacy risk vectors across 3rd party, custom, and business-critical mobile apps, with speed, accuracy, and efficiency.

TAG CYBER DISTINGUISHED VENDORS

1Q 2021

OKERA

Okera provides secure data access and governance at scale. The Okera Dynamic Access Platform automatically defines, enforces, and audits data access policies at the fine-grained level using an intuitive zero-code interface. Okera ensures data privacy compliance and that the appropriate data access policies are configured.

semperis

Semperis provides cyber preparedness, incident response, and disaster recovery solutions for enterprise directory services. Semperis' patented technology for Microsoft Active Directory protects over 40 million identities from cyberattacks, data breaches, and operational errors.

SEPIO SYSTEMS

Sepio Systems offers the first hardware access control platform that provides visibility, control, and mitigation to zero trust, insider threat, BYOD, IT, OT, and IoT security programs. Sepio's hardware fingerprinting technology discovers all managed, unmanaged, and hidden devices that are invisible to other security tools.

White Ops®

White Ops is a cybersecurity company that protects enterprises and internet platforms from digital fraud and abuse. The company verifies 10 trillion+ interactions per week, protecting customers' sensitive data, reputation, compliance, bottom line and customer experience as they grow their digital business.

TAG CYBER