TAG

Security Annual

2ND QUARTER 2024

IN FOCUS:

What Is the State of Cybersecurity Today?

ARTICLES / OPINIONS / INTERVIEWS

WHERE WE ARE NOW

DAVID HECHLER, EDITOR

So much attention these days is focused on the future, as we here at TAG are acutely aware. TAG Infosphere expanded our focus to include climate science last year. Researchers and entrepreneurs are straining to forecast our fate as our planet changes before our eyes. And we are with them.

If that weren't enough, TAG added artificial intelligence to our portfolio. You want to talk about hyperspeed? It can make your eyes water to watch AI advance at such an astonishing (some would say terrifying) pace. How do you keep up?

All of this makes returning to the here and now of cybersecurity a genuine relief. We decided to celebrate in the feature section of this Q2 Quarterly by doing a spot check: What is the state of cybersecurity right now? We asked our analysts to focus on whatever aspects felt most important and tell us what they see.

One writer noted that the reality is different for different constituencies in this fragmented environment. So she did three spot checks.

Another writer sees this moment as one that requires security professionals to adopt a new approach to cybersecurity. They must stop viewing it through the lens of technology and think of it as part of their company's business strategy.

Our CEO wrote an article that highlights the top 10 issues cited by our enterprise and government customers as the ones most important to them right now. And you probably won't be surprised if I add that he tells you what he thinks about each.

A fourth writer identified one problem that wasn't on our CEO's list. Too many cybersecurity programs are being over-managed and under-led. And that's because chief information security officers are too often managing instead of leading—and those functions are not the same.

Finally, our last writer opined that most people in the United States—meaning people who don't work in this field—view cybersecurity as a black box. They know it's dangerous. They know it can hurt them and their companies. But they're not getting information that helps them understand what they're supposed to do.

How about you? What do you see?

dhechler@tag-cyber.com

INTRODUCTION 2

FOCUS: WHAT IS THE STATE OF CYBERSECURITY TODAY? 5

The States of Cybersecurity
Joanna Burkey 6

Redefining Cybersecurity From Defensive Measures to a Strategic Business Strategy
David Neuman 9

Top 10 List for the State of Cyber in 2024
Dr. Edward Amoroso 14

Cybersecurity Leadership Versus Management
Al Palimenio 18

The Invisible Crime
David Hechler 22

INTERVIEWS 25

Shaping the Future of Workload Security
Kevin Sapp, Aembit 26

Securing Cloud-Native Applications
Gilad Elyashar, Aqua Security 29

Digital Protection for Executives & Families
Chris Pierson, BlackCloak 32

An Offensive Approach to Continuous Attack Surface Discovery
Seemant Sehgal, BreachLock 35

Modernizing Incident Response Practices
Matt Hartley, BreachRx 38

Elevating Security Validation: A New Approach
Nir Loya Dahan, Cymulate 41

Revolutionizing Cybersecurity with Hardsec
Adam Maruyama, Garrison 44

Exploring Cutting-Edge Security Automation
Cody Cornell, Swimlane 47

Cutting-Edge Access Security Solutions
Ev Kontsevoy, Teleport 50

Enhancing Enterprise Data Security
Brian Vecci, Varonis 53

ANALYST REPORTS 55

Apple and Google are Suppressing Innovation in Mobile App Security: Here is Why You Should Care 56

Hyperautomation for Windows Endpoint and Vulnerability Management: An Overview of the Aiden Solution 65

Empowering Leadership for Secure Innovation: Integrating Security by Design in Corporate Culture 70

Contextualizing Cyber Risk and Strategy in Business-Friendly Terms Using X-Analytics 78

DISTINGUISHED VENDORS 80

TAG EXCHANGE 83

TAG Cyber
Security Annual
1ST QUARTER 2024

Lester Goodman, Director of Content

David Hechler, Editor

Contibutors

Dr, Edward Amoroso
Joanna Burkey
Pete Dinsmore
David Hechler
Moriah Hara
David Neuman
Al Palimenio
John Rasmussen
Joe Sullivan
Jay Wilpon

Editorial & Creative

Lester Goodman
David Hechler
Jaimie Kanwar
Miles McDonald
Rich Powell

Research & Development

Matt Amoroso
Shawn Hopkins

Sales & Customer Relations

Rick Friedel
Michael McKenna
Laurie Mushinsky
Julia Almazova
Jane Mangiamele

Administration

Liam Baglivo

Dr. Edward Amoroso, Founder & CEO

Volume 10, No. 2

Publisher: TAG, a division of TAG Infosphere, Inc.,
45 Broadway, Suite 1250, New York, NY 10006.

May 1, 2024

IN FOCUS:

WHAT IS THE STATE OF CYBERSECURITY TODAY?

THE STATES OF CYBERSECURITY

JOANNA BURKEY

To get a real picture of the state of any given topic, it's common best practice to ask the experts. And there certainly are plenty of experts in cybersecurity to ask these days. In fact, just reference the other articles in this publication. But what about topics that are so far-reaching, so broad that they have a consistent and direct effect on an audience far larger than only experts? Cybersecurity is, without a doubt, one of these topics. It is difficult if not impossible to find anyone that is not in some way affected by this topic, so let's look at the state of cybersecurity from a few additional points of view.

We hear frequently that "perception is reality." And for three groups of people in particular, their perception of cybersecurity—and more importantly, their reactions in response—have a tangible and daily impact. These groups are: company employees, company officers and directors, and everyday citizens. The understanding of cybersecurity, and how understanding guides the actions of each of these groups,

can have an outsize effect on the success or failure of cyberattacks that are in motion at any given time. So what is the prevailing zeitgeist amongst these particular populations? And is there a single one, or multiple, co-existing mindsets?

COMPANY EMPLOYEES

Let's start with the company employee, quite often and truly referred to as the most important company resource. It's certainly inarguable that the actions of an enterprise's individual employees are one of the most important factors on the scope and impact of a potential cybersecurity incident. Knowing this, CISOs for years have attempted to create a more "cyber savvy" workforce through a variety of tools: cybersecurity training, phishing tests, tabletop simulations (just to name a few).

IT IS OBVIOUS TO ALL THAT ALLOWING AN UNAUTHORIZED, BADGELESS INDIVIDUAL INTO A SECURE BUILDING IS A THREAT, BUT TRANSLATING THIS EQUIVALENT INTO THE DIGITAL WORLD IS EXTREMELY DIFFICULT FOR ANYONE WHO IS NOT A TECHNOLOGIST.

So why are we still in a place where most employees don't feel particularly empowered or educated? In fact, the emotion they express most often about cybersecurity is that it is "frustrating." Frustrating in all senses—either the employee has to contend with technology intended to make them safer, but that instead just gets in the way, or the employee is relied upon to make good cybersecurity decisions without having any particular cybersecurity expertise. This situation can also be frustrating for the CISO. If it's so straightforward for employees to understand that letting someone tailgate into a building is bad practice, then why isn't there the same intuitive understanding of the ills of password sharing?

Technology has moved so fast, and, driven by digital transformation, taken over so many of our ways of working, that we now have large numbers of company employees who understand how to use the technology but not actually how the technology works behind the scenes. It is obvious to all that allowing an unauthorized, badgeless individual into a secure building is a threat, but translating this equivalent into the digital world is extremely difficult for anyone who is not a technologist. As the pace of technology adoption, and the exponential curve of digital complexity increase, it is becoming more and more critical to consider the employee experience. Too often, technology is adding complexity and creating impediments to the employee function. This has an adverse effect not only on security but also on employee productivity overall.

OFFICERS AND DIRECTORS

Moving on to a smaller subset of the broader employee population, let's look at the C-suite and, by extension, the board of directors. The high-level strategic decisions made by company leaders have the potential to dramatically influence the cybersecurity posture of any given enterprise. This fact is well understood. For some years now it has been impossible to avoid discussing cybersecurity and its criticality in the boardroom and at the CEO level. What has been more elusive is how to translate that criticality into appropriate action and oversight.

Board directors and C-suite members are no strangers to risk discussions. It's not overly dramatic to say that risk discussions are literally the lifeblood of what the senior executives discuss and decide on every day. However, these risk discussions usually occur in a common, business-centric lexicon and relate to

well-known topics such as the net present value (NPV) of a new project. Technology, and cybersecurity in particular, often bring their own jargon that can be difficult to put into analogous business terms. On the surface, the analogies between maintaining a fleet of company cars and maintaining a fleet of firewalls—software upgrades are like oil changes!—are obvious to practitioners but not obvious at all to business experts, who generally comprise the majority of board and C-level roles.

The outcome of this disconnect is the perception that cybersecurity is a new, strange animal when in reality it is business risk and opportunity in a different form. Without tech leaders and CISOs who can make that translation, the members of the C-suite and the board will continue to struggle to understand cybersecurity in relatable terms, impacting their ability to make optimum strategic decisions.

AVERAGE CITIZENS

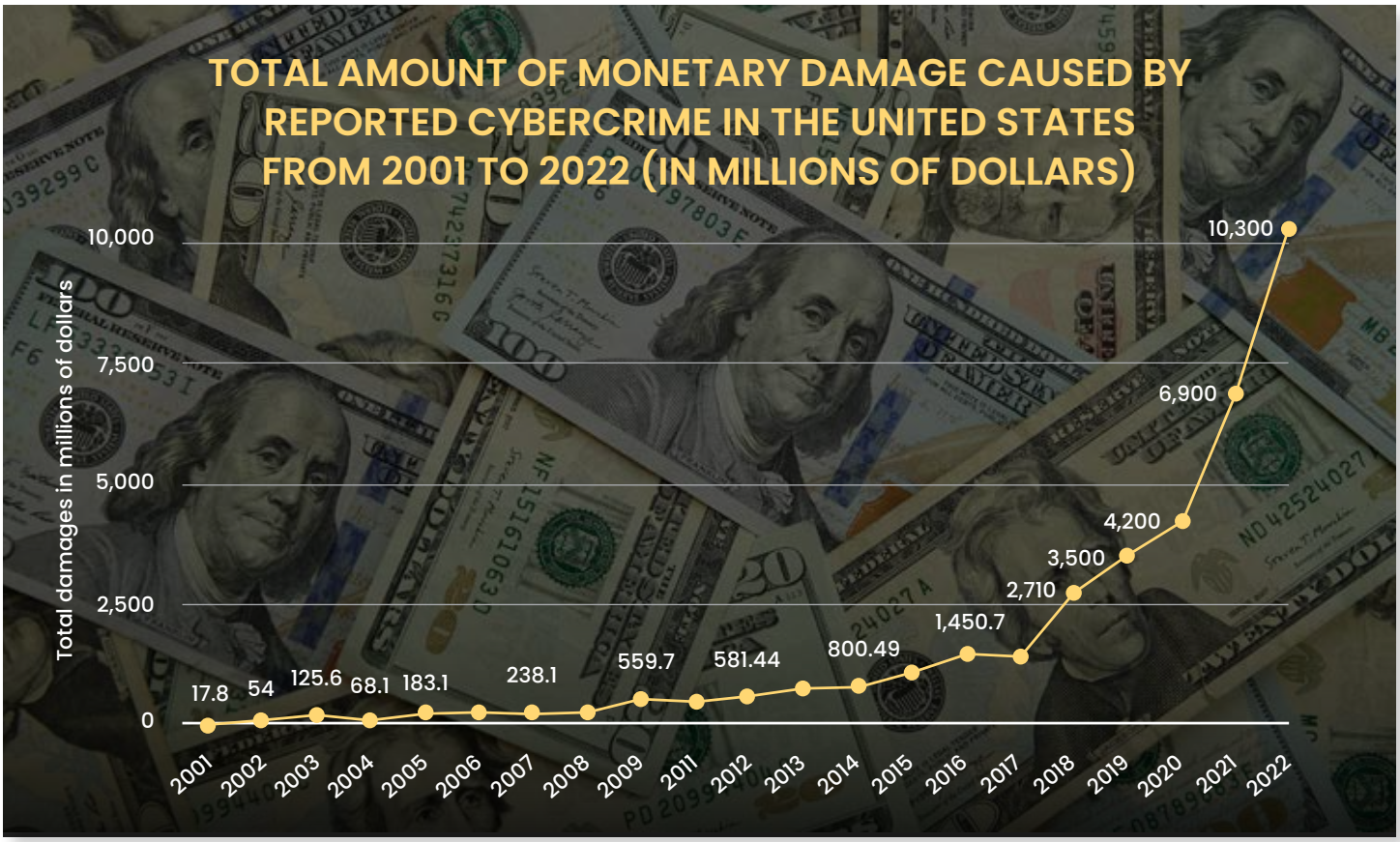
Now broadening the aperture, do we see similar states of mind in everyday citizens? Just as there's a disconnect between the 3D world and the digital world for the everyday worker, and between "business as usual" and cybersecurity for senior executives, we see people across society grapple with how to identify cyber threats and avoid joining the line of global victims. A similar analogy to the office tailgating example comes to mind. It is easy to understand how locking a door protects the house, or how putting a seat belt on protects the passenger in a car. It is extremely challenging for most people to intuitively understand what the equivalents are in the digital world to these basic protections.

The state of mind this has engendered is one of confusion, fear, and helplessness. When so much of life is digital, as it today, the effects of a cyberattack can be fundamentally destabilizing, if not life-threatening. The ability of average citizens to conceptually understand the digital tools that surround them, and then use that understanding to guide appropriate action, is not at the level needed for a "cyber-savvy" society. This can manifest, at one end of the spectrum, in extreme avoidance and mistrust of the digital ecosystem; and at the other end, in a complete reliance on the producers of technology to protect their user base.

THE BOTTOM LINE

In conclusion, there is no single "state of cybersecurity"—unless we want to posit that the state is one of fragmentation, with more opacity than clarity. Each population discussed here struggles to make parallels between their world as they know it, and how to avoid and/or mitigate cybersecurity threats.

While cybersecurity experts define and implement enterprise strategies, ultimately the bottom-line impact of cybersecurity on the lives of everyday people depends as much on those same people as it does on the experts. The ability to make good choices while living and working in the digital world will continue to require better conceptual models for understanding—and an increased focus on developing frictionless guardrails in the digital medium.



Source: Statista 2024

REDEFINING CYBERSECURITY

FROM DEFENSIVE MEASURES TO A STRATEGIC BUSINESS STRATEGY

DAVID NEUMAN

In 2022, the monetary damage caused by cybercrime reported to the United States' Internet Crime Complaint Center (IC3) reached a historic peak of $10.3 billion, which represented a year-over-year increase of around 50%. This is despite 2023 global spending on cybersecurity and risk management reaching $181.1 billion. It's projected to rise to $215 billion in 2024. Given these numbers, why aren't we seeing a reduction in the cyber threat or in the material damage to businesses?

As industries grapple with the escalating digital complexity, sophistication of cyber threats, and the cost of defeating them, the traditional stance on cybersecurity—primarily focused on defensive technical operations and compliance—is proving to be ineffective. It is imperative to have a strategic pivot towards viewing cybersecurity through the prism of business enablement and risk management.

This change is driven by the need to safeguard assets and business operations and harness cybersecurity as a catalyst for competitive differentiation in the marketplace. It highlights the pressing need for cybersecurity to evolve in purpose from a defensive, technical posture to a proactive strategy that aligns with and propels business objectives. Moreover, it emphasizes the necessity for technologies and processes that are both adaptive and swift, mirroring the pace of business innovation. Through this lens, we gain clarity on why cybersecurity must transcend its traditional boundaries and be reimagined as a core component of business strategy, enabling organizations to navigate the digital age with confidence and strategic advantage.

IF YOUR SECURITY BUDGET IS BASED ON CONTINUING INCREASES THAT ARE TIED PURELY TO ADDITIONAL COSTS FOR MORE TECHNOLOGY PLATFORMS VERSUS BUSINESS OUTCOMES, THEN YOU ARE LIKELY NOT PROVIDING A COMPETITIVE ADVANTAGE.

THE LEGACY MINDSET: A BUSINESS STRATEGY DISASTER

For too long, the prevailing approach to cybersecurity has been reactive. Too often products and services are designed with functionality as the primary focus, and security is bolted on as an afterthought. This leads to weaknesses attackers can exploit, resulting in costly redesigns, reputational damage, and potential fines for noncompliance.

"Security by design" means baking security into the development process from the outset. The alternative can lead to disaster. For example, a software company releases a new product with exciting features but fails to incorporate security. The product is riddled with vulnerabilities, leading to a major data breach that erodes customer trust and forces costly remedial efforts. We saw this recently in the attack against Microsoft Exchange Online. As reported by the DHS Cyber Safety Review Board, the breach was attributed to Chinese espionage and advanced threat actors who accessed U.S. government agencies involved in sensitive diplomatic issues with China. This suggests the problem affects enterprises and companies of all sizes. We can all do better.

Many organizations rely on static security architectures that are ill-equipped to handle the dynamic nature of today's business environments. An enterprise that relies on a rigid security architecture, if they have one at all, will struggle to adapt to the rapid adoption of cloud services and artificial intelligence, among other digital imperatives. This creates security blind spots, exposing the organization to new attack vectors and slowing growth.

If your security program or IT and product platforms have not adopted this approach under the guidance of experienced experts, then you are likely accepting significant business risk. On the other hand, if your company's architectures are flexible and can evolve alongside changes in technology, business processes, and the threat landscape, cyber resiliency can be a competitive advantage.

CYBER LEADERS AS BUSINESS LEADERS

Cybersecurity leaders often lack the business acumen needed to effectively communicate risks and justify security investments to business partners and corporate leaders. This disconnect can lead to underinvestment in cybersecurity and a failure to align security initiatives with broader business objectives. It's crucial to bridge this gap between technical experts and business leaders to have a deep understanding of business strategy.

TAG Infosphere tracks over 4,700 cybersecurity vendors in a taxonomy of 20 categories. In a recent conversation with a chief information security officer (CISO) of a large enterprise, I asked, "How many of these taxonomy categories do you have a a technology in? His response was, "All of them. In fact, I have as many as three technologies for some of them." We agreed that more tools do not mean better security and don't necessarily equal business enablement. Many CISOs are trapped in sustaining these large security ecosystems, making it difficult for them to adapt to business demands and contribute to the growth the company is trying to achieve.

1. APPLICATION SECURITY	11. IDENTITY AND ACCESS MANAGEMENT (IAM)
2. ATTACK SURFACE MANAGEMENT	12. SECURITY OPERATIONS AND RESPONSE
3. AUTHENTICATION	13. MANAGED SECURITY SERVICES
4. CLOUD SECURITY	14. MOBILE SECURITY
5. DATA SECURITY	15. NETWORK SECURITY
6. EMAIL SECURITY	16. OPERATIONAL TECHNOLOGY SECURITY
7. ENCRYPTION AND PKI	17. SECURITY PROFESSIONAL SERVICES
8. ENDPOINT SECURITY	18. SOFTWARE LIFECYCLE SECURITY
9. ENTERPRISE IT INFRASTRUCTURE	19. THREAT AND VULNERABILITY MANAGEMENT
10. GOVERNANCE, RISK, AND COMPLIANCE (GRC)	20. WEB SECURITY

TAG Cyber Taxonomy

If your security budget is based on continuing increases that are tied purely to additional costs for more technology platforms versus business outcomes, then you are likely not providing a competitive advantage. Nor are you addressing the business risks for your organization. As indicated above, many security programs have duplicative technologies performing highly similar functions. This means higher complexity, costs, and a demand for highly skilled people. The result may be the equivalent of a two-mile freight train going five miles an hour, unable to move or change at the speed of the business.

We are seeing rightsizing in the cybersecurity technology market, which indicates that many security organizations, especially those in large enterprises, are rationalizing their existing portfolios instead of buying more technology solutions. That is a step in the right direction. Still, the rationale must include more than the technological capability and extend to ensuring that the solutions map a path to business outcomes, and that talent development and growth are part of it.

THE PATH FORWARD: CYBER RESILIENCY AND TRUST AS STRATEGIC ENABLERS

If your organization is considering a real pivot, there are some things you should consider. No two organizations are identical, and there are no easy buttons, so it's impractical to suggest a common playbook. But some focus areas are a good starting point.

1. ESTABLISH SHORT AND LONG-TERM PLANNING.

Many organizations claim to do strategy when what they are doing is planning—for their own teams and business units. In some cases, this is understandable. It may be because the organization lacks a comprehensive strategy. But in most cases the security organization is unaware of the business objectives and how they fit in. This isn't a company problem; it's a security problem. If you are doing any strategy or planning and have no direct insight or influence in what the business is doing, you are likely creating disruptions instead of enablement.

Your strategy should always begin with the business ambitions and desired outcomes. A series of questions arises from those insights. Are you positioned, with existing capabilities and services, to enable the outcomes the business seeks—near- and long-term? If you are not, can you adjust or rationalize your portfolio? Last, do you have the right skills and leadership to work with other business stakeholders? If the answer to any of these questions is no, you should consider fundamental changes to your strategy.

If your answer to these questions is yes, start influencing the messaging among external stakeholders that cyber resiliency and trust are differentiators. It may sound like a play on words, but you may be able to stop focusing on security and instead change your company's value generation story as part of product and service delivery.

2. SET RISK EXPECTATIONS AND SPEAK CLEARLY.

The security community has far too many cliches and tag lines the business doesn't understand and can't relate to. "Defense in depth is key to our cybersecurity strategy." "Zero trust is the future of security." "We must stay vigilant against advanced persistent threats." These make it hard for others you need for support to understand what you do and why it's important. Additionally, security teams all too often talk about what they do and not the business or the market they serve. Instead of spending time explaining advanced persistent cyber threats, try putting your concerns in terms of potential business disruption and what that could mean to your customers or business partners. Spend time spreading awareness of the risks in your market. Let your customers know what you do and why, and how your approach differentiates you from your competitors.

What you don't do is sometimes just as important as what you do. The security team cannot accept business risk on its own because it doesn't own much of the business it is charged to protect. In addition, not every cyber risk requires a cyber solution. This means emphasizing that not all issues in the realm of cybersecurity can be effectively addressed solely through technological or security means. For example, cybersecurity risks can also arise from weaknesses in the supply chain, where third-party vendors or partners may inadvertently introduce risks into an organization's systems and networks.

While implementing cybersecurity measures within one's organization is important, it may not be sufficient to address supply chain risks that lead to operations disruption or that compromise product integrity. You're going to get attacked—embrace it and prepare for it. This is what it means to be resilient. There are risk tolerance guardrails the security team must help business stakeholders understand so that they can participate in remediation (and value generation), and, more importantly, so that they won't make incorrect assumptions about their risk exposure.

3. BUILD AN ADAPTIVE AND HIGH-PERFORMING TEAM.

A 2023 report from the International Information Systems Security Certification Consortium (ISC2) highlights a shortage of almost four million cybersecurity professionals globally. Frankly, I don't buy it. I'm not suggesting that ISC2 has done something wrong. Still, there is too much ambiguity in our jobs and the positions we need to fill. And our existing workforce lacks professional development. We also are addressing only our needs today and yesterday instead of focusing more attention on the organization we'll need to be tomorrow. To seize the opportunities of tomorrow, we must develop a workforce of innovative thinkers and creative doers, not just technical experts. This entails personal and professional skills, including the ability to communicate, understand how an organization is organized and operates, and build relationships. The skills are essential in building a resilient organization.

As an adjunct university professor who teaches cyber operations and threat hunting, I ask students about their career ambitions. They almost unilaterally say, "I want to work in cyber." When I ask for more specifics, they seem lost. Why is that? I believe we have produced a generation of security tool administrators when we need critical and analytical thinkers and problem solvers. The security industry needs to drive the demand for more of these thinkers and fewer holders of professional certifications, which have become an industry themselves.

Too often security team member development is relegated to technical competency training. I'm not suggesting this is wrong; it's just incomplete. If technical skills are all a person brings to the table by the time they are promoted into leadership positions, they will be disadvantaged, as will the organizations they belong to. We must build well-rounded teams to solve business risk problems and take advantage of opportunities beyond security and technology. If deliberate training, development, and career progression plans are discretionary budget items, companies will not recruit or retain the top talent needed to compete and succeed. People are vital to the effective execution of strategy.

4. WORK TO ACHIEVE OPERATIONAL EXCELLENCE.

Organizations must transcend procedural efficiency and evolve into dynamic learning entities, constantly honing their defenses against ever-shifting threats. Embracing a learning organization mindset, they foster curiosity, innovation, and a relentless pursuit of improvement throughout their organization.

This approach entails more than just investing in technical prowess; it's about cultivating a collective intelligence that thrives on feedback, reflection, and shared knowledge. By promoting ongoing training, encouraging experimentation, and institutionalizing robust incident response processes, organizations equip themselves to navigate the complexities of modern cybersecurity with agility and resilience. Moreover, they recognize that cyber resiliency is not a static discipline but a fluid landscape where adaptability and innovation are paramount.

Ultimately, by prioritizing a culture of continuous improvement, organizations elevate their capabilities from reactive measures to proactive planning. They leverage each encounter with cyber threats as an opportunity for growth, distilling insights from successes and failures alike. Through this commitment to learning and evolution, organizations fortify their posture against cyber exploitation, safeguarding their digital assets and resilience in an increasingly hostile digital landscape.

FINAL THOUGHTS

The consequences of outdated approaches are significant. Companies find themselves locked in a never-ending arms race against cybercriminals and nation-state threat actors, constantly pouring resources into upgrading defensive technology. This leads to bloated cybersecurity budgets that drain resources from more value-adding initiatives. In addition, the reactive nature of legacy security models often results in a material impact on companies and their customers. According to IBM's report on the Cost of a Data Breach 2023, the average is $4.45 million. The reputational damage can be even more devastating, eroding customer trust and hindering long-term growth.

TOP 10 LIST FOR THE STATE OF CYBER IN 2024

DR. EDWARD AMOROSO

Here are the issues that we hear are important to our enterprise and government customers about the present state of cybersecurity. This is a safe way, of course, for me to present these ideas to you, because if you really like and agree with the list, then I will take all the credit. But if you hate the list, then I can just point to our TAG customers as having the wrong ideas. (I'm just kidding. Well OK—not really.)

I should tell you that when I say "customers," I mean three groups. First, there are the enterprise and government agency security teams we support through our TAG Research as a Service (RaaS) offering. It's somewhere north of one hundred major customers (you'd know their logos), and we interact with them frequently. We have the advantage in our offering, by the way, of speaking more with the worker bees than with their bosses (aka CISOs). This provides great insight, we believe.

Second are the vendors, and this is a massive group. We count about 4700 cyber vendors in our portal, which has the usual pareto effect. That is, you'd know the top 10%, and you'd sort-of-know the next 10%, and you'd have no clue about the long-tail 80%. This is not to diminish the importance of the smaller, less well-known vendors (collectively, they supply more entropy than the biggies), but we do tend to interact more with the top 20%.

And third, there are the investors, usually venture capital groups and private equity companies that are primarily interested in making money. There is nothing wrong with making money, obviously, but this financial motivation helps to serve as a truth serum for what is likely to be truly meaningful in the marketplace. That is, if no one is investing in a given area, then it probably will not succeed. (Note that we said *probably*.)

Without further ado, here's the list:

10

CYBERSECURITY VENDORS NEED TO DO A BETTER JOB SECURING THEMSELVES.

This one makes us crazy. Commercial vendors, for example, who sit in front of the big cloud security companies, perhaps doing posture management, undermine the security decision to outsource workloads when they introduce bad security into the mix. C'mon vendors—you know the cobbler-with-the-shoeless-kids story. Improve your internal protections please. Use some of that $100M you got way back in the fat funding months of 2021.

9

BOARDS ARE GETTING BETTER AT CYBER, BUT THEY ARE STILL RELATIVELY WEAK.

We're being kind. Boards are still quite terrible at cybersecurity. Usually they will employ a head-turner, which is the one board member with a computer science degree or some modest cyber experience, and is thus expected to opine on anything cybersecurity-related. This is a ridiculous way to cover any important topic. Imagine, for example, all financial decisions being relegated to one knowledgeable former CFO. That would be silly, of course, but it is how cyber is covered today..

8

MULTIFACTOR AUTHENTICATION (MFA) IS FINALLY BEING ACKNOWLEDGED AS PHISHABLE, HENCE THE NEED FOR FAST IDENTITY ONLINE (FIDO) AUTHENTICATION.

Attacker-in-the-middle tools can now sit between you and that mobile push application you bought, and they can listen for the special code and then—yes, through the usual in-the-middle process, they can spoof your identity. Sorry, but it is true. And it's why we get angry when CISA and other agencies tout MFA blindly. They miss the fact that there is secure MFA (passwordless, FIDO) and insecure MFA (phishing vulnerable mobile push). CISOs are finally learning to spell FIDO. *Sigh*.

7

SOFTWARE AS A SERVICE (SAAS) IS GRADUALLY BECOMING AS IMPORTANT AS CLOUD FOR SECURITY.

This is an interesting one. We all have come to gradually understand that outsourcing now usually means relegating some function to a SaaS or managed application. You do your payroll, calendar, collaboration, conferencing, customer relationship management (CRM), email, and other functions that way. And so, the security issues have also become obvious for SaaS. This should have been better predicted. Vendors doing SaaS security will probably make good money..

6

THE H1B PROCESS FOR FOREIGN COMPUTER SCIENCE STUDENTS IS NOT WORKING.

This is not yet well-understood, but it's being increasingly referenced. We talk about skills gaps in cybersecurity, and then we send the many, many foreign students studying here and working the baroque H1B process home after they lose on three spins of the US immigration roulette wheel. This is borderline (sorry for the pun) craziness, and if someone says once more that we have a skills gap in cyber when we are sending awesome CS majors back to India, I might scream.

5

ZERO TRUST IS FINALLY SOMETHING THAT INFORMATION TECHNOLOGY AND NETWORK TEAMS ARE ACCEPTING.

This is a good story, one that we see every day. Yes, IT and network teams are actually using the phrase zero trust, and they seem to understand what they are saying. It is impressive. The basic notion here is de-perimeterization, and most technical and operations staff have come to see what work-from-home and hybrid cloud imply in terms of security. This is a wonderful trend, and we honestly believe that the cyber security threat diminishes when a company adopts zero trust.

4

VENDORS ARE ADDING AI TO EVERY BROCHURE, WHETHER IT APPLIES OR NOT.

This one is kind of funny. Here is a typical example: A SIEM or SOAR vendor will feel like a total loser if they cannot tout their AI-enabled automation. So, they add an LLM to the threat hunting mix, usually with some thin security interface skin and some data to train security use-cases. And thus is born their AI capability. This might support brochure-ware today, but these companies will soon be called out. They should be ready. TAG will be at the forefront calling them out. We promise.

3

CISOS ARE CONCERNED (FREAKING OUT) ABOUT THE SEC RULES.

Just spend some time listening to the personal stories of Tim Brown or Joe Sullivan and you'll get an idea of the unfairness in what is happening at the SEC today regarding cyber. In short, the SEC has taken a good idea—namely, raising awareness of cyber at the senior leadership and board levels, and implemented it poorly by going directly after the CISO. We think this should involve going after the CEO, but the SEC did not ask our opinion. This SEC problem is on every CISO's mind.

2

ENTERPRISE TEAMS ARE SEEING THEIR BUDGETS LEVELING OFF.

Unfortunately, the Elon Musk concept of "who needs all these people" is rooting in the cybersecurity ecosystem of many companies. At a time when the nation-state and criminal threats are growing, the budgets for CISOs are sadly leveling or even shrinking. The problem has been too much focus on platforms and not enough attention to common sense approaches. Maybe the lower budgets will be good. But we know that vendors will not like this.

1

AI USAGE IS BREAKING OUT LIKE WILDFIRES, AND CISOS NEED TO FIND GUARDRAILS.

This is the clear No. 1. Every company we deal with, and there are many, is grappling with the question of what to do about AI usage and the potential risk it introduces to the organization. This is a massive topic—one that is too big to summarize here. But suffice it to say, the No. 1 issue on the minds of CISOs we speak with today is how to address the unclear set of threats that appear to be emerging from the use of artificial intelligence across the enterprise.

Please let us know your thoughts on the list. You can always contact us here. Whether you agree or disagree with our top ten selections, we're always keen to hear your comments.

*"We had to deal with the budget cuts **somehow**."*

CYBERSECURITY LEADERSHIP VERSUS MANAGEMENT

AL PALIMENIO

Are cybersecurity programs, and even the profession, suffering from a state of being over-managed and possibly under-led? This question is not meant to cast a disparaging light on any chief information security officer (CISO). Instead, it's meant to shed light on the expectation that, in this very fast-paced profession, CISOs will be called upon to both manage their programs and lead them, which may be one task too many.

While often used interchangeably, leadership and management are very different. Let's look for a minute at a fire department. Firefighters are called upon to put out fires, perform search and rescue, and to provide emergency first aid and medical services, to name just a few of their critical functions.

This is in stark contrast to the role of the fire chief. While at the core, a fire chief is responsible for the extinguishment of fires and the protection of life and property, just as a firefighter is, they are accountable at a significantly different level. They are responsible for overseeing the community's fire prevention program as well as providing administrative direction and strategic planning (staffing, training, equipment, etc.) for the entire fire district.

A fire chief will not routinely respond to every call, but instead focus their engagement on larger fires or more critical events, where the situation may benefit from their higher-level guidance. Their job is not to come on scene and grab a hose and start to extinguish a fire.

This is very much akin to the roles of security analysts and CISOs in the cybersecurity profession. Cybersecurity analysts, engineers, incident investigators/responders, and intermediate mangers find themselves fighting fires on a regular basis. Whether it's the investigation of a lost device, the mitigation of a new zero-day vulnerability, or the compromise of an asset by a bad actor, these activities, like fires in a community, are all too common to a cybersecurity professional. And like the fire chief, the CISO must pick and choose where and how to engage. They must focus on situations that will benefit from their engagement versus those the firefighters already have under control.

SHOULD MANAGERIAL TASKS BEGIN TO CONSUME TOO MUCH OF THE CISO'S TIME AND FOCUS, THE CISO RUNS THE RISK OF OVERLOOKING THE IMPORTANCE OF LEADING THEIR STAFF AND PROGRAM.

For all of us, our time is finite. CISOs can find themselves being pulled in countless directions by risk issues, privacy issues, and legal/regulatory issues, to name just a few. With this constant demand for your time, a CISO must be very judicious with this precious resource. That said, a CISO cannot afford to over-rotate, to be too much of a manager at the expense of being a leader. This may be even more critical for young or new cybersecurity leaders, or newly promoted CISOs.

Should managerial tasks begin to consume too much of the CISO's time and focus, the CISO runs the risk of overlooking the importance of leading their staff and program. CISOs must not allow themselves to fall victim to this, even if this is easier said than done. Let's explore some of the key attributes and actions of an effective CISO.

ESTABLISHING A STRATEGY, DIRECTION, AND CULTURE

It starts with the articulation of a cohesive strategy with security staff buy-in. In other words, they agree on the direction and own it with you. Not because you told them they would, but because they can see themselves in it and believe in it. You want a strategy that senior leadership and others external to the program can understand and support. If they do, it will speak volumes about the confidence they have in the program and the people within it.

The success of a program will have a lot to do with the culture. Establishing a culture in which staff members feel trusted and empowered, and in which their opinions matter and are valued, starts with the leader. Effective CISOs must recognize that they are setting the tone of their cybersecurity programs. The tone and culture should demonstrate confidence. From the outside in, they build confidence that the program is conhesive and effective; and from the inside out, they build trust and empowerment.

As the CISO, you can choose to lead from on high or you can meet the people where they live. That is a leadership choice. I'm not saying the fire chief should grab a hose and start putting out the fires. What I am saying is that you are there during those hard moments, offering support, hearing their concerns, and you make yourself available to them. All the while letting the firefighters fight the fire and cheering them on with your support. At the end of the day, your staff needs to know you have their backs.

ACQUIRING AND DEVELOPING TALENT

An effective leader, CISO or otherwise, must recognize that a talented team is their most valuable asset and should be treated as such. You've most likely seen the semitrucks on the interstate whose trailers are emblazoned with the statement "Our Most Valuable Resource Sits Here," referring to the drivers. These trucking companies recognize that they are nothing without their drivers, and they make this public proclamation.

While we don't all have rolling billboards to make this statement, recognition of the importance of your team should be expressed through your investment in them, which can start with how you acquire talent. First, respect the hiring process. Invest the necessary time to find and identify the best talent for your team. To achieve this, you may need to be creative. We cannot expect to acquire the top talent every time if we routinely fish in the same ponds as our competition. Consider identifying talent pools which are not as readily visible or pursued. Two of my favorite choices over the years have been colleges/universities and military bases.

WE CANNOT EXPECT TO ACQUIRE THE TOP TALENT EVERY TIME IF WE ROUTINELY FISH IN THE SAME PONDS AS OUR COMPETITION. CONSIDER IDENTIFYING TALENT POOLS WHICH ARE NOT AS READILY VISIBLE OR PURSUED.

I've found great talent with huge upsides and few bad habits in college interns. Engage in college fairs, expand your reach beyond those schools in your backyards or those with the big names. Consider smaller colleges and universities or engage with the historically Black colleges and universities for diverse talent; they have great curriculums and produce top-notch talent.

Do your homework and find the gems that are out there. While this approach will most likely not be able to address immediate staffing or talent needs, if you invest in these individuals early, sophomore or junior year, with meaningful assignments that deepen the relationships, you can cut out the competition upon graduation.

Military bases house yet another severely under-pursued talent base. What you get with a veteran is an individual who is mission-oriented, trainable, and motivated. A perfect addition to any cybersecurity talent stack. Military bases have programs designed to help veterans transition to corporate America. They're a great venue to identify talent and, in this case, give back to those who have given so much.

Once you've hired great talent, it's important to invest in their growth and professional development. One way you can do this is through stretch assignments. These involve tasks that push people to achieve beyond their current level of knowledge or skill. They can make people uncomfortable, but they also produce growth. If your team knows you have their back, they will approach the opportunity with confidence, knowing that you won't let them fail.

You can also establish a meaningful and robust training budget, which embraces mutually identified training and educational goals that benefit both the individual and the program. This investment is priceless. Its an investment in your program and the future of our profession.

These approaches to talent development imply that you understand your organizational needs, but maybe more importantly, you know the professional aspirations of the staff. As we manage talent, it's key that we get to know them well. We need to understand how they are wired, what motivates them, what drains them, and what they are seeking to achieve through their careers. As we better understand them as human beings, we can better apply their talents and aspirations in a mutually beneficial manner.

Talent development is an expensive proposition and may be time-consuming, but it's not only worth it—it's necessary. Through an investment in talent, CISOs can not only boost the future of their programs, they may also bolster our profession. You may even develop your future successor.

MOVING THE NEEDLE

An effective leader is always watching the competition and looking for opportunities to improve their position. In business, that might mean acquiring a greater market share, expanding into a new territory, or launching a new product. This is no different for a cybersecurity leader. A CISO must always be looking to take new ground, moving the needle in risk management. This may mean introducing a new control or changing a business process, all in the name of better managing IT risk for the business.

To achieve this, a CISO must be confident and humble. They must be confident enough to make a hard decision or to step into vague environments with limited information. And at the same time they must be humble enough to revisit previous decisions and accept that they may no longer be appropriate.

In sum, the CISO should lead first and manage second. As the CISO applies these tactics in the cyclical planning process, acquiring and training talent along the way, each iteration of the program is better than the last. And the strength that results from successful leadership will help reduce the pressures of managing.

MY TAKE

DAVID HECHLER

Cybersecurity has certainly arrived. Everyone knows that word. You want proof? CrowdStrike ran Super Bowl ads in **2024** and **2023**. This was confirmation that the company has made it. And CrowdStrike obviously had confidence that viewers knew what the ads were talking about.

But what do most people know about cybersecurity? That is, people who do not make their living trying to prevent, mitigate, or respond to cyberattacks. It's an important question because for years research has shown that people are the weak link in cyber defense. We get fooled by phishing emails and we click on links that endanger our companies. And it's not just lower-level employees who are the problem.

The recent book TAG published on cybersecurity, called **Guiding Cybersecurity from the Boardroom** (which can be downloaded for free), was designed to address a dangerous gap in cyber defense that many companies suffer from.

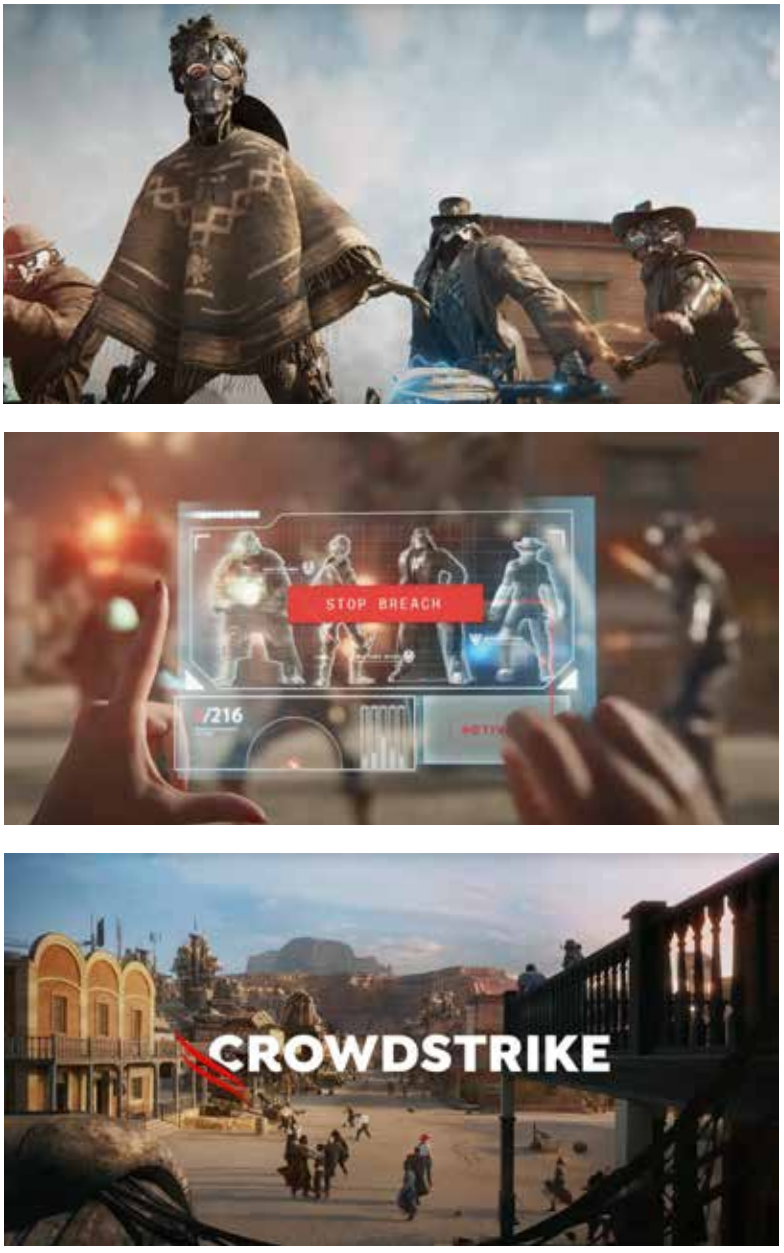
Their boards of directors are not necessarily better prepared to help prevent cyberattacks than the employees.

The more I think about it, the more I think that cybersecurity is a black box to nearly everybody in this country. We hear about it. We know it does damage and costs money. We know we're supposed to be careful to avoid being fooled into clicking on a dangerous link. But beyond that, what do most people really know?

WHAT MAKES CYBERSECURITY DIFFERENT

There's one way in which these attacks are at odds with the way we generally think about crime. It's the absence of perpetrators—or rather, perpetrators we can see. It's hard to think about crime without thinking about criminals. But we rarely see the criminals behind the attacks. If they are identified at all, it's often by the name of a gang or their nation of origin. And those nations rarely have extradition treaties with the United States.

For the vast majority of us, cybersecurity is the invisible crime. We don't see it happening. Companies and individuals who are victimized rarely want to report it or talk about it. As for the criminals, we've come to assume that they're all far away and they work for, or are protected by, nation-states. No pictures appear on the front pages of newspapers to show the world the latest big hack. It's almost as if the danger is beyond perception—like Covid-19.



Stills from CrowdStrike's 2024 Super Bowl ad

One of the biggest attacks in recent years that received a lot of media attention was SolarWinds. Recently it was in the news again, but it was because the company itself faces an SEC enforcement action, along with its chief information security officer (CISO). But still we see nothing about the criminals responsible—just the attribution that it came from Russia.

Maybe it's no coincidence that in CrowdStrike's most recent Super Bowl ad, the bad guys are aliens who look as though they just stepped out of one of those weird bars in Star Wars.

THE EXCEPTION

There is one case I can think of that was an exception to this rule. It happened here in the United States. There were charges filed. Several defendants pleaded guilty and testified in court. One man who seemed to be on the side of the good guys—he was responsible for security in the company that had been hacked—stood trial.

The case, of course, involved Uber and has proved highly controversial. Many professionals who work in security supported and continue to support Joe Sullivan, who in October 2022 was convicted by a jury of obstructing justice and covering up a felony. Sullivan was not charged with the hack. Two men pleaded guilty to that, and one testified against Sullivan, as did a former Uber in-house lawyer. (In the interest of full disclosure, Sullivan now works as a TAG senior analyst.)

Was this the case designed to open the public's eyes about cyberattacks? Hardly. The focus was not on the hack; it was on the effort prosecutors said was designed to conceal anything resembling a crime by calling the hack research and the $100,000 payment to the hackers a bug bounty. These were the issues the testimony highlighted. For friends and former colleagues of Joe Sullivan (and there are many), it was just another effort to blame the chief security officer when things go wrong.

NO PICTURES APPEAR ON THE FRONT PAGES OF NEWSPAPERS TO SHOW THE WORLD THE LATEST BIG HACK. IT'S ALMOST AS IF THE DANGER IS BEYOND PERCEPTION—LIKE COVID-19.

When SolarWinds' CISO, Tim Brown, was included in the SEC's enforcement action against his company in October 2023, a year after Sullivan's conviction, it struck some people in the field as yet another tightening of the screws. In this instance the problem wasn't breaches. The SEC charged that Brown and his company had failed to let shareholders know about security vulnerabilities he and his colleagues were aware of and concerned about.

THE TAKEAWAY

But let's set aside the specifics for a moment. Let's not try to prelitigate or relitigate these two cases. If the nation were determined to learn lessons about cybersecurity that would help us all better understand the challenges we face, what can they teach us? What do they tell us about the nature of cybersecurity?

The short answer: Companies don't like to be hacked. And when it happens, or when they fear it might happen, they seem highly motivated to keep the details to themselves.

Law enforcement, Congress, and the Cybersecurity and Infrastucture Security Agency (CISA) have been trying for years to convince companies to share with the authorities, and with each other, the dangers they hear about or encounter. The goal is to help build defenses against the virulence, the way vaccines aimed to counter Covid-19. The government seems to think this approach would shine more light on these invisible crimes and bolster the nation's defense.

It's hard to see how recent events have advanced that cause. A number of angry CISOs have argued that heavy-handed enforcement has spurred veteran security professionals to consider moving on—and aspiring ones to reconsider their options. It's hard to see any way in which the public is now enlightened and better prepared to deal with future cyber threats.

If only the criminals looked like bad sci-fi characters, and CrowdStrike could chase them back to their home planets.

INTERVIEWS

AN INTERVIEW WITH KEVIN SAPP,
CTO AND CO-FOUNDER, AEMBIT

SHAPING THE FUTURE OF WORKLOAD SECURITY

Every security expert knows that identity and access management (IAM) is the new primary control for protecting infrastructure from cyber threats, emerging as the perimeter is no longer an effective control with the shift to zero-trust networks. However, IAM has primarily focused on user identity despite the rise of workloads as active entities on a network. We recently sat down with the team from Aembit to understand how their commercial platform supports workload IAM. We were interested in learning about applying the basic tenets of user IAM in a workload context, and the interview below summarizes the main points of our discussion.

TAG: What exactly do you mean by "workload IAM?"

AEMBIT: Let's build off the User IAM analogy. With users, you use a policy-based system to manage which users have access to which software systems. Enterprises have a centralized point of management (like Okta or Entra/Azure AD) to manage access policies and quickly make changes. Workloads—applications, scripts, even the SaaS services your applications depend on—have no similar model today for securing access to other sensitive workloads. There is no centralized way to create visibility, enforce access, and ease the compliance process for workload-to-workload access.

In a world where workloads are growing exponentially (sometimes 45 workloads for every user in an organization), and workloads themselves are a prime attack surface for bad actors, there is a strong and growing demand for a Workload IAM system that accomplishes and automates what User IAM systems do today.

TAG: What legacy solutions exist to authenticate and secure workload communication and interaction?

AEMBIT: We see a number of solutions for addressing the challenge—and this is part of the problem. Organizations have been trying to cobble together coverage from several different tools. For example, Cloud IAM can help within one particular cloud, but what about multi-cloud, SaaS, or on-prem? Secrets managers can store secrets, but how do you verify the identity of workloads or implement conditional access before workloads get to your trove of stored secrets? How do you securely enroll workloads into the secrets manager in the first place?

Aembit is forming the foundation of workload Zero Trust by combining cryptographically verifiable workload identities with least-privilege access policies.

These challenges often lead companies to build custom solutions, further exacerbating the challenges for teams to maintain their existing infrastructure. As teams cobble together these solutions, they face security gaps, tool overload, context-switching fatigue, and, inevitably, a significant amount of manual work just to maintain the status quo.

TAG: What are some of the principles, approaches, and methods used in user IAM that apply to workload IAM?

AEMBIT: Let's talk about some similarities and some differences. After all, if it were all the same, you could also use your User IAM system to manage workload identities. It all starts with Identity: You need a trusted, verifiable way to determine "who" is asking for access. With users, you have usernames/passwords, MFA, FaceID, etc. There's no MFA for workloads, so we rely on Identity Federation and Attestation to verify workload identity.

In user-land, we manage access, not secrets. We've moved away from having a password ("secret") for every app. Instead, you need to access your IAM system, which brokers your access based on policy. That's spot-on with what we're doing at Aembit, albeit for workloads.

We also meet workloads where they are, which is a significant difference between User and Workload IAM. User IAM systems have standardized AML and OIDC for authentication. However, workloads use a variety of credentials (API keys, username/password, JWTs, etc.) and protocols. The workload IAM system's job is to interoperate with this wide variety of elements so that operators can simply declare policies that define which workloads others can access.

TAG: Does your platform work well in a zero-trust environment?

AEMBIT: As you know, identity is the foundation of Zero Trust, and that's true for workloads and users. Aembit is forming the foundation of workload Zero Trust by combining cryptographically verifiable workload identities with least-privilege access policies and layering on dynamic posture assessment.

Leveraging our expanding partnerships with organizations like CrowdStrike and Wiz, customers can go beyond access policies to assess the security posture of their workloads before providing them access to sensitive customer data, secret vaults, or other vital assets.

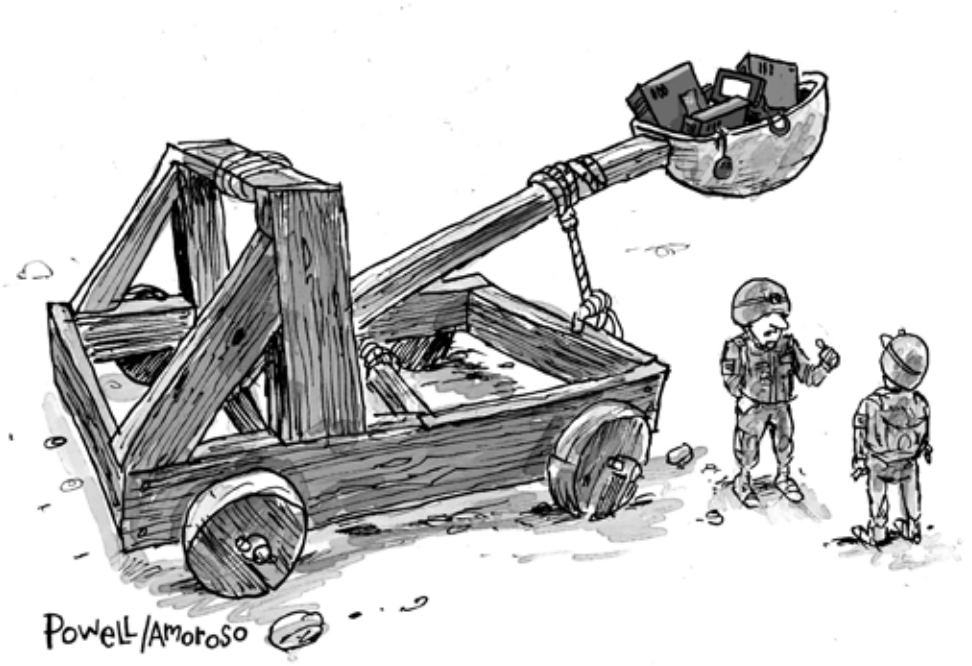
TAG: Any predictions regarding cybersecurity and workload identity security, particularly for the coming years?

AEMBIT: Unfortunately, we will see increased attacks in the coming year, where workload access credentials are the initial access point. Workloads have become "low-hanging fruit" in the

way user credentials were a few years ago, so a new front door for attacks is emerging.

In three years, 50% of developers will write code as if they don't need credentials for workload-to-workload access (No API Keys! No tokens! No Oauth calls!).

The reason is that auth will be built in "as-a-service" into the platform run by their company, enabling no code auth. In five years, the combination of Workload IAM and identity federation means that organizations will move from storing long-lived credentials in their apps to short-lived, secretless identity and access credentials, leading to the death of secrets.



"I don't think our commander quite understands cyber war."

AN INTERVIEW WITH GILAD ELYASHAR,
CHIEF PRODUCT OFFICER, AQUA SECURITY

SECURING CLOUD-NATIVE APPLICATIONS

Cloud computing fundamentally changed how enterprise teams create, store, access, and use resources. Developing the so-called cloud-native application protection platform (CNAPP) now represents a critical development in our cybersecurity industry. We recently spent time with leading cloud security vendor Aqua Security to gain insights into modern CNAPP developments, including how their customers use the platform for application security across the entire lifecycle.

TAG: What is your team's experience stopping attacks on cloud-native applications?

AQUA SECURITY: Today's cloud-native attacks continue to increase in volume and sophistication. The emergence of AI-driven cyber attacks makes it easier for threat actors by giving them the tools and the speed to automate and expand their foothold within cloud-native environments. This new era of attacks prioritizes closing the loop faster by expanding threat detection to include automated prevention and blocking.

Aqua goes beyond identifying and prioritizing attacks on cloud-native applications and can stop attacks in real time. Using the Aqua Enforcer agent, Aqua's platform identifies and prevents various attacks, including signature-based attacks (malware, IOCs around malicious IPs, DNS, etc.) and novel, behavioral-based attacks. Supported by high-fidelity research from the Aqua Nautilus research team, Aqua offers "prevention-grade" recommendations for automatically blocking detected malicious activities.

Additionally, Aqua aids in preserving the immutability of customer environments by identifying and blocking drift and ensuring the security and stability of deployments. We foster deep trust with our customers and recognize the initial hesitation in enabling automatic blocking features. By starting in audit mode, customers can align with Aqua's high-accuracy detection results and gradually move from detection to prevention.

TAG: Tell us about the importance of container security in the context of CNAPP.

AQUA SECURITY: Container security is crucial in the CNAPP framework due to the increasing adoption of containers and Kubernetes in cloud-native

This new era of attacks prioritizes closing the loop faster by expanding threat detection to include automated prevention and blocking.

applications. Gartner predicts that 90% of global organizations will run containerized applications in production by 2026, indicating a big shift towards cloud-native applications from traditional virtual machines. This trend is expected to continue as organizations adopt cloud-native practices.

The cloud-native approach has made application development more agile and flexible, but containers pose unique security challenges that require a different approach. Container security covers the applications and the infrastructure inside the containers, and automated controls are crucial for effective container security from code to cloud. Aqua is a recognized leader and pioneer in container security, emphasizing the importance of full lifecycle protection. As containers and Kubernetes dominate, Aqua's capabilities are increasingly vital to the market.

TAG: Are there any unique challenges in addressing cyber risk across all aspects of the development lifecycle?

AQUA SECURITY: The critical challenge for end-to-end vs. point solutions is their ability to integrate and connect insights from code to cloud seamlessly, which is vital for mapping and understanding interconnected risks throughout development.

Vendors offer insights into pipeline areas like cloud control planes, code security, supply chain security, and vulnerability management in container images. However, the most significant impact on risk mitigation is synthesizing these insights to allow cross-pollination that enhances risk assessment and prioritization. This approach requires a robust presence at all stages of the development lifecycle.

Aqua connects these dots for customers—from code through build to runtime—and identifying the relationships between components in each environment is crucial. This holistic view enables scenarios that provide customer value while managing and mitigating cyber risks.

TAG: How critical are security posture assessments for both cloud and Kubernetes?

AQUA SECURITY: Security posture assessments for cloud and Kubernetes environments are paramount to ensuring infrastructure is securely configured, reducing the attack surface accessible to potential attackers across two main categories.

The first category involves infrastructure risks, encompassing the management of Kubernetes and cloud environments, including network configurations, identity management, and the settings of various cloud services to secure the underlying infrastructure that supports applications.

The second, often underestimated, category pertains to the application layer, which involves identifying vulnerabilities within the applications, covering code scanning and vulnerability management, and monitoring runtime behavior to detect anomalies or malicious activities. This layer is critical for spotting sophisticated attacks that exploit unique vulnerabilities or misconfigurations at the application level.

A notable example is the Aqua Nautilus discovery, HeadCrab, an advanced threat actor that utilizes state-of-the-art, custom-made malware to target application-level vulnerabilities and configurations, making it undetectable by agentless and traditional anti-virus solutions.

A comprehensive cloud-native security solution must address infrastructure and application-level risks. Organizations can form a unified risk profile or security posture by integrating these assessments. This holistic approach is essential for effectively safeguarding against the evolving landscape of cybersecurity threats.

TAG: Any predictions regarding cybersecurity and cloud security for the coming years?

AQUA SECURITY: The cybersecurity and cloud security landscape is quickly evolving towards prioritization and contextualization, aiding organizations in navigating security findings across their infrastructures, application codes, and cloud environments. Due to advanced attacks and complex cloud services, organizations will need better security support. The next phase in cybersecurity evolution will focus on actively fixing vulnerabilities through code remediation, posture adjustments, and/or real-time attack mitigation by blocking threats.

This progression highlights the transition from identifying to actively solving cybersecurity challenges. The industry faces the emerging challenge of securing generative AI-based applications into their code and infrastructure, presenting new attack vectors, and necessitating further protective measures.

In summary, the future of cybersecurity and cloud security is set to build upon the current foundation of prioritization and contextual awareness, moving towards a more proactive problem-resolution stance. This shift is about keeping pace with advancing threats and adapting to the complexities introduced by new technologies, including AI, ensuring a holistic and resilient approach to cybersecurity.

AN INTERVIEW WITH CHRIS PIERSON, FOUNDER AND CEO, BLACKCLOAK

DIGITAL PROTECTION FOR EXECUTIVES & FAMILIES

High-value employees have become the path of least resistance and a key source of compromise for corporations. Attacks against executives can compromise their personal accounts, enable corporate breaches, and compromise their reputation, wealth, and physical security. Cybercriminals, fraudsters, and identity thieves regularly target individuals and families with wealth, access, status, and reputation.

Security afforded at work cannot transfer into personal digital life, and consumer solutions cannot withstand targeted attacks. The Pioneer of Personal Cybersecurity™, BlackCloak, provides concierge protection for the digital personas of executives and other high-profile individuals, including their families, who might be at personal risk and placing their organization at risk of cyber threats.

TAG: Can you start by giving us an overview of how your digital executive protection solution works?

BLACKCLOAK: BlackCloak offers its Digital Executive Protection and Concierge Cybersecurity & Privacy™ Platform, combining proprietary technology and software with white-glove service in a single SaaS-based platform. BlackCloak also provides the unique ability to ensure separation of church and state between the executive and the company. We help to maintain each executive's privacy while allowing the company to extend that enterprise-grade protection and support (via BlackCloak) to the executives and their families.

Once a new member enrolls, we guide them through a comprehensive onboarding process to ensure they understand the breadth of support and service we offer. After onboarding, the BlackCloak Concierge team provides our members white-glove client service via video, phone, email, and secure messaging. Our threat intelligence analysts notify members of a potential event as quickly as the severity of the threat warrants and send actionable "Cybersecurity Alerts" on trending threats and vulnerabilities via email and push notifications.

Organizations allocate millions to protect information assets and employees but neglect to safeguard key executives' and board members' very vulnerable digital assets and lives. Sponsored by BlackCloak, Ponemon Institute surveyed **553 IT and IT security practitioners** knowledgeable about programs and policies to prevent cybersecurity threats against executives and their digital assets. This national survey reveals

The Pioneer of Personal Cybersecurity™, BlackCloak, provides concierge protection for the digital personas of executives and other high-profile individuals.

that while Digital Executive Protection is a top-of-mind concern, most organizations either lack the resources or are unequipped to manage the ramifications of a cyberattack on an executive's personal digital life.

A key takeaway from this research is that while cybercriminals will likely target executives' digital assets and lives, organizations do not respond with much-needed strategies, budgets, and staff. 58% of respondents say preventing cyberthreats against executives and their digital assets is not covered in their cyber, IT, and physical security strategies and budget. Moreover, only 38% of respondents say there is a dedicated team to prevent and/or respond to cyber or privacy attacks against executives and their families.

TAG: How do malicious actors typically target executives' online digital personas?

BLACKCLOAK: Cybercriminals often target personal devices, email addresses, and physical addresses, which they can buy from data broker websites. Additionally, they seek out password information, often found on the deep or dark web or even stolen/hacked websites. Many common scams perpetrated by these cyber hackers when looking to compromise an individual include tech support scams, social media scams, malware/ransomware attacks, and extortion scams. Tech support scams are scams which can include Google number searches and inbound calls. Social media scams can occur through a personal account or a friend's hacked account.

We also see malware/ransomware attacks that involve enticing the individual to click on a link within an email or SMS message. Unprotected devices without virus scanners or are not up to date with the latest operating system can also be vulnerable to scammers. Extortion scams can either include fake emails or a targeted threat such as "we have your child." These scams are designed to fool even the most technically sophisticated individuals.

TAG: What are the specific types of services you offer customers?

BLACKCLOAK: BlackCloak offers a four-pronged approach to protecting an individual's personal digital assets. We safeguard privacy through device hardening, data broker removal, dark web scans, and VPN usage. We also protect a member's devices from deception, hacking, or malicious activity. We secure the member's home by conducting weekly vulnerability scans and network reviews. Lastly, we protect our members' peace of mind through prevention, rapid incident response, and our award-winning concierge service.

TAG: Does your solution extend to assist executives' families with their digital profiles?

BLACKCLOAK: Absolutely. We know that it is essential for executives to ensure their family members are also protected from bad actors. We not only have the ability to protect executives with our service, but because we can harden home networks and devices, we can extend that protection to family members as needed.

TAG: Any predictions regarding cybersecurity and executive security for the coming years?

BLACKCLOAK: According to this year's **IC3 Report**, cybercrime is increasing as a whole. There were a record number of cyber complaints in 2023, with a 10% year-over-year growth. The overall financial losses as a result of cybercrime increased 22%, exceeding $12.5B. As cybercriminals become even more sophisticated, they will look for new ways to compromise businesses and individuals. We expect the risks from deep fake and AI-generated tactics will likely become more prominent. It will be necessary for our clients to stay vigilant and develop strategies to combat these types of personal attacks.

"I'm sorry, we moved our men's room to the cloud."

AN INTERVIEW WITH SEEMANT SEHGAL, FOUNDER & CEO, BREACHLOCK

AN OFFENSIVE APPROACH TO CONTINUOUS ATTACK SURFACE DISCOVERY

Enterprise security teams have come to understand the importance of continuously monitoring their attack surface before the next potential incident occurs. With an offensive security strategy for continuous attack surface discovery and penetration testing, BreachLock, a pioneering cybersecurity firm, offers a novel approach to protecting your threat landscape.

In this interview, we highlight BreachLock's unique methodologies, strategies, and experiences, offering insights into their offensive approach to identifying and mitigating potential vulnerabilities in an attack surface. Our goal is for readers to gain useful ideas on dealing with this increasing need to view exposed cyber assets.

TAG: Let's start with you sharing a little about what led you to found BreachLock?

BREACHLOCK: After gaining experience at renowned global enterprises known for setting cybersecurity standards, I noticed a significant disparity in resource allocation between defensive and offensive security technologies. Upon analyzing the return on investment (ROI) from defensive versus offensive strategies, it became clear that offensive security consistently produced better results. For example, each penetration test identifies vulnerabilities and proactively addresses and closes potential entry points for hackers. So, I decided to delve into the reasons behind companies'relatively lower investment in penetration testing. Subsequent conversations ensued with multiple Chief Information Security Officers (CISOs) revealed an unmet need and gap in the market, with penetration testing methods proving inadequate for modern business requirements.

I identified four key shortcomings of traditional penetration testing: accuracy, agility, scalability, and cost-effectiveness, which stemmed from the fact that security tools operated on a point-in-time basis. Testing for system vulnerabilities was a singular event, typically conducted periodically or in response to impending audits or compliance requirements. At that time, the security industry had yet to develop the concept of continuous security. Human intelligence drove the existing offensive security landscape, while cybercriminals were already ahead of the game, using automated technology, and in some cases, AI, to scrape the internet for easy victims. Now, this battle is unwinnable without the use of technology.

Our automated algorithms and supervised NLP-based AI models help to refine BreachLock's proprietary Pen Testing framework.

That pivotal moment led me to address these challenges, culminating in establishing BreachLock in 2019 to pioneer the world's first full-stack Penetration Testing-as-a-Service (PTaaS) solution long before its widespread recognition or understanding. I conceived PTaaS to address the pressing demand for Offensive Security and a more continuous approach to safeguarding against an ever-evolving and expanding attack surface.

TAG: What is it about BreachLock that has catapulted you from a PTaaS start-up to a global cybersecurity leader in a short span of five years?

BREACHLOCK: Start-ups take two key areas for granted that ultimately make a difference to customers: the talent they hire and customer service. In recent years, a recurring pattern has emerged within the cybersecurity sector—a succession of start-ups buoyed by investor enthusiasm embarked on aggressive hiring sprees, often overcompensating employees to showcase rapid growth. This strategy, aimed at appeasing investors and projecting stability, ultimately proved unsustainable. When investors clamored for substantial returns and consistent revenue growth, these companies' unrealistic targets culminated in inevitable staff reductions.

I had no desire to entangle my company in the complexities of managing millions in investor funds or relinquish the autonomy to steer it according to my vision. Consequently, I chose to bootstrap BreachLock during its inaugural year. Then came the unforeseen challenge of COVID-19, where I couldn't meet my team face-to-face for the initial year and a half. Despite these obstacles, we surpassed $1 million in revenue, witnessed expansion and growth, and this became part of our initial success story. Our commitment extends to investment in innovative technology, sales, and customer service personnel.

At BreachLock, we recognize the importance of laying a robust foundation with our clients, dedicating ample time to establishing clear, tangible metrics that reflect an organization's security performance. In today's landscape, clients seek more than just security solutions—they require the ability to articulate a genuine return on investment to their executives and boards.

TAG: How does continuous attack surface discovery benefit from taking an offensive approach? Is being proactive a major component?

BREACHLOCK: Yes, a proactive or offensive approach is at the center of attack surface discovery. Continuous attack surface discovery is the ongoing assessment and monitoring of security controls, configurations, and potential vulnerabilities across the surface. This approach relies heavily on security automation, continuous monitoring, and integration as key enablers.

The idea of continuously monitoring the attack surface is born, once again, out of necessity. With the rise of automation and integrated security tools, it is no longer a wish but a viable part of an ongoing and proactive cybersecurity process focused on identifying and monitoring potential attacker entry points in an enterprise's digital environment. This approach involves constantly assessing and analyzing assets, networks, and systems to detect new or changing attack surfaces for weaknesses and exposures.

TAG: How is your platform designed and integrated with your offensive security solutions? What makes your platform different from your competition?

BREACHLOCK: BreachLock has conducted continuous security testing for over five years, performed thousands of penetration tests, and accumulated comprehensive knowledge of potential attack paths and Tactics, Techniques, and Procedures (TTPs) tailored to diverse technology stacks and contexts. Aligned with industry standards such as MITRE & ATTACK, OWASP, NIST, and OSSTMM, our automated algorithms and supervised NLP-based AI models help to refine BreachLock's proprietary Pen Testing framework. Integrated seamlessly into the BreachLock Platform, our framework safeguards precision and quality, automating routine tasks like report formatting, proof of concept integration, and basic vulnerability identification.

TAG: What future advances do you see in cybersecurity innovation? BreachLock already offers a unique AI/ML technology, so what's next?

BREACHLOCK: The future of cybersecurity has the potential for exciting developments, but one thing is certain: we will continue to face a never-ending battle against attackers and their increasingly sophisticated and covert methods. However, one significant trend likely to continue is the advancement of AI and ML in cybersecurity.

AI and ML technologies are already enhancing threat detection, automating responses, and identifying patterns indicative of cyberattacks. Over the next few years, we can expect these technologies to become even more sophisticated and pervasive. Conversely, attackers are increasing their use AI to exploit weaknesses and launch attacks on systems and applications.

AN INTERVIEW WITH MATT HARTLEY, CO-FOUNDER & CHIEF PRODUCT OFFICER, BREACHRX

MODERNIZING INCIDENT RESPONSE PRACTICES

Managing incidents is now a critically important requirement for any enterprise team dealing with cybersecurity threats. Security teams must become world-class in incident management and response, especially in public companies.

We spent time recently with the management team from cybersecurity startup BreachRx to learn more about their platform. We were keen to learn how their software as a service (SaaS) platform provides purpose-built support to security and legal teams for handling cybersecurity incident management and reporting.

TAG: What specific problem does your platform address?

BREACHRX: Companies have traditionally dealt with incident response by hoping for the best, waiting until an incident happens, and attempting to solve the problem with limited resources, stale paper plans, and outdated procedures. Security is overwhelmed, and talent is scarce. Legal teams demand minimal records to minimize fallout. Teams aren't prepared, with annual tabletop exercises that don't effectively challenge them or their leaders. Everything is manual, slow, and expensive. Recent court cases show CISOs wrongfully taking the blame for breaches when entire chat server contents are made available to the prosecution. This "best practice" for incident response is outdated and needs to be replaced.

BreachRx is the first intelligent incident response platform that provides enterprise operational resilience. Our SaaS platform supports all stages of incident response, enabling customers to shift to a proactive stance for cyber risk operational resilience and incident preparedness. The BreachRx platform includes the latest regulatory requirements and compliance standards, encourages transparency and communication while protecting legal privilege, and provides a comprehensive, rapid response plan tailored to each incident. This results in efficient resource utilization, cost savings, and a record that protects CISOs, corporate executives, and board members.

Our SaaS platform supports all stages of incident response, enabling customers to shift to a proactive stance for cyber risk operational resilience and incident preparedness.

TAG: Can you give us an overview of the platform's features?

BREACHRX: Our patented incident response platform is designed for the entire business. It automatically generates tailored incident response plans and guides all enterprise stakeholders through every complex decision at every step of the response to control the chaos of an incident, managing and reducing the risk of impacts.

BreachRx offers a comprehensive platform for incident response management, cybersecurity, privacy, and data breach regulation compliance. The platform provides dynamic and automated incident response plans tailored to the most common incidents, including instructions with deadlines for every task. It also covers over 200 cybersecurity, privacy, and data breach regulations, breaking down the requirements to comply.

With BreachRx, automation rapidly achieves compliance for incident response with a wide range of stringent global laws and frameworks, including ISO, SOC 2, NIST CSF, SOX, NIS2, and many more. The platform also offers workflow automation to ensure that all stakeholders in the enterprise know what to do for any incident and a safe-haven portal for real-time communications to coordinate all teams.

Additionally, BreachRx is a central system of record that provides a transparent audit trail of actions taken and strengthens and protects privileged communications to ensure compliance, replacing the now clearly flawed head-in-the-sand approach of the past and shielding CISOs and executive leadership from personal liability.

Our customers, like Joe Greene, First United Bank CISO, consider our platform their hub for incident response: "We chose the BreachRx platform as our incident response hub due to its purpose-built design and ability to integrate with the organization's incident response program—from security, IT, legal, and compliance to communications, risk management, and business lines." All our customers build world-class incident response programs around BreachRx to protect their teams, companies, and themselves.

TAG: Do some of your customers use the BreachRx platform to help deal with new SEC rules for reporting?

BREACHRX: Absolutely. The BreachRx platform stays current on the 200+ global cybersecurity, privacy, and data breach regulations, including the SEC rule. Even the biggest, best-intentioned legal and compliance teams struggle to stay on top of these rulings without automating the process. Our customers love that BreachRx takes on the burden of understanding the applicability of these regulations in each incident, eliminating any ambiguity.

We build the latest rulings into our playbooks and action plans so organizations can move quickly and confidently when an incident happens. And we bridge the gap between legal, compliance, and security so everyone understands what needs to be done and when.

TAG: Help us understand the role of automation in the operation of your platform.

BREACHRX: The nearly eight major incidents per day last year underscore the threat landscape's scale, and to keep customers safe, we must replace the unfair burden teams face from the old way of running incidents with automation. Proactively, customers use our compliance workflows to ensure they cover every incident response requirement for all major global frameworks while meaningfully preparing for incidents.

Our no-code workflow automation platform allows customers to tailor everything, from data schema to playbooks, tasks, and regulations. With easy-to-use wizards and out-of-the-box integrations, customers can seamlessly launch cases, and our tailored response plans provide exact instructions for every incident step. Plus, the platform enables teams to practice, exercise, and simulate incidents, improving preparedness through training. This drives unprecedented consistency and accuracy in every response.

TAG: Any predictions regarding cybersecurity and compliance reporting for the coming years?

BREACHRX: Unfortunately, Incident response will only become more challenging for companies. We must all be more proactive and consistent in our cybersecurity practices, risk management, and compliance. Incident response cannot continue to be an afterthought or add-on. Supply chain attacks, harsher extortion by ransomware groups, use of generative AI by threat actors, and the targeting of OT systems will continue and grow, so we hope compliance auditors step up their depth of focus on incident response preparedness.

In addition, regulations, like EU's NIS2 and CIRCIA, will continue to come, regardless of whether a company is public. The pace will continue to be relentless, and with over $2.1B in GDPR fines alone last year and CISO and CEO lawsuits and directives, companies can't wait. With incident response records now audited like financial records, the new era of accountability is already here.

AN INTERVIEW WITH NIR LOYA DAHAN, VP OF PRODUCT, CYMULATE

ELEVATING SECURITY VALIDATION: A NEW APPROACH

The frantic state of find-fix vulnerability management is not working. Exposure management acknowledges that you can't immediately patch or fix every vulnerability, so you need to take an attacker's view of what they can reach and the resulting damage. Validation provides a significant difference between exposure and traditional vulnerability management because validation provides proof of breach feasibility that drives focused remediation based on validated threats.

Cymulate is a market leader in exposure validation, with a platform that validates the security of deployed controls and prioritizes exposures based on what attackers can access. Cymulate combines the best elements of traditional capabilities, such as breach and attack simulation (BAS) and automated red teaming with exposure assessment data from attack surface discovery and integration with vulnerability scanners and the security infrastructure. Below is a summary of recent discussions on these topics.

TAG: Tell us how your platform works.

CYMULATE: Our SaaS platform validates cyber defenses and threat exposures with continuous offensive testing and context of critical assets, controls, and active threats. To constantly challenge your security, Cymulate combines BAS with automated red teaming for production-safe testing that tests controls and attempts to penetrate defenses. The platform correlates these control gaps and weaknesses against the attack surface of assets, applications, and systems and their vulnerabilities to prioritize exposures and baseline cyber resilience.

Cymulate creates a risk-profiled asset inventory and consolidated view of vulnerabilities and weaknesses by scanning the attack surface and integrating with vulnerability scanners and the security infrastructure. Breach and attack simulation tests control with over 120,000 attack scenarios that emulate actual techniques and active threats to validate controls, identify weaknesses, and provide guidance and specific policies and rules to harden the defenses. Automated red teaming offers flexible, repeatable, and scalable testing to validate defenses against full kill chain campaigns and assess attack paths to critical assets. You can base this testing on known threat actors or user-created scenarios.

Through automated offensive testing and complete context of the attack surface, we provide the proof and evidence to validate your security, prioritize gaps, and baseline your cyber resilience.

Our SaaS platform validates cyber defenses and threat exposures with continuous offensive testing and context of critical assets, controls, and active threats.

TAG: Do you see exposure validation as an evolution from BAS solutions?

CYMULATE: For years, blue teams have successfully run BAS to validate controls, identify gaps, tune protection policies, and build new detection rules. However, security leaders now see the value in combining automated security validation with vulnerability management to better focus and prioritize remediation on validated exposures.

Exposure validation correlates offensive testing from BAS and automated red teaming with the context of the attack surface, vulnerabilities, and critical assets. The exposure assessment or identification overlap with offensive testing can then prioritize remediation and action on proven accessible weaknesses and projected impact.

The evolution and adoption of exposure management require security teams to look for solutions that consolidate multiple forms of offensive testing with the exposure assessment – or at least data from vulnerability scanners and the cloud security posture. Consequently, we're seeing fewer BAS being run in isolation as security programs demand cross-functional teams to collaborate more to run purple teaming exercises and analyze vulnerabilities by filtering what's reachable and how controls can mitigate what can't be patched.

In the right platform, exposure validation gives security teams and cyber executives a single source of truth to know your attack surface, critical assets, weaknesses, and the business impact of disruption. It allows you to test each weakness based on actual threat actor techniques and the latest campaigns, focus remediation on the gaps that attackers can reach, prove the state of cyber resilience, and measure changes based on the evolution of attack surface and latest threats.

TAG: What is the role of continuous automation in how your platform performs security validation?

CYMULATE: Security teams can't build exposure validation into the ongoing operations of cyber programs without automation. While the industry has always valued the security validation provided by manual penetration tests, the value of that penetration test decreases exponentially as it ages. Unfortunately, the manual effort – and the associated expense – prevent daily or weekly penetration tests from being feasible for most organizations.

Offensive security testing has evolved with technologies like BAS, continuous red teaming, and automated network penetration testing, enabling continuous security and exposure validation automation. This automation allows for the most advanced offensive testing to be run in parallel to vulnerability scans so you correlate results and focus on the proven gaps.

Daily tests simulate the latest threats to validate defense against current active campaigns and threats that target new vulnerabilities. Continuous automation enables recurring tests that baseline cyber resilience and benchmark the cyber program as new initiatives roll out. You can measure the tangible results with evidence of your ability to take a punch.

TAG: Will AI be an important component of validating threat exposure?

CYMULATE: Yes. Over the past year, we've seen AI unlock doors that we thought were permanently shut. People and organizations are using this technology in weird and wonderful ways. Just as attackers lean more on AI, security and exposure management also introduce and expand the use case to think more like an attacker – to strengthen your defenses.

Cymulate is applying AI to advance exposure validation by rapidly developing new offensive testing techniques, targeted assessments, and guidance on optimizing security validation as part of security operations. In the very near future, you'll see Cymulate introduce AI-powered features, including tailored testing schedules based on user-driven inputs such as industry, cloud vs. on-prem environments, and forecast events such as penetration tests and board meetings.

Additionally, Cymulate will provide insights and summarized remediation priorities based on a series of recent assessments and enable user-created simulations built on the inputs of published threat advisories, blog posts, vulnerability disclosures, and more. The platform will also offer mitigation guidance that creates endpoint policies and SIEM rules based on the specifics of the attack scenario, along with customized attack simulations and production-safe exploits targeted at the vulnerabilities and weak points discovered by attack surface scanning and reconnaissance.

TAG: Any predictions regarding cybersecurity and attack surface management for the coming years?

CYMULATE: In the very near future, cyber insurance will demand security validation. While some insurance companies have already updated their policies to state that organizations must have ongoing continuous security validation and provide reports to receive any payouts after an attack, a stronger stance is coming soon. With additional pressure from the SEC and other regulatory bodies to report attacks within a short period, organizations must adopt BAS and other forms of continuous security validation if they want to continue receiving cyber insurance. There's simply no way around it anymore.

AN INTERVIEW WITH ADAM MARUYAMA, FIELD CTO, GARRISON

REVOLUTIONIZING CYBERSECURITY WITH HARDSEC

The protection of endpoints is a rich discipline in cybersecurity often equated (mistakenly) with anti-malware agents on the PC or desktop. In recent years, however, the best security teams have come to deploy solutions that isolate the end-user's browser using creative technology that can protect the endpoint from malicious content.

Garrison Technology is a leader in offering a high-assurance product that implements this critical control. We recently learned more about how Garrison combines the best elements of hardware security with the flexibility and convenience of a cloud-hosted solution in Garrison ULTRA®.

TAG: What are the primary cyber threats that Garrison serves to address?

GARRISON: We defend our users from the most common threats of web access, like phishing, ransomware, and other malware. These threats are increasingly prevalent and insidious as corporate dependency on the web browser increases. To make things worse, most browsers don't distinguish between trusted websites that have been rigorously evaluated and contractually guaranteed (e.g., GSuite, Office365, and SalesForce), public sites with unknown but assumed-good security controls (e.g., news sites, LinkedIn, and retailers), and unknown or actively untrusted websites (e.g., Reddit, and sites used for threat intelligence). All these sites either receive the same system level of privilege as the browser – introducing a security risk – or are blocked altogether – negatively impacting user morale and productivity.

TAG: Can you give us an overview of how your platform works?

GARRISON: We offer a solution to allowing unchecked websites to access high system privileges in browsers. Instead of risking security or slowing down operations by allowing or blocking by default, Garrison introduces a new option: "sanitize by default." This feature presents an interactive video stream of browsing activity without introducing foreign web code, thus eliminating malware risks to organizational endpoints.

Our platform relies on nine years of evolving hardware security (hardsec) technology. Trusted by top government organizations in the US and

Instead of risking security or slowing down operations by allowing or blocking by default, Garrison introduces a new option: "sanitize by default."

UK, it employs two separate processors per browsing session. This ensures that no web code is processed on the endpoint; users receive an interactive webpage stream. This approach allows users to deliberately navigate to malicious pages and observe their effects without risking system compromise.

ULTRA seamlessly integrates with customers' existing proxy or secure web gateway through a simple JavaScript redirect code snippet on a custom block page or a Chrome or Edge plug-in. Our goal is to transform a block page into a sanitized one. Rather than being blocked from accessing vital information, we sanitize the page of technical risks and provide real-time risk notifications in our secure environment instead of their native browser. As users' trust in ULTRA grows, administrators can transition from a permissive proxy posture to trusting only secure sites, moving from "allow by default" to "sanitize by default."

TAG: What is the role of hardware security in the assurance associated with your solution?

GARRISON: Remotely exploiting software is easy; remotely exploiting hardware is nearly impossible. By enforcing our isolation mechanism at a hardware level – using an FPGA between two discrete processors to verify that only an audio/video stream of the web browsing conducted on a remote "sacrificial" processor is presented to the second processor, which then compresses the video for presentation to the endpoint – we ensure that our underlying security mechanism cannot be subverted, even by advanced toolsets used by nation states and sophisticated cybercriminals. In contrast, achieving the same effect using virtualization or containerization software would render it vulnerable to escape attacks.

In addition to robust security, ULTRA provides an unmatched user experience. Each active user has access to their processor pair, eliminating the need for load-balancing resources. This means even resource-intensive content like streaming video and Javascript-heavy sites can be accessed without degradation using ULTRA. Achieving this with software would require compromising either security or user experience.

TAG: How do customers make use of your solution? Are you offering a service from the cloud?

GARRISON: We've realized that cloud-first and cloud-native architectures are here to stay, and we're committed to providing a high level of security and user experience for organizations using those architectures. To achieve this, we've provisioned data centers worldwide with our hardware-enforced technology and created a cloud infrastructure that our customers can use to access those devices via the proxy or secure web gateway

mechanism I described earlier. Garrison engineers take care of all the maintenance, updates, and support for the devices themselves, providing organizations with a solution that's easy to set up and even easier to keep running.

TAG: Any predictions regarding cybersecurity and browser isolation for the coming years?

GARRISON: Over the past few decades, we've learned that the information advantage will be the decisive strategic advantage of the 21st century in business and statecraft. The most sophisticated adversaries realize this and have dedicated themselves to making the Internet increasingly dangerous through novel vectors, exploits, and effects. The current approach of detecting, containing, and expelling attackers from our systems falls short in addressing this threat.

This became evident earlier this year when the Directors of the FBI and CISA, along with the Commander of US Cyber Command, testified before Congress that VOLT TYPHOON and other APTs had infiltrated and remained undetected in US critical infrastructure for years. We need to think differently about security, and hardware-enforced browser isolation is the first step in building solutions and architectures that are truly secure by design.

Discovering zero days in browsers and cybersecurity software is a nearly monthly event; as a result, attackers consistently achieve footholds in sensitive systems. We can't keep building increasingly complex cybersecurity software platforms and expect different results. I hope other critical security functions can achieve the same level of assured security that we've brought to RBI with ULTRA.

AN INTERVIEW WITH CODY CORNELL, CO-FOUNDER & CHIEF STRATEGY OFFICER, SWIMLANE

EXPLORING CUTTING-EDGE SECURITY AUTOMATION

The security operation center (SOC) has become a functional component of every enterprise, serving as the main coordinating point for data analysis, incident review, security monitoring, threat hunting, and many other tasks. To provide for automation in this context, teams must select the best available industry partners.

Cybersecurity company **Swimlane** has been a leader in supporting automation in the modern SOC for many years. Their low-code security automation platform extends beyond security orchestration, automation, and response (SOAR), leveraging generative AI to improve security workflows in or beyond the SOC. The interview below outlines their evolving approach.

TAG: Tell us a bit about the evolution of your platform and its current set of offerings.

SWIMLANE: When building our platform, we focused on scalability, composability, and flexibility. Unlike other SOAR companies (like Phantom and Demisto) that built pre-set SOC playbooks, we aimed to create a flexible automation engine. As the world's most capable security automation engine, we can integrate and automate anything, becoming the system of record for any security use case or function.

Turbine, our low-code security automation platform, is known for being the world's fastest and most scalable security automation platform, executing over 25 million daily actions—ten times faster than any other platform, provider, or technology. The cloud-native platform has the future of SecOps in mind and can adapt to constantly evolving environments, exceeding the modern SOC's pace of change.

This year, we **announced** Canvas and Hero Artificial Intelligence (AI), our **new Turbine innovations** empowering security teams to build automation in seconds with limitless integrations and dramatic time and resource savings. **Turbine Canvas** unveils the true power of low-code—it democratizes automation and leverages modular and reusable programming components so users can build playbooks with intuitive, ultra-simple visual interfaces.

Hero AI enables customers to be generative AI applications in the Swimlane Turbine platform. Its potent combination of human and machine intelligence optimizes SecOps workflows and maximizes analyst productivity and return on

Turbine, our low-code security automation platform, is known for being the world's fastest and most scalable security automation platform.

investment. These transformational innovations now make Swimlane Turbine the triple threat of automation, GenAI, and low-code, solving the most challenging problems across the entire security organization.

TAG: What is the role of automation in the SOC, and how does your platform support this goal?

SWIMLANE: Security teams face a shortage of qualified staff, an overwhelming volume of alerts, and underutilized security tools that don't work together. The result is wasted resources and increased vulnerability to evolving threats. Automation is the solution to this critical gap, providing security teams with the necessary tools to protect their organizations fully.

Recognizing this urgent need, we revolutionized our Turbine low-code automation platform with advancements that strengthen security teams by connecting them, their telemetry, and technology through a human-centric AI and automation building experience. Turbine's automation solutions can ease the burden on security teams, enabling them to tackle more complex threats and deliver greater value to the organization.

TAG: Is AI a vital component of the automated support you provide for customers?

SWIMLANE: Automation and AI have the power to be the ultimate human enabler, but neither will entirely replace the value of the human mind. Instead, AI-enabled features can empower humans to make faster and more effective decisions.

While AI holds immense promise in SecOps, its implementation hinges on experienced human oversight. The talent shortage in cybersecurity creates a vulnerability gap where even advanced AI faces the limitation of bias and unforeseen scenarios. Human expertise is crucial for responsible use, issue identification, and critical decision-making. Like automation, AI in SecOps should involve close human collaboration.

Security automation serves as a valuable foundation for responsible AI adoption. Like the "human-in-the-loop" approach, automation strategies emphasize human involvement in critical decision-making, which aligns with the need for human oversight in AI-powered security. By automating threat detection and log analysis, security professionals can focus on complex situations and strategic decisions where human judgment is irreplaceable.

TAG: What do you see as the interaction between SOC analysts and the tools they use to process and analyze data?

SWIMLANE: SOC analysts face data overload from disparate security tools, which hinders threat visibility and forces analysts to constantly task-switch across tools, browser tabs, and

disjointed views. Automation centralizes and enriches information automatically, making teams more effective and efficient.

Collaboration is key. Analysts act as guides, identifying data feeds and defining rules for automation to prioritize threat investigation and response. Automation eliminates irrelevant data and highlights suspicious activity, freeing analysts to investigate high-priority alerts, leverage automation for deeper analysis, and build feedback loops to improve their tools.

The interaction is cyclical. Analyst insights are fed back into the tools, continuously improving threat detection and response. Automation isn't a replacement—it's a force multiplier that empowers analysts to become strategic decision-makers focused on the most critical cybersecurity tasks.

TAG: Any predictions regarding automated security in the SOC for the coming years?

SWIMLANE: AI and security automation are easing the cybersecurity talent shortage by accelerating the onboarding of security analysts. At Swimlane, we process billions of signals for our customers and estimate that our automation does the work of several thousand security analysts. SOC teams will look for ways to do more with less in the coming year—AI and automation will help address this challenge by reducing manual tasks and streamlining workflows. Automating repetitive, time-consuming tasks frees employees to focus on more strategic and creative activities. In addition, powerful AI models can be trained to aid security analysts, further improving this massive efficiency gain.

AI will be a true enabler for security teams by ensuring they are well-equipped to analyze and generate playbooks that build off the team's past actions for specific investigations. By leveraging generative AI for investigations, this tool will ultimately become a readily available knowledge source for security analysts and become critical to shortening the onboarding time for security teams with high attrition rates.

AN INTERVIEW WITH EV KONTSEVOY, CO-FOUNDER AND CEO, TELEPORT

CUTTING-EDGE ACCESS SECURITY SOLUTIONS

New platforms are being developed to support common, converged access from both human beings and also machines, devices, and resources, none of which will be easily supported via methods such as biometrics or passwords. Thus, Identity-based security is the new foundation for creating a secure access infrastructure. We recently talked with a commercial vendor called Teleport, which has developed platform support based on the best practices adopted by hyperscalers for the type of secure access mentioned above. We wanted to learn about the platform at a high level and how it supports enterprise access, identity, and policy.

TAG: Let's start by having you share the specifics of how your platform works.

TELEPORT: The Teleport Access Platform brings industry best practices for access control for humans and machines to the critical resources of modern infrastructure. It is based on four core principles.

First, the Teleport platform prioritizes cryptographic identity, enforcing the cryptographic identity of all users, devices, machines, and resources. This ensures secure access and makes infrastructure resilient to identity attacks.

Second, it upholds the principle of Zero Trust, implementing Zero Trust connections between users/machines and resources. This approach enhances infrastructure security by making it resistant to network-based breaches and pivot attacks.

Third, it emphasizes ephemeral permissions, enforcing the principle of least privilege access. Providing ephemeral privileges that expire when work is completed eliminates standing or stale privileges, thereby enhancing security.

Last, it promotes Unified governance, unifying enforcement, and observability. Identity and policy governance create a single source of truth for who is doing what in the infrastructure, which enables infrastructure leaders to identify and remediate weak access patterns or manage policy from one central place across all infrastructure components.

The Teleport platform prioritizes cryptographic identity, enforcing the cryptographic identity of all users, devices, machines, and resources.

TAG: How is machine identity different from user identity?

TELEPORT: Machine accounts are far more numerous. They are ephemeral by nature, and historically, high overhead has burdened the management of machine identities and privileges. Meanwhile, machines often have highly privileged access, like CI/CD pipelines.

At Teleport, we believe that human and non-human identities should be treated in the same way and governed by the same policies and processes. The fragmentation of identity and policy creates risk for organizations and raises operational costs.

Unifying access control across human and non-human identities is even more important in the age of AI. Companies need to have the correct access control in place for intelligent bots that consume data and for the humans that can interface with them. This is a challenge that companies already face with some automated processes that handle customer data.

TAG: Do you see your solution complementing or replacing existing means for secure access?

TELEPORT: Most existing access is based on credentials, which are not secure. Credentials and other forms of secrets have become the number one target for threat actors, who focus on human error and identity-based attacks as the means of breaching organizations.

Further, most infrastructure is still based on perimeter-centered security. Applying zero trust principles to access infrastructure and allowing the microservices inside your infrastructure to talk to each other hardens infrastructure against network-based infiltration.

Finally, modern infrastructure is complex! Humans make mistakes. Fragmented access control relies on humans for configuration and deployment, which inevitably has attack surfaces capable of being compromised.

Teleport makes infrastructure immune to human error and identity-based attacks by eliminating secrets and standing privileges and unifying identity and policy.

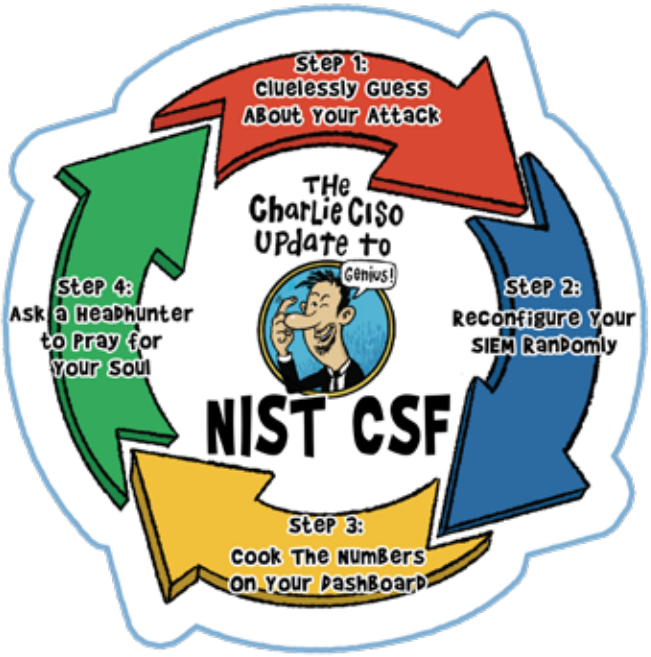
TAG: Can you share any data regarding the return on investment (ROI) for enterprise teams using your solution?

TELEPORT: Companies who have deployed Teleport often report that they have removed technology that is no longer needed, such as VPNs, bastion hosts, PAM solutions, or isolated machine solutions, which shouldn't be siloed.

However, they are often most excited that by implementing Teleport, they have ALSO improved their engineer's productivity, protecting time to market on critical business initiatives. It's a win/win for security and engineering organizations.

TAG: Any predictions regarding cybersecurity and access security for the coming years?

TELEPORT: I see the following four key themes: Engineering and security teams will partner to protect infrastructure from growing identity attacks. An increasing frequency and cost of breaches due to human error will force organizations to adopt secretless access. We will see more M&A activity that consolidates tool sprawl. The industry will see more regulatory pressure. I would also like to give special attention to AI – that as AI becomes incorporated into infrastructure, it will need to be governed by unified identity and policy rather than as a separate access silo. This will begin to drive access and data security strategies in new, integrated ways.



AN INTERVIEW WITH BRIAN VECCI, FIELD CTO, VARONIS

ENHANCING ENTERPRISE DATA SECURITY

Data protection is perhaps the most mature and well-known aspect of data security. The need to avoid financial or reputational losses by discovering, classifying, and labeling sensitive data has grown significantly, and enterprise teams now require assistance from the best commercial vendors in this area.

Varonis has been a data protection leader for many years, with a rich portfolio of solutions that support tasks such as data security posture management (DSPM). We talked recently with the Varonis team to get a better idea of how they work in support of enterprise data security needs.

TAG: Let's start with an overview of the Varonis platform and how it supports data security.

VARONIS: The Varonis platform stops and thwarts cyberattacks by taking a data-centric approach to security. We scan on-prem and cloud environments to automatically discover, classify, and label sensitive data, analyze permissions and remediate excessive access and limit the impact of cyberattacks, manage the posture of cloud apps to proactively close security gaps, and monitor user and device behavior to detect and stop threats.

We also include a Proactive Incident Response service with all of our SaaS subscriptions. Varonis solves many security use cases with a single data security platform. Core use cases include DSPM, SSPM, DLP, Data classification, and UEBA/threat detection. We leverage automation to augment security teams and help them achieve security outcomes with minimal effort.

TAG: The automation of your platform seems critically important. Do some teams still perform manual tasks in support of data security?

VARONIS: There will always be a need for manual remediation for data security, but it's almost all going to be tactical rather than strategic and generally reactive. In a world where access to data is gated by identity, application and platform configuration, container access controls, and user-created collaboration links, manual remediation will never be able to address explosives at scale, especially since security teams are stretched so thin. Teams should, of course, be able to react to security posture and configuration issues quickly, but automation is critical to ensure that data is protected.

TAG: What is your team's view of AI and its prospects for data security?

VARONIS: Every conversation about AI is a conversation about data—using it, creating

We leverage automation to augment security teams and help them achieve security outcomes with minimal effort.

it, and monetizing it in some way. Organizations face two strategic challenges when it comes to AI and data security. First, enterprises use AI to increase revenue and productivity by leveraging AI Copilots. Because of the vast amount of data they have in platforms designed for easy collaboration, there are massive security and privacy risks because of oversharing and a lack of governance. Without addressing these gaps, organizations won't be able to deploy Copilots and realize their benefits safely. In addition, AI workloads built on extensive, proprietary data sets need to be monitored and secured so that internal data isn't exposed or misused. Do you want your customer support chatbot to reveal proprietary information to the public?

On the other hand, security teams can realize tremendous gains in productivity by leveraging AI-based security tools to help analyze and enrich security telemetry. This can help reduce the time to detection and time to respond to security incidents and minimize the blast radius of a compromised account or device. Threat actors will use modern tools, and security teams must fight fire with fire.

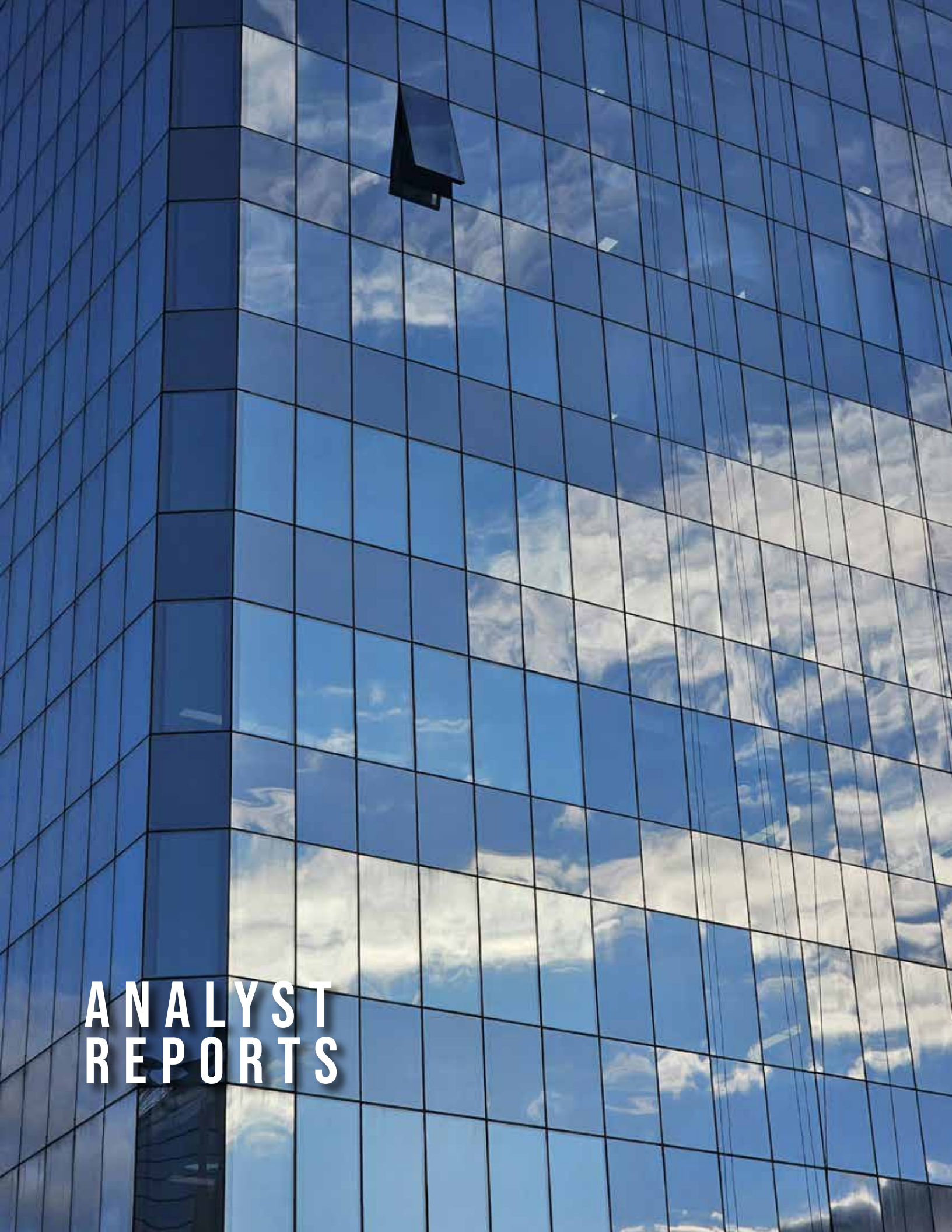
TAG: What trends do you see in data moving between legacy and cloud infrastructure?

VARONIS: While legacy infrastructure isn't going away completely, and some organizations prefer it for certain types of data, cloud stores and applications generally offer greater functionality for collaboration, productivity, and interconnectivity. Organizations generally prefer to onboard new data stores and infrastructure in the cloud and are moving many legacy systems to modern cloud options.

However, cloud stores being more secure by default is a myth—cloud infrastructure providers leverage a shared responsibility, and organizations still need to ensure their data is secure. However, since cloud stores are by design connected via APIs and collaboration functionality can increase exposure, in many ways, the job of a threat actor is easier in the cloud. There are just more ways in and more ways for data to be exposed. And data is always the target!

TAG: Any predictions regarding cybersecurity and data security for the coming years?

VARONIS: We're far from the first Copilot-aided data breach. AI copilots make users more productive but can also make threat actors more productive. We'll soon learn of a breach where a threat actor used an AI copilot to identify credentials and secrets to move laterally or elevate privileges to get access to and exfiltrate valuable data. Because they leverage data in cloud stores that are often cross-connected with other applications—your Salesforce data can be accessed through Microsoft 365 and then accessed via Copilot, for instance—the blast radius can be much bigger than people realize.



ANALYST REPORTS

ANALYST REPORT

APPLE AND GOOGLE ARE SUPPRESSING INNOVATION IN MOBILE APP SECURITY: HERE IS WHY YOU SHOULD CARE

DR. EDWARD AMOROSO, CHIEF EXECUTIVE OFFICER, TAG INFOSPHERE[1] AND RESEARCH PROFESSOR, NYU[2]

TED MIRACCO, CHIEF EXECUTIVE OFFICER, APPROOV[3]

Apple and Google are exhibiting monopolistic behavior that is suppressing technical innovation in mobile app security.[4] With cyber threats growing, such behavior from these massive companies is not in the best interest of consumers. Alternative mobile app security approaches are discussed with emphasis on addressing the inevitable complications that arise with proposed changes to familiar systems and infrastructure.

[1] *TAG Infosphere provides research and advisory in cybersecurity, artificial intelligence, and climate science for enterprise teams and government agency practitioners and commercial vendors. See* https://www.tag-infosphere.com/.

[2] *NYU's Center for Cybersecurity (CCS) is an interdisciplinary academic center in which leading edge research, teaching, and scholarship are directed into meaningful real-world technology and policies. See* https://cyber.nyu.edu/.

[3] *Approov is a team of developers dedicated to making the future of mobile secure. With offices in Edinburgh, Scotland (UK), and Palo Alto, California, the company focuses on developing the world's most complete end-to-end solution for mobile app security from the device into the cloud. See* https://www.approov.io/ *for more information on the company and its mobile app security solutions.*

[4] *During the development and review of this article, the US Department of Justice sued Apple over its purported monopoly on smart phones. Obviously, this issue bears some relation to the arguments made here, but readers must understand that our focus here is on cybersecurity and we make concrete recommendations on how Apple (and Google) should take steps to fix the issues. The authors are not policymakers, but rather cybersecurity experts supporting practitioners. See* https://www.theverge.com/2024/3/21/24105363/apple-doj-monopoly-lawsuit.

INTRODUCTION

The thesis of this report – namely, that Apple and Google are increasing long-term consumer cyber risk through monopolistic behavior, is driven by two basic beliefs: The first is that bad actors have an inherent advantage over cyber defenders. Readers will recognize the aphorism that attackers need succeed only once, whereas defenders must succeed always.[5] This security concept is well-known and universally accepted by experts.[6]

The second belief is that monopolists tend to suppress innovation. One reason for this effect is that monopolists naturally prefer the status quo. Another is that monopolists are usually large, which tends to slow down the pace of change. Regardless of the justification, we view this claim as well-accepted. As an illustration, recall that AT&T was divested in 1984 for precisely this reason – namely, to increase innovation by nurturing competition in telecommunications.[7]

At first glance, our monopoly complaint might seem misplaced with respect to these larger companies. We all know, for example, that consumers knowingly buy into Apple's sandbox ecosystem, driven by Apple's strict policing of their environment to obsessively control what types of software are allowed and under which conditions.[8] Google also claims a strong security approach, albeit one based less on a controlled sandbox.[9]

Readers might be surprised that we agree that both companies, especially Apple, currently do a reasonable job with cybersecurity. The baroque measures that both companies take to ensure high integrity in mobile apps in their on-line stores is admirable and has been mostly successful addressing advances from outside adversaries. It is not easy, for example, to find major mobile app-related breaches that have occurred based on negligence from Apple or Google.[10]

We believe, however, that the relative success of Apple and Google addressing offensive pressure from nation states, criminal groups, and other capable threat actors is not likely to continue indefinitely. The conditions are too ripe, in our estimation, for the offense to not find seams, gaps, or other means (perhaps using AI) to break through the monoculture protection that emerges from any monopoly. Apple and Google should not be left alone to do this work, nor should they be allowed to set the security standards for what are considered safe apps.[11]

Furthermore, it should be evident that the mobile app security solutions from Apple and Google are specific to their respective closed ecosystems. As a result, there will not be great incentive for either company to support cross-platform initiatives that address mobile app security more comprehensively. This is despite the fact that developers and end-users are increasingly being held accountable for cross-platform breaches.

---

[5] *This belief is generally viewed as an informal observation, but more formal government-funded reports have analyzed the offensive and defensive balance and have pretty universally concluded that it is much easier to attack than defend when it comes to cybersecurity. See* https://cyberdefensereview.army.mil/Portals/6/Documents/2022_summer_cdr/08_Valeriano_CDR_V7N3_Summer_2022.pdf, *for example.*

[6] *We are hardly the first business commentators to suggest that Apple and Google are intentionally behaving as monopolists. See* https://www.wired.com/story/googles-app-store-monopoly-ruled-illegal-jury-epic/, *for example, which explains that a court recently came to the same conclusion. Our perspective here is on the cyber security implications of such behavior, a perspective that we believe has been underrepresented in most discussions on this topic.*

[7] *Many articles, books, and lectures are available on this topic. The following report from the Department of Justice is interesting and reviews the rationale and results of the 1984 AT&T decree:* https://www.justice.gov/archives/atr/att-divestiture-was-it-necessary-was-it-success.

[8] *Apple does an excellent job with its sandbox approach for software and we admire the focused attention on ensuring that software is properly reviewed and vetted. See* https://www.apple.com/business/docs/site/AAW_Platform_Security.pdf, *for example.*

[9] *Google also provides world-class cybersecurity with a team of experts who are focused on making certain the cyber risk is properly minimized. See h*ttps://safety.google/stories/micklitz-pietraszek/, *for example.*

[10] *Of course, there have been serious mobile app security breach incidents. Vendors such as NowSecure, which supports mobile app security testing, have aggressively pointed these out. See, for example,* https://www.nowsecure.com/mobile-app-breach-news/.

[11] *By way of comparison, consider that the OWASP® Foundation works to improve the security of software through its community-led open- source software projects, hundreds of chapters worldwide, tens of thousands of members, and by hosting local and global conferences. See* https://owasp.org/www-project-mobile-top-10/.

In this report, we make the specific case that the monopolistic behavior for mobile app security exhibited by Apple and Google must cease immediately. We explain how this behavior is occurring today, and we examine its ramifications. We also look at some alternative approaches, being careful to reference the geopolitical and other challenges (mostly related to Chinese manufacturers) that could result from such change.

ILLUSTRATIONS OF MONOPOLISTIC BEHAVIOR

A reasonable definition of monopoly is the exclusive possession or control of the supply of, or trade in, a commodity of service.[12] The general notion here involves an entity or group of entities restricting the ability of competing entities to participate in some desirable activity such as mobile applications. An interesting paradox is that real monopolies do everything possible to claim the opposite, whereas startups try to claim exclusive control of some target area.[13]

The problem with monopolies is that the drive to innovate diminishes because there is little or no fear of competition. They can also control scarcities, drive prices up, and decide on the level of quality that best suits their needs. Admittedly, Apple and Google are wonderful companies with amazing products that consumers generally love. The problem instead is an emerging issue, one that can create problems as the intensity of offensive methods increases.

The general issue we reference here is that Apple and Google essentially control the entire mobile app ecosystem. As a non-security-related illustration, consider that when Spotify mobile app users download music, a fee of between 15% and 30% is paid from Spotify to Apple. This might seem fair (tenants pay landlords) until one recognizes that Apple also competes with Spotify – and thus maintains a significant and seemingly unfair advantage.[14]

Another example is the on-going battle between video game developer Epic and Apple, and the issue is roughly the same as with Spotify. That is, when Epic innovates to develop new games or features, the profit margin is obviously squeezed by Apple taking its cut of the fees from consumers. Antitrust probes led right up to the Supreme Court, but we suspect that this issue will continue to reappear and cause problems for consumers.[15]

EFFECT ON MOBILE APP SECURITY VENDORS

The reason we care about such behavior has nothing to do with the philosophy of business or the attendant legal considerations. We leave that debate for others, but we have come to recognize that monopolies are not good for cybersecurity – and this is, in fact, our area of expertise and focus. Hence, it makes sense to review our security concerns about how Apple and Google might be placing consumers and society at risk.

The first hint that there is a problem is the honest observation that innovative startups and entrepreneurs in mobile app security are struggling. Where we have observed commercial vendors in adjacent areas such as cloud and API security reaching significant levels of growth and valuation, we have seen the mobile app security vendors struggle to reach similar levels of accelerated sales and customer adoption.

---

[12] *Any number of definitions of monopoly can be found on the Internet (ignoring references to the board game). A good sample definition of a monopoly is available here:* https://www.merriam-webster.com/dictionary/monopoly.

[13] *One of the authors (Amoroso) has noticed this behavior in his research and advisory work at TAG Infosphere where cybersecurity startups desperately try to convince observers that they essential dominate a particular area (usually proof that they do not) whereas legitimate monopolies such as Apple and Google in the context presented here, will do everything they can possibly muster to demonstrate that they compete with everyone (usually proof that they do not).*

[14] *Our attention in this report is on the cybersecurity of mobile apps and how Apple and Google are misbehaving in this context, but the Spotify case offers useful insight into the problem. While we are not experts in this music debate, we do follow the narrative – and here is a typical post explaining the seeming back-and-forth between the companies and regulators:* https://forums.appleinsider.com/discussion/233654/spotify-speaks-out-against-apples-30-commission-fee-again.

[15] *We also do not purport to be experts in the gaming battles between Apple and companies like Epic, but we encourage readers to dive in to learn more. Here is a typical post:* https://appleinsider.com/articles/20/08/23/apple-versus-epic-games-fortnite-app-store-saga-the-story-so-far. *If this interests you, spend some time reviewing both sides of the story and hopefully come to your own conclusion. Our interpretation is that Apple is clearly exhibiting the behavior of a typical monopoly. It looks textbook to us, but again, our primary interest is on security.*

An analysis of cybersecurity vendors reveals high valuations for companies such as Wiz, Crowdstrike, CyberArk, Palo Alto Networks, SentinelOne, Fortinet, Check Point, Vectra, Obsidian, Okta, Fastly, and more. These companies address security for cloud, endpoints, privileged access, networks, and related enterprise assets – but despite the central role that mobile apps play in our lives – none of the truly major cybersecurity vendors work in this area.[16]

The reason this situation matters is rooted in the importance of mobile apps for consumers, as well as business, government, and general society. We have learned that malicious actors target the most valued assets, and we believe this increasingly involves mobile apps. By placing the bulk of security responsibility to provide attendant protection in this area on two monopolies, we are following a path that misses the value of open competition and innovation.

The implication, we believe, is that unless we take a different approach toward mobile app security, one that encourages fair use, competitive development, and entrepreneurial risk, then we will run the risk of placing our defensive eggs into one basket (in this case, two baskets) and that if we expect this to sufficiently cover the growing threat from nation state-sponsored actors, then we believe we have misplaced our hopes and trust.

CASE STUDY: GOOGLE MOBILE SERVICES

To illustrate our point, let's review how Google Mobile Services (GMS) maintains a lock on Android mobile apps, which in turn makes life difficult for external mobile app security vendors. Again, the issue is not the current state of GMS or whether Google does an acceptable job providing security. Our issue is that by stifling competition, innovation slows (or ceases) and the gap between offense and defense will widen.

GMS is a reference to a collection of Google applications and services that are preinstalled on Android devices.[17] These services provide functions such as Google Play Store, Google maps, Gmail, Google Drive, and so on. Our observation and experience are that these are solid utilities and applications, and that Google consistently provides excellent software and support. They have even improved their update process for their suite of apps.[18]

The problem comes when a device is used without GMS, perhaps because a mobile user or organization would prefer that Google not have access to their private data or because they would like to make use of non-Google apps for functions such as location or data storage from non-Google app stores. The mobile app experience is immediately less integrated, and the range of apps available becomes limited with the device connected into GMS.

Third-party developed versions of Android which are generally referred to as custom ROMs (they also known as Android skins) are also available to users. Usually created from the source code of the Android Open-Source Project (AOSP), which is the same base that Google uses for Android, these custom ROMs are intended to support a range of new features and to enhance the performance, capabilities, and features of the device.[19]

---

[16] *Readers are welcomed to review any number of cybersecurity valuation estimates available on the Internet or privately. There must be dozens of good analysis reports and they all show comparable results – namely, that commercial mobile app security vendors are literally nowhere to be found on leaderboards of corporate valuation, growth, revenue, sales, or any other financial metric. The report that we reference above is here:* https://www.finrofca.com/news/cybersecurity-startups-valuation-and-multiples-2024.

[17] *Here is something funny. We were looking for a nice reference on GMS and found a decent explanation on the website of Hong Kong-based HONOR, which is a provider of smart devices. The reason it's funny is the obvious use of ChatGPT to generate their article. It has phrases like "In the ever-evolving landscape of mobile technology, GMS stands as a cornerstone . . ." and so on. We have no quibble with this, but it's funny that non-English speakers cannot sense the subtle awkwardness that comes with Generative AI. We have nevertheless used their AI-generated document to help explain GMS. We thought you'd enjoy that – and no, this article (and this footnote) was not generated by AI, but rather by living, breathing, and biased humans. Here is the site in case you need a chuckle:* https://www.hihonor.com/sa-en/blog/what-is-gms/.

[18] *One of the authors (Amoroso) was directly involved as CISO of AT&T for two decades in the early days of Android apps on iPhones and other devices. Things were bad in those early days in terms of the long process of getting software updated on a smartphone. It's beyond the scope of this article but suffice it to say that the Android process has improved. Apple, as you'd guess, always did this well because they control the entire ecosystem, which does bode as points for them in the context of security. Monopolists always control their end-to-end experience better than non-monopolists. We will give them that.*

[19] *See* https://medium.com/@theentrepreneurreview/7-best-custom-roms-for-android-f091d5caee90/ *for a description of custom ROMs for Android.*

It would thus seem like GMS should not be necessary in every Android device. The difference would be that a non-GMS Android device would omit apps such as Google Maps, Google Chrome, YouTube, and other Google apps. Alternatives do exist for these apps (an argument against the monopoly) and many of these GMS apps aren't required in an Android device supporting a specific function such as in certain industrial settings.[20]

The problem, however, as was evident in a recent court case that found Google to be a monopoly,[21] is that mobile app security companies operate at a significant disadvantage when having to deal with GMS. Consumers and businesses might not expect this to be relevant, since it doesn't have a near-term financial impact for them, but our concerns for emerging threat coverage will most certainly have security consequences for mobile app users of all types.

ALTERNATIVES TO GMS

When one begins to consider alternatives to GMS, one finds (especially American readers) that the options begin to look somewhat foreign and perhaps even uncomfortable. That is, most of the activity that is currently on-going to address such monopoly behavior in the mobility ecosystem are being done in countries such as China, the Middle East, and Africa. These are markets that are generally considered non-relevant to the typical US consumer.

For example, one leading manufacturer of non-GMS mobile phones is Transsion, a Chinese smartphone manufacturer known for brands like Tecno, Itel, and Infinix.[22] Transsion has grown to become the world's fifth-largest smartphone manufacturer, focusing on markets in Africa, the Middle East, Latin America, Asia, and Oceania. They have a strong presence in Africa and offer affordable smartphones while also venturing into new technologies like foldable devices.

Similarly, Huawei, Xiaomi, and Oppo are Chinese manufacturers of non-GMS mobile phones. Huawei, despite facing challenges due to U.S. sanctions, continues to produce phones like the Mate 60 Pro and is striving to re-establish itself in the global market.[23] Xiaomi, known for its affordable phones, has a strong presence worldwide, shipping millions of phones annually. Oppo, Vivo and Xiaomi have been gaining market share globally especially with young buyers.[24]

These various companies, most of whom will be largely unknown to American buyers, are all part of a group of vendors focused on competing against the Google Play Store by allowing developers to upload apps simultaneously to their app stores. Overall, Huawei, Xiaomi, and Oppo are the most prominent manufacturers of non-GMS mobile phones that offer a diverse range of devices catering to different market segments.

The problem, obviously, is the geopolitics associated with these companies. The authors here, both Americans, clearly understand the awkwardness and implausibility of shifting toward Huawei from Google and GMS to improve security.[25] This would be a ridiculous recommendation, and it is hardly our intent here. That said, we do offer these foreign use-cases to illustrate the type of focus required to build non-GMS mobile app ecosystems.

---

[20] *See* https://emteria.com/blog/gms-vs-non-gms/ *for a more detailed information and useful discussion on the topic and implications of non- GMS Android apps.*

[21] *See* https://www.theverge.com/23994174/epic-google-trial-jury-verdict-monopoly-google-play *for an excellent explanation of the case, its details, and its implications.*

[22] *For more information on Transsion, see* https://www.transsion.com/?lang=en.

[23] *Many interesting articles are available on the Internet that explain and comment on business-related issues for companies such as Huawei in the context of US restrictions. See, for example,* https://www.cnet.com/tech/mobile/huaweis-2023-revenue-soars-despite-us-sanctions/.

[24] *See* https://www.mi.com/us/ for more information on Xiaomi.

[25] *It should be pointed out that one of the authors of this report (Miracco) is the Chief Executive Officer of an international mobile app security company (Approov) that is headquartered in Edinburgh, Scotland (UK) and Palo Alto, California (USA). See* https://approov.io/info/company.

THE CYBER THREAT THAT ARISES WITH MONOPOLY

Perhaps the best way to understand the type of threats that arises when a large company behaves in a monopolistic manner regarding cyber is to compare the mobile app security ecosystem with the cloud security ecosystem. The resulting comparison helps to explain how and why we are so concerned that Apple and Google are operating as they are, despite doing an acceptable job of security today.

If we begin with the cloud security ecosystem, we must baseline the three massive services – namely, Amazon Web Services (AWS), Microsoft Azure, and (ironically) Google Cloud Platform (GCP). The vast majority of enterprise cloud usage scenarios start with these cloud services, which in many cases must be used in the context of a multi-cloud architecture requiring coordination, integration, and orchestration of workloads and applications.

Into this multi-cloud ecosystem, the security industry has enjoyed a plethora of highly successful and valuable companies such as Palo Alto Networks and Wiz, which address the cloud security needs of buyers based on tough competition, high demands for innovation, and the on-going need to track threats from malicious actors ranging from hackers to well-funded nation-states. The resultant diverse cloud security ecosystem is represented as in Figure 1.

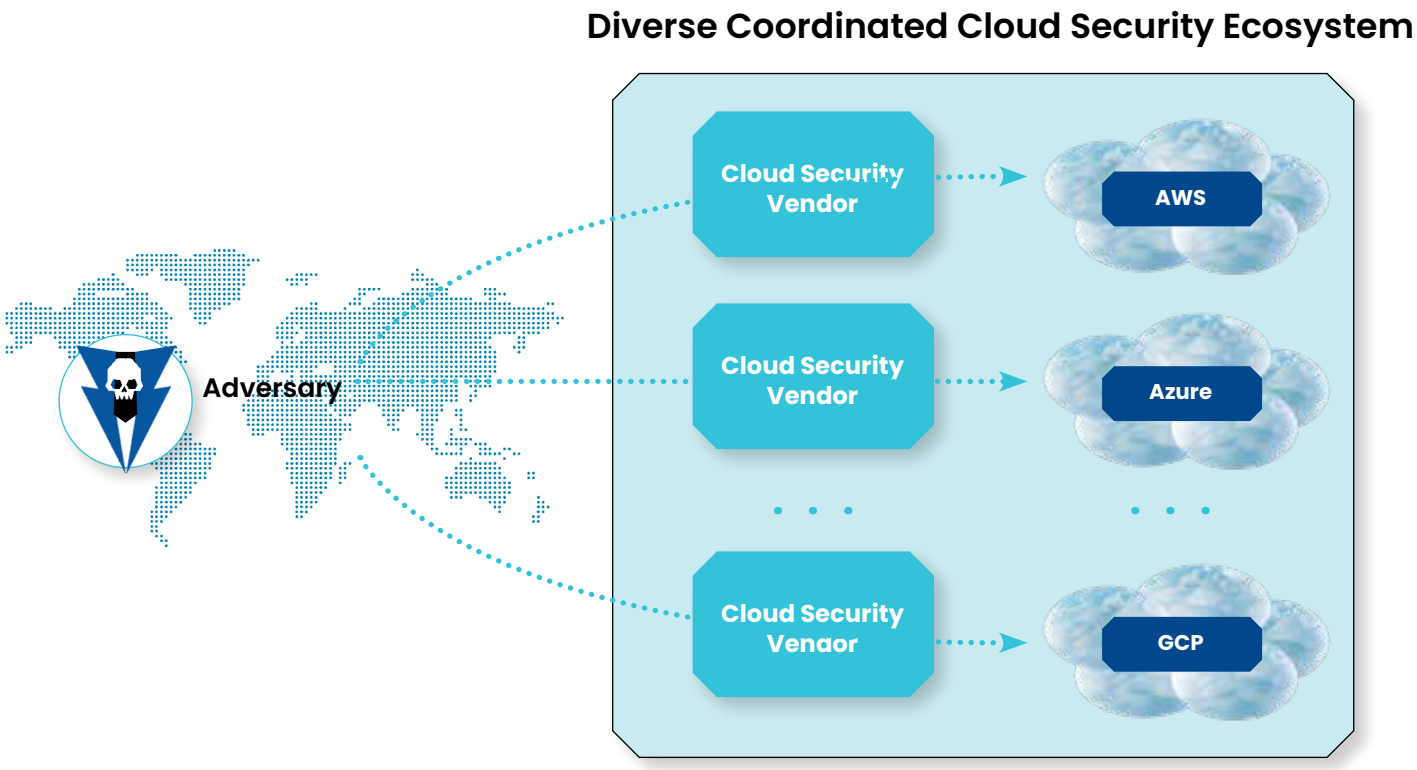


Figure 1. Diverse Cloud Security Ecosystem

Similarly, the mobile app security ecosystem also must be baselined with large companies – namely, the two focused on in this report: Apple and Google. Whereas, however, the three cloud service providers (which, as mentioned above, includes Google) provide a basis for security vendors like Wiz and Palo Alto Networks to sell products and services, the manner in which this is done for mobile app security stifles establishment of similarly successful vendors.

That is, what we see are two powerful mobile operating systems companies bundling the majority of security themselves. The perceived success of Apple and Google provides comfort to consumers who seem satisfied with present levels of security.[26] Our concern, however, is that in any monopolistic monoculture, the adversary need only exceed the capability of one company, rather than a diverse ecosystem of successful vendors and providers (see Figure 2).

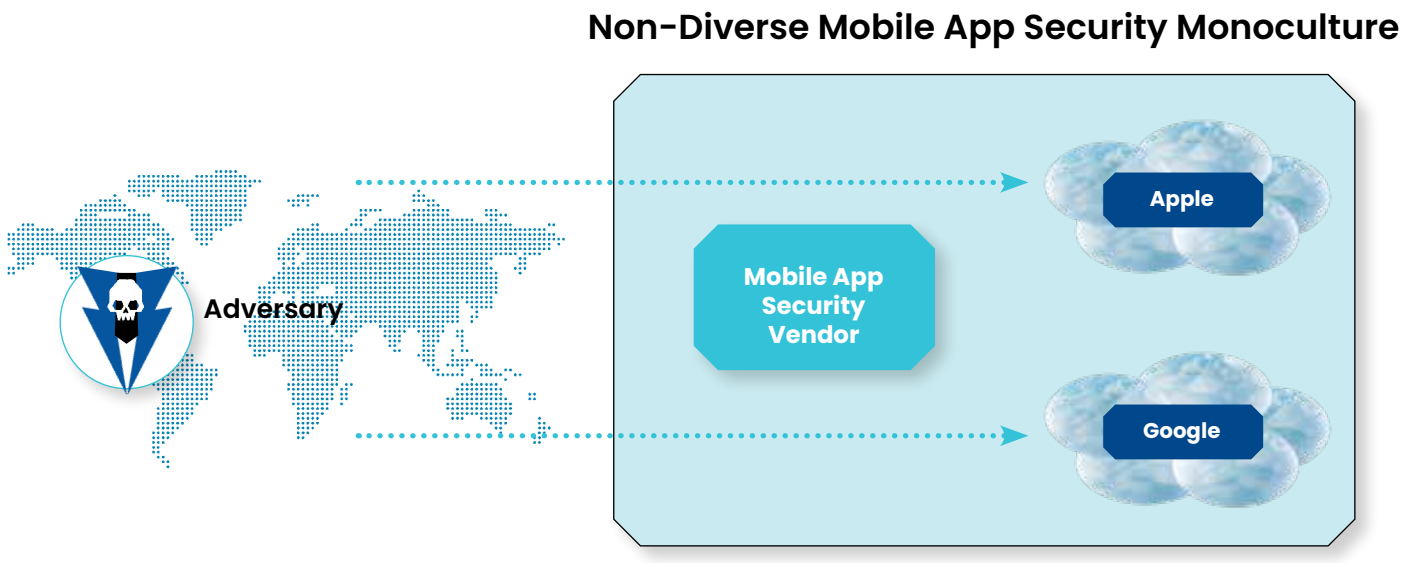


Figure 2. Monoculture Mobile App Security Ecosystem (Bypassing Security Vendors)

Recommendations for Mobile App Security

In this section, we make our series of five recommendations. We feel obliged to underscore that readers should understand our motivation as having nothing to do with geopolitics. That is, we are neither touting nor recommending shifts away from Apple and Google toward providers located in China. Instead, our motivation is to enhance the spirit of global competition to drive greater levels of innovation for all users, both inside the United States and out.

Each of our recommendations below is offered as an action statement, followed by a technical explanation and business rationale. We would hope that global policy influencers and corporate decision makers in both public and private organizations will read these recommendations and perhaps consider their suitability for government and business strategy. Both authors are available for comments, suggestions, and questions from readers.

Recommendation: Apple and Google must facilitate the use of third-party mobile app security vendors more effectively.

Apple and Google should open their ecosystems to third-party mobile app security solutions.[27] Such a strategic move, which could be associated with a vendor certification and review process, would enrich the security landscape with new and innovative approaches and would attract more specialized expertise. A partnership model could be established where certified vendors are recognized within the app stores, thus ensuring compliance with high standards.

---

[26] *We must mention that companies such as NowSecure and Approov have well researched reports showing that 85-95% of apps are leaking credentials and API keys. There are also long lists of privacy concerns where app developers are abusing access rights to contacts.*

[27] *Again, this is hardly the first time this suggestion has been mentioned or written about. Here, for example, is a typical article explaining the various means by which organizations such as the European Union have pushed for, or passed laws for, a more open app ecosystem:* https://www.bloomberg.com/news articles/2022-12-13/will-apple-allow-users-to-install-third-party-app-stores-sideload-in-europe.

If one wonders why Apple and Google would do this, we would offer three reasons: First, it would lower the sole burden for both companies of having to stay ahead of capable nation- state adversaries in cyber. Second, it would have zero impact on Apple and Google's bottom-line revenue. In fact, one could imagine it removing many barriers to mobile app usage (e.g., for future elections).[28] And third, it would remove the possibility for future legal action.[29]

Funding such ecosystem development and support should also be a simple process for two companies whose combined market capitalization is almost five trillion dollars.[30] That number, combined, is larger than the gross domestic product (GDP) of every country in the world except the US and China. These companies hold staggering valuations so asking them to enhance the mobile app ecosystem to avoid future threats is hardly unreasonable.

Recommendation: Apple and Google must financially incentivize developer-led mobile app security initiatives.

Developers who invest in robust security measures, either through third-party vendors or by implementing their own solutions, should be rewarded with reduced commission rates. This approach would not only encourage better security practices but would also provide financial relief to developers working in this area. A structured verification process, aligned with industry standards, could assess these security measures for efficacy and compliance.

It is clear to the authors that incentivizing developers has always been the best way for large companies to influence their industry. This point is made not just for individual developers who work in isolation or as consultants, but more so for ones who might make the decision to start new companies focused in this area. They must see a path to significant hyper-growth akin to vendors such as Wiz and Palo Alto Networks before they will take the risk.[31]

Apple and Google should also implement a tiered discount system on commission fees for developers using certified security solutions. These massive companies can easily create a financial incentive to prioritize high-quality security. This system would recognize and reward the efforts of developers to adhere to the highest security standards, thereby enhancing the overall security posture of apps within the ecosystem.

Recommendation: Apple and Google must adopt open standards for mobile app security evaluation.

Transitioning to widely recognized open standards, such as those developed by the Open Web Application Security Project (OWASP) for app evaluations would help to democratize the cybersecurity review process for mobile apps.[32] This strategy would ensure that security measures are being judged against a transparent and equitable benchmark, thus fostering trust among developers, security vendors, and users alike.

---

[28] This point regarding elections is only mentioned in passing but is worth emphasizing. It is a sad fact that elections today do not utilize mobile apps, and the potential for hacking of these mobile apps is the primary reason for paper use. For future generations to truly trust the mobile app ecosystem, we believe an open and collaborative model must be in place to drive greater confidence amongst citizen voters. It seems inconceivable that without vibrant, well-incentivized startups and vendors supporting mobile app security with high valuations and growth that we will ever see public elections held using iPhone and Android devices. Obviously, these security issues would not be the sole factor in driving such a transition, but it would be a major one.

[29] The EU's Digital Markets Act was a strong move that produced an interesting non-response from the White House which included verbal response, but no substantive objection. See https://www.washingtonpost.com/technology/2024/03/07/eu-digital-markets-act-biden-dma/.

[30] Obviously, this goes up and down, but the number is directionally correct. See https://www.businessinsider.in/stock-market/news/apples- market-cap-is-larger-than-all-but-6-of-worlds-top-economies/articleshow/106032676.cms.

[31] One of the authors (Miracco) obviously understands the risks and challenges of building and operating a mobile app security company – and our request here for Apple and Google to incentive developers would certainly create more competition for Approov and other vendors working in this area. The suggestion is made here, nevertheless, because it is clear that such action would be in the best interest of the mobile app ecosystem and with greater competition will come a more vibrant market.

[32] The excellent app verification and review standard from OWASP that we would recommend for use in the mobile app security context is explained here: https://owasp.org/www-project-application-security-verification-standard/.

Of all our recommendations, this one seems the most straightforward, since it drives the set of evaluation criteria to an open process. That said, we suspect that this recommendation might be the least welcome by Apple and Google, given their traditional focus on great secrecy in how they provide security. Every security expert knows, however, that security through obscurity, even when done by highly capable actors in strong organizations, eventually fails.[33]

It is perhaps worth adding here that such standards adoption should extend to the mobile payment ecosystem. We believe that Apple and Google should allow developers to utilize alternative certified payment systems. Such action could reduce transaction costs for these third parties and would increase autonomy, provided that such systems adhere to stringent security and privacy standards.

---

[33] Perhaps the greatest on-going experiment in security through obscurity lies in the global intelligence community, where classification and clearances are used to create legal walled gardens. Despite such baroque actions, organizations such as the National Security Agency (NSA) have had spectacular breaches, often from insider action, which call into question such means. We are not suggesting that NSA declassify their operations, but instead are pointing out that cybersecurity at the enterprise level benefits from open standards and community collaboration.

ANALYST REPORT

HYPERAUTOMATION FOR WINDOWS ENDPOINT AND VULNERABILITY MANAGEMENT: AN OVERVIEW OF THE AIDEN SOLUTION

DR. EDWARD AMOROSO, CHIEF EXECUTIVE OFFICER, TAG

This report from the industry analyst team at TAG Infosphere[1] explains the benefits of hyperautomation for Windows endpoint and vulnerability management in enterprise environments. The commercial solution from Aiden Technologies[2] is used to illustrate this modern approach to information technology (IT) and security in practice.

INTRODUCTION

Any security practitioner will attest to the frequent exploitation of Windows endpoints by malicious adversaries. Similarly, any IT manager will reference the difficulty that has existed for many years dealing with the day-to-day challenges of managing Windows endpoints. This includes handling trouble tickets, performing troubleshooting, supporting patching, and generally maintaining the desktop images selected based on IT and security needs.

A key organizational difficulty that we've seen emerge frequently across our TAG Research as a Service (RaaS) base of enterprise customers is the siloed responsibilities that exist between IT and security teams. This gap is exacerbated by the fact that so many commercial platforms tend to target one group or another – offering this platform for the security teams and *another* platform for the IT teams. Silos are never welcome in an enterprise environment.

We were thus delighted when we began to investigate and learn about the approach being taken by startup company Aiden. They have shared with us their approach to Windows endpoint management and also cybersecurity, with emphasis on the integration required to make sure that both concerns are met seamlessly. The resulting benefits for cyber hygiene, digital end-user experience, and compliance are impressive.

This report focuses on the underlying force behind Aiden's solution, which they have described to us as *hyperautomation*. The idea, as we will discuss below, is to leverage automation powered by artificial intelligence (AI) to streamline the various IT and security tasks referenced above. The result, as we have come to understand and admire, is a software-powered service that combines intelligent software packaging, an AI bot, and reporting into a unified solution that works seamlessly with an [3]existing deployment tool.

MODERN IT AND SECURITY CHALLENGES FOR WINDOWS

It doesn't take a rocket scientist to realize that enterprise-deployed Windows systems are vulnerable to cyber threats. Accordingly, the process of keeping up with Windows vulnerabilities has remained a significant challenge for IT and security teams, with exploitable flaws and bugs being reported on an ongoing basis virtually every month.[4] This requires considerable time and expense from enterprises to remediate.

Several options exist to handle this challenge. First, enterprise teams might reduce their use of Windows products, but this is neither advisable nor reasonable. Microsoft provides such high value to organizations with its amazing suite of software solutions that it would be ill-advised to avoid use of such products. Instead, clear trends exist that show nothing but an increase in the use of Microsoft software in the enterprise.[5]

A second possibility would be to increase staff and ask teams to be more diligent, and to just work harder. This is also not reasonable, especially given the amazing progress that enterprise IT and security teams have made since Microsoft patches became an important issue, arguably after the 2003 SQL/Slammer worm. Since then, one could make the case that most security teams have created highly efficient processes, albeit barraged by growing advisories to handle.

The best choice in our estimation to handle this problem involves the selection, deployment, and use of an automated platform that manages the Windows environment efficiently, replaces manual tasks with workflow, and that takes advantage of the best available technology such as artificial intelligence, to ensure that the automation is complementing existing processes and dealing with the highest priority issues.

BENEFITS OF AI-POWERED AUTOMATION FOR WINDOWS

The general advantages of hyperautomation are beginning to become much better understood across the IT and security ecosystem. Earlier-generation practitioners in these areas might have been somewhat wary of relying too heavily on automated platforms, tools, and processes, but recent advances in AI and related technologies have made automation no longer a preference but an absolute requirement. The key advantages come in three areas:

- **Reduced Complexity** – This is imperative in the context of Windows infrastructure, given the many different desktop images, build processes, software deployments, and helpdesk ticket support that exist in a typical environment. Reduction of complexity should be the number one goal, and hyperautomation is a strong solution to this problem.
- **Reduced Cost** – The operating costs associated with Windows management are often overlooked. Experience dictates that operating expenses are related to complexity (as explained above), so when complexity is reduced, every aspect of budget allocation will see relief in terms of staff, tool, and consulting costs.
- **Reduced Lifecycle Time** – Whenever IT and security teams are asked about their greatest challenges supporting complex Windows environments, the discussion eventually turns to long cycle times for the various tasks, including deployment and patching. The obvious solution here is automation, but as has been explained above, this must be implemented with care.

- **Improved Context for Reporting** – The deployment of hyperautomation for Windows systems increases the accuracy and relevance of the context associated with real-time reporting of both the present and desired states for all endpoints and servers. As one would expect, this context ensures that tasks such as updates and patches are done appropriately.

These advantages of hyperautomation in the context of IT and security for Windows might seem elusive and perhaps even academic, but the good news is that practical solutions are available today that can be used to leverage a more automated support ecosystem. In the next section, we provide a brief overview of just such a commercial solution from a company called Aiden Technologies.

AIDEN PLATFORM OVERVIEW

Founded in 2020 and headquartered in Texas, Aiden Technologies provides an automated IT solution that utilizes hyperautomation powered by AI to streamline software packaging, deployment, patching, and compliance for Windows-based systems. Their solution lines up well with the types of issues raised above, and they provide an excellent case study in how a commercial solution can succeed in this area.

The goal of Aiden is to support the day-to-day needs of an IT team with their Windows infrastructure. The specific components of the solution and the company that uniquely address this IT and security goal for customers include the following:

- **AidenBot** – This works by leveraging the existing Windows software deployment tool already in place for an enterprise. What AidenBot does is use a desired state policy, written in English, to set up and maintain all your computers based on a defined schedule that is determined by each customer. This is possible by using hyperautomation to create complex task sequences of AidenCore packages, and then using the deployment tool's agent to start the process on each device.
- **AidenVision** – This is a policy-based dashboard that supports compliance by making recommendations for improving the endpoint security posture, usually with guidance on update, configuration, and security state. As one might expect, this approach is invaluable to drive a more proactive compliance program.
- **AidenCore** – This is the underlying core library of intelligent software packages that is leveraged by the AI-based processing in support of the overall Aiden experience.
- **AidenLabs** – As one might expect, despite the fact that automation is the primary goal, Aiden maintains an expert team of automation engineers who work with customers to help them achieve their goals to ensure packages are created and customized according to the needs of the enterprise. This is especially important in specialized environments with unique software in place.

The Aiden solution is by no means a replacement for existing Windows deployment tools, but rather makes the maintenance of deployed infrastructure much easier to manage, much simpler in terms of resource needs, and much more in line with the goal of continuous compliance and cybersecurity. To that end, Aiden has developed deeper integrations with some platforms, such as 1E, and already works natively to automate the software deployment work in common platforms such as Microsoft's Endpoint Manager suite (SCCM, Intune/Autopilot, and WSUS), Automox, BigFix, ManageEngine, Tanium, Workspace One, and many more.

RECOMMENDATIONS FOR ENTERPRISE

Based on our experience at TAG working with many dozens of corporations trying hard to streamline, simplify, and automate their Windows endpoint deployments, update processes, security, and management, we would offer the following recommendations for IT and security teams to consider as part of the immediate-term action plan to improve service levels and reduce cost:

Recommendation: Perform a comprehensive inventory review of your existing deployment tasks and tools in place today for Windows systems.

We strongly recommend that, as a base task, every IT and security team engage in an inventory review of their existing IT tasks and support systems in place for Windows. This should include a review of hardware deployment, configurations (e.g., OS, machine refreshes), software deployment, updates, upgrades, removals, rollbacks, and security (e.g., ransomware response, disaster recovery).

Our experience is that improvements to inventory are always a good idea, regardless of any subsequent management action. Commensurate with this task analysis, we also recommend a deep dive into the deployed commercial, open-source, or even home-grown tools that are in place to support these tasks. A pro/con analysis is recommended for each one to determine the future plan.

Note that solutions such as Aiden are not intended to replace these existing systems, nor are they intended to fundamentally change the required tasks that must be done for Windows devices. The solution is intended to make these tools and tasks operate more effectively – hence, the development of an accurate inventory will help to better define the baseline on which to deploy a solution such as Aiden.

Recommendation: Review the current posture of Windows device lifecycle management from a support and cost perspective.

This posture review task can be done in a qualitative or quantitative manner (or best case – both). The objective here is to determine where the strengths in an existing Windows support program exist, and there might be many areas in which the current process, platforms, and staff are working quite effectively. This is often determined by asking the user base, perhaps through formal or informal research, interviews, or surveys.

The weaknesses and gaps, however, might require a more in-depth analysis, especially in terms of operating costs that might be higher than necessary for deployments, patching, and other required Windows device tasks. A comprehensive review would be best done with involvement from a variety of teams including IT, security, finance, and even business units who are dependent on their Windows devices to support the local mission.

As with the inventory, the purpose of the posture assessment is to establish an accurate baseline on which to begin planning for hyperautomation. Our experience at TAG is that the number one reason automation programs might not realize their full potential is that they are often done across systems that are too complex and for which the support team does not have a good understanding and insight.

Recommendation: Review the current posture of Windows device lifecycle management from a support and cost perspective.

As one might have expected, our final recommendation is that IT and security teams immediately begin the review, source selection, test, evaluation, and deployment process for a hyperautomation solution along the lines of what we've discussed throughout this report. We also recommend that AI serve as a key requirement since this really does make a difference in the accuracy and effectiveness of a given tool.

Our experience with Aiden Technologies is that their solution really fits the bill in terms of the requirements we've emphasized above. Obviously, every environment will be different, so we will leave it to readers to engage directly with Aiden to determine the appropriateness of a 90-day happiness guarantee or other suitable platform evaluation. Local tools, unique software, and other legacy situations can be reviewed during such activity.

As always, our team at TAG Infosphere is available to readers to help them with their IT, cybersecurity, and compliance-related decisions about commercial vendors and other practical matters. Subscribers to our TAG Research as a Service (RaaS) can reach out to us directly through their portal accounts, and others can contact this author at the email address listed at the top of this report.

---

[1] TAG Infosphere is a New York City-based research and advisory firm founded in 2016 and focused in the areas of cybersecurity, artificial intelligence, and climate science/sustainability. TAG provides analyst reports such as this one as a general service to the industry with unbiased and expert judgment focused on the needs of enterprise and government practitioners. See https://www.tag-infosphere.com/.

[2] The automated IT security platform for Windows endpoint and vulnerability management from commercial vendor Aiden Technologies is explained in detail on the company's public website: https://www.meetaiden.com/. The Aiden team assisted with the technical content here.

[3] It is worth mentioning that most organizations can handle addressing vulnerabilities but might lack the budget ad staff to effectively manage the growing number of threats. The result is a need for automation to avoid gaps.

[4] As a recently published example, see this security advisory from the Center for Internet Security (CIS) on the on-going stream of Microsoft Windows vulnerabilities: https://www.cisecurity.org/advisory/critical-patches-issued-for-microsoft-products-march-13-2024_2024-027.

[5] In Microsoft's FY24 Q2 earnings release, available on their website, they reported growth in revenue across different segments, indicating an increase in sales, including to enterprise clients. Key highlights include a total revenue of $62.0 billion, marking an 18% increase. Specifically, the Productivity and Business Processes segment, which includes Office Commercial products and cloud services, saw a 13% revenue increase.

EMPOWERING LEADERSHIP FOR SECURE INNOVATION: INTEGRATING SECURITY BY DESIGN IN CORPORATE CULTURE

DR. EDWARD AMOROSO, CEO, TAG

GETTING STARTED WITH SECURITY BY DESIGN

Software developers and cybersecurity practitioners interested in engaging in a new program of Security by Design are encouraged to keep in mind several design principles that we've found to be effective in practice. The first principle involves recognition that modern security leaders have considerable challenges that must be addressed. This implies that process improvement is focused on solving real problems.

The second principle is that Security by Design is best adopted and maintained as a combined executive and corporate initiative. That is, the approach is not to be done in isolation but rather through an integrated program of executive sponsorship and developer adoption. This includes the provision of the proper resources and support so that the design approach can be translated into actual security preventive actions.

A third principle worth mentioning is that the roles and responsibilities for achieving Security by Design should be clearly identified. Leadership, in particular, should be tasked with driving a culture that supports doing things correctly from the beginning, rather than waiting for problems and responding afterward. Such emphasis on culture ensures that involved developers and security team members will make good decisions in practice.

ESTABLISH EXECUTIVE ALIGNMENT

As suggested above, leadership must set the tone for Security by Design. The 2023 Secure by Design paper by CISA and others acknowledges that it must be both an executive and a company-wide initiative. Full buy-in at the senior executive level is crucial, ensuring that even if initiated by middle managers and application security leaders, they receive full senior executive support.

This means Security by Design requires alignment throughout the organization, from setting correct priorities and incentives at the executive level to implementation and follow-through at the operational level. This alignment should not dictate specific development decisions, like the choice of threat modeling tools or AI assistants but should ensure that development team priorities are in line with the organization's overall mission and goals.

ENSURING FULL GRASSROOTS ACCEPTANCE

While executive buy-in is critical to a culture of Security by Design, the organizational focus must always be on the software developers. Introducing this new development paradigm involves a significant change in the lifecycle approach, and it is thus often met with resistance (as with any type of substantive change). Developers may question its applicability or impact on their workflow.

For example, if an executive explained to an entire company the goal to integrate and implement Security by Design *today*, then this will almost certainly create immediate resistance. Developers might say things like, "Well, I don't know if it's going to work for us." Or they might say, "I don't understand what this means to me or how it affects my workflow." These are common responses to any executive demand for change.

To address these concerns, teams should implement proper cultural change, including basic practices such as running pilots, finding the right teams to adopt the technology first, encouraging teams to adopt new practices, and embedding Security by Design into the performance review and incentive process. These commonsense steps will help to ease an organization into the more preventive approach for software security.

The overall approach may also be enhanced by recruiting developers who are passionate about security and are willing to be trained as security champions so that there are embedded security-trained developers within the working groups who are responsible and accountable for delivering secure code. This serves to create cultural train from within the software development community.

THE IMPORTANCE OF CULTURE IN SECURITY BY DESIGN

Security by design involves integrating security from the very beginning of the development process. But one of the most critical aspects of driving this approach involves the culture that embraces this attention, and that is perhaps the hardest part of building in security by design because it references people, processes, and their interactions during development.

The first step in establishing a strong culture of Security by Design involves convincing developers to make security a key requirement. This is not to say there aren't security aware and responsible developers, but when it comes to their job function, they might not be compensated or incented to focus on security. Tools and co-pilots will help, but mindsets and incentives must shift.

We've consulted Security Compass, experts in Security by Design and they agree that it's common to encounter developers who are wholly aligned to the production of value for end customers, but less so on ensuring security. They focus on shipping features, fixing defects, and other tasks that are directly related to the customer's needs. And while security might be important to an individual developer, it's too often not seen as their particular job responsibility.

Referencing the CISA paper once again, there is motivation to provide security as a default feature of products (and the software and applications within them) rather than as a luxury feature. So, with this proposed shift in customer expectation for security, there's an emerging trend to shift the development culture to consider security as a valuable product feature as well.

SUPPORTING DEVELOPERS ON SECURITY

At TAG, we have observed that in many companies, developers will say that it's the CISO-led team's responsibility, usually in an application security group, to ensure the security of code. The problem, obviously, is that the cybersecurity team is not the group developing and writing code. Furthermore, it is not uncommon for application security teams to have only a surface understanding of the actual software development process.

Security Compass's survey revealed that 74% of developers engage with security after the design phase. Responders claimed to not think much about security in the design phase. They don't have the right tools, they're building software too quickly, and they don't have time to slow down and think about security. They are also not traditionally trained in security and will usually see it as slowing down their coding.

When the Security Compass team explains Security by Design, they emphasize providing developers with the required security support and training they need on methods such as threat modeling, secure coding, and other proactive means. The goal is to drive integration of security into the planning and coding phases of the DevOps lifecycle. At TAG we believe that this might be the secret to significantly reducing the intensity of breaches.

ROLE OF SECURITY EDUCATION

Rather than viewing security as the sole responsibility of some different department, software teams must learn to embrace security, starting with the design process. This shift in emphasis requires that excellent security educational resources be available to develop security skills and to establish grassroots support across all aspects of the software lifecycle teams. Executives should ensure support for such objectives.

The Security Compass team recommends starting the Security by Design journey with an intense focus on creating and maintaining world-class cybersecurity education for teams and their members. We agree wholeheartedly with this approach. In fact, this can include in-house or external support, but education is an essential component of establishing a culture of Security by Design.

The next step is to embed this security knowledge within the development teams. One way of doing this involves establishing security champions or security coaches into the development team and making them the steward for security in that team. Their job is to localize and tailor the learnings and best practices developed across the organization. With background and training in development and then a specialized focus on security, they will have the right empathy and understanding for the day-to-day concerns of the development organization.

SECURITY AS PRODUCT QUALITY

A key question for developers is whether they have sufficient confidence in their software. Think about the pride developers have in functional and elegant code. Now, what if they could also build up their pride in coding securely? What would happen if a typical developer could be willing to discuss with a compliance regulator or external auditor the specific preventive design steps that were taken to integrate security into the software?

The good news is that this trend is changing for the better. There are white papers being put out in countries such as the United States, Australia, Canada, the UK, and many other countries around the world about shifting the balance toward security by design and more preventive approaches to software security. The emergence of artificial intelligence co-pilot tools is consistent with this shift left toward creating better software from the start.

CREATING IMPROVED SOFTWARE

Are there other events that motivate developers to develop functionally as well as securely? A recent US Executive Order, for example, discussed improving the nation's cybersecurity and specifically addressed software supply chain through use of tools and constructs such as software bill of materials (SBOM). This method involves automated development of a list of open-source components that the software includes so that users know what they need to patch and where there might be inherent vulnerabilities.

But that executive order also created and helped to spur the NIST secure software development framework, which is a comprehensive approach to addressing security in the SDLC. And this is especially welcome because for one reason or the other, the software community hasn't had good standards for security by design considerations.

The implications for software by design in different industry verticals is encouraging. For example, the US Food and Drug Administration (FDA) could begin requiring threat models in pre-market submissions for medical devices, the payment card industry (PCI) could demand security by design as a mandatory strategy for software, and this can continue across all type of critical sectors.

An impact of all this is that there are additional external factors that can influence the developer organization's motivations and mindset. Software companies must reflect on their obligations to these external stakeholders that make security a requirement and that contribute to the case for security by design.

VALUE PROPOSITION FOR SECURITY BY DESIGN

Ultimately, the goal is to establish a clear value proposition for each stakeholder in the company regarding Security by Design. And this value proposition is rooted in changes around how developers work today, with the goal of finding ways to improve their work and the quality of the software they are producing.

It's key, when establishing a value proposition, that the right stakeholders be included in the process. If the right stakeholders have input to the Security by Design plan, then they can help reduce the likelihood that developers see no problem that needs solving, which can lead to resistance. This can happen at any level of the organization including executives.

The time to implement is also a key consideration. If you tell development teams that they must immediately implement every tenet of Security by Design, then you might introduce serious conflict with requirements promised to customers or included in a delivery schedule. Development teams need time to adjust, so the process should be introduced incrementally.

ADDRESSING SCALE IN SECURITY BY DESIGN

Another common problem that emerges with any change in the development paradigm involves the challenge of scale. For example, a small group of developers might decide to buy into some useful technique such as threat modeling or AI assistance and they might begin to use this in their local software process. This is usually a good decision from a security perspective and will help the quality of their code.

But the scaling of this decision across a large development team usually demands more than just word-of-mouth sharing. Instead, proven methods such as threat modeling must be associated not only with an initiative to scale but must be connected to the deployed platforms that support automation and continuous operation, two features that are absolutely necessary for scale.

This implies that careful consideration must be made into the number of hours required for Security by Design activities, as well as other staff and resource requirements. We've seen proposals for threat modeling, for example, that would introduce hundreds of hours of work to a development process that must deliver in weeks. Obviously, this would cause problems in the time planning for the development team (as well as serious push back on the proposed changes).

PROVING THE VALUE OF SECURITY BY DESIGN

Let's suppose that an important goal is to drive adoption of Security by Design at the grassroots level. The hope is that developers will start to integrate the basic tenets, including methods such as threat modeling or AI support immediately into all aspects of their software development lifecycle, for all the reasons cited above.

A common complaint is that Security by Design is too conceptual and theoretical. And the question emerges: *Can you prove to me that this is worth the time and effort?* Our assessment with Security Compass is that the proof emerges with application. That is, by beginning the process of applying the basic principles, immediate value begins to emerge.

The most common benefits are more secure software with fewer vulnerabilities. Developers immediately begin to see that they are spending less time on manual tasks, because they have introduced automation. In short, the idea here is to prove value by implementing. This does demand that management have the courage, determination, and skills to drive piloting.

ACHIEVING RESULTS WITH SECURITY BY DESIGN

The payoff for Security by Design must be results. Without tangible, measurable improvement, cultural changes and methodologies will quickly fade away. Developers are too busy to be worrying about the latest fad in software security or process improvement. So, achieving results quickly is a mandatory aspect of the process.

The good news is that Security Compass reports having seen amazing results. In one study with a customer, the company saw an 85% reduction in high-risk vulnerabilities. That means lower risk, but it also means less unplanned time for developers. And if there's one thing that every developer knows, it's that unplanned work kills both quality of code and productivity of work.

This implies that one of the core benefits of Security by Design involves knowing what your work is going to be ahead of time. This helps avoid the situation where you are constantly trying to catch up, fixing vulnerabilities when they come up unexpectedly. With Security by Design, you are implementing security controls at a pace you can control.

MOVING FORWARD WITH SECURITY BY DESIGN

Our advice at TAG – and this is consistent with the guidance we've received from Security Compass – is that to start, managers should focus on two primary benefits. First, they should address the quality of work and software process improvements mentioned above. This lies squarely with the developers, and it demands buy-in at the grassroots level and agreement to focus on improvements to culture and enhancements to platforms through automation.

But second, managers must address more hardline issues such as cost. Our experience is that return on investment (ROI) for Security by Design can be significant, and this will be of interest to finance and senior leadership teams. The basis for the involves fewer vulnerabilities driving less reactive and unplanned work. Those hours get focused on building features and delivering benefits to your users.

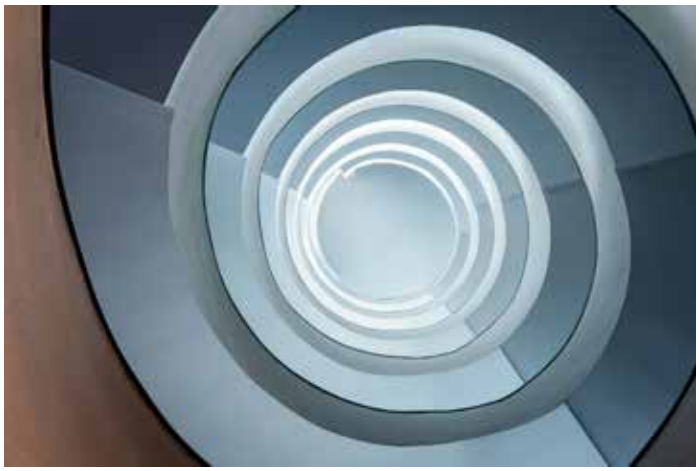
The cost savings can be enormous. We have seen many companies who claim that a more proactive approach to software security using Security by Design might be the highest ROI component of their entire application security program. This should be intuitive – namely, that avoiding problems up front should save money – and it does.

SECURITY BY DESIGN ACTION PLAN

Let's discuss next steps for your organization. We strongly believe that all software teams should have an action plan in place to drive a Security by Design approach. We assume this would be done in the context of modern DevOps and CI/CD environments, but it can be introduced into any software process paradigm in place.

The action plan should be a multi-step journey, one that involves cultural change. It also needs the active involvement of your people, process, and technology. Work the action plan across all layers of management, up to and including your executives. But recognize that your grassroots developers ultimately will have to buy into the action plan.

At TAG and Security Compass, we are committed to helping your team with your Security by Design objectives. Security Compass has organized its entire company and support for customers around this key concept. Security Compass believes that partnership with their customers can be a critical support element in achieving the goal of Security by Design.



ANALYST REPORT

CONTEXTUALIZING CYBER RISK AND STRATEGY IN BUSINESS-FRIENDLY TERMS USING X-ANALYTICS

DR. EDWARD AMOROSO, CEO, TAG

This report from the industry analyst team from TAG Infosphere[1] explains how cyber risk can be contextualized for executives and boards in business-friendly terms. The commercial solution from X-Analytics[2] is used to illustrate such risk management reporting in practice. The approach shown to represent an effective means for boards to improve their communication with security leadership.

INTRODUCTION

The formal presentation of cyber risk information by Chief Information Security Officers (CISOs) to the senior leadership of an organization, including their board of directors, is now commonly included in all executive communications. Board meetings, for example, will routinely include detailed reports from CISOs, often with substantive coverage of key internal and external security issues of potential interest to the executives.

A nagging problem, however, is that despite good intentions, a communications gap remains between CISOs who must address day-to-day technical issues and their leadership teams who must focus more generally on business themes such as finance, marketing, and operations. Care must be taken by CISOs to avoid the trap of over-simplifying their reporting. Executives can be led astray by such simplification, often thinking that security itself is simple.[3]

An additional issue is that the US Securities and Exchange Commission (SEC) has significantly increased pressure on executives to be more open and communicative about material breaches. This requires good coordination between boards, senior leadership teams, and security executives. Fostering such communication is in everyone's interest, despite the fact that most reporting tools today are geared toward practitioners.

In this report, we offer guidance on how CISOs should be contextualizing their reporting of cyber risk to executives. We show how this is best done with focus on providing guidance that is presented in business-friendly terms, but never through over-simplification. The commercial platform from X-Analytics is used to illustrate this executive reporting approach in a practical executive reporting environment.[4]

OVERVIEW OF CYBER RISK REPORTING

A major recent change in how corporate boards address risk with their executive teams is that cybersecurity has emerged as a high priority consideration in discussions. This should come as no surprise since business risk is best viewed in the context of those assets viewed as necessary to achieve the organizational mission. Since cyber assets are at the heart of most company operations today, cyber risk emerges accordingly.

On first glance, such emphasis might seem like a minor shift in focus, perhaps requiring some additional training for board members less schooled in modern technologies. The problem, however, is that board members often make decisions based on instinct, sentiment, and experience – and since in the context of cyber these are all commonly lacking in board directors, chief information security officers (CISOs) cannot expect boards to rely upon these instincts in cyber.

Several solutions are available to deal with this communication challenge – in addition to the training option just referenced. One approach is to recruit one or more new board members with sufficient cybersecurity expertise as to complement the backgrounds of the other members. This works on occasion, but many cyber experts lack the general backgrounds required to be good board directors.

More commonly, the solution is for CISOs to work with a competent commercial vendor that can support the need to present cyber risk issues in a manner that board directors can accurately understand and use as the basis for their judgment. As suggested above, this cannot oversimplify, but rather must present the relevant risks in terms that are meaningful to senior decision-makers.

IMPORTANCE OF BUSINESS-FRIENDLY TERMS

The best approach, in our estimation, is for CISOs to begin understanding how to express their findings, requests, and challenges in the context of business-related issues. This implies that CISOs begin to use and reference more business-friendly terms so that the executive conversation can proceed more effectively, especially when cyber-related issues must be normalized and compared with non-cyber issues.

Consider, for example, that an executive team and board might have to considered whether to address risk-related issues related to changing climate in certain regions. These executives will listen to the experts who will provide such guidance in the context of impact to business operations, costs to adjust, and quantified implications if no action is taken and worst case (or most likely case) scenarios emerge.

To compare such investment decisions against comparable risk-related issue in cyber demands that the CISO present the information in similar terms. If a board, for example, hears that not moving a data center to a less climate-impacted region could result in tens of millions of actual dollars in losses, then comparing this to a CISO requesting funds to reduce cyber vulnerabilities from the thousands to the hundreds will have no meaning to the executives.

CASE STUDY: X-ANALYTICS PLATFORM

X-Analytics functions as a comprehensive cyber risk analysis and management software. It aggregates vast amounts of data from diverse sources, including threat intelligence feeds, industry benchmarks, historical incident data, and emerging threat trends. This data is then analyzed using advanced algorithms and analytics techniques to generate actionable insights into an organization's cyber risk posture.

X-Analytics supports improved communication via a standardized framework for assessing and quantifying cyber risks. By utilizing a common language and metrics, the platform enables security leaders to communicate the severity and potential impact of cyber threats to the board in terms that resonate with business objectives and priorities. This standardized approach reduces ambiguity and facilitates more informed decision-making at the executive level.

X-Analytics offers customizable dashboards and reports that present cyber risk data in a clear and intuitive manner. These visualizations highlight key risk indicators, trends, and mitigation strategies, enabling board members to grasp the significance of threats and understand the mitigations being taken. This enhanced visibility promotes constructive dialogue between the board and security leaders, which leads to a collaborative approach to managing cyber risks.

X-Analytics also facilitates scenario-based risk modeling, allowing organizations to simulate cyberattacks and assess their potential impact. By presenting the business, financial, and reputational implications of attack scenarios, the platform enables boards to prioritize investments in security measures and allocate resources effectively. This proactive approach to risk management helps organizations stay ready for threats, as well as inquiries from the SEC.

Finally, X-Analytics supports ongoing monitoring and reporting of cyber risk metrics, enabling business leaders and boards to track progress over time and evaluate the effectiveness of their risk mitigation efforts. By providing up-to-date business exposure and financial insights into the evolving threat landscape, the platform empowers organizations to stay ahead of emerging risks and proactively adjust their cybersecurity strategies as needed.

NEXT STEPS FOR ENTERPRISE

The decision to use a platform such as X-Analytics will typically involve several stakeholders, including the CISO, senior leadership including possibly the Chief Executive Officer, the secretary and other leaders of the Board, and perhaps key IT staff who will support the installation and use of the platform. Our experience to date is that most of these stakeholders are generally amenable to the use of a commercial platform for such use.

The challenge that emerges any time multiple stakeholders are involved in the selection and purchase of a commercial platform is where the budget should align for such purchase. We highly recommend that boards consider carrying the license fee here to free the CISO of such burden. Vendors selling solutions to boards such as cyber, as well as Director & Officer (D&O) insurance, or board reporting platforms might consider bundling platform such as X-Analytics in with their offer.

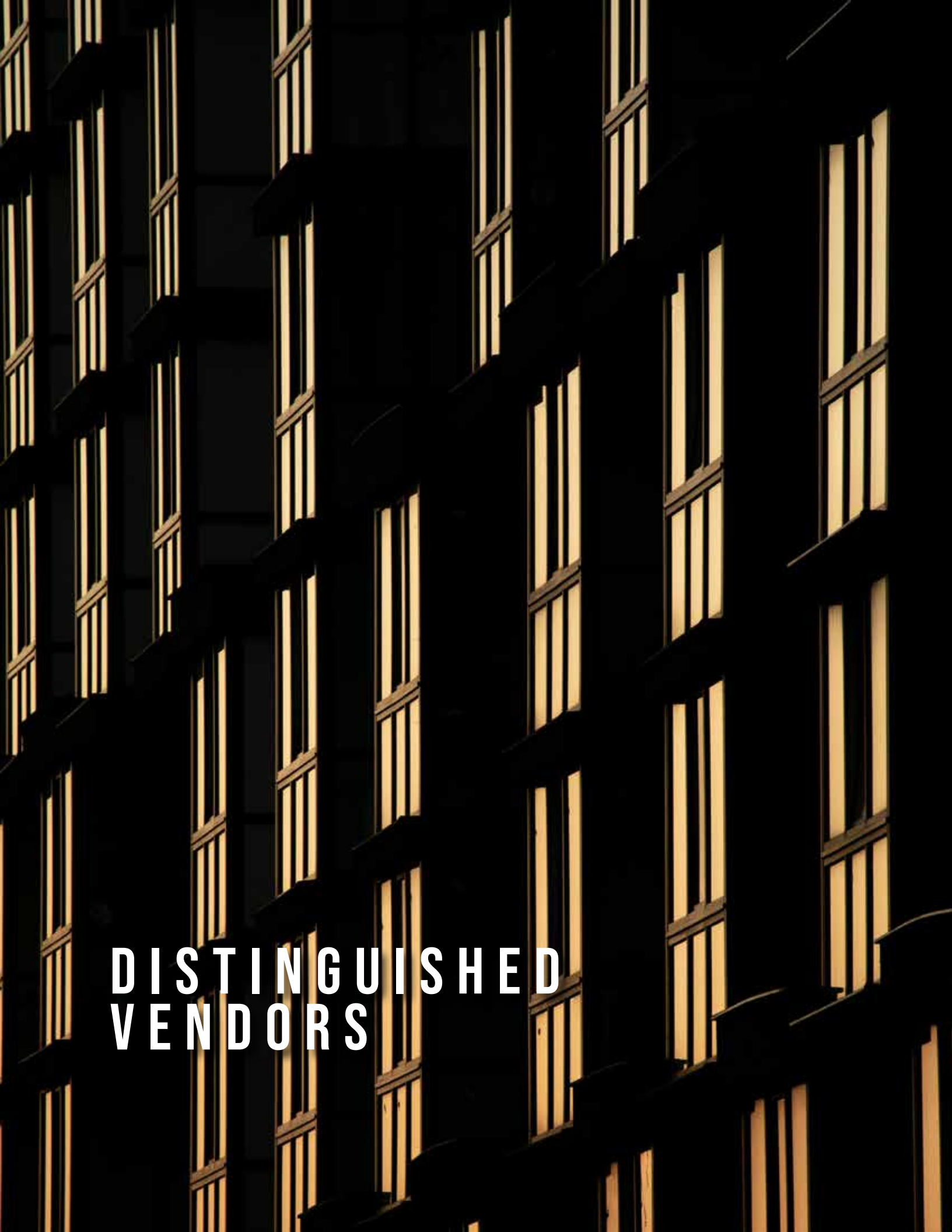
---

[1] TAG Infosphere is a New York City-based research and advisory firm founded in 2016 and focused in the areas of cybersecurity, artificial intelligence, and climate science/sustainability. TAG provides analyst reports such as this one as a general service to the industry with unbiased and expert judgment focused on the needs of enterprise and government practitioners. See https://www.tag-infosphere.com/.

[2] The risk management platform from commercial cybersecurity vendor X-Analytics is explained in detail on the company's public website: https://x-analytics.com/. The management team from X-Analytics was helpful throughout the generation of this report offering detailed guidance on risk analytics and insights into how executives and boards are presently ingesting information related to cybersecurity. We also spent considerable time discussing budget issues and how X-Analytics might be bundled into existing commercial offerings for boards.

[3] Einstein is famously quoted as having said the following regarding the avoidance of over-simplifying a given concept: "Everything should be made as simple as possible, but no simpler." While this is a great point, and can certainly be applied here to our comments on cyber risk reporting, it is worth noting that what Einstein actually said in a 1933 lecture was the following: "It can scarcely be denied that the supreme goal of all theory is to make the irreducible basic elements as simple and as few as possible without having to surrender the adequate representation of a single datum of experience." See https://www.nature.com/articles/d41586-018-05004-4.

[4] The management and technical leaders from X-Analytics were directly involved in supporting the writing here, offering full access to their commercial platform details and team experts to provide insights into how contextualized reporting is implemented in their commercially available product.



DISTINGUISHED VENDORS

DISTINGUISHED VENDORS

Q2 2024

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

ACCUKNOX

Accuknox innovates in comprehensive multi-cloud and hybrid cloud security solutions. With a decade of industry influence, Accuknox excels in delivering Zero Trust Security through its Cloud Native Application Protection Platform (CNAPP). Their commitment to flexibility, openness, and integration ensures robust cybersecurity for organizations navigating dynamic cloud environments.

aembit

Aembit is a Workload Identity and Access Management platform that secures access between workloads across clouds, SaaS, and Datacenters. With Aembit's identity control plane, DevSecOps can fully automate secretless, policy-based, and zero-trust workload access.

allot

Allot Ltd. (NASDAQ: ALLT, TASE: ALLT) is a provider of leading innovative network intelligence and converged security solutions. Allot's multi-service platforms are deployed by over 500 mobile, fixed, and cloud service providers and over 1000 enterprises worldwide. Our industry-leading Security-as-a-Service solution is already used by many millions of subscribers globally.

aqua

Aqua Security sees and stops attacks across the entire cloud native application lifecycle in a single, integrated platform. From software supply chain security for developers to cloud security and runtime protection for security teams, Aqua helps customers reduce risk while building the future of their businesses.

TAG CYBER DISTINGUISHED VENDORS

2024

Balbix enables businesses to reduce cyber risk by automating cybersecurity posture. Our SaaS platform ingests data from security and IT tools to create a unified view of cyber risk in dollars. With Balbix, you can automate asset inventory, vulnerability management and risk quantification, leading to lower cyber risk, improved team productivity and tool cost savings.

BlackCloak protects corporate executives and high-profile individuals from cybersecurity, privacy, financial, and reputational risks. Our members have peace of mind knowing their family, reputation, and finances are secured. Companies are assured their brand, intellectual property, data, and finances are protected against threats coming through executives without invading their personal lives.

BreachLock is a global leader in Continuous Attack Surface Discovery and Penetration Testing. Continuously discover, prioritize, and mitigate exposures with evidence-backed Attack Surface Management, Penetration Testing and Red Teaming. Elevate your defense strategy with an attacker's view that goes beyond common vulnerabilities and exposures. Each risk we uncover is backed by validated evidence. We test your entire attack surface and help you mitigate your next cyber breach before it occurs.

BreachRx is the first intelligent incident response platform that provides operational resilience for the entire enterprise. Its patented technology automatically generates tailored incident response plans and guidance for all stakeholders. Integrated privileged communications and audit trails ensure compliance with rapidly-evolving regulations and standards to proactively protect CISOs from personal liability.

Cymulate is the leader in security validation and exposure management. Over 500 customers rely on the Cymulate SaaS platform to provide the single source of truth for threat exposure and the actions required to close security gaps before attackers can exploit them. For more information, visit www.cymulate.com.

Garrison pioneers hardsec cybersecurity solutions, reshaping the industry amidst escalating cyber threats. With roots in National Security tech, Garrison tackles flaws in the cybersecurity market, offering ultra-secure cloud infrastructure and hardsec-based protection. Named a Technology Pioneer by the World Economic Forum, Garrison leads the charge in securing tomorrow's IT landscape.

TAG CYBER DISTINGUISHED VENDORS

2024

Nasuni is a leader in hybrid cloud storage, revolutionizing file data solutions. Their File Data Platform offers unmatched scalability, edge performance, and data security, eliminating traditional NAS limitations. With innovative features like ransomware protection and seamless transitions, Nasuni empowers businesses to scale efficiently, reduce risks, and optimize operational costs.

Sophos is a worldwide leader and innovator of advanced cybersecurity solutions, including Managed Detection and Response (MDR) and incident response services and a broad portfolio of endpoint, network, email, and cloud security technologies that help organizations defeat cyberattacks. As one of the largest pure-play cybersecurity providers, Sophos defends more than 500,000 organizations and more than 100 million users globally from active adversaries, ransomware, phishing, malware, and more.

Swimlane delivers automation for the entire security organization. Swimlane Turbine is the AI-enabled, **low-code security automation** platform that unifies security teams, tools, and telemetry in-and-beyond the SOC into a single system of record to reduce process and data fatigue while quantifying business value and ensuring overall security effectiveness.

Teleport modernizes infrastructure access, improving the efficiency of engineering teams, fortifying infrastructure against bad actors or errors, and simplifying compliance and audit reporting. The Teleport Access Platform delivers on-demand, least-privileged access to infrastructure on a foundation of cryptographic identity and zero trust, with built-in identity security and policy governance. For more information, visit **www.goteleport.com**.

Varonis' platform stops and prevents cyberattacks by taking a data-centric approach to security. Varonis scans on-prem and cloud environments to automatically discover, classify, and label sensitive data, analyze permissions, and remediate excessive access to limit the impact of cyberattacks, manage the posture of cloud apps to proactively close security gaps, and monitor user and device behavior to detect and stop threats.

Secure Systems Innovation Corporation (SSIC), the innovators behind X-Analytics, are on a mission to help organizations make the best cyber risk decisions for their business. X-Analytics helps organizations drive continuous improvement through effective C-suite and board-level engagement. For more information, please visit **www.x-analytics.com.**

TAG EXCHANGE

TAG Infosphere offers the world's first Cybersecurity Vendor Exchange where enterprise businesses, government agencies, venture capital and private equity companies can identify and research prominent industry vendors. The Exchange gives vendors the ability to share their story and maintain and regularly update their vendor page on our Research as a Service (RaaS) platform. Vendors also have access to an annual briefing with the TAG Senior Analysts team, where they can obtain insight and guidance from our industry leading practitioners.

TAG WELCOMED THESE HIGHLY CAPABLE VENDORS TO OUR EXCHANGE IN Q1 2024

ADAPTIVE SHIELD

aiden®

Onyxia

TRUEFORT™

wirex

WITNESS AI

WIZ

FOR MORE INFORMATION PLEASE CONTACT LAURIE MUSHINSKY
laurie@tag-cyber.com • 412 .427.2829