TAG Cyber

Security Annual

1ST QUARTER 2022

A SPECIAL SECTION:

RESEARCH AS A SERVICE

ARTICLES / OPINIONS / INTERVIEWS

WELCOME TO THE 2022 TAG CYBER SECURITY ANNUAL 1ST QUARTER EDITION

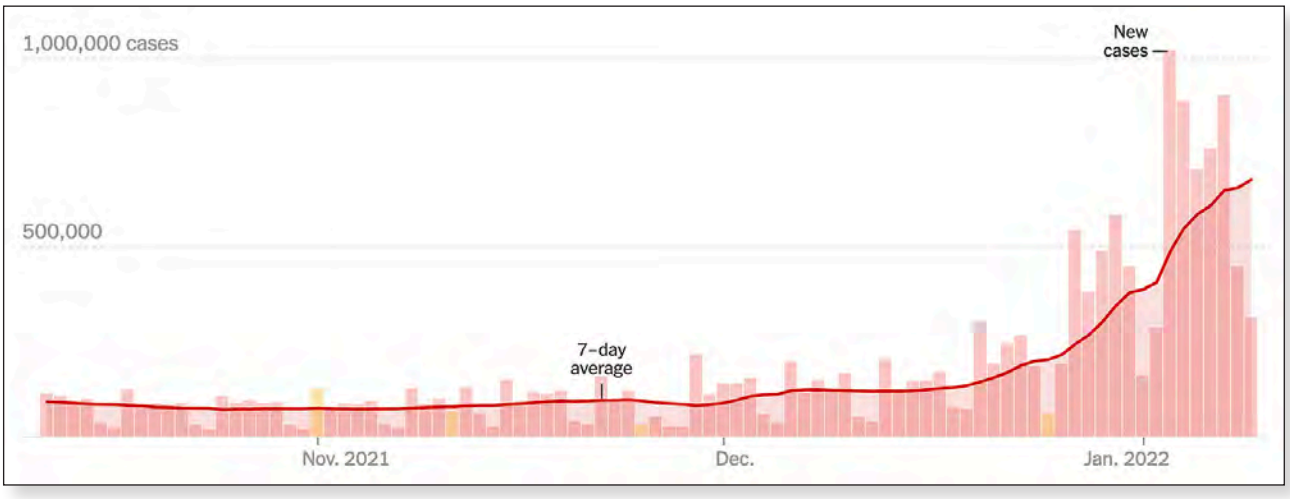
Our publication comes at a time when we continue to deal with this nagging Covid virus. The RSA Conference, originally slated for February 2022, was pushed ahead to June—and one wonders if this will be possible. None of us at TAG Cyber are holding our breaths.

The societal reasons for the continued challenge of Covid and Omicron—and the associated medical foundations—are for another publication. We are neither social scientists nor medical doctors. You are welcome to go and debate what's been mismanaged.

But the mathematical reason for the continued surge of this virus is indisputable: It is the power of exponentiation. And for those of you who skipped sixth grade math, exponentiation involves raising some quantity to the power of another. Two to the three. Five to the six. And so on.

Every cybersecurity expert should respect—and yes, fear this concept. To date, it has worked against us, as evidenced by attacks that accelerate like falling boulders. But perhaps such power might be redirected in our favor. Hmmmm. Let's think about this one for a moment.

Here is a picture of the Omicron spread in the United States for the months from October 2021 to January 2022 (taken from The New York Times website):



The reason things look so flat for the month of November and the early part of December is that the power of exponentiation had yet to take hold. But once things started to accelerate, the graph starts to jump. And fast. Look at how it goes up and to the right.

Now, any security expert will tell you that a simple generalization of the graph above (set the X axis to time and the Y axis to spread) produces a shape of how just about every cyberattack accelerates. It's how APT attacks grow. It's how worms explode. And it's scary.

But what if we could turn things around? Would it be reasonable for cyber defenders to create some means to accelerate security? Could we build technology where the exponentiation is used in our favor? It would be like making the Y axis correspond to healing.

Here's an example of how this might work for autonomous vehicles. We know that future communication mesh architectures for vehicle robots will require that every car talk to every other one. It'll be like a moving robot society. (Uh, yes—creepy.)

Anyway, if one car learns that something is amiss on a highway—maybe some smart road sign is infected with malware—well, then it might tell two other cars. And they might pass this intel along to two more cars. And so on. You can create the R-value for such a thing.

The result could be exponential security. It would involve turning the power of powers in our favor. Wouldn't that be a welcome change? Security would grow and accelerate at a rate that keeps up with the accelerating growth of our offensive nemesis.

As analysts, we've not seen this type of thinking much from vendors and practitioners. Most are too obsessed with framework compliance—and with keeping their dopey boards happy—to be innovating. And this must be addressed. We need to be a thousand times more creative.

We hope this volume of the TAG Cyber Quarterly helps in this regard. We include interviews with interesting experts, and papers that we hope shake you up a bit. Our analysis is always intended to be new and interesting. We want to make you think.

And if we work hard, we should be able to soon show graphs like the Omicron histogram that illustrate the rate of improvement. But this will only occur by challenging our community to think differently. We hope you do so—and we hope you enjoy our volume.

–Ed Amoroso

"Eva is coding her cloud app containers at only a third-grade level. I'd suggest some remedial coaching."

TAG Cyber Security Annual
1ST QUARTER 2022

Ed Amoroso, Founder & CEO

Lester Goodman, Director of Content

Contibutors

Ed Amoroso, Senior Analyst
Jennifer Bayuk
David Hechler
John Masserini
Gary McAlum
Stan Quintana
Chris Wilder

Editorial & Creative

Lester Goodman, Editorial Director
David Hechler, Senior Editor
Judy Lopatin
Miles McDonald
Rich Powell

Research & Development

Matt Amoroso
Shawn Hopkins

Sales & Customer Relations

Rick Friedel
Trish Vatis
Laurie Mushinsky

Marketing

Scott Krady
Tony Taddei
Leona Laurie

Administration

Liam Baglivo

Volume 8 No. 1

January 15, 2022

A SPECIAL SECTION

RESEARCH AS A SERVICE

(RAAS)

A SPECIAL SECTION

RESEARCH AS A SERVICE

(RaaS)

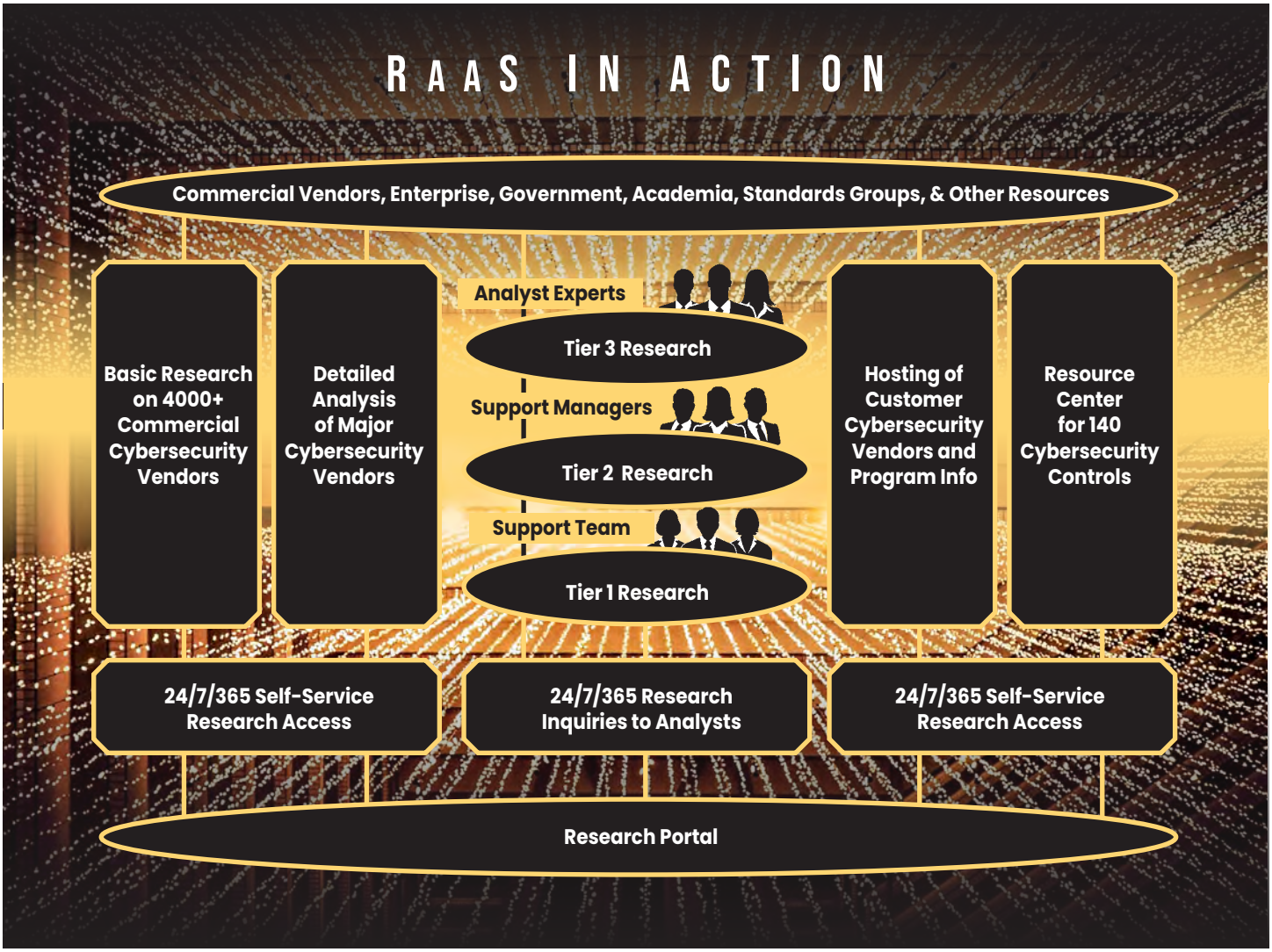
EDWARD AMOROSO

If you share a generation with me, then you'll immediately recognize this song lyric: *"If there's something strange in your neighborhood, who ya' gonna call?"* I've always expected some security vendor to use this jingle for their value proposition. But sadly, I've come to learn that most security business cases go sour when customers are calling for help. Giving answers is tough and expensive, so it's better to discourage questions. Or so goes the narrative.

In a nutshell, *Research as a Service (RaaS)* involves answering questions. At TAG Cyber, we do this today for cyber security, and we will soon be announcing comparable RaaS services for climate science, artificial intelligence, and decentralized finance. RaaS is all about inviting questions that require answers from real experts. It involves offering expertise on-demand, in real-time, on a 24/7/365 basis. The idea is to *invite* questions – not to avoid them.

Our RaaS approach at TAG Cyber focuses on non-operational security problems such as needing advice on a vendor, requiring assistance on how to implement some new security acronym (like SASE, CIEM, etc.), requesting guidance on how to replace this thing with that, and so on. RaaS involves answering customer questions – not avoiding them. And yes, this requires hiring experts who have spent time in the seat.

Gartner and Forrester approach this differently. Here's an illustration: If, for example, a security practitioner is struggling with selecting a GRC vendor, then they will be handed a completed analyst report (from a template) with a pay-for-play quadrant. The CISO then observes from the visual that (by way of analogy) a Ferrari is better than a Hyundai. Never mind that the Hyundai might be a much better (and more cost-effective) selection for that CISO.



At TAG Cyber we do it differently: That CISO would visit our RaaS portal for guidance on GRC, where information on many dozens of GRC vendors would be available with reports, videos, and other resources offering guidance. A Tier 1 security specialist would be available to help the CISO navigate this information. If the CISO wants help narrowing things down, then a Tier 3 analyst would jump in to provide tailored assistance – *immediately*.

We started our RaaS service as an Alpha earlier in 2021, and we signed up about 20 major customers including 20% of the Fortune 15. Based on their questions and feedback, we've tailored the service to a Beta offering which we are now selling actively. Most teams pay us monthly for the service, often just putting it on a credit card. We've never had a customer balk due to cost. Our customers save more than they pay us.

I hope you'll take a moment to visit us and request a briefing on our RaaS solution offering. If you are spending hundreds of thousands, or millions, or even tens (or *gulp* – hundreds) of millions of dollars on your vendor investments, then shouldn't you spend a tiny percentage of that on optimizing your portfolio, strategy, and approach? We think the answer to this question is obvious.

And we look forward to hearing from you soon.

UNDERSTANDING INFLUENCE AND THE ANALYST'S IMPACT ON TECHNOLOGY STARTUPS

CHRIS WILDER

One of the bright sides of today's market uncertainty and the looming intrusion of big government on the tech industry is the emergence of self-reliance and entrepreneurship, especially in the cybersecurity industry. We have seen a massive growth of innovation in the cyber market that has provoked many cybersecurity startups to take a go-big-or-go-home attitude to rise above the competitive noise. For example, TAG Cyber's Research as a Service (RaaS) portal has initiated ongoing coverage of nearly 4,000 cybersecurity vendors across approximately 160 different technology segments (our initial view includes company profiles, SWOT analysis and, in some cases, technology evaluations). Compounding the market noise is an enormous increase in the funding of cybersecurity companies with crazy unicorn valuations. This has led security companies not as well funded to find significant value when dealing with analysts for product validation, contacts and exposure in the industry, simply to compete. However, before engaging with analysts, analyst relations (AR)/marketing pros must have their proverbial ducks in a row.

Unfortunately, most technology companies focus too much on their products and what they do—feature and function—rather than the value they bring to their customers. Many vendors feel compelled to reach out to the analyst community prematurely, while others wait too long. That said, startup executives need to discuss a broad range of topics consistent with their industry, and analyst input is essential to help organizations drive their strategy and direction.

Announcing too early means that the natural evolution of product and market plans will start to look like the strategy du jour of a floundering vendor or, worse yet,

For Cybersecurity Vendors, Research as a Service (RaaS) Makes It More Important Than Ever to Be Prepared and Focus on the Relationship.

a solution searching for a problem. Another challenge for startups is overcoming analysts' reasonable skepticism, especially those catering to enterprises or technology buyers.

Frankly, startups come and go at an alarming speed. Their demise is mainly due to the lack of experienced professionals to staff all these new companies that lack real-world experience, skills and domain expertise in the investment community. Consequently, new vendors need to go into their initial analyst briefings fully prepared to demonstrate not just "an insanely great idea" but their ability to execute as well.

AR is about relationships, so the company needs to own that relationship from beginning to end. We recommend NOT using your PR firm for anything other than scheduling briefings and managing the calendar. That said, you must ensure that you have the following completed before engaging with the analysts:

Have Your Strategic Positioning Statement in Place. A crisply articulated strategic positioning statement (SPS) is a standard requirement for any analyst interaction. The SPS includes who you are, what you do, why you are different, and why people buy from you. Vendors should tweak their message to meet the needs of each constituent or vertical while maintaining the immutability of their SPS.

A Product Should Be Demonstrable. There are a few exceptions to this rule. Before talking with the analysts, vendors should have, at a minimum, a late beta version of their product ready—or, for early-stage startups, a coherent vision and product road map. Ideally, there should also be a few beta customers, but as a rule of thumb, no referenceable customers (early adopters) = no briefing, period. Even a software company whose initial product is more "consultantware" (i.e., a nearly unique piece of software code for each customer) has a better opportunity of validating its vision than a vendor without any customers or references. In some cases it is OK to check in at conceptualization time, but that depends on the firm and the relationship that the firm has with the analyst.

Well-Thought-Out Plans Should Be in Place. A vendor can start building credibility with the analysts by showing that it understands the various challenges and market dynamics that it intends to address. These vendors have a prioritized plan to address the problems and have a road map for acquiring the resources required. Even if the vendor does not have all the answers, it should, at a minimum, know the questions. It is essential to predetermine what should be in the analyst's mind at the end of the briefing. Not only will this help focus the conversation, but it will also drive the creation of the presentation and supporting materials.

The best analyst relations teams are rooted in relationships and best practices. Further, successful programs require an all-hands-on-deck approach, especially with tier 1 analysts. Below are the traits and activities of top analyst relations programs when building a world-class program.

They Target the Right Analysts. With limited resources and budgets, many startups tend to focus on the analysts that pay them the most attention. Focusing on these analysts causes executives to waste time speaking to analysts who cannot help them drive revenue and exposure. It is essential to focus on the most influential analysts in your market, not just those who write about you or provide a comment for a press release. The value of analyst influence is 20 percent what they write and 80 percent what they say to buyers about your company (source: The Knowledge Capital Group). That is why it is essential to work with analyst firms that influence end users or buyers (98 percent of analyst firms have little or no influence with buyers).

However, AR pros need to understand the business models and how the less influential analyst firms can provide value before any targeting exercise. If 98 percent of analysts have little or no direct influence with end-user customers, how can they help?

- Nearly all analysts can help with third-party messaging validation and market advice for executives.
- Many can help marketing teams promote the message and generate content to objectively explain a product or marketing strategy.
- Product marketing/development teams leverage analysts for research and intelligence gathering on the market and the competition.
- Sales organizations use analyst research against competitors in contested opportunities.

They Establish a Compelling Vision and Differentiation. With so many security vendors introducing themselves to the analyst community, it is essential to show that they have solid insight into their market and are not "me too" latecomers. For startups and growing companies, providing validation points such as customer wins, first-to-market advantages and significant product milestones should lead the conversation.

They Demonstrate an Understanding of Key Industry Issues. The desired outcome is to prove to the analyst that the vendor has a realistic view of their world, with plans and priorities that appropriately match the product vision and available resources.

They Put a Stake in the Ground to Establish Future Credibility. Because of a paucity of actual reference customers, new security vendors need to lay out milestones for the next two to three quarters, the execution of which will be the foundation for building credibility and the cornerstone for future success.

Most Importantly, They Show Their Ability to Execute. Although many companies start as "two guys in a garage," security startups currently must show that they have the management skills, people and financial strength to survive the startup phase.

THE DARK AND AMBIGUOUS TRUTH ABOUT THE ANALYST INDUSTRY

There is no school where you can learn to become a technology analyst. Most buy-side analysts end up surprised that they have this job in the first place. How, then, does a person end up creating and tracking IT markets, influencing decisions with technology buyers, and wielding such substantial power over vendors?

"Honey, that's what happens if you listen to Gartner analysts."

Since the job traditionally involved professors performing research, teaching/speaking and writing new ideas, the field often attracted pedagogical types who perhaps were not thrilled by the dismal money paid to teachers and opted for an analyst job. In addition, our research shows that many have been consultants or researchers from the start, with no vendor or practitioner experience at all. Even fewer are from the ranks of technology buyers, and many are young—just out of college. Other analysts might have fancied themselves financial analysts but were afraid to join that cutthroat industry. Instead, they decided to be a pundit in the more flexible, rules-free technology sector.

In any case, no analyst will ever know more about the products that you are selling than you. Still, an analyst can give you a perspective on your company relative to other companies in your market. How?

Buy-side analysts act as the gatekeeper to their firm's client base, one that is likely to contain your prospects and clients as well. Often, the analyst will hide this information from you, usually for one or more of five reasons:

- The prospect or client has requested anonymity.
- The analyst is lying about the extent of the relationship.
- The analyst wants to maintain power over you so that you continue to purchase their research.
- The analyst hopes to hide their lack of knowledge by using the client base as a "smokescreen."
- An analyst also receives information from all vendors, including your competitors, and frames them in a radar, much like an air traffic controller. Each of these vendors offers information about itself to achieve favor with the analysts.

Therefore, the analyst, who has no formal training outside their firm's research methodology, sits in the middle of a needy client base and eager vendors. But how can someone who has never used your product and only talked to three of your clients for perhaps 30 minutes each (if that) suddenly influence the decision of the next buyer?

The most accurate analysis comes from examining the link between the client base and vendors. The best analysts serve as interlocutors between the two groups (the lesser analysts just pretend that they do). How do you deal with an analyst whose knowledge and client bases are suspect? Here are some practical realities and best practices for dealing with this:

- **Analysts know less than you do.** Do not assume that analysts know more about your company than you do. They may have information on your competition or clients, and this access gives them some authenticity. Still, client access and references alone are not good research sources from which to make recommendations.
- **Analysts use most meetings as intelligence gathering**. You expect cogent recommendations from a briefing or inquiry. However, the analyst uses these meetings to do their primary research, while later complaining that the interactions are "vendor-centric" and, hence, nonobjective.
- **Analysts will lie to you.** Stay in touch with your client base so that you can call an analyst on a suspicious recommendation or assessment.

DEFENSE AGAINST THE DARK ARTS

Manage and know your references. If an analyst calls you for five references, you need to ask how they will use them and when the references will be called (most analysts ask for references but never call the customer). Stress the processes and policies that you have in place for handling references

and request that the analyst respect them. Analysts use client access as one of the primary research resources. Neglect of these relationships with customers will hurt you in the end.

Do not let the analyst contact the references directly. Although analysts will object, ask the analyst for a standard list of five to 10 questions that he wants your clients to answer, send them to the clients, and then mediate the relationship between the two factions very closely.

Follow up with both analysts and clients.

- For the vendor: Did the analyst call? What can you share from the meeting?
- For the analyst: Were all your written questions answered? Can we help you get any more information?

Question analyst research methodologies. Just because the analyst firm is respected does not mean that the analyst knows how to evaluate you effectively. How long has the analyst been there? Are they prepared to offer relevant, well-researched suggestions? Does the analyst have experience or knowledge in your segment? Has the company had an exodus of senior analysts recently and given you a young analyst who has just begun researching their market?

Understand the intangible aspects of technology research. As a vendor, you drive market creation, and analysts will follow you—with some exceptions. You are influential with the analysts because you are a creator and not an evaluator. Often, your meetings with analysts become future research. In the past, vendors sometimes wrote reports for certain analyst firms that simply white-labeled and put their names on them. While this practice is rare, immoral and illegal, it still effectively occurs in verbal information exchanges. Be respectful of the analyst research model. The democratization of research has escalated real-world practitioner expertise as a significant differentiator.

Publish white papers, webinars and case studies. Analysts can utilize this collateral to see you as a thought leader in your market. However, do not send an analyst research written by another analyst firm. Most importantly, do NOT place yourself on an analyst firm's signature research charts such as TAG Distinguished Vendors, Magic Quadrant, Wave, etc.

CONCLUSION

Bottom-line, understanding the inner workings of analyst firms and how the analysts approach their work is an integral ingredient in gaining positive rapport with the analyst community and leveraging their impact on your company's success. Know what to expect when going into an analyst meeting or briefing. Understand the analyst's expectations before making your pitch or presentation. And do your homework when researching the relationship between your current and prospective clients and the analysts. These initiatives are imperative to optimize your investment in analyst relations and your relationship with the analysts. Stay well-informed, and you will be well-armed when engaging the analysts who shape and influence your customers' perception of your company and its offerings.

CASE STUDY: HOW NOT TO MANAGE YOUR SECURITY VENDOR PORTFOLIO

EDWARD AMOROSO

Below is a fictitious account of an enterprise security team with a problem – namely, how to rationalize and manage the commercial investments they've made with cybersecurity vendors. Read the account and see what you would do. We've included discussion questions at the end.

ACT 1: THE VENDOR SPEND

Andrea Miller winced as she glanced over the spreadsheet of cyber security vendors. And wow, look at the amounts being spent! Three-hundred thousand here, four-hundred thousand there, and two million – TWO MILLION – being spent with a vendor that Andrea didn't even know.

She grabbed her iPhone and texted her Chief of Staff Robert: "Get the SLT on Zoom 5PM today. Need to go through this vendor list."

Andrea leaned back in her chair and sighed.

As the new CISO (just three months on the job!) for Acme Manufacturing, a product machining, assembly, fabrication, and test company serving the aviation industry, she'd hoped to quickly control the budget.

"We spend a ton of money on cyber," the Acme CIO had explained to Andrea during her interview. "But we continue to have incidents. And I have this feeling that we're throwing good money at security tools that we don't need."

She glanced at the spreadsheet once again and shook her head at the total on the bottom right corner of the page: $37,587,234.

We could buy an airplane with that kind of money, she thought.

She fumbled around for a moment, and eventually pushed the right Zoom button and the spreadsheet popped up on everyone's desktop. The problem was that the list was so long, it could barely fit on everyone's screens.

ACT 2: THE TEAM EXPLAINS

Andrea held mostly face-to-face meetings at her previous company, but she was now getting comfortable with the virtual collaboration style the Acme Information Security Team had put in place.

"Thanks for getting together so fast," Andrea told her team, as she started the discussion. "I assume you all have the vendor spreadsheet, but I'll try to share my screen."

She fumbled around for a moment, and eventually pushed the right Zoom button and the spreadsheet popped up on everyone's desktop. The problem was that the list was so long, it could barely fit on everyone's screens.

"Let's just start through the list, maybe at the top," she said. "I see that we're almost spending thirty-eight million on security, and – "

"Uh, Andrea – it's more than that," John Graham-Burke interrupted.

As head of vulnerability management, John was always a voice of reason during discussions. Andrea had asked him specifically to be blunt with her – and he was happy to comply.

He continued: "You're just looking at the AIST budget, but we should also include AOIT. They have a bunch of additional vendors."

Andrea recognized AOIT as Acme Operations, Implementation, and Technology, a branch of the CIO's team that did hands-on management of the security platforms, including all identity and access management.

"OK," she replied. "But let's start with what we have here."

"Fair enough," John replied. "But the other numbers are significant."

She nodded and then glanced back at the spreadsheet: "I think we can start at the top," she said. "Let's see, uh – OK, here's one I didn't understand. I see that we're spending ten million with Notable IGA. That seems like a big number. Who, er – who is the owner of this?"

This question was met with a long quiet pause. Finally, Zoe Daschle, who ran the SOC and SIEM, chimed in: "Andrea, we really don't have owners of vendors, per se. I guess you could say that procurement owns them."

"Procurement?"

"Yes."

"Uh, huh," Andrea muttered after another pause. "Why don't we have owners for each vendor?"

"We probably should, but we manage vendors with this Excel spreadsheet and things get a little chaotic."

Andrea nodded again. This is not going well.

"What about this CloudBang EDR?" she asked. "Do we really spend nine million with them?"

Maya Sarabhai, head of security awareness and training, spoke up: "That was from our last endpoint security manager. She had worked there previously, and she signed us up. I mean, it seems like it's been good, so I don't see a problem per se. Or at least no one has complained."

"Did this person leave the company?" Andrea asked.

Maya laughed: "Yes. She went back to work at CloudBang."

"Is that allowed?" Andrea asked.

The question was met with silence.

For the next hour, Andrea went through many names of many other vendors – and she was treated to a range of explanations: This vendor had been there as a legacy. And that vendor has a nice salesperson who gives tickets to nice events. And this other vendor was selected two years ago, and things seemed like they were sort-of OK – and on and on.

After the discussion, Andrea paused and thought to herself: Not acceptable.

ACT 3: DISCUSSING A SOLUTION

Andrea walked into Maya's private office carrying two large pumpkin spice lattes. It had been their custom these past couple of months to take turns running down to the Acme Café on the second floor for mid-afternoon refreshments and snacks.

"Oh, my gosh, what took you so long?" Maya said. "I need coffee!"

Andrea sat down. "You're going to need a real drink when you hear this," she replied. "Dan just set up a half-day review next week to go through all key vendors across IT and security."

The Dan she referred to was Dan Ford, the Number Two in finance. His nickname was Hatchet Dan because he never saw a budget he couldn't cut.

"Next week? Wow, Dan usually gives at least three weeks before he kills every program in the book," Maya replied.

"I need to bring detailed information on every one of our security vendors – and I think it comes to 87 total," Andrea said. "And they want at least two competitors listed for each vendor, along with trending information to justify the spend."

"We don't have that data."

"What about the spreadsheet – it seemed like it had many fields and I saw a bunch of detail in there."

Maya shrugged: "That data is not updated properly. It has some good hints about the vendors, but a lot of the information is just wrong. It still includes our Flunk SIEM, and we got rid of that thing a year ago."

"I didn't know that."

"And I'd also like a toolkit to secure Kubernetes."

"Yea. They kept increasing our bill and no one noticed."

Andrea nodded and Maya was quiet. The two security executives thought for a few moments. They both understood that something needed to be done – and fast. It was not reasonable to spend this much money, without having some means for rationalization.

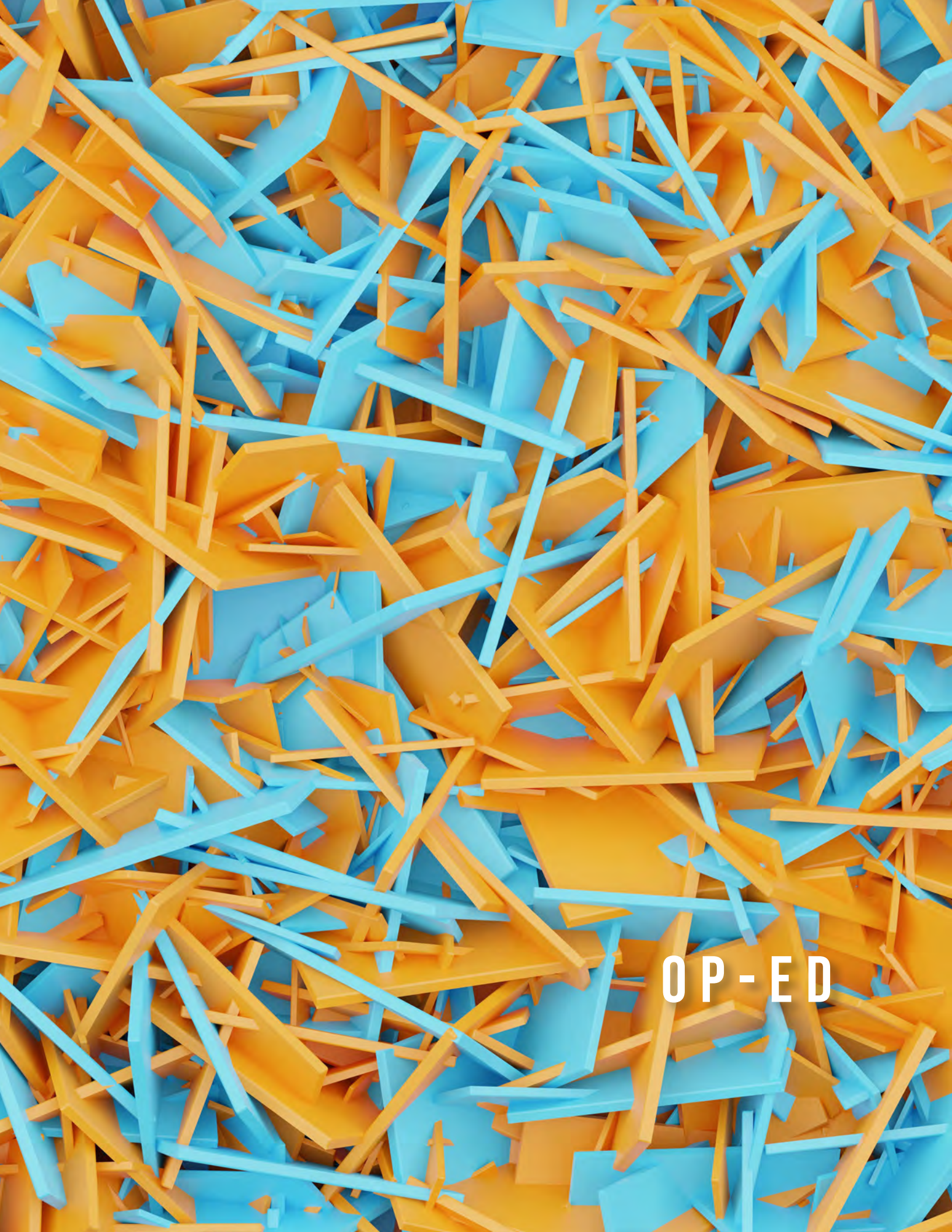
"Any advice on what to do?" Andrea asked.

Maya thought for a moment and then smiled: "Interns?"

* * *

QUESTIONS FOR GROUP DISCUSSION

1. Do you think the problem here stems from neglect by the security team or should the procurement team be doing a better job?
2. Do you believe it is common for enterprise security teams to have a poor understanding of their commercial portfolio?
3. Is an Excel spreadsheet the right mechanism for storing, maintaining, and sharing information about cybersecurity vendors?
4. What types of services would you like to see from analysts, advisory firms, or consulting teams to assist with this type of work?
5. Are you familiar with TAG Cyber's Research as a Service (RaaS) with its embedded portfolio management support? (Hint: Call us!)


OP-ED

A COMPANY'S MISSION IS OPENING MINDS TO NEW SOLUTIONS

DAVID HECHLER

Mark Fabro works in a small but critical cybersecurity niche. He's president and chief security scientist of Toronto-based **Lofty Perch**, which helps companies that are part of a country's critical infrastructure protect operational technology. But his ideas are broad and wide-ranging, and the implications will be of interest far beyond his clients—or the engineers he **teaches** at places like Carnegie Mellon University's Heinz College.

In a lengthy interview, Fabro talked about the differences between companies he's worked with that were well prepared to deal with ransomware attacks, and the businesses that were not. He also described how those differences played out.

The longer we spoke, the more apparent it became that his job requires not just technical skills, but an understanding of psychology. The reason is simple. Executives unwilling to entertain new ideas can inhibit their companies' ability to adopt new solutions. For example, when some people hear the word "blockchain," they immediately think of the cryptocurrency that enables ransomware payments. And they never consider the innovative ways different blockchain technology can be used to protect against the same attacks. Fabro endeavors to help his clients explore all of their options, he said.

Since its founding in 2005, Lofty Perch has helped clients understand and respond to risks that may not be picked up by traditional cybersecurity programs. Most of Fabro's 15 colleagues are engineers, and their work often begins with advanced assessments and analyses designed to help clients understand what damage a competent adversary could exact, given the opportunity. "And this is unique in the landscape," Fabro said, "because it helps uncover things that may have been traditionally seen as benign by an organization."

Blockchain technology can be used to create backups that guarantee the data has not been seen or touched.

DIFFERENT RESPONSES TO RANSOMWARE

Ransomware attacks continue to command the attention of security teams, who have reason to feel vulnerable. Companies that are ill-prepared to defend against them often spend a lot of time trying, Fabro said. Many have a response protocol in place, "but it hasn't been vetted and tested in a scenario-driven environment," he noted. "They haven't run a tabletop to actually see whether or not things were going to work." The result is often "chaotic," he said. "It's difficult to watch because you are seeing the ramifications of an awful lot of preparatory work not fulfill its promise."

Mark Fabro

By contrast, the organization that's prepared for a ransomware attack has practiced, has run through the scenarios. In some cases, Fabro said, the preparation was a previous attack that occurred when the company was not primed. As a result, it modified its response plan and worked out the kinks. When it happens again, the defenders are likely to be much more calm, he said.

Their preparation and emotions produce divergent reactions. The ill-prepared firm often reacts with frustration, Fabro explained. "I don't really want to know what happened," they say. "Let's just get back up and running." The team that's ready is likely to get back faster, "and almost concurrently they can begin to do the analysis specific to, 'How did it happen?'" And then they "plug those holes and mitigate that risk," he said.

"I don't really want to know what happened," says the company ill-prepared for a ransomware attack. "Let's just get back up and running."

In one respect the two groups are similar. They do not spend time ruminating on who did it, or why, Fabro said. As far as he can tell, their focus is on dealing with the reality they're facing.

Lofty Perch does not advise clients whether to pay the ransom demanded. "We don't really deal with that at all," Fabro said, "because they've got some other function with law enforcement or lawyers. That's not us." But the consultants do offer advice about the crucial matter of backups. And this may involve delicate conversations.

BLOCKCHAIN FOR BACKUPS

Clients in heavily regulated industries sometimes find that auditors and regulators want to see verification that the backup a company has restored is sound. Fabro has found that clients sometimes field a series of probing questions: "What's your level of attestation? How can you confirm that this data that you're bringing back hasn't been seen, hasn't been touched? And when you put it back in the system, it's actually going to do what it's supposed to do?"

There's one method that Fabro said is failsafe: backing up using blockchain technology. A company can decide to take its data, whether it's medical information, or contracts or design secrets, and back it up locally (as most already do). Then move the same data to a blockchain. And then take the information that explains how to access that data, and secure it in another blockchain.

What's the payoff? "Nobody can see it. Nobody can touch it. Nobody can read it. Nobody can get it," Fabro said. This provides "a mathematical guarantee that the data hasn't been seen and hasn't been touched."

Fabro quickly added some caveats. This pitch doesn't appeal to all companies. Some don't want that level of security. Or need it. "There's a lot of people that just want some data back up and running," Fabro said.

But Lofty Perch is constantly looking for new solutions, he continued. And this approach is not designed "to replace your backup or your storage solution. This is something to augment and complement a preexisting backup capability for a larger, more secure archive." It's a protection, he said, against a ransomware attack or some physical event—whether natural or human-made—that destroys a company's servers.

As far as the nuts and bolts, it's easy to do. It can be set to automatically update every day at 5:00, or every 10 minutes, Fabro said. He would not offer a range of costs, but he did say that "storage is not very expensive"—especially compared to the potential price tag of lost data.

A MATTER OF PSYCHOLOGY

This doesn't make the concept an easy sell. Fabro acknowledged three reasons why. First, when executives hear "blockchain," many associate the technology with bitcoin, the cryptocurrency you must pay to unencrypt your data after a ransomware attack. That's an unmitigated negative. Second, they already have cloud storage and backups. The executive may be thinking, "I've already got that in place. I paid for it. I checked the boxes. I know it works and it's reliable." When told of this new idea, the executive may think (whether or not it's articulated): "You're using words I don't actually know. And I can't quite understand how it supports anything that I would actually need."

It's that third hurdle—the novelty—that requires a delicate conversation. And that's where psychology enters the picture "because there's no question of the technology," Fabro said. "It's how to get the buy-in from the senior level executives to think a little bit differently." What drives the need for innovation, he explained, is the "rapidly changing threat landscape." The adversaries have led the way, consistently catching defenders off-guard. Getting executives to consider new options, however, involves luring them out of their "comfort zones." This requires a dialogue in a language they understand, he said.

The technical conversations can come later, and they're easy because the Lofty Perch engineers are comfortable talking with the client's CISO and IT professionals. That's their sweet spot. "When we're delivering our work," Fabro said, "our customers who are engineers are interfacing with actual engineers."

But none of that happens unless the C-level leaders are willing to move beyond conventional wisdom and older approaches. He believes the current climate is helping convince executives to consider new options and do just that.

A BRIEF HISTORY OF INDUSTRY ANALYSTS

CHRIS WILDER

The technology analyst industry has thrived for nearly 60 years. However, when most think of the market, they mostly associate it with the gorilla of all analyst firms, Gartner. While Gartner was the first to break through the enterprise or technology buy-side market, Pat McGovern, founder of IDC, introduced the concept of a syndicated, multisponsored model for providing quantitative research services to the industry in 1964.

This article will look at the historical roots and development of the analyst industry over the last 60 years. This short history of the analyst industry came from a book I co-authored, Influencing the Influencers. While researching the book, we had the opportunity to interview many of the industry pioneers to get their stories. Below is a synopsis of our research.

Three luminaries forged the way for the IT analyst industry. Pat McGovern introduced a syndicated model of quantitative IT research through his company, IDC. Howard Anderson, who started Yankee Group, developed the high-touch, inquiry-driven, qualitative approach to subscription research for vendors in the telecom space. Gideon Gartner was the first to tap into the needs of technology buyers by initially helping end users navigate and negotiate with IBM.

Thriving in Chaos and Confusion While Creating an Opportunity

The analyst industry has always thrived on disruptive change and its uncertainty. Below are their stories:

PATRICK MCGOVERN, IDC

In February 1964, Pat McGovern launched IDC on a train ride from New York to Boston. McGovern was an associate editor for a small Boston-based magazine, Computers and Automation. His assignment was to take the train down to New York to attend a press briefing run by RCA and then meet with the CEO of Univac, which was then the world's second-largest computer company.

> **"Our analysts have one job to do every day. Go home and pray for confusion … the more confusion there is, the more money we make."**
>
> **Manny Fernandez, Gartner CEO (1994–99)**

At the morning briefing, McGovern was struck by how RCA was disconnected from its potential marketplace. RCA's engineers were proudly touting a new semi-random access memory technology that they had developed, but they couldn't provide answers to questions about its purpose and application. "Oh, we hadn't thought about an application," they said. RCA was convinced that providing "the most clever random access memory methods" in the marketplace was enough to dominate the market.

Their responses didn't sit well with McGovern. When he met with the Univac leader in the afternoon, he voiced his concern that the millions of dollars invested in technology addressed no clear market need. "You are 100 percent correct," said the CEO. "That is just what I worry about, that all this money is going without guidance from the marketplace."

He explained that Univac could not collect adequate data about its market or even the installations and applications of its customers. The CEO wondered if someone could build a database of computer installations, current configurations, critical applications and additional requirements.

McGovern, who was then 27 years old, saw an opportunity. He suggested conducting a custom research study that addressed most of these matters. McGovern wrote the proposal to his boss on the train ride back to Boston. However, the CEO had one final idea that proved to be quite consequential. He said, "Don't only sell it to me, but offer it to the other computer companies, and you'll have more resources to build the best database to help our industry understand the future needs in the market." That marked the beginning of IDC and the concept of syndicated, multiclient research.

HOWARD ANDERSON, YANKEE GROUP

Howard Anderson was a very successful young independent consultant. Having spent his first year out of Harvard Business School offering strategy and marketing advice to any company that would hire him, he decided that it was necessary to specialize. So Anderson started consulting and writing reports on telecommunications. It wasn't long before he realized that he could make more money producing reports—and selling them as part of a subscription service—than he could as a consultant.

Yankee Group launched in 1970 with its first research report, called "The Unbundling of AT&T." It predicted that the telecom behemoth would get sued for monopolistic practices and lose in the courts. The news was greeted with a big laugh among the industry executives who received it, but Anderson was soon proved to be an industry sage. At one industry trade show at which Anderson spoke, he even observed the president of AT&T, Charles Brown, actively scribbling notes as he spoke. When he asked Brown why he was so interested in the remarks, the AT&T chief said, "Howard, this stuff is at least as good as anything my guys are coming up with." As Anderson explains now, "It was such a new world. In the land of the blind, the one-eyed man could be king."

Yankee Group quickly found a strategy: creating a research portal, building a seminar around it, and launching a new subscription service. The key to the business all along, however, was its renewable, subscription-based model. "I always felt that this was a different model," says Anderson. "I was amazed that McKinsey and Booz Allen had never figured it out.

Looking back, what's particularly interesting about Yankee Group is all the talent that Yankee developed, and its people continue to impact the analyst industry today significantly. For example, Anderson hired Dale Kutnick in 1977 to act as his chief operating officer. Having worked at IDC, Kutnick would later work at Gartner and then launch his firm, META Group, in the late 1980s. He also hired George Coloney, founder of Forrester, and Frank Gens, retired chief research officer for IDC. In 2005, Gartner acquired META for $162 million in cash, consolidating its buy-side consulting and advisory business strength.

GIDEON GARTNER, GARTNER, INC.

While over 98 percent of the research and advisory business derives most of its revenue from IT sellers (vendors), it was Gartner that finally figured out how to build a business model around selling to the buyers (end users) of technology. Gideon Gartner was an analyst at Oppenheimer in the early 1970s. At that time, brokerage commissions were fixed, and the industry operated much like a protected cartel. Exorbitant fees were made possible by exchanging "soft dollars" from institutions in exchange for favorable analyst treatment. In 1975, the federal government intervened and charged the brokerage industry with price-fixing.

> **"The Magic Quadrant is the most overused, misleading, worst representation of anything."**
>
> Gideon Gartner, as quoted in Business 2.0 (06/2001)

After several more years at Oppenheimer experimenting with ways to sell his research for hard dollars, Gideon launched Gartner Group in early 1979 with a business partner, David Stein. Having worked at IBM in the 1960s and later following it as an analyst, Gartner knew that there was plenty of money to be made by helping clients better understand and negotiate with the computer behemoth. Consequently, Bessemer Securities and Warburg Pincus, whose bankers had benefited from Gartner's stock advice, were eager to provide the firm's initial round of funding.

Gartner eventually became the single largest analyst research company in the industry. Further, under the leadership of Fernandez and Flesher, Gartner made several key acquisitions. One of the most important was Gartner's $75 million purchase of Dataquest in 1995, which bolstered the company's strength in quantitative and vendor-focused research.

Gartner rolled out new services to cover all essential IT software, hardware and services, and vertical markets. Thanks to the company's acceptance by the end-user community, Gartner subscriptions became a staple among all sizable IT buyers and most technology vendors. Gartner's consulting business stepped in to challenge the traditional IT consulting firms, and the events business grew to over 50 events, boasting over 30,000 attendees. Gartner is the largest industry analyst firm, with over $4.5 billion in revenue and 17,000 employees. From a revenue perspective, we estimate that Gartner is at least three times the size of all their competitors combined.

CONCLUSION

For over 60 years, many industry analyst firms have come and gone. New research models are emerging, and the need for analysts with real-world experience is in high demand. Sadly, most firms, especially Gartner, Forrester and IDC, lack a level of experience as practitioners. They focus more on those analysts who can adhere to the research methodology du jour. The next generation of analysts will have the experience, knowledge and background to serve both the vendor and end-user communities. There is tremendous value in engaging the industry analysts; it's essential to understand their business models and their origins. The value of the analysts is 20 percent what they write about you and 80 percent what they say about you (source: The Knowledge Capital Group).

IS THE GOVERNMENT'S VERSION OF ALL IN THE FAMILY A REALITY SHOW?

DAVID HECHLER

The **Aspen Cyber Summit** focused on the federal government's need to work collaboratively with the private sector in order to protect the nation's critical infrastructure. It was called "Exploring Collective Defense in a Digital World," and the emphasis throughout the two days was most decidedly on "collective." It could have been called "We're All In This Together."

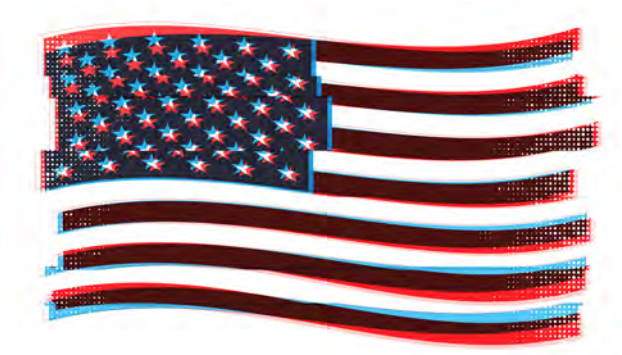
But just a few weeks earlier, Josephine Wollf, an assistant professor of cybersecurity policy at Tuft University's Fletcher School of Law and Diplomacy, wrote an article that suggested government agencies had serious problems working with each other. Specifically, she noted serious tensions between the offensive and defensive sides of the government's house. As I prepared for the conference, I wondered whether any of this would come up.

THE NEW KID ON THE BLOCK

In **"CISA Can't Succeed in the Pentagon's Shadow,"** Wolff argued that the U.S. Department of Homeland Security has never been given enough power to properly defend the nation's critical infrastructure, which is what its Cybersecurity and Infrastructure Security Agency (CISA) was created to do. CISA actually has several important roles, including working with regional officials to help secure elections. But the main focus for this conference was its role in helping to protect U.S. critical infrastructure by working with the companies involved, about 85 percent of which are in civilian hands.

Since its inception in 2018, CISA has been overshadowed by the Department of Defense, Wolff wrote. The National Security Agency and U.S. Cyber Command are the real powers in charge, she said. The Biden administration has expressed a desire to "marshal a whole-of-nation fight to confront digital threats," Wollf noted. But to do so, she continued, "it needs to embolden CISA so that it can begin to compel businesses and critical infrastructure operators to take the necessary steps that will actually protect the country's most vital systems and networks."

At a recent conference, government officials seemed intent on showing that they could work effectively not just with the private sector, but also with each other.



She suggested that one recent development might be a hopeful sign. In July, Jen Easterly was confirmed as CISA's director. Easterly is a former NSA official herself. She helped launch Cyber Command. So "it's possible to interpret her new position as a sign of just how far the two departments have come in finally being able to work together and how well established and respected the DHS cybersecurity operations finally are," Wollf wrote. It's also possible to view Easterly's selection as a sign that the military has achieved hegemony, she added, pointing out that the top cyber officials in the White House, Chris Inglis and Anne Neuberger, are also former NSA officials.

Easterly was the conference's first speaker. She spent much of her time reviewing her 10 weeks on the job. She had plenty to say about collaborating. The most eye-catching piece was the new group CISA established in August: the **Joint Cyber Defense Collective** (JCDC). The partners include all of the government's heavy hitters: DoD, NSA, Cyber Command, DOJ, FBI, and more. From industry they've lined up Amazon Web Services, AT&T, CrowdStrike, Google Cloud, Microsoft, et. al. No signs of any friction there.

Interestingly, her bookend as the day's last speaker was Rob Joyce. Joyce is the government's fourth leader in the cyber realm, and he has not only spent much of his career as an NSA official, he's the only one of the four who is there now. He heads its **Cybersecurity Directorate**. Earlier in his career there he led the offense. His new job mostly involves intelligence.

Between Easterly's **presentation** and Joyce's, lots of examples of partnerships were discussed. (I wrote about some of them here.) But there was also talk about the need for an offensive response to the onslaught of attacks. "We can't only play defense," said Kevin Mandia, CEO of FireEye. He wasn't alone in urging more from the government. One example that drew praise from many quarters was the clawing back of at least some of the ransom that Colonial Pipeline paid to regain control of its data. In this instance, the FBI rather than Cyber Command was credited for the accomplishment.

THE NSA TAKES THE STAGE

When Joyce finally took the stage (yes, most of the panelists were really there), he was joined by journalist and author Garrett Graff, who directs cyber initiatives for Aspen Digital. Graff's first question was about a warning the NSA had just released concerning VPN vulnerabilities. "This was a **document**," Joyce responded, "that talked about what you should have in consideration for securing your VPN. And it was done jointly with CISA. They are our deep partner these days. There's almost nothing we put out that we don't do jointly with CISA—often CISA, NSA, and FBI together."

There was more along these lines. For instance, Joyce said that NSA has stood up its own **Cybersecurity Collaboration Center** to build relationships with private industry. It lacks the scope of CISA's JCDC, but it is a notable development for an agency with a go-it-alone ethos. But Joyce was not there to discuss his agency's conversion to collaboration. The topic of the session was "The Next Generation of Threats," and Graff skillfully probed for answers.

During the first year of the Trump administration, Joyce served as cybersecurity coordinator on the National Security Council for about a year before the position was eliminated. Graff asked him what's changed four years later. "The idea that cyber crime has become a national security issue," Joyce replied. "That to me is a dramatic change. And you see the government utilizing all elements of our power to include the foreign intelligence team, the offensive cyber team in the efforts to work against ransomware."

So what are the country's top threats? Joyce listed ransomware as No. 1. No. 2 is disinformation, he said, which is both "a cybersecurity problem and a malign influence problem." After that comes the nation-state threat. "Russia, China, Iran, North Korea: they roll off so easy," he said, "because those are the big ones we always see doing very obnoxious things in cyberspace." And the last is critical infrastructure. It's

an area that "we've always known and worried about," but in the last five years it's grown urgent to lock down "for our national security."

"You are the author of what is probably the most famous line about nation-state cyber threats," Graff said. "Russia is a hurricane; China is climate change."

It's still true, Joyce said. Russia is a disruptive force, often seeking to tear down adversaries by disseminating misinformation and malign information. And they actively gather intelligence on both governments and critical infrastructure. All make them dangerous, he added.

China still looks like climate change to him. "Scope and scale," he said, "China is off the charts." Its number of cyber actors "dwarfs the rest of the globe combined," he observed. "You talked about the difference four or five years ago to today," he said to Graff. "The difference I see is we respected them less. It was always broad, loud and noisy." But what they're finding, he went on, is that based on those numbers, the elite members of that group "really are elite." That makes them a sophisticated adversary.

Rob Joyce heads the NSA's Cybersecurity Directorate.

"Scope and scale, China is off the charts," said Rob Joyce. Its number of cyber actors "dwarfs the rest of the globe combined."

The required response? Understand, disrupt and find ways to push back, Joyce said. "Defense is really important," he acknowledged. "But you also have to work to disrupt." The strategy is "continuous engagement," he said. "We've got to put sand and friction in their operations so they don't just get free shots on goal."

When people hear terms like "continuous engagement," he went on, "they think offensive cyber. It is," he said, "but I would say that the releases we've done jointly with CISA and FBI about the **N-day vulnerabilities** that those [adversary] teams like to use, that knocks them back just as much, and is just as important." As is working with the international community to establish "the expectation that these things won't be tolerated," he added.

What about Bitcoin, Graff asked. Is ransomware a cryptocurrency problem as much as a criminal problem? "Certainly without profit there is no ransomware problem," Joyce agreed. And crypto is the mechanism. But he called it both "a benefit and a liability." The transactions can be watched. "They're all very public," he said. "The question is, can you de-anonymize and connect them?" That's the challenge.

The other big challenge is **quantum-resistant cryptography**. When quantum computing arrives, unless they're prepared with cryptography that can withstand it, security will quickly dissolve. Confidentiality algorithms, encryption algorithms, and authentication protocols will all be vulnerable, Joyce said. Now is the time to plan, he explained. That's their Y2K problem, but "orders of magnitude bigger." Asked how it's coming along, Joyce said "I'm feeling really good." For the classified networks, "we already have the protocols and the encryption technology," he said. And they're working with NIST to select commercial standards. "After you have all those things," he said, "it's the retrofit—it's the get it into everything and build it backwards."

THE BOTTOM LINE

So what are we to make of Wollf's concerns that CISA has been minimized? And if she had a point, were the conference presentations reassuring? To some extent, I think they were.

Even if the conference primed the pump for partnership, it does say something that so many individuals, including speakers from the private sector, spoke about the need for collaboration. Likewise, the decision by CISA and the NSA to create organizations designed to facilitate more effective cooperation between the public and private sectors—and in CISA's case, between government agencies as well—doesn't guarantee these will yield results. But it proves it wasn't just talk.

As for the way the government balances the two sides of its house, it's no secret that the offense in cyberspace has long outstripped the defense. And that's not going to change just because people talk a good game. It's also true that the offense is always going to get more credit (when its activities are made public). But if there was ever going to be a time to recognize that the country needs both sides functioning effectively, this is it.

I think it does make a difference that Easterly made a name for herself at the NSA. And she has decades of high-level, relevant government experience. But what may be even more important is that defense suddenly seems top of mind. The country may never have appeared more visibly vulnerable.

The public heard about SolarWinds, and it sounded bad. But it was hard for a lay audience to understand what had happened. And then it only seemed to be about spying. Colonial Pipeline was very different. It was the infrastructure. And there were tangible results. Long lines at gas stations were on the evening news. All of those scattered ransomware attacks suddenly hit home in a big way. And they have not abated.

Where was the government?

At the conference, Rob Joyce talked about getting "left of theft." We need to be able to prevent these attacks, he said. "We really don't want the government, or any institution, to be really good at incident response. We've got to get ahead of that."

It's been a humbling time. The president of the United States had a talk with the president of Russia and told him the attacks had to stop. But they haven't. The talk about cooperation at the Aspen Cyber Summit didn't feel staged to me. It seemed to come from a bit of humility and a sense of necessity.

HUMBLE LEADERSHIP; SOME SUGGESTIONS

EDWARD AMOROSO

Witness **Fred Donner**, GM Chairman during the 60's, commuting to work using a 15-cent subway token. And witness **Ed Whitacre,** during his time running GM, eating his TexMex lunch with employees in the RenCen cafeteria. And witness every Bell System exec during the company's heyday, parking their modest sedans in employee lots. And yes—witness me in **TAG Cyber's** new digs at **45 Broadway** seated in a tiny booth just big enough for a desk.

These witness scenarios might confuse those of you trained to believe that perks and pleasures track with corporate promotion, and that the boss truly deserves to recline with a vodka in Seat 1A on Virgin Atlantic to London. Well—the truth is quite different and if you are still developing your own leadership skills and habits, then here are three basic suggestions worth absorbing now: (1) Symbols Matter, (2) Eat Last, and (3) Burn the Org Chart. Let's examine each:

Symbols Matter: Your employees watch what you do and how you do it. Their experience thus involves you transferring information to them in units known as symbols. For those of you (like me) who are more comfortable in front of a keyboard than a colleague, here's a tech-style definition: Your team will watch your actions. They will derive meaning from such observation. The units of data transfer are called symbols. Got it?

Here's an example: Your team is emerging from the pandemic into a new office. You're the boss and can pick whatever office is available. Option 1: You take the corner office with the window. This sends the symbol that rank matters. Option 2: You turn the corner office into a software developer room open to anyone who can code. This sends the symbol that rank is less important than code contributions. (So, uh, yes—go call the office planner now.)

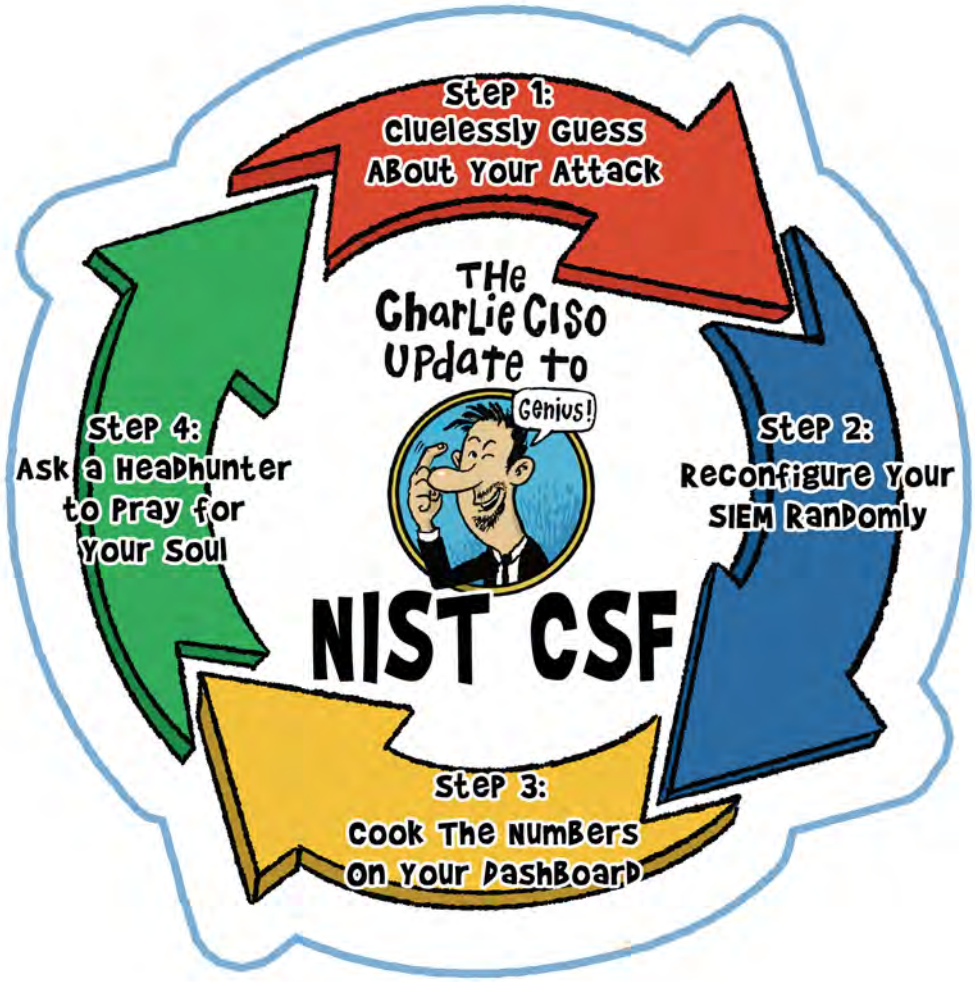
Eat Last. The motivational guru Simon Sinek is big on this one—and he is correct to emphasize the point. The reference is more metaphorical than deliberate, but sometimes it can be taken literally. When I founded TAG Cyber, for example, and hired my first employees in 2017, I created a routine where I would take everyone's lunch order and then go fetch the sushi bowls and tuna melts. I have no idea if this symbolic act worked, but no one complained.

Now—if you do not routinely lunch with colleagues like we do at KuuRamen on John Street, then you'll need to translate this "eat last" metaphor to your local context. For example, I suspect you'll probably be returning to the office soon—and every office has its coffee protocol. You know the routine: Drop in a ten-er occasionally, based on your estimated consumption. Well, if you're the leader, then fill the money tin frequently. You can afford it.

Burn the org chart. This is a painful one for many leaders—especially those people who like to say things like this: "I have two hundred people in my organization." It takes some maturity to disconnect the org chart from the respect your team will give you. Memorize this: Management structure can be announced by HR, but the respect of your people can only be earned. There is no organizational announcement that can make people want to follow you. None.

Here's a suggestion: Get rid of your org chart and draw your team as a series of circles gathered around projects. Conceptualize the team as a series of campfires being tended to by people poking the flames and warming their hands. You, the leader, should be walking around with baskets of kindling that you personally gathered from the woods. That should be your function: Gathering wood to keep your people's fires burning. Now that's a metaphor to remember.

So - if you are trying to lead a team, then I hope you will decide to internalize these three points and make them into daily habits. If you do this, then I can promise that your team will be much more willing to follow you into a tough battle. If you don't—and you send a bunch of bad symbols, and you decide to always eat first, and you continue to brag about your immense power over your lowly staff—well, then you will never have the respect of any team.



LESSONS FROM THE CYBER TRENCHES

DAVID HECHLER

IBM's Security Summit taps the wisdom of tech veterans.

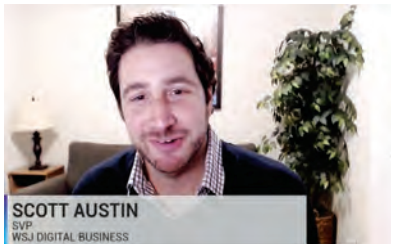
Looking back over the past 18 months, three corporate security professionals sometimes sounded like battle-scarred veterans as they talked about the cyber wars their companies have weathered.

Meredith Harper, chief information security officer (CISO) at Eli Lilly and Company, spoke of the "relentless" adversaries that "take advantage of any opportunity to be able to continue to attack not only ourselves, but also the strategic partners—the supply chains that we work with." Michael McNeil, global CISO at McKesson Corporation, noted that the Covid pandemic created a "perfect storm for threat actors," since workforces suddenly had to abandon offices and work remotely. And Chris McCurdy, general manager of IBM Security, noted the "double-digit increase in ransomware" attacks and ever more sophisticated phishing attacks targeting executives.

Rather than sharing war stories, however, these panelists at the recent **IBM Security Summit** focused on lessons they learned, and what companies should take away from the challenges many have endured. They talked about how to manage supply chain risks, how to recruit and retain tech talent, and how to ask management for resources without resorting to scare tactics.

The moderator of the discussion, Scott Austin from WSJ Digital Business, started by asking about the influence of the global pandemic. Eli Lilly's Harper began on a positive note. One of the biggest surprises, she observed, was how well companies were able to respond to the crisis. "Honestly, I would say that we found out in this moment that, as cyber professionals, we can do anything," she said. "We were able to, at the drop of a dime, convert our organizations from in-person organizations to remote organizations."

McKesson's main focus during the pandemic has been its job as one of the prime distributors of Covid vaccines, according to McNeil. At the same time, there was a large jump in phishing attacks, particularly messages



that lured the unwary with purported information about Covid-19. The required response was vigilance, McNeil said, and the company "doubled down" on training.

IBM was able to take in the threat landscape with a wider lens. "We run one of the largest threat intel organizations in the world," McCurdy said. The company manages and monitors 18,000 different clients globally, he noted. One troubling trend trailed the migration of businesses to the cloud. Attackers followed them there. McCurdy cited "over a 150 percent increase" in attacks in the cloud during the past five years. There was also a home-grown problem — literally. Security incidents caused by **shadow IT** mushroomed, according to McCurdy, as employees working from home used unauthorized systems that violated company policies "because people had to find new ways to work."

SECURING SUPPLY CHAINS

The conversation shifted to supply chains. McKesson recognized a need to monitor its third-party risk management program, McNeil said. And then they wanted to be sure they had a handle on their "secondary and tertiary types of organizations."

Lilly's Harper picked up on this theme. "Don't underestimate the complexity of your supply chain," she warned. Smaller organizations may have different attitudes toward security, which can leave their larger partners vulnerable when attacks multiply and adversaries search for the weak links. "I think sometimes we just kind of trust that the third party we're working with is doing all the right things," she said. "But we're not always verifying that they are." Lilly decided to engage in a global review to ensure that partners were meeting their expectations. "When you do that," Harper added, "be prepared, if you have a third party that is supporting a critical part of your value chain, and they are choosing not to rise to the occasion, to move them out."

IBM's McCurdy took it one step further. "Do you have a backup?" he asked. If there's a problem with the security of a major supplier your company uses, have you identified potential sustitutes you can turn to? For some large companies, he continued, it would not be practical to have replacements picked out for every third party they deal with, which can run into the thousands. But they should at least prioritize their top 10 vendors, and have backups identified for them, McCurdy said.

THE FIGHT FOR TALENT

Moderator Scott Austin asked about the global demand for employees to fill open tech positions. He noted that Michael McNeil had recently spoken on the topic. "It seems particularly dire in cybersecurity," Austin said.

It's challenging, McNeil acknowledged. It's not just a matter of hiring, he said. In this time of the Great Resignation, it's also executing retention strategies that will hold on to them. Because no matter how ambitious they may be, the odds are against any of them rising to be CISO. Others have no such aspiration. So it's crucial to manage expectations. The key, McNeil said, is to understand what new hires need, ensure that they understand the opportunities, and create employee development plans that match the two.

Clearly companies are jittery about their talent pools. Austin asked Harper if she's seeing "an exodus in tech" at Lilly. "No exodus. I thank God for that," she said. The company's recent strategy has been to try to reach women and minority candidates, recruiting at colleges and universities. But entry level hires are not sufficient to fill their needs, she continued. And the search for experienced candidates has led her to bump heads with McCurdy and McNeil "in this war of who can get the best talent," she said. "We're moving people around on the chessboard."

How can they create a more robust pipeline? "We need to look further than just college-age," she

said, answering her own question. “How do we get to the high schoolers? How do we get to the middle schoolers, and introduce them to STEM careers?” The goal: “I want to be able to replicate me in the industry as much as I possibly can.” And a big part of that is supporting them once they arrive, and giving them opportunities to do “some really cool things,” she said. “Don’t underestimate how much that helps team members stay connected to your organization, so they can’t be swayed away by the Michaels of the work, who want to pay them way more than we probably can.”

Scott Austin broke in. “I might have to have you give a pep talk to my daughter,” he said, to “get her more interested in STEM.”

McCurdy also has a daughter, he said. “And diversity and inclusion are extremely important to me.” Like its competitors in the talent sweepstakes, IBM has reached out to secondary schools. And has created summer internships. But it’s found another route as well. “Some of the best security people that we’ve hired are former developers that have security in mind, so they understand the importance of embedding security,” he said. And in the big picture, he went on, “we need to embed security culture at our houses. So that way, whey they come into the workforce, they’re thinking about security as they come in.” McCurdy also expects artificial intelligence will mitigate the problem by taking over lower level security work.

As the session wound down, Austin read a question submitted from the audience. How do you convince management to set aside resources?

EFFECTIVE PITCHES FOR RESOURCES

When you approach management with budget requests, they need to be “risk-based,” McNeil emphasized. “You should never go in with fear, uncertainty, and doubt — the sky is about to fall,” he said. “I guarantee you it’s not sustainable. I guarantee you it’s not believable at the executive levels. You have to present the particular business case, and it has to have the appropriate sets of value propositions.” That approach has worked for him, he added.

Harper agreed with McNeil. And she had this to add: Instead of coming to the board with talk of firewalls and encryption, about which these people know little, bring a story. In the past, she explained, security professionals too often failed to address the company’s business imperatives, and how they could help meet those through technology and security. “I’m not going to go in and start talking about zero trust, even though we’re doing it,” she said. “I’m going to talk about what it will enable, what it will allow us to do. We have to get better and smarter at telling that story.”

Sometimes the perfect story can be crafted from a devastating attack that’s in the news. “If I am smart,” Harper said, “I am going to review and monitor my own organization, to see if some of the conditions are consistent in my organization that allowed that bad thing to happen to someone else.” And if there are similarities, she will present the parallels to Lilly’s executives. “That’s a strong business case,” she said. “We don’t want to be them.”

MY UNUSUAL PATH TO SUCCESS AS A CSO

GARY MCALUM

When I was hired as United States Automobile Association's (USAA) first chief security officer (CSO), I didn't arrive on the typical path security executives take to such a large role. A CSO or a chief information security officer (CISO) often follows a more traditional journey of working in various information technology and business roles before attaining a senior executive role. My journey was quite different, but no less useful in preparing me to lead a team of over 1000 employees spanning multiple security domains. On top of that, I was entering the financial services sector working for a company that focused on serving the military community with a wide range of banking, insurance and financial products.

That turned out to be no problem. I arrived at USAA in February 2010 with a strong background in leadership, cybersecurity and technology. And I also had three important skills in my toolbox that served me well as I navigated a large financial services company and led a new security department. These skills were developed over a 25-year career as an Air Force officer in the functional area of information technology. There I had learned to think quickly and creatively, communicate effectively and simply to a variety of audiences, and lead teams through a personal style of "servant leadership."

In my early days at USAA, I faced a variety of challenges. The first was leading an organization that didn't even exist. Other than a vision of a high-performing holistic security organization spanning information security, privacy, fraud operations, business continuation, corporate investigations and physical security, I was starting with a blank page. All of these organizational elements were already aligned under different leaders across USAA, so there was a myriad of tasks that had to be worked through, including HR, budget and operational linkages. We didn't even have a name for this new department, so in my first staff meeting we came up with "Enterprise Security Group."

U.S. AIR FORCE

I practiced servant leadership, which is a philosophy that says the most effective leaders strive to serve others rather than seek to accrue power or take control.

USAA®

Those first few months required continuous fire-fighting. Besides building the organization's identity, establishing a culture of excellence and connecting all the business areas, we had to keep the trains running! Daily operations, especially in information security and fraud, are a 24x7 activity. What helped me early on was the skill of being able to think quickly and creatively. I think of it as learning agility. Over a 25-year military career, I often moved around to different organizations and had to develop this ability to enter a new environment and quickly assess and prioritize what were the most critical tasks in support of the mission. This is exactly what I did in the early days of the Enterprise Security Group. I had to quickly understand the key processes for all my areas of responsibility, connect the dots back to the lines of business, and develop objectives, performance metrics and a business strategy. In many ways, the challenges I faced at USAA were no different than many of my military assignments. I certainly had to adapt to a corporate environment, but the fundamental skill of learning agility helped me tremendously.

Another indispensable skill that I leaned on heavily was the ability to communicate effectively. I faced the challenge of leading a highly visible, new department and explaining to a wide variety of business stakeholders how our 24x7 activities supported them and enabled their success. As everyone knows, security is not a P&L operation, it's an expense, so explaining the value proposition was critical. The challenge is to communicate complex ideas in language anyone can understand. Fortunately, this was a skill I had developed over the years. Our field of endeavor—cybersecurity—is complicated, hard to understand. Many times, security executives over-index on the technical side when talking to the business and other stakeholders. Of all the qualities of a successful CSO/CISO, keeping it simple has to rate at or near the top. I think I am pretty good at this, whether talking with business leaders, briefing boards or interacting with regulators.

I remember one specific example early on that I used to develop this skill among my team. Faced with explaining to the Board of Directors what a distributed denial of service (DDos) attack was, my team gave me an initial draft of a brief that was an excellent multislide deck on how a DDoS attack actually worked. But it wasn't what we needed to brief the board. They didn't need to understand the detail of an ICMP Flood attack or the intricacies of NTP amplification! I told my colleagues that we needed three slides: one high-level overview of what a DDoS attack does, a slide on the business implications or risk of a DDoS attack against USAA, and a slide on our mitigations. I also suggested they talk to our business continuation team to understand the financial impact, based on the business impact analysis, if our customer-facing systems were down for an hour. The board loved it. Simple, clear, well-received.

"Remember when those idiots thought we'd work with no breaks?"

Finally, the most important skill for any successful business executive is leadership, and the military excels at developing leaders. Throughout my 11 years at USAA, I practiced servant leadership, which is a philosophy that says the most effective leaders strive to serve others rather than seek to accrue power or take control. And you can't practice this kind of leadership while sitting behind a desk. This is not a new concept. Every executive development course or book encourages leaders to get out and about with their troops. But the tyranny of executive calendars quickly

gobbles up that precious white space and the hours race by.

How did I overcome this tyrant? I spent as much time as I could on a regular basis visiting the cyber operations center, sitting with fraud analysts on customer calls, standing with the security officers at the gate, and so forth. There are two great benefits to this model. First, your front-line troops get to know you better, and word gets around. Second, you typically get unfiltered feedback on what's going well and what's not going well. Last, you learn. As a senior executive, I knew I would never have to handle a fraud service call, but over time I became intimately familiar with the processes of how that important interaction worked and what tool improvements the front-line call representatives needed. In fact, after I spent many early days focused on fraud calls, we created an initiative to default our membership to multifactor authentication.

In the military, we called this "leadership by walking around." Military officers are trained from an early stage to be with the troops and lead from the front. As a mid-level officer in a deployable communications unit, I didn't know anything about tactical communications equipment, but during exercises out in the field I often walked around on the night shift visiting each of our "unit type code" systems. I learned a ton that helped me better connect the dots back to the broader mission. More importantly, I got to know lower-level airman and NCOs to a degree that would not have been possible sitting behind a desk.

Successful business leaders take many paths to arrive at increasing levels of responsibility. My path was not a common one. When I started my business career, I had to learn business financials and operations. But a military veteran brings a unique package of skills and experiences that for me were invaluable. And for these I will be forever grateful.

LEGAL

THE ADMINISTRATION'S STRATEGY TO BEAT BACK RANSOMWARE

DAVID HECHLER

Following months of criticism for not responding aggressively enough to a barrage of ransomware attacks, the administration seemed to shake off any hint of lethargy and declare itself fed up. The U.S. Department of Justice has created a crypto currency enforcement team to pursue both criminals who use these exchanges to profit, and the platforms that enable them. The department also intends to use civil enforcement tools, like the False Claims Act, to sue government contractors that suffer data breaches and choose to remain silent rather than report them to the government.

That was the message that Deputy Attorney General Lisa Monaco announced on Oct. 6. The occasion wasn't a press conference. She was interviewed at the annual **Aspen Cyber Summit**, and she had plenty of company reinforcing her talking points. The topic for the two-day event was "Exploring Collective Defense in a Digital World," and the presentations amounted to a full court press on the need for public–private collaboration.

A conference brings together leaders from the public and private sectors to discuss their need to collaborate.

Among the speakers were the administration's cyber security triumvirate: Jen Easterly, director of the Cybersecurity and Infrastructure Security Agency (CISA); Rob Joyce, director of the NSA's Cybersecurity Directorate; and Chris Inglis, the White House's national cyber director. (Only Anne Neuberger, deputy national security advisor for cyber and emerging technology, was missing.) There were also two leaders from the trenches: David Turk, deputy secretary of the Department of Energy, and Mieke Eoyang, deputy assistant secretary of defense for cyber policy. U.S. Rep. Yvette Clarke (D-N.Y.) and Rep. John Katko (R-N.Y.), who are working on a bill in the House that would require companies to report cyber attacks, were joined by Senator Angus King (I-Maine), co-chair of the Cyberspace Solarium Commission. The other speakers were researchers, academics, CISOs, and about a dozen CEOs. In their own ways they all emphasized the importance of working together.

Monaco hammered home the theme. Asked how she feels about "name and shame indictments," she said the department will continue to use them "as one tool." But they are not only about naming and shaming, she insisted. Individuals have been tried as a result of these indictments, she said. More broadly, she continued: "We are building coalitions with partner nations" to prosecute criminals and attack "the ecosystem that supports the malicious cyber activity." She cited the recent takedown of the **Emotet botnet** as an example.

Asked how the government plans to counter ransomware, she described a two-prong defense. First, they want to strip anonymity from payments. And then they want to claw back the illegal profits, as they were able to do after the Colonial Pipeline attack, she said.

On the day Monaco spoke, CNBC published an **opinion piece** she wrote that expounded on her remarks. She called on Congress to enact legislation creating "a national standard for reporting cyber incidents that pose significant risk, including ransomware and incidents that affect critical infrastructure and their supply chains." She went on to say: "In the case of ransomware, such reporting should also include details about any ransom demand or payment." Then she added a sentence that a lot of companies have been waiting to hear: "And victims should not be worse off for helping the government."

WHAT IT MEANS ON THE GROUND

During the conference, amid the embrace of partnership, there were probing conversations in which participants tried to articulate what cooperation means on the ground. For example, during a discussion that focused on nation–states, Sean Joyce, global cyber and privacy leader at PwC, called out the FBI, where he was once deputy director. Channeling his previous role, he said: "I think we could do a better job, as we did recently, tracking the crypto currency [stolen from Colonial Pipeline] and recovering that, And I think we can also accentuate cooperation with the private sector. And we can be more transparent doing that."

Kevin Mandia followed by focusing on the challenge for companies. "We can't just always play defense," said FireEye's CEO. "On offense, even the crappiest hockey players, if they get 1000 shots on goal, will put the puck in the net." And often the private sector is not in a position to respond. "Nations need to hold nations accountable," he went on, "however they've got to do that. If you can't get to the person, and you may not be able to do, you have to hold the nations accountable." And that makes attribution essential, Mandia added.

Mieke Eoyang, the deputy assistant secretary of defense, chimed in. "It's really important, for those of us who are on offense, that people report those incidents." If victimized companies say nothing and secretly pay a ransom, the government learns nothing about the threat, she said. And the government can't help those companies and others that may be at risk.

Earlier, Eoyang had described the circumstance most likely to provoke U.S. retaliation. "We have not seen a nation–state sponsor an attack that is the equivalent of an armed attack," she said. "We've been very clear about that as a red line for the United States. The equivalent of an armed attack is going to get you a response."

"Can you define an 'armed attack'?" asked Joyce.

Eoyang acknowledged that it's tricky. "It's a little bit in the eye of the beholder," she said. "We're talking about destructive, loss of life, serious injury, those sorts of things."

In practice, attacks are not always under control, Mandia noted. "On offense, you can't always predict the consequences," he said. Which makes it trickier.

Eoyang agreed. It can be hard to know what was intended, and what was not, she said. An attacker may not understand the interdependencies of systems, and the way those could lead to unintended consequences.

'THAT'S THE FUTURE'

Another session offered signs of progress. The moderator was Chris Krebs, Easterly's predecessor as director of CISA. The panelists were all from the tech side of their companies. At one point Krebs asked them to talk about risk strategy. Marene Allison, CISO at Johnson & Johnson, said, "Sometimes as security professionals, we really like the idea of perfect security. Patch everything, know everything that's everywhere all the time. But the reality is: Will you ever?" For her, that approach doesn't make sense. "My big pivot was into cyber resiliency and business risk."

Mastercard also aims for realistic security rather than perfection. But Ron Green added that part of its focus is on its ecosystem. If his company is secure, said Green, Mastercard's chief security officer, but the merchants they work with are being compromised, consumers may lose confidence. And that's a threat for Mastercard. The solution is to work with others in their ecosystem to help them "raise their security game by not just telling them what the good thing is," Green said, "but to actually give them things that they can implement in their environment today for free. Just to raise the level of security."

Krebs jumped in. "This dynamic that you're talking about, where the products and services are pushing solutions out further to the edge to protect the user—I think that's the future," Krebs declared. "Whether you're in the software products and services space or in the internet infrastructure space, you're seeing more solutions pushed down to the consumer."

Noopur Davis, CISO at Comcast, quickly agreed. "Anyone who buys a gateway from us, anything that they connect through that gateway—whether it's a wired or wireless connection—is protected," she said. "We look for malware, we look for network traffic, we look for bad sites. It's embedded and it's there by default." It makes sense for companies to boost customer security if they can. "It's mutually beneficial," she said.

Allison said that the focus on resilience has her company's full attention. "It's almost like what we did in those Y2K days," when business continuity planning was so important. J.&J. is trying to prepare in some of the same ways it did back in the late 1990s, but in this case it's to ensure cyber resilience, she said.

Mastercard has seen the same thing. The company's executives and even board members "want to actually review how we respond to a cyber incident—and participate in our cyber exercises," Green said. They want to know because they see how often it's happening, he added.

To Krebs, these attitudes seemed to announce the arrival of a long-held hope. "That's the shift that we've been praying for the last couple of years," he said. "The shift from technical risk to business risk." Green's comments also connected with Krebs's earlier observation about cyber security's most important rule. "It starts at the top," he'd said. "If the leader is not on board, your jobs as CISOs are incredibly difficult."

WHO IS ACCOUNTABLE?

Not long after Monaco's session, there was a lively discussion about the electric grid featuring three leaders who have skin in the game. Moderator Patrick O'Neill from MIT Technology Review asked whether the United States is holding people accountable for attacks like the **Dragonfly assault** on the U.S. electric grid, which has been attributed to Russia.

But it turned out that the panelists were more interested in another question involving accountability—one that was closer to home. Who is accountable for defending the electric grid? That was the one they mostly answered.

Defense requires an active offense, said Connie Lau, who heads Hawaiian Electric. The government is the power the companies depend on to protect the grid, she continued, and has recently demonstrated a greater willingness to use its offensive capabilities to disrupt threats before systems are harmed.

She then asked a question that undoubtedly reflected the concerns of many companies worried about growing security costs. "We all are patriots," she said, "we all want the national security. But at the end of the day, who ends up paying for that?" State ratepayers obviously shoulder some of the costs, she said, and the government has contributed. But it requires a partnership, she emphasized.

Joy Ditto, who heads the American Public Power Association, cited the U.S. attack on the Iranian centrifuges at **Natanz** as the first example of the country flexing its muscles and demonstrating its offensive capabilities. That prowess is important in defending the grid, she agreed. But then she indirectly raised another question: How reliable is the country's commitment in a hyper-partisan political environment? The industry has to keep talking to the government on these issues, and the good news is that "it's a bipartisan conversation," she said. "We almost don't miss a beat when there's a new administration that comes in."

Pedro Pizarro, CEO of Edison International, concurred. "I watched this during the Obama administration. I watched this during the Trump administration. Now I'm watching it in the Biden administration. The arc has continued."

As for O'Neill's original question, Monaco had earlier said that individuals have been indicted and held accountable, but the victories have been small and have not stanched the attacks. The importance of the question was underscored by Senator Angus King later in the day. In a session on cyber security legislation, he was asked what bills he would favor. King used the opportunity to address the issue he is most concerned about, which turned out to be the one O'Neill had raised. "I think the most important thing is for the administration and the president to develop a clearly articulated deterrent doctrine," he said, "to put our adversaries on notice that they will pay a price for attacking us in cyber space.

"Our adversaries," he concluded, "don't fear consequences."

MY TAKE

SILICON VALLEY ACCOUNTABILITY

DAVID HECHLER

There's been a lot of talk about the fast-and-loose culture in Silicon Valley, and the disparity in the way company leaders are treated following controversies. The most recent chatter was prompted by the criminal trial of Elizabeth Holmes, founder and CEO of Theranos. Well before the jury found her guilty on four of the eight charges on which they reached a verdict (jurors were hung on the remaining three), some critics of Valley culture, such as former Reddit CEO Ellen Pao, suggested that sexism was part of the reason Holmes was singled out.

Plenty of other founders have driven startups to impressive heights only to lose control in the clouds. But there was one difference, Pao told **NPR**. "When you see which CEOs get to continue to wreak havoc on consumers and the market," she said, "it's people who look like the venture capitalists, who are mostly white men." Pao knows the territory. She herself joined a venture firm that she later **sued**—unsuccessfully—alleging discrimination.

In the NPR interview and in a New York Times **opinion piece**, Pao emphasized that she wasn't defending Holmes. She believes Holmes deserved to be prosecuted. She just wanted justice to be evenhanded. "Why aren't we holding other people accountable so we can avoid all the harm that is happening in the tech industry?" she asked.

In naming some of the men who got off easily, Pao mentioned Uber's founder and CEO, Travis Kalanick, who **left his company** in the wake of a sexual harassment scandal. But that was only one of the controversies that dogged his tenure. There was another matter that briefly got a lot of attention, and actually led to criminal charges, though not against Kalanick. Some of the reactions it provoked make you wonder if there's really public support for accountability.

It was a 2016 data breach involving the driver's licenses of 600,000 Uber drivers and personal information of 57 million Uber customers and drivers. And to make matters worse, the intrusion looked a lot like one

"I have something sensitive I'd like to update you on if you have a minute," Sullivan texted Kalanick.

Travis Kalanick

Joe Sullivan

that hit the company in 2014. In fact, 10 days before hackers contacted Uber about the new incident, the company had finally completed responding to information requests from the Federal Trade Commission (FTC) about the first one.

There were several very big differences between these two events, according to the criminal complaint. The hackers had not merely identified vulnerabilities in the second instance. They had stolen records. And Uber decided it would not report the breach. Very few people at the company even knew about it, the complaint said.

Travis Kalanick allegedly knew. But he wasn't the person charged with the crime, even though Ellen Pao might have had reason to wonder about that. The individual charged had been Uber's chief security officer, Joe Sullivan. Filed in federal court in San Francisco in August 2020, the FBI's **complaint** charged him with obstruction of justice and **misprision** of a felony for allegedly covering up the 2016 hack. In December 2021, a superseding indictment added three counts of wire fraud in connection with nondisclosure agreements that were sent to and received from the hackers.

No one else who knew about or participated in these events has been charged. But recent developments suggest that this case may have a long way to go. Sullivan declined a request for an interview. He referred me instead to his ongoing battle with his former employer.

His lawyers filed a subpoena to obtain documents from Uber that he claims will demonstrate that, far from operating in secrecy, he worked with Uber's top executives. According to a motion his lawyers filed on January 6, "at least two dozen Uber employees from the company's Security, Legal, and Communications groups played a variety of roles responding to the 2016 Incident." Uber has argued that many of the requested documents are irrelevant or protected by attorney-client privilege or the work product doctrine, including documents it provided to the government in heavily redacted form. Sullivan contends that by selectively revealing otherwise protected information to the government, Uber has waived any privilege it might have enjoyed.

IT STARTED WITH A NEW JOB

Sullivan arrived at Uber in April 2015, having spent the previous five years as the CSO at Facebook. Further enhancing his reputation, in April 2016 President Obama appointed him to the 10-person **Commission on Advancing Cybersecurity** alongside (retired) General Keith Alexander, formerly the longtime director of the National Security Agency.

Though Sullivan wasn't on hand for Uber's 2014 data breach, the complaint noted that Uber quickly tapped him to take the lead in responding to the Federal Trade Commission's demands for information. A member of Uber's so-called A-Team of executive managers, the company chose him to testify under oath at an FTC hearing about the breach.

Less than two weeks later, Sullivan received an email from two hackers who claimed to have discovered a "major vulnerability" in Uber's network, and had already stolen data. Under Sullivan's direction, a small security team confirmed these facts. The CSO continued to communicate with the FTC about the first breach, but he said nothing to the agency about the second. Nor did he tell the in-house and outside counsel with whom he'd been working on the 2014 breach about the new one.

Instead, the complaint said, he chose another course. He instructed his small team to keep the matter quiet; they would handle it using the company's **bug bounty program**. No one needed to know the details.

Like many companies, Uber sometimes paid researchers/hackers a cash bounty for reporting vulnerabilities in their software so that they could patch the flaws before unscrupulous individuals took advantage of the bugs. The token payments were no more than $10,000. But in this instance, according

to the complaint, the hackers were after more than a small gratuity. They had already stolen data, and they were demanding $100,000—in bitcoin.

Sullivan quickly agreed. In exchange, he required them to sign nondisclosure agreements and to promise to destroy the data they'd stolen. At the same time, Sullivan and the hackers maintained in their agreement that no data had been taken, even though they all knew this was false, the complaint said.

Kalanick was never mentioned by name in the complaint—he was referred to as "the CEO at the time"—but he did figure prominently in two passages. One said: "Records further indicate Uber's management team, with the sole exception of Uber's C.E.O. at the time, had no contemporaneous knowledge of the details of the data breach and had no role in the decision to treat the breach under the Bug Bounty program."

Later it recounted an exchange of texts between Sullivan and Kalanick. These occurred in the early morning hours, not long after Sullivan received the hackers' email and confirmed the breach. "I have something sensitive I'd like to update you on if you have a minute," Sullivan wrote.

Records revealed that a series of phone or FaceTime calls ensued. These lasted for five minutes. Then Kalanick texted back: "Need to get certainty of what he has, sensitivity/exposure of it and confidence that he can truly treat this as a bounty situation… resources can be flexible in order to put this to bed but we need to document this very tightly."

FIRST NOTHING, THEN THE BILL CAME DUE

Remarkably, the episode remained a closely guarded secret for nearly a year. Maybe if Kalanick hadn't been pushed out of the C-Suite in June 2017, the silence would have continued. But as it turned out, there was a meter ticking. Two months later, after a series of scandals and an independent investigation into sexual harassment at the company produced a scathing report, Kalanick was out as CEO. He was soon replaced by current CEO Dara Khosrowshahi.

Within weeks the new boss asked Sullivan to brief him on the 2016 incident. Sullivan had his team prepare a summary, but according to the federal complaint, before he turned it over he "removed certain details from the summary that would have illustrated the true scope of the breach." For example, he made it sound as though the hackers had gained access to data, but hadn't actually stolen it.

Khosrowshahi hired outside experts to investigate, and in November 2017, he **posted a blog** reporting what they'd found. "You may be asking why we are just talking about this now, a year later," he wrote. "I had the same question…" He apologized and revealed that he'd fired two employees. One was Joe Sullivan. The other was a lawyer who reported to him named Craig Clark.

Two months later, Sullivan told The New York Times that there hadn't been a breach. "I was surprised and disappointed when those who wanted to portray Uber in a negative light quickly suggested this was a cover-up," **he told the paper**. Kalanick refused to comment.

In August 2018, the two hackers, Brandon Glover and Vasile Mereacre, were indicted and a year later they **pleaded guilty**. The complaint against Sullivan noted that the two had successfully hacked other technology companies after their experience with Uber. "Had Sullivan and Uber promptly reported the illegal hack to law enforcement, the hacks of multiple additional large tech companies and the theft of the personal data of millions of additional customers and users may have been prevented," the complaint said.

The cost of this scandal to Uber's reputation is hard to gauge. When the FTC learned that the company had concealed this second event, the agency withdrew its agreement to settle Uber's 2014

breach. But Uber had so many hits to its reputation during this time that one more may have been indistinguishable.

However, there was also the matter of the lawsuit filed by attorneys general in all 50 states based on the company's admitted failure to comply with state data breach notification laws. The cost of that far exceeded the bounty the company had paid. Uber **settled** the matter for $148 million in 2018. That same year, the U.S. Senate's Commerce, Science and Transportation Committee held a **hearing** on Uber' bug bounty program. The company's own CISO at the time, John Flynn, defended the concept of these programs, but not his company's execution of theirs, which he acknowledged had been deeply flawed.

WAS SULLIVAN JUST THE FALL GUY?

It's not unusual for a CSO to get fired in the wake of an embarrassing breach. If somebody has to take the fall, the CSO or the CISO is often viewed as the logical selection. They usually maintain relatively low profiles, and it can all be done discretely.

But this was different. Sullivan wasn't your average CSO. And Uber was anything but your average company. Every misstep that happened there that year seemed to end up in the media. Coming after Kalanick's abrupt departure, discretion was not an option.

The new CEO was under the spotlight when he learned of the breach. If he had failed to fire Sullivan under these circumstances, it would have been hard for him to maintain that he was establishing new standards—especially since his outside investigators apparently found evidence that there had indeed been a cover-up. Sullivan's lawyers argued in their court filing that Khosrowshahi may have had another motive for blaming and dumping his CSO. At the time Uber was negotiating with SoftBank to sell a 15 percent stake in the company for more than $7 billion. And SoftBank was demanding that Uber disclose the 2016 incident.

Though Sullivan's reputation had undoubtedly taken a serious hit, eight months after he was fired by Uber he was hired as chief security officer at **Cloudflare, Inc.**, where he works to this day. And he seems to retain a good deal of support from the tech community.

As for the criminal complaint against him, some prominent observers were shocked and angered. One of them was Katie Moussouris, CEO of Luta Security, who had testified about Uber and bug bounties at the congressional hearing. "I think that singling out Joe for this is ridiculous," **Moussouris told Wired.** "No company places security and transparency decisions on one executive alone." CSOs should be held accountable, she acknowledged, but they should not be offered up as the "Chief Sacrificial Officer."

A spokesperson for Sullivan pointed to Uber policies that he argued made clear where the ultimate responsibility lay. "Uber's legal department—and not Mr. Sullivan or his group—was responsible for deciding whether, and to whom, the matter should be disclosed," **he told CNN**. So if anyone obstructed justice, it was the company's lawyers. It seems clear from his recent court filing that Sullivan is betting that documents—if he can get them—will back this up.

The complaint, on the other hand, charges that Sullivan kept the lawyers in the dark with one exception—Craig Clark, the lawyer who reported directly to him. And Clark was also dismissed.

THE LEGAL ANGLE

Speaking of lawyers, there's one more angle that seems relevant here. Joe Sullivan is a lawyer himself. Sullivan was once an assistant U.S. attorney for the Northern District of California—the very same office that filed the complaint against him. He worked in the computer hacking and IP unit. Later he was an associate general counsel at PayPal, and he joined Facebook in the same capacity before moving

into the CSO job there. This may help explain why Sullivan required the hackers to sign nondisclosure agreements. It's the kind of thing a lawyer would think of.

Lawyers understand the difference between lies of commission and lies of omission. And they know that lies of omission are every bit as serious. They also understand the danger in which they place themselves when they lie to federal agents. If any CSO should be thoroughly acquainted with his legal responsibilities, one would think it would be Sullivan.

Joe Sullivan worked his way up to an executive job at Uber. He was a CSO who truly had a seat at the table. He had the ear of the CEO, which is something that security officers have long craved. But with that access comes responsibility. And in this case, Sullivan is being held legally responsible for what he and his colleagues did. The big question, of course, is whether that's really the role he played. Or did in-house lawyers (a job Sullivan seemed to have left behind) actually fill that function?

Katie Moussouris may be justified in wondering why no one else at Uber has been charged with a crime. It's the kind of question Ellen Pao may also be asking. The complaint documented that Kalanick was in the loop. But just because the former CEO hasn't been charged doesn't mean that nobody else should be.

Whoever's to blame, it's hard to argue that no one at Uber was complicit in the crime for which two hackers pleaded guilty. It isn't just the "bounty payment" that seems to demand accountability. It's a year of concealing the facts, and pretending all along that nothing was wrong. Executives seemed to play fast and loose with the truth. Until finally the truth, and the law, caught up.

Maybe the Valley needs a dose of that.

WHY IT'S SO HARD TO PROSECUTE CYBERSTALKING

DAVID HECHLER

The founder of **Sightline Security** said she would never have gotten into the security business if she hadn't endured years of cyberstalking in the early 2000s. **Kelley Misata**, who is CEO of the startup that helps nonprofits build cybersecurity into their programs, said she sought advice from law enforcement and nonprofits during that time, but neither had a clue how to help.

Ryan White, a former assistant U.S. attorney for the Central District of California, said he wasn't surprised by the details of Misata's case. "Law enforcement traditionally is used to investigating real-world crime—crimes they can investigate by going out and interviewing people and looking at real footage." In the early 2000s, they had a long way to go to catch up to what was beginning to explode. And despite legal and technical advancements, cyberstalking remains difficult to prosecute even now, according to White, who worked his way up to chief of the cyber and intellectual crimes section before he left the office in 2020, after more than nine years.

A CASE OUTSIDE THE MOLD

Misata described a series of encounters with law enforcement that were frustrating, to put it mildly. The harassment she experienced started in California in 2007 and lasted for about seven years. The man who stalked her was never her boyfriend. There were no nude photographs with which to threaten her. They merely worked at the same company. It says a lot about the state of the law in 2007 that the police reflexively referred to the domestic violence law when they spoke to her. It was the closest one they could find to her situation, even though she'd never had a personal relationship with this guy, much less a shared domicile.

After she moved to Massachusetts, the harassment continued. It wasn't just about tracking her movements and communicating with her. He started intruding on the lives of the people around her. He contacted her friends and family. And not just once. He persisted until it was annoying. And then scary, because he wouldn't

The founder of a cybersecurity company endured years of cyberstalking in the early 2000s with little help from law enforcement. A former prosecutor shares why cyberstalking remains difficult to prosecute, even today.

Kelley Misata, founder of Sightline Security, and Ryan White of Halpern May Ybarra Gelberg

stop. That was when the people Misata counted on as her support network began demanding to know why she'd brought this person into their lives. As if she'd had control. As if this was something she had done. Then she was not only blaming herself for the mess she was in, which is all too common among victims; the people she'd been closest to were also blaming her.

When she reported the harassment to the police, one officer said, "He's thousands of miles away. He can't hurt you." This wasn't an aberration. No one seemed to understand her plight. When a detective seemed equally mystified, Misata tried a different tack. "Are you on Facebook?" she asked the woman. The detective nodded. "OK, what do you post?" Nothing special: "Pictures of my niece, my nephew, this and that." Misata nodded. "You know there are bad guys on Facebook, right? Do you have privacy settings turned on?" The detective said she didn't and suddenly looked concerned. "Can we go set them up right now?" Misata asked. And in the middle of her interview in the police station, they walked into the back office, got on the detective's computer, and Misata showed her what she needed to do.

The cyber harassment Misata was experiencing had not even been defined in the law when she first reported it. And when Misata talked about cyberbullying, the police wondered what that had to do with her. They'd heard about it, but the victims were teenagers, like 13-year-old Megan Meier. She was the schoolgirl who hanged herself after the mother of her former friend bullied her online. The mother, Lori Drew, was convicted by a Los Angeles jury—before the judge reversed the verdict and acquitted her.

The cops didn't see how bullying fit, and Misata didn't understand how the domestic violence laws did. But there didn't seem to be alternatives. "I had one law enforcement agent tell me that if you had bruises or some physical harm, they could do something," she recalled. They seemed stuck "at a time where people were devastated by children committing suicide," Misata said. And parents were wondering "how can stuff that's happening in social media and through text messages affect my child's life so badly that they take their life?" But Misata wasn't mystified. "I understand why they did that," she said. "I understand how dark and sad they were, and how helpless they were feeling."

THE PROBLEMS FOR LAW ENFORCEMENT

But Misata's challenges with law enforcement more than a decade ago were not just a result of a dearth of laws covering online behavior, according to White, who is now chair of the cybersecurity and data privacy department of litigation boutique **Halpern May Ybarra Gelberg** in Los Angeles. Local cops and prosecutors were frequently hamstrung by their inability to subpoena information outside of state boundaries. And often the data—the evidence in online cases—crossed state and even international lines. So investigation and prosecution had to be done by the feds—by the FBI and by assistant U.S. attorneys like him. And the laws they used were the **federal cyberstalking statute**, the **Computer Fraud and Abuse Act** and the **aggravated identity theft statute**.

One reason these cases can be tricky is precisely because there are not likely to be bruises to corroborate crimes. Threats are delivered by emails and texts. And the defense may insist these are protected by the First Amendment. White argued a case, **United States v. Osinger,** before the U.S. Court of Appeals for the Ninth Circuit in which that was a key issue. Christopher Osinger had been convicted of stalking and harassing his former girlfriend.

After she'd left Illinois and moved to California to get away from him, he spoofed a Facebook page that appeared to be hers and sent sexually explicit photos of her to, among others, colleagues at her new job. In appealing his conviction, Osinger argued that the stalking statute was unconstitutionally vague and violated his free speech rights. The court was not convinced. "Any expressive aspects of Osinger's speech were not protected under the First Amendment," the court held, "because they were 'integral to criminal conduct' in intentionally harassing, intimidating or causing substantial emotional distress …"

Even today, the issue isn't easy, White said. What is cyber stalking? "It can be everything from revenge porn, to online impersonation, to text messaging," he said. "And that makes it very difficult to define. And consequently, difficult for the public to understand, for law enforcement to understand, and sometimes to see as a real problem."

> "I think for many victims," Misata said, "they just want it to stop."

Despite the missteps Misata described, she was able to convince the FBI to open an investigation. And they worked on it diligently, she said. But in the end, there was a problem. She hadn't saved any of his early communications. That was the last thing she'd wanted to do at the time. And then he began to anonymize his messages using Tor, software that allows anonymous communication. So all the FBI was able to offer was to do a "knock and talk"—knock on his door and talk to him about what he was doing. And that was the very last thing Misata wanted. All that would do was "poke the bear," she said.

When asked why the FBI couldn't have gotten a subpoena to learn the origins of these messages, White explained that's not really possible with Tor. Messages are sent through a decentralized network of encrypted communications around the world that shuttle randomly through at least three host computers. To trace a message back through these permutations and positively identify it would be next to impossible, White added. Such things are only attempted for national security investigations of the highest priority, he continued, and require the greatest expenditure of resources with no guarantee of success. "For the U.S. government to use those tools, to the extent they even can, they use them very, very rarely."

A QUESTION OF RESOURCES

During White's time as a federal prosecutor, "individual cases became few and far between," he said. That was "in part because they mushroomed, and in part because technology like Tor became more widespread."

Those developments ushered in changes in California. As the cases exploded, White noted, the state began passing laws to better address them, outlawing **revenge porn**, **cyberbullying**, and **e-personation** (electronic impersonation). There were no comparable laws adopted on the federal level. And California created a specialized unit of prosecutors. This meant that more cases, including the individual ones, could be handled at that level. So the U.S. Attorney's Office was even more selective about the cases it pursued.

To justify expending substantial resources, White said that prosecutors consider how "egregious" the conduct was. "Of course it's all egregious," he added, "but there's degrees." One factor is often the number of victims. Another is how much impact a case will have on the community.

He cited examples of cases they took. All involved a substantial number of victims and guaranteed media attention. The most recent, he said, was Richard Bauer, a NASA contractor who pleaded guilty in 2018 to stalking, computer hacking and aggravated identity theft. He hacked into the computers of women he knew and used the information he obtained, including nude photographs, to demand more of the same by anonymously threatening to publish the images he'd stolen—or send them to the victims' families and coworkers.

Hunter Moore ran isanyoneup.com, the internet's best known "revenge porn" website. Individuals submitted nude and sexually explicit photographs of women to Moore, without their permission, and

encouraged him to post them in order to exact revenge. He pleaded guilty in 2015 to computer hacking and aggravated identity theft. And then there was "**Celebgate**," the 2014 scandal in which at least five people broke into the computers of celebrities to steal nude photographs and other private material. The best known victims were actresses Jennifer Lawrence and Mary Elizabeth Winstead, but more than 200 women were victimized.

White summed up the realities. "Defendants can be held to account, and the system certainly can work. And the tools are there," he said. "Is it going to happen for every victim in every case? No. That's unfortunately the way that law enforcement works. And that's not limited to just cyber stuff. That's all crimes." Maybe 1% of all crime that occurs actually gets investigated, he posited. Whatever that number is, he continued, a lot less than that gets prosecuted. "That's just the way it works," he said.

WHAT ARE THE OPTIONS FOR VICTIMS?

Ironically, the **National Network to End Domestic Violence** turned out to be one of the most helpful support organizations Misata has found. It's not only for victims of domestic violence. Another educational experience came from an even more surprising source. Beginning in 2011, she worked for two years as the communications director at the Tor Project.

She'd been unemployed at the time and had gone to a talk given by Andrew Lewman, the organization's executive director, to get a better handle on what Tor was all about. As she'd listened, it hit her that the technology wasn't the harasser. It only facilitated what the people who used it were doing. After his talk was over, Misata went up and asked Lewman for a job. She had a master's in marketing, and he needed someone to write an annual report.

She went from feeling victimized by Tor to defending and explaining it. This new perspective helped her gain a sense of control over the subject. It solidified her perception that the issue wasn't about technology; it was about people. And it led to her next big move: earning a Ph.D. in information security at Purdue University.

She has advice now for victims. File a report with the police. Even if you're not sure a crime has been committed. "Go file the report so you can start that documentation," Misata said. "So you can have something to hold on to." And remember, you don't know all the things the stalker has been doing, she pointed out, so you can't know whether he's been breaking the law. "Keep the evidence," she urged. "It's so important to not just close your eyes" and imagine the horror will disappear.

White concurred. "Don't stop if the first law enforcement contact doesn't understand," he added. "Go to another." Try to take control, as best you can.

For many victims, Misata emphasized, what they want is not necessarily to see the stalker go to prison. Or to successfully sue him for damages. She and White both noted that the penalties, even for some of the splashy criminal cases, are not as severe as one might imagine. A few years in prison tops. And in a civil case, even if a result looks good on paper, often the defendants never pay up.

But that's not the biggest issue. "I think for many victims," Mistata said, "they just want it to stop." Their dream is not for their day in court. Their fondest wish is for a magic button they push and he's gone. But there's no Hollywood ending, she continued. Even if they go to jail, "do you ever have that full assurance that they're going to stop?" she asked. "For many victims, we just don't."

That's not the fault of prosecutors or cops. "Honestly," she said, "the law enforcement agencies that I worked with were amazing. They were great people who cared a lot, who wanted to help, who just didn't have either the resources or the knowledge." And have undoubtedly learned a lot in the intervening years.

She faults herself for not having documented the abuse early on, when there was plenty she could have saved before he started using Tor. Like some forms of disease, catching it early can make a big difference. "If you can get some of these situations a little bit earlier, where it doesn't escalate, then maybe you have a chance to defuse it so it's not so impactful. I lost so much evidence," she said. "I know that my story would have been very, very different if I had more evidence to show."

And now, after all that she's been through, does she finally feel that it's over? "Sometimes I have to remind myself that I have 10-plus years under my belt," Misata said. "I have a Ph.D., I have a community around me. I have all these resources. But in the pit of my stomach, the fear is still there."

Resources:

CA Resources for Victims of Cyber Exploitation

The National Network to End Domestic Violence

The FBI's Internet Crime Complaint Center (IC3)

National Cyber Security Alliance

What to Do If You're a Target of Online Harassment

INTERVIEWS

AN INTERVIEW WITH SANJAY JEYAKUMAR, CTO, ABNORMAL SECURITY

PREVENTING BUSINESS EMAIL COMPROMISE WITH INTEGRATED CLOUD EMAIL SECURITY

Every enterprise struggles today with nagging email security issues leading to loss of data, compromise of credentials, account takeovers (ATO), illegitimate wire transfers and other unwanted threats. Simple measures such as enhanced user awareness certainly help, but it is now clear that advanced technology is required to address the business email compromise (BEC) risk.

Abnormal Security is addressing this challenge. We were particularly interested to understand how the company uses behavioral profiling, known good behavior and end-user preferences to reduce this risk.

TAG Cyber: Why have business email compromise (BEC) risks not been effectively addressed in the past?

ABNORMAL: Email is the universally accepted form of communication for companies. Employees use it to complete daily operations, provide internal communication and do business with thousands of vendors. Unfortunately, it was never designed to be a secure medium. As a result, cybercriminals can take advantage, often with few repercussions.

The arrival of BEC onto the cybercrime scene has been fairly recent, only gaining popularity in the last five years or so. At its core, business email compromise uses social engineering to complete the intended scheme, often to obtain money or sensitive data. Frequently bad actors will perform extensive research on their targets and obtain compelling information that makes victims believe they are having trusted conversations. Once that trust is established, victims will do what is asked—submit a wire transfer, provide login credentials, buy gift cards and worse.

BEC now accounts for more money lost than ransomware, which is a fact that I was initially very surprised to learn. The reason for the success rate is that traditional email defenses evolved from spam to credential phishing to malware, all of which rely on detection by traditional indicators of compromise. These traditional lines of defense are threat intel-based, meaning if the secure email gateway (SEG) sees an attack once, it can stop the attack a million times over. Unfortunately, this is not the case for BEC attacks, which have no payload—no malicious links or attachments. Instead, they are entirely text-based, requiring a new solution to stop them.

TAG Cyber: How does Abnormal Security address this risk?

ABNORMAL: To solve the BEC problem, my co-founder Evan Reiser and I leveraged our AdTech backgrounds from our time at TellApart, a technology startup acquired by Twitter. That was where we used machine learning for customer data and advertising. We used this experience to found Abnormal in 2018, and the platform takes a completely different approach to stopping BEC and other advanced email threats. It uses a combination of API architecture, behavioral modeling and natural language processing (NLP) to detect these never-before-seen threats. It understands the normal in order to block the malicious.

We're now taking this a step further with the introduction of our integrated cloud email security (ICES) solution. The move to cloud platforms has allowed Fortune companies to leverage native security within Microsoft 365 and Google Workspace, both of which provide sufficient protection against run-of-the-mill attacks like phishing, spam, and graymail. Abnormal complements these ecosystems to stop the targeted attacks that consistently get past them.

Unlike a SEG, which requires disabling existing native protection, Abnormal leverages these capabilities already in the Microsoft and Google platforms, and uses the API architecture to auto-train models. As a result, Abnormal receives signals unavailable to the SEG, including sign-in signals and user email folder moves. Abnormal also leverages behavioral profiling, and self-learns the company's mail environments. The platform emulates the best security analyst within each organization, learning the business norms of who talks to whom, where this communication usually comes from and what is "normal" within the environment. From this, we can determine when something appears abnormal, and then block it.

TAG Cyber: How do you establish baseline profiles for your algorithms?

ABNORMAL: We leverage the environment of our customers to learn and baseline "normal" automatically. After implementation, we build a relationship graph of everyone inside an organization to understand their roles, who they are talking to, about what topics, and even at what time of day, along with thousands of additional signals. We combine these unique signals with additional AI-driven technical capabilities, such as utilizing computer vision to assess whether an invoice is authentic and whether it matches with previous email communications.

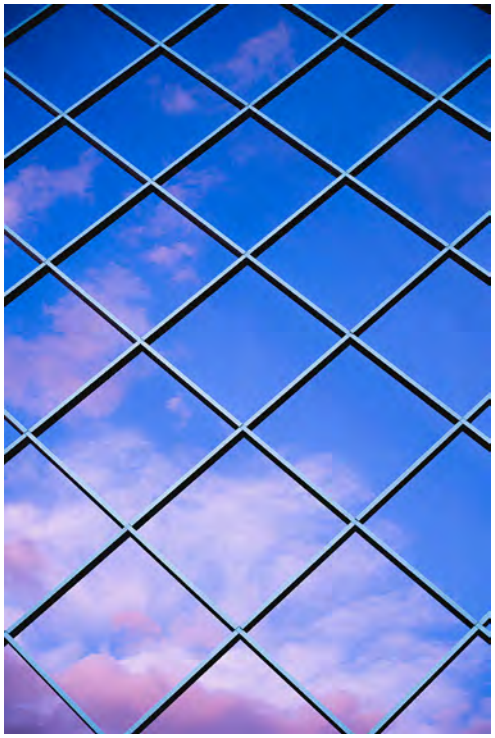
We also use natural language processing to understand how people typically communicate and to whom, recognizing that email tone may change when speaking to a manager versus a vendor versus a coworker. Ultimately, Abnormal can accurately

BEC now accounts for more money lost than ransomware, which is a fact that I was initially very surprised to learn.

determine whether incoming emails are legitimate or fraudulent. This allows our solution to understand the nuances of human behavior, identifying and blocking anything that isn't known good. In addition, Abnormal automatically provides a database of all the vendors through VendorBase, a full database of all partners across all Abnormal customers. VendorBase monitors all vendors and flags any behavioral changes. For example, Abnormal may recognize that a vendor is suddenly sending invoices from the Netherlands when all previous communication has been from the United States. VendorBase will indicate that the vendor may be compromised, and then Abnormal can block those illegitimate invoices across all customers who interact with that vendor.

TAG Cyber: Tell us more about how user preferences work and how this enhances your solution's approach?

ABNORMAL: In addition to the behavioral profiling approach, Abnormal's core differentiation is our extensive integration to the native platform through the API architecture. As opposed to a SEG, which is a hop in the mail flow and thus lacks access to information once an email passes into the platform, Abnormal has access to native experiences within Microsoft or Google. For example, let's take the problem of graymail, also known as bulk or marketing email. The SEG approach would be to block it and send an email digest to the end user, with details about what was blocked. In contrast, Abnormal provides a native solution by maintaining a promotions folder within the end user mailbox.



In the legacy SEG world, the end user would have to click through the email digest and restore messages. With Abnormal, we deeply understand user behavior and harness that to train the ML models. No matter how each individual user likes to organize their mailbox, Abnormal understands that behavior and reacts accordingly, so they never have to worry about an email digest again. Our customer CISOs love this feature, as they do not have to train their employees how to use the security product.

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

ABNORMAL: The cyber threat landscape is rapidly changing due to the move to the cloud. Infrastructure that the CISO used to protect behind a firewall, using on-prem software, is now available to anyone, from anywhere, over various devices like desktops, tablets and smartphones. This means that business email compromise and related attacks will only become more prevalent, particularly because they've been so successful.

INTERVIEW WITH ROB GURZEEV, CEO, CYCOGNITO

ADDRESSING ATTACK SURFACE CYBER RISK

One of the most significant changes that enterprise security teams have had to deal with in recent years is the massive shift that's occurred in the external attack surface that needs to be managed and protected. Discovering, prioritizing and reducing risks associated with this growing and changing attack surface has become one of the most challenging aspects of enterprise security.

CyCognito's SaaS-based platform supports attack surface management. We wanted to better understand how the company uses automation to simulate attacks to probe, test and analyze surface elements with the goal to reduce overall cyber risk.

TAG Cyber: What exactly is an attack surface?

CYCOGNITO: The attack surface, formally speaking, is the sum total of all of the ways an organization is exposed to attackers. When most security professionals refer to their attack surface, they're speaking digitally about all of their internet-exposed assets, like servers, endpoints, applications, cloud environments and the like. These are easily found on the internet and leveraged by attackers to gain initial access into an organization. Because of this, systems that are a part of the attack surface should always be known, monitored and tested for their security.

A key point to note about the attack surface is that it is always changing. Systems come online or get decommissioned. New attack paths are created or revealed with changes to configurations or vulnerabilities in software. We've seen across our customers that the typical attack surface changes by one to three percent *every day*. What this means is that after just a few days, there has been a significant change in the attack surface and attack paths into an organization. And if you don't have a continuously updated view of it, it's possible that you're misjudging your exposure to risk.

TAG Cyber: Are your customers finding incidents originating with attack surface weaknesses?

CYCOGNITO: Absolutely. The honest truth is that there will always be weaknesses on systems connected to the internet. Software vulnerabilities. Misconfigured or missing security tools. Unmonitored systems. Unintentional code issues. Unfortunately, each of these weaknesses presents

We've seen across our customers that the typical attack surface changes by one to three percent *every day.*

a path of least resistance for an attacker to compromise a system and get into an organization.

Another challenge is that the weaknesses are not just part of the infrastructure that is owned or managed by a specific entity. There are also weaknesses within embedded systems and technologies of third parties, which are often unseen and unknown. Pair with these weaknesses the constant change in a typical attack surface that comes from the dynamic nature of today's infrastructure and it's easy to see why this is—and will continue to be—a challenge that needs continuous monitoring and active testing to address.

TAG Cyber: How does the CyCognito platform work?

CYCOGNITO: We built the CyCognito platform to intelligently automate the reconnaissance processes that attackers perform when trying to find ways to get access into an organization. By automating the process and refreshing it continuously, we give defenders the perspective they need to understand how attackers see their organizations and their weaknesses. This insight is critical when setting priorities and developing a remediation strategy and identifying what issues should be resolved first.

Our platform uses internet-wide scanning and machine learning to automatically identify, correlate and security-test the assets that belong to our customers. Once assets are inventoried and weaknesses are known, the platform intelligently prioritizes the weaknesses that present the greatest risk to the organization so that they can be patched first. This prioritization goes beyond just **CVSS score**, layering on the attractiveness of a vulnerability or weakness, determining how exploitable it is and if it's already being exploited via the CISA known-exploited vulnerabilities, assessing how easy it is to discover along with other threat intelligence data that yields Risk Intelligence. This Risk Intelligence is key to appropriately and efficiently understanding, reporting and remediating the issues that face an organization.

TAG Cyber: Tell us more about continuous attack surface visibility and how this represents such a key component of the solution?

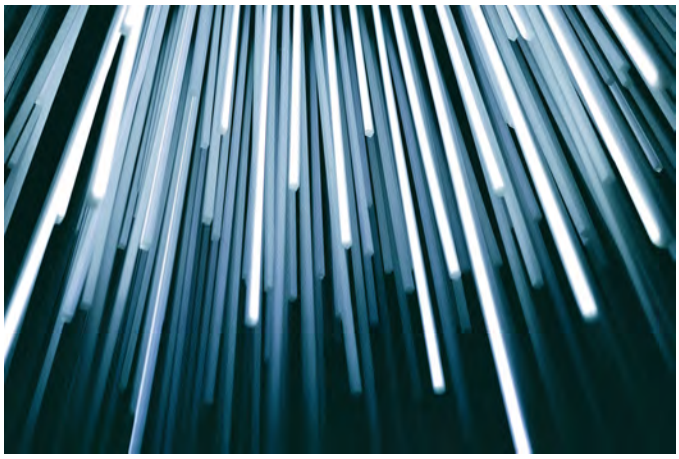
CYCOGNITO: Continuous contextualized visibility is the key to confidently understanding your risk. And visibility is far more than just discovering your attack surface and what you own. It's *visibility* into how you're affected by a particular vulnerability. It's visibility into how attackers are launching attacks in the wild. It's visibility into unknown vulnerabilities and misconfigurations that your teams aren't taking into account to accurately understand risk.

A good example of where this is absolutely critical is when a zero-day vulnerability is announced. Being able to quickly understand IF, HOW, and WHERE you are impacted is crucial to planning and executing your response. Without continuous, comprehensive visibility into everything you own, you may think that you're covered, patched and protected when that simply isn't the case. Continuous visibility also provides the ability to *validate* when issues and risks have been remediated. Timely discovery and awareness of issues is the first step to prioritize their remediation, but equally important is the last step–ensuring that you've correctly addressed the issues and that they're no longer able to be exploited.

TAG Cyber: Do you have any predictions about emerging cyberthreats to business infrastructure?

CYCOGNITO: The attack surface of modern organizations will only continue to grow. It's the nature of the digital economy that we're in. And this means that attacks on organizations will continue, too. Just as business technology has become more complex with cloud adoption, containerization, and the ability to work from anywhere, attackers will exploit these complexities at the same pace.

But I am optimistic that we can beat attackers with new, faster, more intelligent technologies that help provide greater ongoing visibility into the ways organizations are exposed. And smart context can assist security teams in prioritizing issues and resolving how to fix them in order to protect what is exposed to attackers.



AN INTERVIEW WITH ARI JACOBY, CEO, DEDUCE

REDUCING THE CYBER RISK OF ACCOUNT TAKEOVER

Account takeover (ATO) and new account creation fraud continue to provide a means for fraudsters to target websites and other online services. Accordingly, enterprise security teams require identity-based solutions that can offer sufficient insights to detect and prevent these types of attacks.

Deduce has developed an identity network with associated intelligence, insights and reporting to address the ATO risk. The company explained how it approaches this key enterprise protection challenge.

TAG Cyber: How do ATO attacks work?

DEDUCE: Account takeover attacks take place when fraudsters gain access to a victim's account and leverage that access in order to steal funds, information, rewards or perks. They can also make purchases or leverage application functionality for other forms of intended gain. It's an unfortunate condition that a plethora of static identity data has already been breached due to massive historical attacks, and this data continues to be available on the dark web.

Static identity data extends beyond credentials, often linking static credentials with digital fingerprints. These readily available attributes enable an adversary to extend techniques beyond credential validation attacks, leveraging fracture points such as account recovery processes or access to an individual's email account to successfully complete their attacks. As more complete data attributes about an individual become available and linked over time, the complexity and cost of successfully executing ATO are reduced, making this form of fraud more attractive to bad actors. Modern techniques by attackers undermine the intended goals of friction. If identity and authentication controls predominantly rely on static data to prevent ATO, an organization is at a longer-term disadvantage.

TAG Cyber: How does the Deduce solution address this ATO risk?

DEDUCE: We have created the Deduce Identity Network, a consortium of over 150,000 participating websites with the objective of sourcing the maximum amount of real-time activity data for a given user as they traverse

the internet. The intent is to rival the visibility and scale seen at internet giants, and commercialize an offering for risk teams. With over 400 million unique identity profiles that collectively generate in excess of 1.2 billion daily interactions, Deduce sees the majority of the U.S. population transact in real-time, several times a week, in four principal threat vectors: device, network, geography and activity.

Built on top of the Deduce Identity Network, we offer two solutions to combat ATO fraud. The first is Identity Insights. This consists of risk and trust signal data to empower risk teams with a DevOps-friendly approach to managing identity and authentication risk. The data includes telemetry from real-time activity information packaged into risk signals (impossible travel, device downgrade, unfamiliar device, previously unseen email, etc.); trust signals (familiar network, familiar device, familiar city, familiar activity, etc.); and scores for simple ingestion into a risk engine. This solution is intended to be used as a high fidelity approach to identifying suspicious activity while decreasing unnecessary friction. Deployed as an API, Insights are consumable in any risk engine, CIAM or application stack. Deduce is typically consumed at registration, authentication, checkout and risk moments such as change of primary contact, like email or phone.

Our greatest strength is the ability to correlate device, network and geographical information against a particular account to build predictive telemetry about the expected behavior of an individual.

The second solution to combat ATO fraud is Customer Alerts. We send an alert—typically a first-party branded email—asynchronously on behalf of the Deduce customer to their end users on suspicious logins to enable a proactive stance against ATO. Customers are prompted to confirm or deny the activity. A negative selection will cause all active sessions to be terminated and proactively enable a user to reset their credentials.

TAG Cyber: How does your team keep track of aggregate historical data to support your solution?

DEDUCE: Our system is designed to correlate event-level telemetry data, augmentative data sources and first-party feedback data to create hundreds of data features on a data-driven platform. We derive these insights by deploying code directly to user touch points across the web while aggregating information in a secure, encrypted and privacy-compliant environment.

Historical features used in our model provide predictive analytics on user behavior based on access patterns. These include devices users leverage, geographies they sign in from, networks they frequent, activity across the web and security preferences—for instance, privacy-conscious individuals typically leverage VPN. This visibility facilitates dynamic, real-time responses to human behavior while stopping fraudsters and bad actors in their tracks.

Here's an example. If a user is seen successfully authenticating at dozens of websites from a new city in the last day, it can be inferred that the user is traveling. Deduce's system references against successful ATO from its first-party Alerts and from network behavior before providing this insight to the enterprise. Or, if a given IP has been shown and confirmed by third-party sources to be a benign residential IP node, then suddenly sees a spike in high authentication failure rate paired with many new attempted usernames, it can be inferred that there is malicious activity typically indicative of a compromised node.

Deduce recognizes that risk data is continuously evolving and maintains a rich solution which provides user metadata, trust and risk signals, and scoring, providing never-seen-before data and explainability to security/fraud forensics teams. Powering a long list of use cases, Deduce's customers use this technology to solve an array of cybersecurity problems, such as verifying that the user behind the screen is really who they claim to be, optimizing user experiences by removing authentication friction or stopping fraudsters at authentication.

TAG Cyber: Tell us more about how intelligence is used to power your processing algorithms?

DEDUCE: Our greatest strength is the ability to correlate device, network and geographical information against a particular account to build predictive telemetry about the expected behavior of an individual. Using a combination of statistical, unsupervised and supervised machine learning models allows us to understand the characteristics of specific actors and imposters over hundreds of data features in the digital world.

Again, let me give you examples. Statistical data features establish baseline behaviors across the dimensions of activity, network, geography and device in the context of individual activity. This creates a basic understanding of a particular user's behavior. Unsupervised machine learning models observe user activity in real-time, continuously determining trust and risk factors to facilitate immediate cybersecurity responses to quickly evolving threats.

Supervised machine learning models augment Deduce's understanding of particular fraud profiles, blending fraud feedback data with observations across the network to surface specific threat actors. Using a fully horizontally and vertically scalable deployment model, Deduce is able to process billions of transactions daily while maintaining blazing fast response times across it's cloud infrastructure.

TAG Cyber: Do you have any predictions about emerging cyberthreats to business infrastructure?

DEDUCE: As fraudsters have become increasingly sophisticated and strategic, outdated approaches and implementations requiring months of planning and implementation no longer work. Increasingly, the most effective anti-fraud tools are those that support agile deployment in hours and can be adapted quickly to address the constantly changing threat landscape. It is imperative that we all band together to form a collective defense against online adversaries, and leverage systems designed with knowledge-share in mind to defeat attackers as they evolve.

AN INTERVIEW WITH HASEEB AWAN, CEO, EFANI

PROVIDING ULTRA-SECURE MOBILE SERVICES

Cyber criminals have been targeting telecommunications companies for many decades, and service providers have done the best they can to ensure an acceptable level of security for users. Nevertheless, some customers will require much higher levels of security for services such as mobile.

Efani is a company that has created a security-enhanced mobile service. We were interested to learn how this service can help enterprises protect their proprietary data. We were particularly eager to hear how it can help customers of cryptocurrency products, given the frequency with which they are targeted for account takeover by fraudsters.

TAG Cyber: How does Efani work?

EFANI: We've created a specialized mobile service focused on the security and privacy of our subscribers. We've set up multiple layers of security to prevent a variety of common problems. We stop unauthorized SIM swaps by requiring many more data points from a subscriber to ensure they are who they say they are. We collect the bare minimum of information from subscribers, then encrypt that data and decouple if from their phone numbers, so any attack on our servers can't leak subscriber data.

Our network can detect and block an SS7 attack or a phone connecting to an IMSI catcher (fake tower). We also block access to the location data that SS7 collects, so no one can track a subscriber's physical location. We filter out spam calls and texts, along with malware. To back it all up, we provide $5 million insurance coverage to every subscriber to cover possible financial losses if we fail to fulfill our promises.

TAG Cyber: Do you see cryptocurrency account protection as a primary use case?

EFANI: It's funny because we think there a lot of consumer "VIPs," if you will, who should use a secure mobile service for a wide array of use cases. I'm talking about attorneys, business executives, people in critical government roles, even celebrities. Anyone whose identity, data, texts and calls must remain confidential. But yes, some of our earliest subscribers are involved in cryptocurrency. I have a background in crypto, and I was a SIM swap victim myself. So when I started Efani, I told the people in my network that Efani could help keep them safe from attacks that might steal their keys, and they started signing up.

But our consumer business is also adding celebrities, doctors, lawyers, you name it, whether or not they're into crypto. They just want to avoid identity theft and account hijacking. And basic things like having spam calls and texts

I have a background in crypto, and I was a SIM swap victim myself.

blocked are really nice quality-of-life improvements. And we're just starting our B2B business, selling tens or even hundreds of lines at a time to enterprises that want to keep their intellectual property and corporate data safe.

TAG Cyber: How do you scale your service to large customer bases?

EFANI: We use the radio access networks of the big players, like AT&T and Verizon, so we don't face any scaling issues. And we don't put any software on the subscriber's phone, so we avoid that hassle. Our network core is SaaS, built in one of the big three cloud providers, so scaling up is straightforward. For us, the key to scale will be continuing to hire great people and training them to provide fast, personalized, white-glove service that includes shipping SIM cards to new subs, and making sure scammers are never able to port out one of our subs.

TAG Cyber: How would a user provision Efani? Do you mail a SIM card?

EFANI: Right. They call our toll-free number or fill out our web form to get the process started. We verify them, then ship them a new SIM card. They pop that in their phone and they're on the Efani network. We can even provide a new phone to the subscriber with the SIM already installed, if they like. We really want this to be not just a secure service, but a high-end, "VIP" service as well. That's why we take all the hassle out of setting things up.

TAG Cyber: Do you have any predictions about emerging cyberthreats to business infrastructure?

EFANI: Now that "business infrastructure" largely means mobile devices (often employee-owned) connecting to SaaS solutions (or company-owned software in the cloud), businesses have to validate the data security practices of their providers. They want to see SOC 2 attestations of their SaaS and cloud providers, for example. And they want to install MDM apps on employee smartphones. That's what "cybersecurity" means today—and going forward.

Cellular networks are now a big, de facto, part of every company's infrastructure. But companies don't have control over how the big mobile carriers validate a SIM swap request, and they have no say in what data the carriers collect and store, nor how they secure that data. We see that as a big weak link, and it's a problem that we're trying to solve.

In addition, now that 5G is rolling out widely, we think it may replace Wi-Fi in some business environments. And if it does, we think **femtocells**, deployed inside businesses, will get more attention than they have in the past. For that to happen, companies will want to be assured that the cellular connection is secure, and that it can block out unwanted content.

AN INTERVIEW WITH JONATHAN NGUYEN-DUY, VP, FIELD CISO STRATEGIC SERVICES, FORTINET

A COMPREHENSIVE SECURITY FABRIC FOR ENTERPRISE

The cybersecurity industry includes some iconic firms—ones that have supported customers for many years and have managed to build a portfolio of offerings that successfully match up with the evolving cyberthreat experienced across a wide range of sectors. One of the most prominent such iconic firms is Fortinet.

We have long understood that companies like Fortinet have deep insight into the community, and provide excellent analysis of the right priorities for cyber defenders. As always, we were eager to learn more about Fortinet's ongoing initiatives.

TAG Cyber: Let's start with network firewalls. What are some of the latest advances in this important area?

FORTINET: When we started 20 years ago, we were already offering the second generation of firewall technology. That was about application content security. We're now entering the third generation, which includes network, cloud, endpoint, IoT and application security components. This convergence of networking and security, what Fortinet calls Security Driven Networking, sees the integration of SD-WAN and the NGFW security stack. Indeed, Fortinet is the only vendor offering a Secure SD-WAN solution with advanced routing functions, next-generation firewall (NGFW) and zero trust network access (ZTNA) proxy on a single appliance or a single virtual machine (VM) to deliver secure networking capability. The Fortinet solution can be deployed in a virtual or physical format, on-premise or as a VM in the cloud.

In the last 20 years, we've moved from point defense products to more integrated platforms and fabrics. The Fortinet FortiGate NGFW has developed from an edge point defense product to the center of the Fortinet Security Fabric—a broad, integrated and automated security platform that converges networking and security across LAN, WAN, data center and cloud network edges. With Secure SD-WAN and a full suite of security capabilities, this platform enables consistent performance and security for today's work-from-anywhere strategies, branch office transformations and highly distributed networks. This is the type of integrated platform that will be needed to facilitate adoption of SD-WAN, Zero Trust Network Access and Secure Access Service Edge solutions.

Organizations often end up with a heterogeneous set of technologies in use, with disparate cloud security controls in various cloud environments.

TAG Cyber: What is the role of continuous cybersecurity? Do you see this as a major aspect of Fortinet products?

FORTINET: From a cybersecurity perspective, the network perimeter is now harder to define. Because network edges are everywhere, many organizations have had to deploy an array of point security solutions. Unfortunately, this approach does little to meaningfully integrate and automate systems. The resulting vendor sprawl has now grown too difficult and too expensive for many enterprises to manage. It's common for organizations to "bolt on" disparate security tools to protect a function or one segment of the network in isolation. However, this practice makes maintaining organization-wide visibility and consistent policy enforcement, the basis of continuous cybersecurity, next to impossible.

Many enterprises are moving from multivendor solutions to a single security platform that provides foundational security services and centralized policy management and orchestration, such as the Fortinet Security Fabric. This platform spans the extended digital attack surface and cycle, enabling self-healing security and networking to protect devices, data and applications. The broad, integrated and automated Fortinet Security Fabric offers a number of key benefits.

It allows companies to protect any edge and any app at scale with advanced threat protection. It provides convergence of network and security, secure sockets layer (SSL) decryption, and network automation. It offers complete and simplified access layer security via direct and integrated control, configuration, and management, which extends next-generation firewall (NGFW) to the local-area network (LAN) edge.

It also affords secure, business outcome-driven wide-area networking (WAN) through deduced cost and complexity, with better application performance and integrated security. And businesses can control every device on every network with simplified network deployment, automatically discover devices, and apply policy at scale.

TAG Cyber: Tell us about the evolution of cyber intelligence. Fortinet has been such a leader in this area. We'd love to understand how you view this task.

FORTINET: As attack sequences get more complex and innovative, and organizations struggle to deliver the expected secure, consistent high-performing user-to-application connections, it's clear that traditional non-integrated, piecemeal approaches to security operations are no longer viable. Real security requires threat intelligence that can be applied automatically at speed and scale, as well as services to suit specific requirements.

FortiGuard Labs is the threat intelligence platform and research organization at Fortinet. It comprises experienced threat hunters, researchers, analysts, engineers and data scientists. Its mission is to provide customers with the industry's best threat intelligence platform to protect them from malicious cyberattacks. FortiGuard Labs' threat research can be customized per customers' requirements to keep them informed of the latest threats, campaigns, actors, and trends so they can take proactive measures to better secure their environments.

TAG Cyber: What are your views on cloud and SaaS-based security? Is this an important part of your future strategy?

FORTINET: As the use of business-critical, cloud-based applications continues to increase, with a distributed infrastructure of remote and branch offices and an expanding workforce that requires work-from-anywhere capabilities, organizations need to adapt. Securing consistent performance for digital transformation is a very important part of our strategy. Today's highly distributed computing environment, characterized by hybrid environments and workspaces, means that organizations are increasingly reliant on secure cloud solutions and infrastructures. Yet, organizations often end up with a heterogeneous set of technologies in use, with disparate cloud security controls in various cloud environments.

Fortinet Adaptive Cloud Security Solutions provide the necessary visibility and control across cloud cybersecurity infrastructures, enabling secure applications and connectivity from data center to cloud. Organizations are seeking solutions that converge networking and security, and that are integrated with a cybersecurity mesh platform, to provide them with superior quality of experience at scale, operational efficiencies and secure dedicated internet access. Fortinet's Secure SD-WAN is the only solution that integrates SD-WAN, next-generation firewall (NGFW), advanced routing, and ZTNA access proxy functions that are essential platform elements for consistent cloud and SaaS performance—and ultimately better business outcomes and user experiences.

AN INTERVIEW WITH JONATHAN GOHSTAND, DIRECTOR OF SECURITY PRODUCT MARKETING, HP INC.

ENHANCING ENDPOINTS WITH BUILT-IN SECURITY

Given the heightened importance of endpoint security in enterprise, it should come as no surprise that modern cyber defenders have finally begun to recognize the importance of protecting devices from the ground up. This involves creating so-called trusted computing bases at the core of a computing device (such as a laptop or PC) that derives cyber protection directly from the hardware.

HP is integrating enhanced security controls directly into its products. For enterprise security teams, this implies that cyber risks associated with PCs, printers and other HP peripherals will be greatly reduced. Welcome news in an era where cyberthreats directly target endpoints for campaigns such as ransomware.

TAG Cyber: How does HP build security into its products and services?

HP: In a nutshell: Bottom up; full-stack. Because HP is a hardware vendor, we're in a unique position to embed secure principles at all levels of the technology stack for PCs and printers. We start from the bottom with the motherboard hardware, and build secure layers one by one to create a trusted execution environment for applications and data.

TAG Cyber: What are the roles of hardware and firmware in the protection of HP endpoints?

HP: The overarching role is that of platform assurance. Each layer in the stack can trust that the layers below it are free from corruption. Just as you can't build a skyscraper on a weak foundation, you can't build a trusted computer environment on a platform that may be compromised. As a more tactical example, the dedicated security hardware on our business PCs includes secure storage that is used to store secrets required by upper layers and to complete trusted firmware images. And that secure storage can't be accessed from software running on the CPU.

TAG Cyber: Do most companies understand the importance of a trusted base in establishing world-class endpoint security?

HP: It varies. Those organizations that are particularly concerned about supply-chain assurance, such as government agencies and cloud providers, have understood this for some time, which is why NIST has produced guidance documents on the topic. Others frankly consider

Because HP is a hardware vendor, we're in a unique position to embed secure principles at all levels of the technology stack for PCs and printers.

it a lower priority. They do understand that if a particular application or data store is in-scope for a control, then in theory all the layers that support it are also in-scope. But they have limited capacity for projects and ongoing operations, or may not feel they have the necessary supply- chain control. Recent attacks are starting to change the paradigm, but vendors must also strive to make trusted platform acquisition and operations as easy as possible. This is currently a focus area for us.

TAG Cyber: How might a team use enhanced endpoint security to address issues such as ransomware?

HP: Ransomware is a conceptually simple attack that takes advantage of the fact that PC applications typically have unfettered access to local files and the network. HP's approach is to isolate tasks that are likely to harbor such malware, like untrusted websites or email attachments, so that they can't encrypt local files or move laterally in the network. We believe this is a superior approach because it dispenses with the need to reliably detect the presence of the malware, and doesn't degrade user productivity. It's classic zero trust: Don't trust it; let it execute; contain its behavior.

TAG Cyber: Do you have any predictions about emerging cyberthreats to business infrastructure?

HP: Making predictions these days is clearly fraught with disappointment, but a few things are safe bets. First, threat actors continue to be successful with social engineering attacks that trick users into doing things that help them. From their perspective, "If it ain't broke, don't fix it." Second, the shift to hybrid work will continue to create problems for organizational security. The volume of unmanaged and unsecure devices has created a wider attack surface. Since the home (or local café) is less secure than the typical enterprise, this is an obvious attack vendor. Lastly, supply-chain risk exploded onto everyone's radar with the SolarWinds incident. And the recent Log4j vulnerability is more of the same. So we expect that organizations will reevaluate their risk-based controls in this area and take them more seriously.

AN INTERVIEW WITH JAMES HADLEY, CEO, IMMERSIVE LABS

OPTIMIZING CYBER RESILIENCE ACROSS THE ENTERPRISE

Establishment of cyber resilience within an organization is gradually rising as one of the more important priorities for senior management. In the past, this goal existed primarily within the enterprise security team. But more recently, it has emerged as a holistic concern starting at the board room. This has greatly expanded the urgency to build such a capability.

We wanted to know how Immersive Labs is working with enterprise customers to help them improve their ability to increase, measure and demonstrate their full capabilities in cybersecurity—especially in dealing with actual business compromise scenarios.

TAG Cyber: What specifically is cyber resilience?

IMMERSIVE: Cyber resilience is about being able to continuously deliver business outcomes in the face of an ever-changing risk. Prevention, response and remediation in the face of adverse cyber conditions are vital—for both technical and nontechnical teams. It's about keeping your organization moving forward despite adversaries desperately trying to hold it back. There's a perception that cyber resilience is solely the responsibility of the geeks in the basement—the security teams. It's not. I'd even say that this perception is putting organizations at risk, because it's leaving them woefully under-prepared when the worst happens.

Cyber resilience lies in the hands of every business function, from the executives who must make rapid, confident decisions when facing a cyberattack; to the legal, comms and customer teams that must be able to effectively communicate the issue; to developers who must write secure code. Everyone has a part to play.

TAG Cyber: Is training sufficient to build resilience?

IMMERSIVE: Alone? No, it's not. Building the technical knowledge of your people is just one aspect of a continuous cycle of cyber workforce optimization. Sure, that cycle starts with training, but it must be complemented with continuous measurement to help your people keep pace with the ever-changing threat landscape. Organizations need data to see how their people's knowledge, skills and judgment impact their overall cyber resilience.

Our platform continuously tests, measures and improves human cyber capabilities.

Human capability is notoriously difficult to measure, which is why organizations fall back on certificates and qualifications to assess their employees' capability. But these assessments date almost as soon as they're awarded, and shed little light on what really matters: your cyber resilience. The net result is that your people—and their vast unmet potential as defensive assets—take second place to technological countermeasures. To be truly cyber resilient, your organization needs to be able to measure human cyber capabilities, see where their strengths and weaknesses lie, and inject targeted simulations and exercises to optimize their knowledge, skills and judgment.

TAG Cyber: How does your solution work?

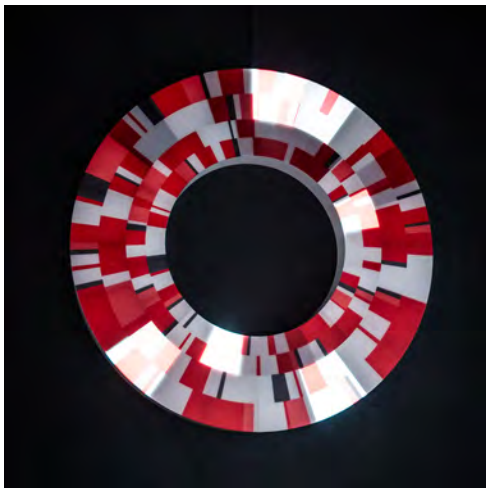
IMMERSIVE: Our platform continuously tests, measures and improves human cyber capabilities to achieve cyber workforce optimization. This allows organizations to demonstrate true confidence in their cyber resilience by simulating real-world cyber issues relevant to individual business functions in a single platform.

Powered by these data-driven insights, we enable an agile cycle to develop the capabilities of individuals and teams, all from within a single enterprise platform. This cycle has three parts. The first exercises current knowledge, skills and judgment through realistic, role-specific, cyber simulations across the entire workforce, with minimum impact on resources. The second evidences human capability by mapping data and insights to accepted risk frameworks for a real-time picture of cyber resilience and risks. This can then be benchmarked to peers. The third part equips your people with new cyber knowledge, skills and judgment to plug any identified gaps using scalable content experiences tailored to each individual, based on the person's role and business risk.

TAG Cyber: Tell us more about how you engage specifically with customers.

IMMERSIVE: Historically, customers came to us looking for online training labs. However, a number of critical developments and innovations now allows us to bring far wider-reaching benefits. The first was the realization that cybersecurity is no longer the responsibility of the geeks in the basement. The risk and impact of a cyberattack now permeate every business function, so the whole workforce must be prepared to tackle one when it comes their way. We are always expanding our suite of content to help develop role-relevant knowledge, skills and judgment across entire workforces, with offerings such as our Cyber Crisis Simulator, Application Security modules, Offensive and Defensive labs, and more.

Next was a significant investment in our data analysis capability. By building the world's first data engine for analyzing human



capabilities, we have allowed our customers to use cyber knowledge, skills and judgment in a far more strategic way. By allowing customers to measure and map human capabilities to emerging risk, organizations can keep pace and report on this at a business level. This effectively allows them to take human cyber capabilities on a more relevant maturity journey—one that is continually updated in a never-ending cycle of cyber workforce optimization. This is how we engage with our customers now, and it's the reason we work with some of the largest institutions in the world.

TAG Cyber: Do you have any predictions about emerging cyberthreats to business infrastructure?

IMMERSIVE: I expect to see more vulnerabilities emerge in obscure but widespread software that is deeply embedded into organizations' environments. Unfortunately, companies have been using open source libraries for years without effective dependency management processes in place, and the resulting vulnerabilities can be massively widespread, incredibly hard to find and often trivial to exploit.

Moving away from the technical side, I expect to see a greater onus on executive teams and board members in responding to cyber crises. As I've mentioned, cyber resilience is no longer just in the hands of technical teams. Cyber incidents and crises now impact every business function, which ultimately must become more accountable for mitigation. I hope that as we progress through 2022, we'll see a mindset shift, and people will start to think of gaps in human capability as comparable to threats and vulnerabilities in technology.

AN INTERVIEW WITH CRYSTAL MICELI,
VP, SOLUTIONS MARKETING, IVANTI

DRIVING ZERO TRUST SECURITY IN THE EVERYWHERE WORKPLACE

The path to the Everywhere Workplace was certainly well underway long before the Covid-19 pandemic emerged. Nevertheless, in the years since 2019, the enterprise has shifted to a more virtual and distributed model. This has introduced the need for more flexible approaches to enterprise and IT service management—not to mention the cybersecurity controls that come with such support.

Ivanti knows a lot about these shifts in enterprise service management, and how cybersecurity integrates into the responsibility. The company has been active in obtaining new security capabilities in recent years, so Ivanti's insights in this area are particularly valuable.

TAG Cyber: What are some of the key challenges in modern enterprise service management?

IVANTI: We see a few big shifts that create challenges different than what we've seen in the past. The biggest changes in enterprise service management today stem in no small part from the pivotal forces the pandemic placed on IT. With large numbers of employees working remotely or in hybrid fashion, IT and other functional organizations like HR and Facilities have all been forced to quickly learn how to service employees in non-traditional ways. These prioritize consistency and contextualization, so that the employee experience is not degraded and may even be optimized. At the same time, the proliferation of devices outside of the corporate walls have made it critical that IT prioritize the security of all endpoints and networks. And they must do this in a way that doesn't create unnecessary roadblocks for remote employees.

Because of the increased load on IT, another challenge we're seeing is the need to find the right balance with automation and human interaction, as IT continues to shift left. The more organizations are able to proactively resolve incidents before an employee even notices they have a problem, the lower the burden on the IT staff and the better the experience for the employee. While this sounds like a panacea, the organization and its processes and workflows need to mature to realize the true benefits of automation.

Along with the shift left, another fundamental movement we've seen in service management—and this began long before the pandemic—is the

Better synchronization of security and service teams and processes is imperative to proactively secure organizations from the next cyberattack.

move from project to product orientation, and the rise of DevOps as an integral part of service management. Integration with the DevOps toolchain and support for more agile workflows have become a priority for many organizations. However, we've also seen a greater need to address security as part and parcel, and we think the real challenge is integrating *DevSecOps* with service management workflows.

TAG Cyber: What is the role of cybersecurity in IT service management for enterprise?

IVANTI: In today's world, cybersecurity is everyone's job. With the rapid acceleration of security threats, we can't afford to think of security and ITSM as separate organizational functions. Better synchronization of security and service teams and processes is imperative to proactively secure organizations from the next cyberattack. This starts with knowing about all assets in the environment, whether they are corporate-owned or personal devices. Ensuring each and every one is accounted for, patched and secure is the domain of both IT service management and security teams.

TAG Cyber: Tell us about the new Ivanti security portfolio. It is quite impressive.

IVANTI: With Ivanti Neurons, IT can query edge devices with sensor-based architecture and natural language, get intelligence across the enterprise in seconds, and then take the right action at the right time to effectively defend against cyberthreats like ransomware attacks. By automating repetitive data-intensive tasks, Ivanti Neurons allows IT departments to reduce complexity, anticipate security threats, reduce unplanned outages and resolve endpoint issues before users report them. This improves the cost, speed and accuracy of the services IT delivers, and allows IT to focus on the most critical and complicated tasks at hand.

Ivanti is laser-focused on its mission to secure the Everywhere Workplace. As part of the company's commitment to further protecting customers and mitigating threats as quickly as possible amid the uptick in sophisticated cyberattacks, Ivanti recently acquired RiskSense. This pioneer in risk-based vulnerability management and prioritization helps us drive the next evolution of patch management. The combination enables organizations to shrink their attack surfaces. They can also prioritize vulnerabilities to remediate and reduce their exposure to cyberthreats and ransomware attacks by taking a proactive, risk-based approach to patch management.

TAG Cyber: Tell us more about how the full suite of Ivanti solutions are deployed across the typical enterprise.

IVANTI: The enterprise is now everywhere—with data residing everywhere, work happening everywhere and communication taking place everywhere. The Ivanti Neurons platform enables companies to autonomously discover, manage, secure and service all endpoints and IT assets in the new Everywhere Workplace. Customers can collaborate and innovate more freely, while reducing the risk of data breaches. Ivanti Neurons addresses the rapid growth and complexity of devices and data, as well as the increasing number of cyberthreats and the shift to a hybrid workforce. It's the only solution on the market that combines unified endpoint management (UEM), enterprise service management (ESM) and security. It automates IT services and offerings to streamline business tasks, while simplifying the way organizations manage, configure and secure their device endpoints with a single user interface.

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

IVANTI: In 2022, we can expect to see more sophisticated phishing scams. For example, we may see threat actors targeting marketing firms and tools used by email marketers to achieve maximum impact. Since marketing emails come from trusted domains, end users are likely to trust them and click on links, increasing the success rate of attacks. Ransomware is a universal problem that is not going away. Following the rapid shift to remote work, remote access services became easy and primary targets, with phishing often used as the attack vector. Ransomware has continued to evolve, with attackers increasingly leveraging known vulnerabilities that have remote code execution and privilege escalation capabilities. In 2022, we can expect ransomware attackers to continue to mature their tactics, expand their attack arsenals, and target unpatched vulnerabilities across enterprise attack surfaces.

AN INTERVIEW WITH ELIAS MANOUSOS, CEO, RISKIQ

PROVIDING SECURITY INTELLIGENCE TO REDUCE DIGITAL RISK

Digital risks have changed considerably in the past few years—mostly in the direction of becoming more intense. Organizations undergoing digital transformations during the advent of Covid-19 have confronted a vastly increased attack surface with more impactful attacks targeting ubiquitous technology.

RiskIQ, now part of Microsoft, is helping enterprise teams handle digital risk management. We were keen to understand the evolution of this important control, and learn how the company's solution will integrate into the Microsoft portfolio.

TAG Cyber: How are digital risks managed today?

RISKIQ: Risk is relative to the business, so it varies. Usually it depends on the size and maturity of the company and can range from manual processes to automation via software. Most organizations understand employee machines and their core product infrastructure. However, they often miss anything outside of that process, and decentralization from Covid has only made this worse. Regardless of the size and maturity level, any organization can benefit from having a complete understanding of the composition of its attack surface.

TAG Cyber: How does the RiskIQ platform work?

RISKIQ: Our global collection technology continuously extracts, analyzes and assembles internet data to define the internet's identity and composition. Our systems fingerprint each component, connection, service, IP-connected device and other infrastructure to show customers how they—and attackers targeting them—fit within it. This Internet Intelligence Graph helps customers discover and assess the security of their entire enterprise attack surface—in the Microsoft cloud, AWS, other clouds, on-premises and from their digital supply chain. With over a decade of scanning and analyzing the internet, RiskIQ can help enterprises identify global threats and better understand vulnerable internet-facing assets.

RiskIQ's global threat intelligence is collected from across the internet and crowd-sourced through our PassiveTotal community of more than 100,000 security researchers. This data is then analyzed using machine learning. With this next-gen intelligence, customers gain context

into the source of attacks, tools and systems and indicators of compromise to detect and neutralize attacks quickly.

TAG Cyber: Do security teams have the primary responsibility for handling digital risk, or is this a more general concern across the typical enterprise?

RISKIQ: As organizations pursue their digital transformation and embrace the concept of zero trust, their applications, infrastructure and even IoT applications are increasingly running across multiple clouds and hybrid cloud environments. In many cases, managing risk across this attack surface lives in different siloes with different teams across the organization. This segmentation severely hinders cohesive and effective response to risk. The combination of RiskIQ's attack surface management and threat intelligence empowers security teams to assemble, graph and identify connections between their digital attack surface and attacker infrastructure and activities to help provide increased protection and a faster, concerted response.

TAG Cyber: Tell us more about the plan to integrate RiskIQ into the Microsoft portfolio.

RISKIQ: Microsoft **acquired RiskIQ** to help customers build a more comprehensive view of the extended enterprise attack surface. Our combined capabilities will enable best-in-class protection, investigations and response against today's threats. The combination of RiskIQ's attack surface management and threat intelligence empowers security teams to assemble, graph and identify connections between their digital attack surface and attacker infrastructure and activities. The result is that it helps provide customers with increased protection and faster response. As part of Microsoft, RiskIQ can create a safer internet by bringing an outside-in intelligence perspective, enabling every Microsoft solution to be adversary-aware.

RiskIQ's global threat intelligence is collected from across the internet and crowd-sourced through our PassiveTotal community of more than 100,000 security researchers.

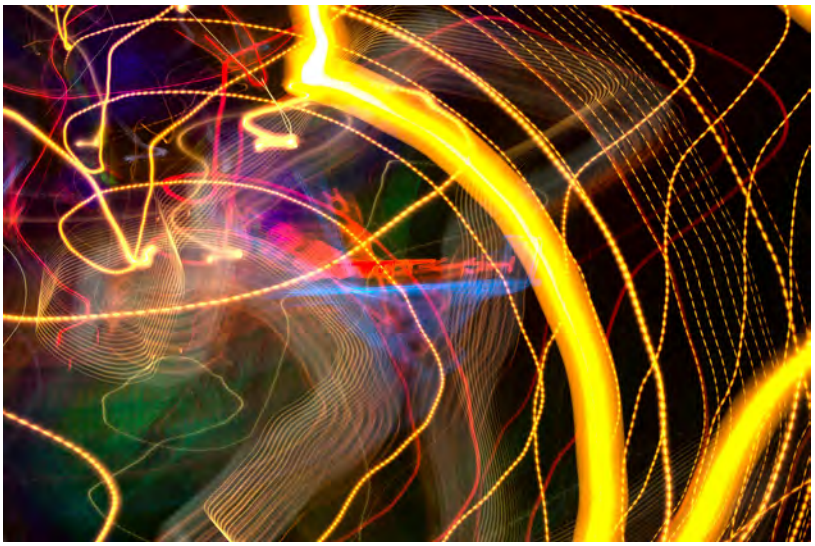
As Gartner has said, RiskIQ can enhance the impact of Microsoft's security solutions: "[With RiskIQ], Microsoft has the opportunity to give clients an outside-in view and continuous asset inventory … [along with] improving Secure Score by quantifying risk from both internal and external dimensions, then connect to controls and defense with Sentinel, ASC, and Defender."

TAG Cyber: Do you have any predictions about emerging cyberthreats to business infrastructure?

RISKIQ: As we've seen over the past several years, the global attack surface is so intertwined and interdependent that threats and vulnerabilities can affect all of us simultaneously. The latest example is the Log4J security flaw. As a result of this new reality in cybersecurity, we will see organizations pursue zero trust more aggressively than ever. However, proper zero trust

can't be achieved unless your organization has a complete view of its extended enterprise attack surface, with an in-depth understanding of what it owns and the software running at every level of the technology stack.

Microsoft has long delivered end-to-end cloud-native security in multicloud and hybrid cloud environments. With its leadership and innovation in this area, it was clear that RiskIQ's capabilities could help the parent company continue to provide leading solutions amid a dramatically changing threat landscape. Attacks like Log4j are bound to continue into 2022, and you will see other large security companies follow suit and acquire startups that enable a global view of the extended enterprise attack surface.



AN INTERVIEW WITH DR. BEHZAD NADJI, VP, CORE TECHNOLOGIES, SERTAINTY

ADVANCED DATA PRIVACY FOR THE ENTERPRISE

Enterprise teams continue to struggle to avoid data breaches and privacy violations, so the goal to find creative solutions remains a high priority. Existing solutions such as perimeters, conventional encryption and data leakage tools certainly help, but new approaches are necessary.

Sertainty is using a technique known as self-protecting data to avoid breaches. We were interested to learn how this solution differs from other security measures, and how it can be effectively deployed into the typical environment.

TAG Cyber: How does self-protecting data work?

SERTAINTY: This question comes up often. Most of the data protection schemes talk about protecting the environment in which the data resides, using policies and procedures, physical barriers to the data, firewalls, networks, VPN, computer access, identity access management or management apps. These are all there to protect access to the data. When it comes to data itself, however, we usually think of it as a passive and inert collection of bytes. We don't think of it as having the capability of defending itself.

But that was before the concept of self-protecting data. We now have technologies that provide the data with all that it needs to defend itself. So functions like access controls, risk mitigations and defensive mechanisms are actually embedded within the data itself. Sertainty Unbreakable Exchange Protocol files are heavily encrypted and policy-protected and are inaccessible to any form of intrusion. Even when the data is taken out of the environment that is protecting it, it can still protect itself. In other words, if somebody puts the data on a memory stick and takes it out of the company, or that data is emailed outside of the enterprise, it can protect itself and will not allow access to its contents because the technology that Sertainty embeds inside the data is carried along with it and protects it like a nutshell.

TAG Cyber: How does the Sertainty solution integrate with existing protection tools and infrastructure?

SERTAINTY: Secure Unbreakable Exchange Protocol (UXP) will work alongside all infrastructure, application, network and access

We have the technology that allows you to insert, within the data itself, all that it needs to defend itself and track usage.

management policies that may be in place. It works with existing security infrastructures, but it does not rely on them to be safe all the time. A UXP file protects itself even if all other infrastructure security measures are breached.

Sertainty products can be used to enhance the data security of existing applications or to create new secure applications. Currently, there are three ways to include this protection. Sertainty libraries can be linked to the application directly and be used through their APIs as if they were part of the original application. Sertainty functionality can be accessed through web services calls. The web server providing the Sertainty web services can co-reside with the app on the same machine or can be external. Or the web services can reside in a Docker container and be "dropped in" within any environment supporting Dockers and be used immediately without the need for major installation and deployment.

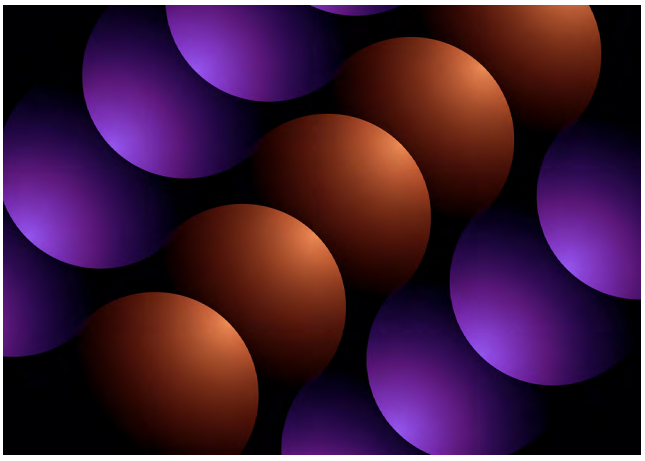
TAG Cyber: Many teams have tried to develop digital rights management (DRM) in the past with varying success. How is the Sertainty approach different?

SERTAINTY: There are different implementations of DRM. It is used to protect digital assets, mostly in the entertainment industry, games, audio, video and movies. DRM is not designed to be a zero trust solution or to be completely hack-proof. There are free software packages that are available on the internet that can break most DRM protection systems. There are even websites that rank and order DRM breaking software, and there are user groups dedicated to breaking this protection, sometimes even before the products come out in the market.

DRM and UXP have different business models. The industries that use DRM do not rely on their scheme to be hack-proof. They rely on DRM to protect their asset against customers who may want to casually copy an audio or video file and share it with their friends but don't have the expertise to break the DRM. At Sertainty, we do not have the luxury of tolerating breaches. We have to be 100 percent secure. Our existing and potential customers are major banks and financial institutions protecting critical financial data, governments protecting national security information, health care systems protecting confidential patient data and enterprises protecting their Intellectual property and designs. Even a single data breach in such cases can be catastrophic. We have to have zero tolerance for data breaches. And UXP is designed for that. In addition, UXP technology allows one to define policies to exert controls and trigger mitigating actions. We have the technology that allows you to insert, within the data itself, all that it needs to defend itself and track usage. DRMs are generally not designed to have that scope.

TAG Cyber: Tell us more about how policies are established for accessing data in your approach.

SERTAINTY: In addition to requiring user authentication for accessing the data, you can incorporate policies within the data that further limit access. Then, even if you have an authorized user who's trying to violate those policies to get out the information, that user may not be able to access the data. These policies fall into different categories. Some are based on time and calendar, and they say you can only access this data within the next 10 days, or on weekdays, or during business hours. You can also have policies that are environmentally based. These may say that the data can only be accessed within a 25-mile radius of New York City. We can define a secure perimeter for the data access, or tie it to a network, or tie it to a specific system and say the data can only be opened on this very system. The violation of any of these policies can trigger mitigating actions. Denial of access could be one. Or you can provide some sort of a false reality within the data itself—like a honeypot—so that if the policies are violated, we can correlate quietly and hand over false data. You can also have the data self-destruct. And while this is happening, you have audit and access logs as well as events that are generated that can call home and tell your central security operation center what's happening.



AN INTERVIEW WITH BRIAN VECCI,
FIELD CTO, VARONIS

SUPPORTING A DATA-FIRST SECURITY APPROACH FOR ENTERPRISE

Data security has become a significantly greater challenge as organizations have expanded their operations beyond traditional perimeters to public cloud services. The urgency to understand where sensitive data resides, who can access it and how it is being used is more important than ever, with increasing cybercrime and stricter privacy regulations.

Data security company Varonis shared insights into how it's developing all-in-one data security solutions for enterprise. We were especially keen to learn how Varonis reduces data exposure, detects unusual behavior and supports compliance.

TAG Cyber: How have data security requirements evolved in recent years?

VARONIS: With the Covid-19 pandemic, we saw the digital transformation accelerate rapidly. Collaboration tools like Microsoft 365 and SaaS apps like Box and Google Drive saw massive adoption because business needed people to be able to access data from anywhere and easily share and collaborate. This shift brought a whole new level of data security challenges, since there are now so many more places data lives and so many more users and devices creating, accessing and sharing it. Cybercrime is more prevalent and profitable than ever, and privacy regulations continue to have sharp teeth. Everyone can agree data security is important, but the reality is that it's incredibly complex.

TAG Cyber: What is the impact of privacy regulations and requirements on data security?

VARONIS: Privacy regulations like GDPR and CCPA require data protection to be built into the design of the processes and technology where personal information is collected and used. That means that you have to know where your regulated data is, watch how it's used and limit who can access it. We find that an average employee has access to millions of files, most of which have nothing to do with his or her job. That's far from privacy by design! Privacy regulations are stern disciplinarians, and companies big and small are paying massive fines when they get caught with all this data exposed.

TAG Cyber: How does the Varonis platform work?

VARONIS: We protect data from overexposure and cyberthreats. We automatically find and classify

Organizations that don't secure and monitor their data will continue to be case studies in cybercrime.

sensitive and regulated data, map exactly who can access that data and how, and monitor data usage and other relevant behavior so that organizations automatically know what normal looks like and get alerts on abnormal or suspicious behavior. Varonis automatically reduces access and safely implements stricter controls. This means we can proactively reduce risk and prevent cyberattacks.

TAG Cyber: Tell us more about how an enterprise would deploy and use your solution across its network.

VARONIS: We offer a free data risk assessment to any company that's interested in seeing what its risk profile looks like. We'll scan the environment, monitor activity and point out where data is exposed and how it's being used. We'll do all the heavy lifting of installing the software and delivering a true-to-life report on where sensitive data exists in the environment, where it's exposed, how's it's being used and whether there's suspicious activity. The results are for the organization to keep—no strings attached.

TAG Cyber: Do you have any predictions about emerging cyberthreats to business infrastructure?

VARONIS: A lot of security teams are focused on securing endpoints. This has been an increased focus as a result of the explosion of remote work and the devices that do it. But if you really think about it, most of an organization's data doesn't live on someone's laptop or phone. It's stored in a company SharePoint site, someone's OneDrive, in a Slack or Teams chat or in your Salesforce. And since all these devices and systems are interconnected, an attacker only needs one way in to get access to all that data. The best defense from ransomware, malicious insiders, advanced persistent threats and other cyberthreats is to watch the target: data. Ransomware will evolve past encryption and operational disruption to extortion. If you've got data, someone wants it, and it's a matter of time and motivation until it happens. Organizations that don't secure and monitor their data will continue to be case studies in cybercrime.

AN INTERVIEW WITH ANDREW GINTER, VP, INDUSTRIAL SECURITY, WATERFALL SECURITY SOLUTIONS

MITIGATING ICS AND SCADA SECURITY ATTACKS WITH UNIDIRECTIONAL GATEWAYS

The protection of critical infrastructure from cyberthreats has become one of the more urgent issues—not only in the security industry, but for society. Successful attacks on targets such as nuclear generators, refineries and large transportation or water systems can result in significant safety consequences and loss of life.

Waterfall Security Solutions aims to protect critical industrial control systems (ICS) and their associated SCADA controls from malicious threats such as advanced malware. We wanted to know how its technology works.

TAG Cyber: How do bad actors target systems such as ICS?

WATERFALL: Last year's big problem was targeted ransomware. The Colonial Pipeline was shut down "in an abundance of caution," because a ransomware group took over its IT network. Colonial, JBS meatpacking and many other companies suffered expensive production shutdowns because of IT-targeted ransomware.

Then there was the threat of cloud-seeded ransomware, like the attack that hit Kaseya customers in May. A ransomware group used a Kaseya cloud service to seed malware simultaneously into 1500 IT networks. A comparable attack on a cloud service that is used by ICS networks would be devastating.

TAG Cyber: How does the Waterfall platform work?

WATERFALL: Our flagship product is the Unidirectional Security Gateway. Each gateway is a combination of hardware and software. The hardware is physically able to send information in only one direction, from the ICS network out to the IT network. All cybersabotage attacks are information. If no information gets back into the ICS network, then no attacks get back in, no matter how sophisticated those attacks may be today, or may become tomorrow.

Unidirectional Security Gateway software uses the one-way hardware to make copies of ICS servers, such as historians or OPC systems. IT users and applications use these IT copies normally. All of the ICS data that is allowed to be shared with IT is present in the copies and is updated in real time.

We will very soon see public safety incidents and casualties resulting from attacks on water treatment systems.

TAG Cyber: Many teams want the ability for bidirectional communication into and out of operational Technology (OT) systems. How do you deal with this situation?

WATERFALL: All remote control and remote access is fraught with risk. How many computers on the open internet *should* be able to reprogram a large power plant's safety systems? Or a refinery's control systems? "None!" is the answer most people offer. But think about it—every computer in an engineer's hotel room, using a VPN to connect into the ICS after a day at a conference, every one of those computers is on the open internet, isn't it? Why is this safe?

At Waterfall, we caution and educate our customers about these risks, and we provide alternatives. Unidirectional Remote Screen View lets vendor support people look and advise, but not touch. Secure Bypass units provide physical control over when trusted insiders have access to industrial sites. Waterfall for IDS is a unidirectional product customized to the needs of OT IDS sensors. Our FLIP product enables disciplined, scheduled updates of antivirus signatures, production orders and other information. These and many other products are each the most secure solution for a specific need.

TAG Cyber: Can you tell us more about how and where unidirectional gateways might be deployed and managed.

WATERFALL: They can be deployed in many places. For example, one third of North America's power generation, by name-plate capacity, is currently protected unidirectionally. A similar fraction of the world's refining capacity is protected unidirectionally. The world's passenger rail and metro control systems are adopting the technology very quickly. The same is true for large human-consumables producers and even consumer goods manufacturers. These businesses are all looking to benefit from visibility into OT systems, without suffering the risks of ransomware or other attacks leaking back into OT networks through firewalls.

How do these work? The gateways are deployed most commonly as the sole IT/OT interface at any given industrial site. Most often, the gateways connect many ICS networks to one or more IT networks through a single, secure interface. Other times, the gateways are deployed between ICS mirror ports and OT IDS sensors, or are deployed to protect OT networks from OT-to-cloud/internet connections that otherwise bypass defense-in-depth ICS security designs.

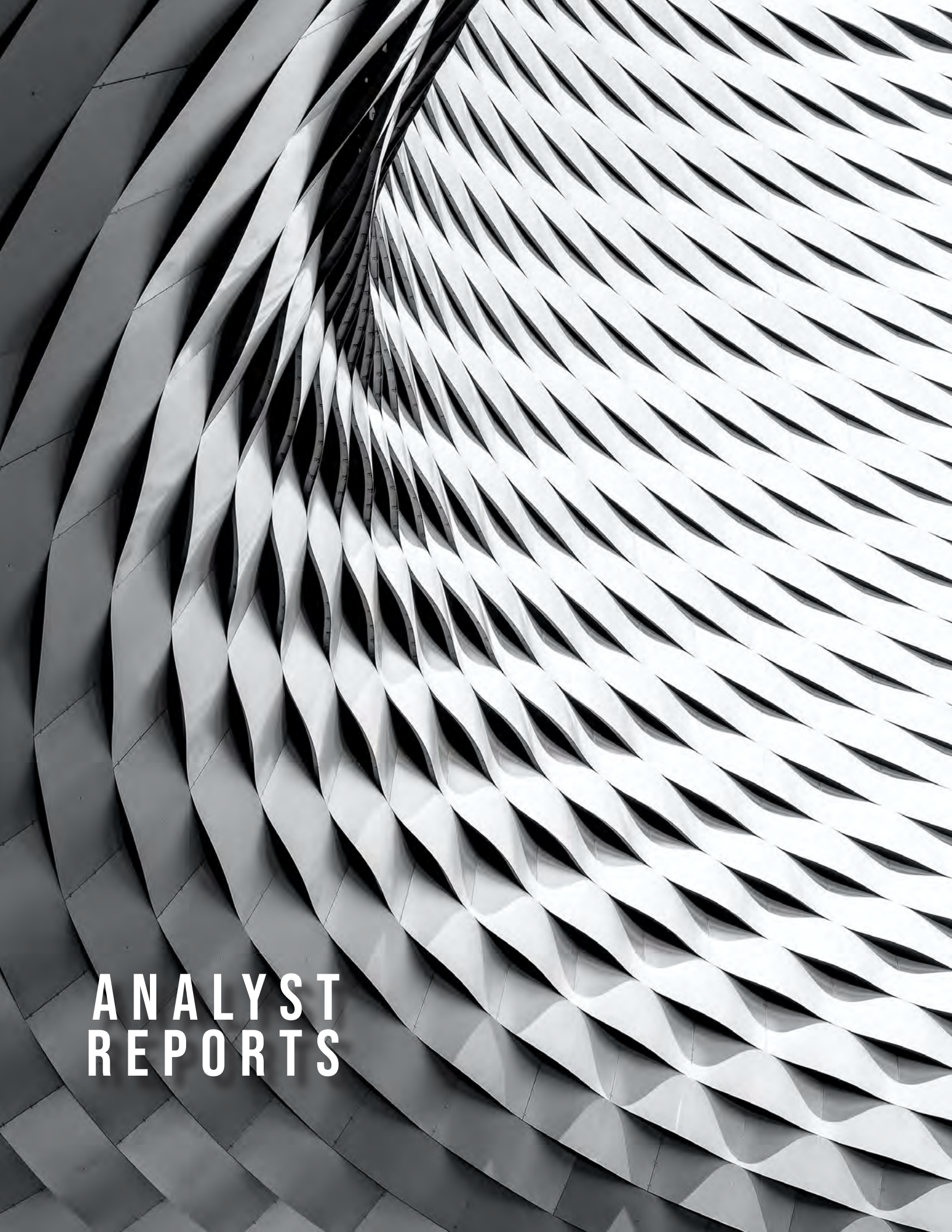
The gateways require minimal management. Unlike firewalls, the gateways do not need a constant churn of configuration changes, because all of the data that is allowed to be shared with IT is already available in the unidirectional copies of OT

servers. And unlike firewalls, Unidirectional Gateways do not need intense scrutiny of logs to detect attackers "knocking at the door." The physics of the unidirectional hardware means that no cyberattack can penetrate the gateways back into ICS networks, no matter how much "knocking" goes on.

TAG Cyber: Do you have any predictions about emerging cyberthreats to business infrastructure?

WATERFALL: Ransomware groups are already targeting one kind of critical infrastructure intensely: hospitals. In 2021, these groups also observed how very profitable it is to target industrial infrastructures—everything from semiconductor fabs and breweries to pipelines and manufacturers. It is only a matter of time before ransomware groups target industrial infrastructures more systematically, with both "one at a time" and massively parallel/cloud-based targeting.

Analysts have predicted that cyberattacks on OT networks will cause injuries and deaths within a small number of years, citing the **2017 TRITON incident**. These predictions are too cautious. We already see human casualties from cyberattacks in hospitals. We will very soon see public safety incidents and casualties resulting from attacks on water treatment systems. And unfortunately, we can look forward to even more serious problems in the future, resulting from the sabotage of rail switching systems and other industrial infrastructures. Ransomware groups and other adversaries breach IT and IT/OT firewalls routinely. The time has come to protect ICS and OT systems unidirectionally, at least at sites where the worst-case consequences of compromise are unacceptable.



ANALYST REPORTS

ANALYST REPORT

SECURE ACCESS AS A SERVICE: AN INTRODUCTION TO THE AXIS SECURITY PLATFORM

EDWARD AMOROSO

Traditional remote access based on virtual private networks (VPNs) is being replaced with new methods that are influenced by zero trust and related network security models. The Axis security solution[1] exemplifies this new generation of establishing zero-trust based connectivity to critical business resources.

INTRODUCTION

On occasion, the security community will collectively identify the need for a significant shift from some well-known control to an approach that is more effective. The transition from the use of single-factor passwords to multi-factor (or passwordless) authentication is one such example. The transition from signature-based antivirus to advanced endpoint detection and response (EDR) tools is another prominent example.

In this report, we review a third transition — one that has seen recent acceleration due to increased cyber threats, as well as the shift to work-from-home models, spurred along by the COVID-19 pandemic[2]. Specifically, we focus here on the transition from conventional virtual private networks (VPNs) to more advanced secure access solutions that are consistent with cloud-hosted applications and which are typically offered to customers as a service.

The establishment of secure connectivity to apps and data is one of the more prominent initiatives in modern IT and cyber security. This approach helps

The establishment of secure connectivity to apps and data is one of the more prominent initiatives in modern IT and cyber security. This approach helps companies achieve zero trust objectives and is a major component of the shift from existing secure business networks to cloud-based network control. The commercial Axis security platform is used to exemplify this modern approach in practice.

TRADITIONAL ACCESS

The traditional means for providing access to resources has involved three primary use cases. First, end users working from home or otherwise outside the office have used VPNs to remotely connect to corporate networks. The objective has usually been to access applications such as email, human resources tools, and business systems. These VPNs were often supported by large technology companies who would market both the clients and the server to the organization.

Second, business suppliers, partners, and other third parties have used a variety of means for accessing the networks, systems, and applications of their customer organization. In the early days, this might have been a private line access, but it eventually evolved into IPSec or SSL tunnels and other means for establishing secure connectivity to an internet-facing gateway. Such schemes have resulted in many well-known third-party breaches.

Third, businesses have engaged with service providers to create hub-and-spoke networks using multi-protocol label switching (MPLS) technology[3]. The resulting networks were designed to connect remote users to networks, and branch offices to the corporate data center. This arrangement worked well when applications were monolithic and premise-hosted behind a firewall, but the more recent shift to cloud has made these architectures awkward.

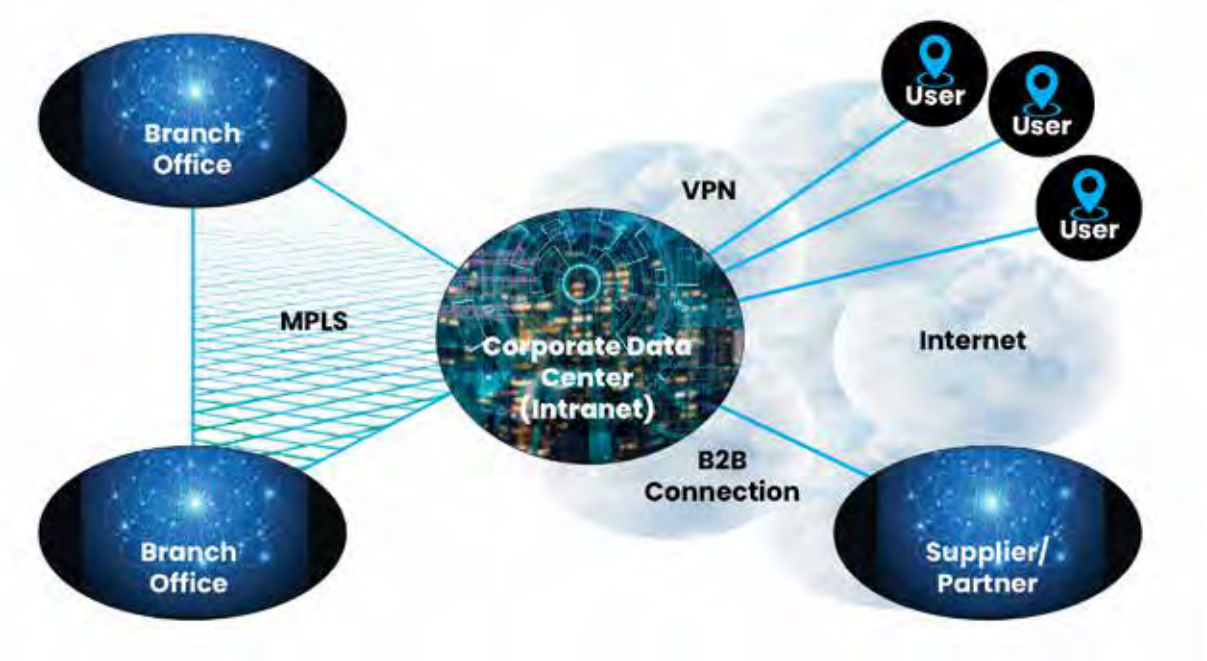


Figure 1. Traditional Use-Cases for Secure Access

While none of these traditional means for remote access have been perfect in terms of user experience and threat avoidance, all have served their purpose acceptably for decades. As such, it is correct to view all three technologies as successful engagements for which the security community should be grateful to the designers. Without these three secure access methods, cyber security might have been even more unruly these past decades than it was.

SECURE ACCESS DISRUPTIONS

With the advent of modern accelerated use of cloud-based services, including software as a service (SaaS) applications, all three traditional secure access use cases mentioned above are being severely disrupted. Driving such disruption are two conceptual models that are being adopted across

the security community to drive new designs — ones for which the session matters more than the perimeter, and for which control has been pushed to the cloud.

Zero Trust

The zero trust model[4] provides an accurate depiction of the condition that results when a perimeter can no longer protect an enterprise. This often involves the dissolution of the corporate firewall as a primary control for data security. When this occurs, any organization's clients, endpoints, servers, and the like can no longer trust the local network for privacy and security — hence, the zero trust moniker.

A good way to explain zero trust is to start with the firewall-protected perimeter case, where two entities can share freely with no need for mutual authentication. Security depends on the boundary protection of the firewall, but this model is porous, and malware can traverse this arrangement freely. In zero trust, all entities must share using mutual authentication and other security controls, because the boundary protection is removed.

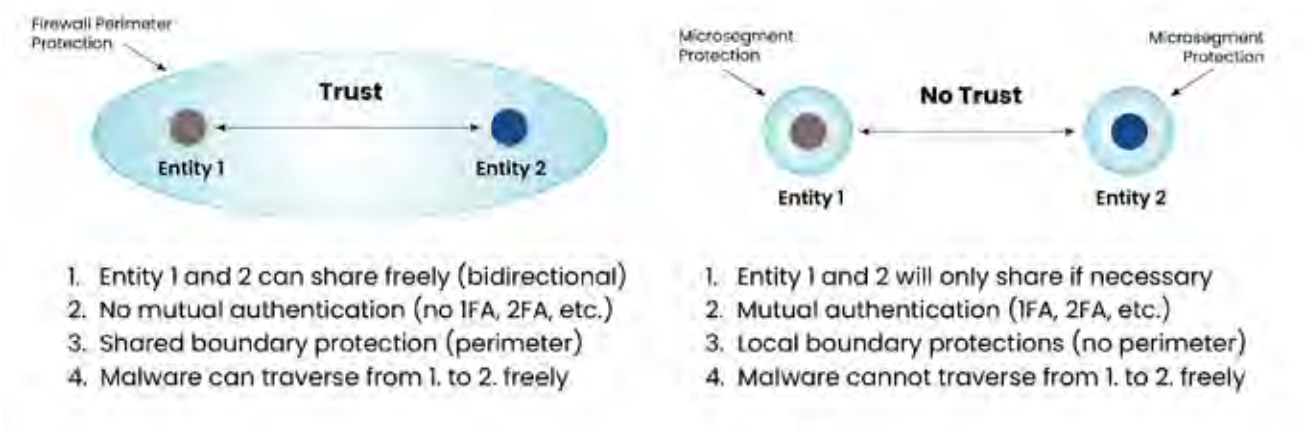


Figure 2. Zero Trust Model

The primary influence of zero trust on modern replacements for VPNs is that it reinforces the need to avoid dependence on any perimeter. This is a key difference between VPN usage and modern secure access methods. Where traditional approaches included the goal of establishing remote connectivity to the perimeter-protected enterprise, more modern methods are focused on supporting secure sessions from user devices to cloud- or premise-hosted applications.

SSE

The security services edge (SSE) model[5] references the evolution of modern business networking toward more cloud-oriented management. Such control is a natural progression from early separation of the data and control planes on a network. This innovation, found on modern multi-protocol label switching (MPLS) networks, allowed for all control activity to be implemented in a centralized manner using cloud.

From the perspective of the service provider, the SSE model shifts control into the cloud in a manner consistent with the design of new point of presence (POP) components. This allows for a distributed architecture where enterprise users can access cloud workloads across a network of control gateways that will include the desired security function — with secure access being one of the most important such capabilities.

While the SSE model generalizes network support beyond the user-access case covered by VPNs, it does reinforce the need in modern SAaaS for control to be centrally offered via cloud systems, and for cyber security requirements such as data leakage protection (DLP) and multi-factor authentication to be supported if VPNs are being replaced and upgraded.

While the SSE model generalizes network support beyond the user-access case covered by VPNs, it does reinforce the need in modern SAaaS for control to be centrally offered via cloud systems, and for cyber security requirements such as data leakage protection (DLP) and multi-factor authentication to be supported if VPNs are being replaced and upgraded.

OVERVIEW OF AXIS SECURITY PLATFORM

Launched in 2019 and headquartered in San Mateo and Tel Aviv, Axis Security provides a commercially available secure access as a service offering for enterprise customers. While the timing of the launch coincided with pandemic-initiated work-from-home practices, the evolution toward working-from-anywhere had long since started. Zero trust and SSE both exemplify the shift away from VPN access to perimeter-protected networks.

Goals of the Axis Security Platform

The Axis Security Platform is designed with the following major objective: To secure the modern workplace environment based on a foundation of zero trust. This is done through attention to security for work-from-anywhere, securing the business enterprise including all access by third parties, and modernizing the infrastructure with emphasis on transition from hub-and-spoke MPLS to multi-cloud usage by enterprise.

At a more detailed level, the platform uses 350 points of presence to deliver zero trust-based secure access for three primary purposes: (1) To support secure access to private apps in a typical hybrid work arrangement, (2) to ensure security of data as it moves between third-party apps and other services, and (3) to secure SaaS apps as they are accessed by end-users, including from branch offices and data centers.

Application Access Cloud

The commercial implementation from Axis Security delivers secure access and related capabilities through what it refers to as its Application Access Cloud. The infrastructure supporting this Application Access Cloud is designed to allow users to connect directly to applications via a central hub. This has the strong security feature of allowing such access without having to grant full access to an enterprise network.

The approach replaces VPN tunnels and agents in a manner consistent with both zero trust and SSE and supports security analysis and management of every access instance. Such cloud-based control also simplifies deployment and reduces the complexity of the configuration work to support secure access. It supports access for employees, contractors, administrators, and other remote workers to both cloud and premise-based applications.

Figure 3. Application Access Cloud From Axis Security

Secure Access as a Service

From an enterprise customer perspective, the Application Access Cloud enables provision of a secure access as a service (SAaaS) capability. This is encouraging, because traditional VPNs involved a product orientation that required considerable administration and complex configuration work by the customer. By offering secure access in this cloud service model, Axis greatly simplifies one of the major aspects of both zero trust and SSE.

Key Security Features

The centralized hub model also enables the provision of security features and analysis tasks for each access instance, as well as across aggregated access for a company or other group. Desirable security features that are enabled by the Application Access Cloud model include the following:

1. **Application access without network access** – Axis brokers secure 1:1 connections between authorized users without placing users on the corporate network, and places all apps behind the cloud where they are made invisible to Internet-based threats
2. **Inline inspection of traffic** – This capability allows IT to gain visibility into the specific activity that employees and third-parties, brush stroke by brush stroke, for the first time
3. **Continuous adaptiveness** – Customizable policies and Integrations with IDP and endpoint security ensures that access is always adaptive. As context changes, Axis will automatically adapt access rights, and sever any existing connections if the sessions fails to pass the policy check.
4. **Behavioral analysis** - By running secure access through a cloud-based hub, Axis can integrate behavioral analysis to help identify security anomalies, attack campaigns, and other patterns consistent with unauthorized access to resources.
5. **Agent or agentless deployment models** – The Axis agent supports all ports and protocols, and even access to apps like VOIP, P2P and server to client workflows. Agentless allows secure access to web apps, and can even record browser-based RDP sessions, without the need for client

Enterprise customers interested in more information on Axis Security should contact the team directly.[3] The TAG Cyber analysts have spent considerable time reviewing the platform and have concluded that its feature-rich access cloud represents just the type of zero trust and SSE design that is required to advance secure access for enterprise. Their SAaaS is worth taking the time to review.

1 https://www.axissecurity.com/

2 https://www.brookings.edu/blog/order-from-chaos/2020/12/28/experts-discuss-the-growth-of-cyber-threats-amid-the-pandemic/

3 https://en.wikipedia.org/wiki/Multiprotocol_Label_Switching

4 The original model was introduced by Forrester (see https://www.forrester.com/blogs/tag/zero-trust/) and much of the research requires paywall entry.

5 The original model was introduced by Gartner (see https://www.gartner.com/en/documents/3957375/invest-implications-the-future-of-network-security-is-in) but the research requires paywall entry.

ANALYST REPORT

HOW DEVICE VULNERABILITY ILLUMINATION FROM FINITE STATE ENABLES COMPLIANCE WITH THE EXECUTIVE ORDER ON IMPROVING THE NATION'S CYBERSECURITY

EDWARD AMOROSO
JENNIFER BAYUK
STANLEY QUINTANA

In May, the Biden administration issued Executive Order 14028 on Improving the Nation's Cybersecurity ("EO 14028" or "EO"). Section 4 of the EO requires departments and agencies of the federal government to institute specific practices and protections designed to improve cyber security in government infrastructure, with a specific focus on software supply chain security.

These new requirements are currently under development (principally by the National Institute for Standards and Technology [NIST]), but the general direction and intent of the pending regulations are already clear. While Section 4 of EO 14028 is focused on regulating sales of software to the federal government, we anticipate that the influence and reach of these emerging requirements will affect the entire software industry. Starting in early 2022, a wide array of companies will be compelled to implement these requirements if they want to remain competitive.

With this in mind, we reviewed the capabilities that Finite State has assembled in its platform for analyzing the cyber risk of connected devices. We found that the Finite State platform delivers key features to enable compliance with what we expect to see when the government issues final regulations under EO 14028.

INTRODUCTION

It is clear that in the past few years, there has been a significant increase in the frequency and sophistication of published cyber attacks. We are seeing more attacks targeting supply chains and critical infrastructure. This development poses significantly increased risk of devastating impacts on the economy and on individual lives. Despite the fact that this trend (and its concomitant warning signs) has been observable for years, there have not been improvements in cybersecurity laws or regulations that could be expected to result in improved cybersecurity practices sufficient to thwart such threats.

As a result, with some notable exceptions, cybersecurity practices across nearly all sectors of the economy have left many to wonder when we will experience a cyber attack with sufficiently grave consequences that it drives the political will necessary to deliver mainstream action.

The Biden administration is taking a different approach, simply using its purchasing power and contractual relationships to drive improvements in protection of critical infrastructure and prevention of supply-chain attacks. EO 14028 is the centerpiece of this efforts. The EO directs the development of regulations to require that software companies implement key practices to:

1. Improve the security of software development,
2. Standardize security testing of software, and
3. Mandate transparency (to verify compliance with #1 and #2).

While this is a welcome change for those pushing for improvements in cybersecurity practices, particularly with respect to the security of Internet of Things (IoT) devices, it brings with it the potential to impose challenging compliance requirements on companies that develop and sell software.

OUR FOCUS

From our perspective, the key area of critical infrastructure protection that deserves special attention is the threat to connected devices and embedded systems. Traditionally addressed by operational technology (OT) groups with limited experience in cyber, this aspect of critical infrastructure has emerged as being vulnerable to a range of attacks that could produce devastating consequences. The EO draws much-needed attention to this area of cyber risk.

In this paper, we examine the direction and focus of the mandates in EO 14028 and line them up against the software testing platform developed by the cybersecurity company Finite State. The Finite State platform enables both manufacturers and owners of connected devices to assess and manage software and supply chain vulnerabilities and, as we will demonstrate, can help companies to close key gaps in complying with the regulations to be issued under EO 14028.

CYBER RISKS TO CONNECTED DEVICES

It is well-understood that connected devices pose a significant cyber risk across virtually every sector. One need only appreciate how such devices are used (medical devices, industrial control devices, electronic control units in automobiles) to comprehend the potentially grave consequences that could result from security flaws.

What is less well-understood is how the diversity and fragmentation of components used in connected devices complicates the challenge of securing such devices. Each type of connected device will tend to have its own unique software and hardware footprint, usually optimized to the task being addressed. This can extend to the device's hardware components, network interfaces, and different modes of connectivity (Bluetooth, WiFi, cellular, Zigbee, etc.). Moreover, these hardware components are usually accompanied by specialized software to power them (e.g., a cellular modem has a baseband processor that runs proprietary instructions).

All of this dramatically increases the complexity of the available attack surface and significantly adds to the difficulty in conducting software composition analysis, which is essential in understanding risk and prioritizing the steps to mitigate that risk.

Figure 1 shows just a small sample of the alternative choices faced by manufacturers of connected devices. These are exemplary alternatives within each choice category.

As a result, connected devices in the modern organization must be identified, managed, and secured to avoid the risk of remote access, remote control, and other types of targeted attacks. Such enhanced protection will require coordination between users and their connected device suppliers through third-party controls. With the contractual requirements emerging under EO 14028, many of these functions will become mandatory for government suppliers. Meeting these requirements for connected devices will not be a trivial matter.

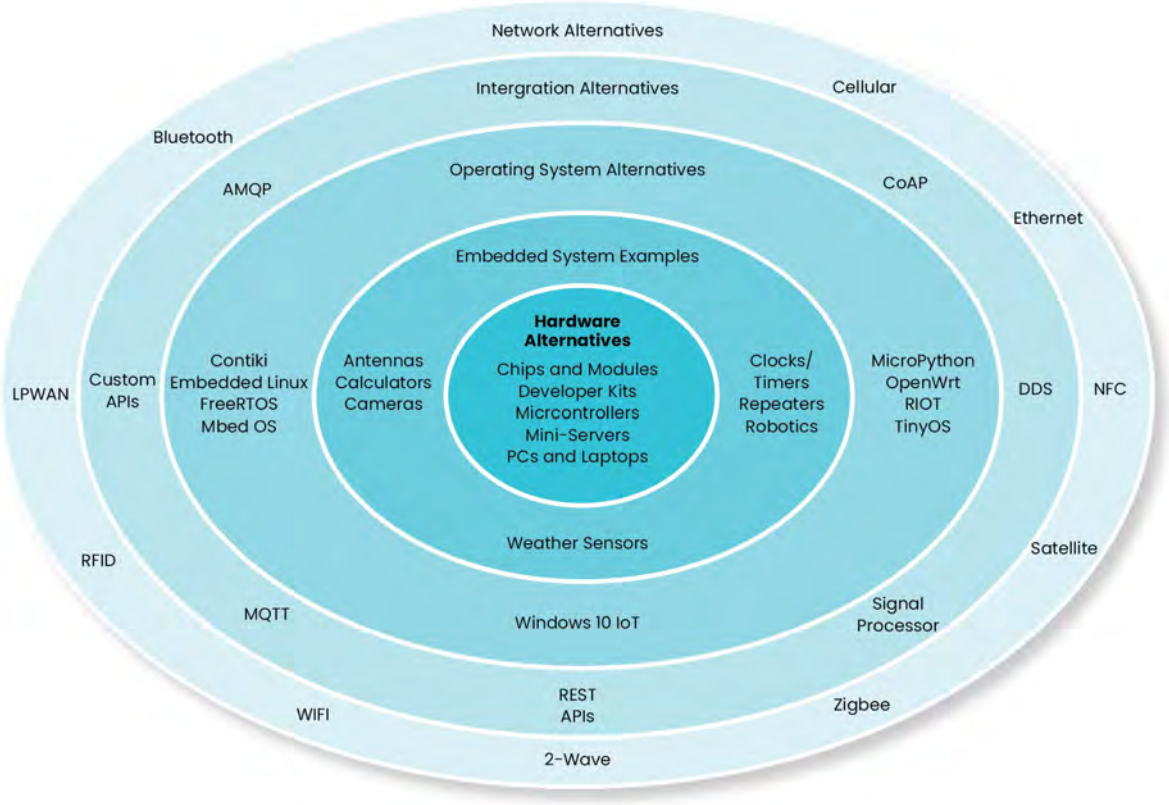


Figure 1. Illustrating the Cyber Risk Challenge of Connected Devices

A MANDATE FOR TRANSPARENCY

It's important to note that we expect the requirements issued under the EO to track with much of what are already understood as best practices in software development and testing. There are two key features that represent the potential for a sea change in the level of transparency in cybersecurity threats and countermeasures: (1) government contractors will likely make these turn the new requirements into standard features available to commercial customers, and (2) the EO's recommendations for improving information sharing between public and private sectors should serve to increase the availability of threat intelligence generally across technology service providers.

The primary mechanism through which the EO will enforce this transparency is the Software Bill of Materials (SBOM). While there are a few existing standards for the structure and content of the SBOM, the basic construct requires software providers to present basic (but critical) information about all of the components included in their product.

Figure 2 shows the format of an industry-standard SBOM listing with a simple example of a product and one of its components.

Supplier Name	Acme	Apache
Component/Package Name	Acme IoT Device	CentOS-Stream
Unique Identifier	SN:2348829	CentOS-Stream-8-x86_64-20210811-boot.iso
Version	2.6	8
Component Hash	Qx423	e38192400212796085b7996f218aa8f8a...
Relationship to Project	Self	Included in
Author/Creator	Acme	CentO5 Project

Figure 2. Basic Elements of an SBOM

As early as 2014, Congress was considering legislation that would have made the SBOM mandatory for the federal government's procurement of software. The proposed legislation never became law, and, seven years later, the executive branch now is using the EO to mandate the SBOM without the help of Congress.

NIST has been clear on the importance that it places on the use of the SBOM in providing the kind of transparency necessary to protect against supply chain threats:

> An SBOM model achieves this systematic sharing by tracking component metadata, enabling mapping to other sources of information, and tying the metadata to software as it moves down the supply chain and is deployed.

Requiring software developers to provide an SBOM will highlight the diversity of components in connected devices (and the challenge involved in securing them). This will likely be the linchpin of EO 14028 and among the most prominent compliance requirements.

MAPPING FINITE STATE TO THE EXECUTIVE ORDER

In this context of increasing focus on and understanding of software supply chain threats, Finite State has developed a solution that enables compliance with the emerging requirements under EO 14028.

The Finite State platform is a commercially available cybersecurity solution designed to provide visibility into the components and vulnerabilities resident on a connected device. Armed with this information, device manufacturers and owners can assess the risk associated with the software embedded in a device — and prioritize efforts to mitigate that risk.

With that in mind, we have undertaken a review of the features and functions of the Finite State platform and how they map to the regulations that we anticipate will be issued under the EO.

To determine the effectiveness of a given platform in supporting a set of requirements such as in the executive order, it is helpful to focus on the set of assertions within the requirements that characterize the contribution of cyber security technology to the overall compliance. In the case of the executive

order, these requirements are included in Section 4: Enhancing Software Supply Chain Security. In particular, in Section 4(e) we see the most detailed insight into the actual requirements that will emerge in the regulations that will be issued under the EO. The TAG Cyber team mapped the executive order components to Finite State software feature(s).

After the initial mapping, it became clear that both device manufacturers and owners can leverage the Finite State platform in implementing a program to comply with EO 14028. This is similar to the model used by cloud service providers. In this construct, not only does a compliant manufacturer require software features such as those provided by Finite State, but that manufacturer also must establish internal process, standards, and procedures to incorporate Finite State usage into its software development process and present artifacts of those controls to demonstrate compliance. Likewise, the manufacturer's customers, the device owners, may use Finite State to demonstrate compliance with the executive order as they incorporate the connected device into their own operations. Therefore, we annotated the feature descriptions with the following characteristics:

- *Activity* – Specifies the step in the software development or operations lifecycle that the manufacturer or device owner's procedure or standard is most effectively incorporated from a cyber security perspective.
- *Responsibility* – Suggests whether the control is considered solely a Finite State product feature or, in addition, should be part of a procedure or standard to be adopted by a device manufacturer or device owner using Finite State software.
- *Method* – Identifies whether the feature is fully automated or requires some manual activity to ensure that the feature's control objective is met.

As we mapped Finite State features to the software development lifecycle activities that they support, it became apparent that the main contribution of the Finite State software was in support of a secure SDLC test phase. These functions are used by both manufacturers and device owners. They are fully automated and produce artifacts that may then be used by manufacturers in their Code, Build, Update, and Release stages and by device owners in their Procure and Monitor stages. Figure 3 shows the distribution of Finite State features to software development lifecycle activities and control implementation methods. The details on the specific features included in the Finite State platform are listed in Appendix A.

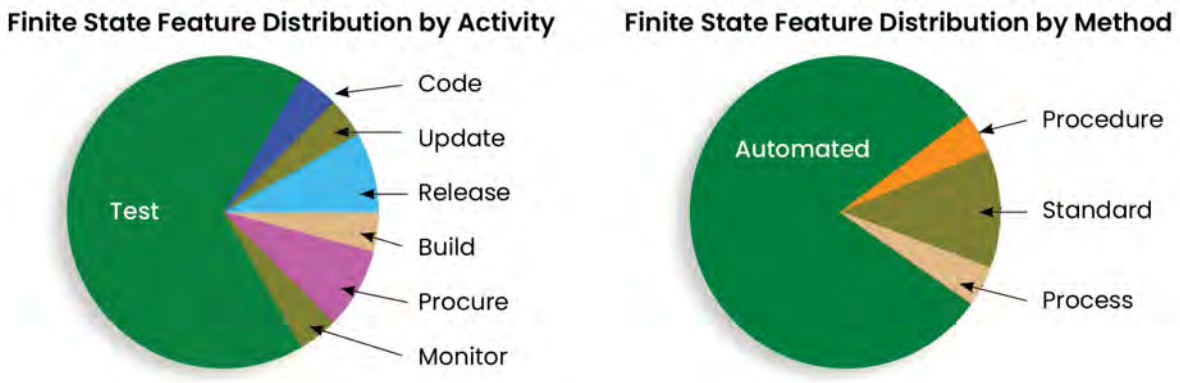


Figure 3. How Finite State Supports Manufacturers and Device Owners

In Appendix B, we have mapped the Finite State features against the provisions in Section 4(e) of EO 14028. This mapping demonstrates that the Finite State platform provides capabilities that are likely to be crucial in achieving compliance with the newly forming regulatory regime.

It is worth focusing attention on the manner in which Finite State maps to the EO's SBOM requirement. Through an automated process, the Finite State platform then generates an SBOM for each device analyzed. This SBOM is in line with existing industry standards and meets the minimum requirements established by NIST under EO 14028.

Finite State goes beyond the standard format of an SBOM and analyzes each component of the software in seven cybersecurity dimensions, offering a visual representation of the product of interest. We found this to be particularly important, as simply offering a "parts listing" in an SBOM may have limited utility in practice.

Figure 4 offers an example output of this analysis. The main axis shows whether all software components in the device are identifiable, while the other axes show the extent to which they are secured to industry standards. This analysis lines up precisely with the EO's intent of providing visibility into the components of software and the security risk they present. Moreover, new automated assessment techniques are constantly under development, and may be easily incorporated into such a presentation.

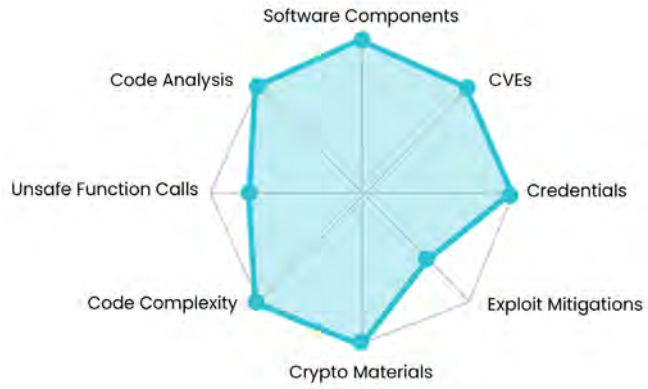


Figure 4. Example of How Finite State Visualizes SBOM-Derived Risks for a Device

IMPLICATIONS AND RECOMMENDATIONS

The key implications for manufacturers and end users of this analysis are as follows:

Any organization selling or utilizing connected devices (in particular, in connection with sales or services provided to the federal government) must comply with EO 14028. In establishing a compliance process, we recommend reviewing the Finite State platform as an exemplary tool in that compliance process. Our analysis has determined that using the Finite State commercial platform will go a long way toward meeting the emerging requirements, in particular with respect to the SBOM.

Connected devices and their complicated supply chains represent a significant attack surface through which malicious actors can gain unauthorized access into targeted networks. Information critical to identifying and mitigating SBOM-related vulnerabilities, such as that provided by the Finite State platform, is an essential component of any assessment of cybersecurity risk presented by connected devices. By addressing such vulnerabilities and weaknesses, IoT vendors and connected devices service providers can demonstrate due diligence in assessing cyber risk posture. Capability in this demonstration will provide much-needed cyber security control assurance for both government and commercial customers.

APPENDIX A: DETAILED FINITE STATE FEATURE MAPPING

In the mapping below, Finite State features are paraphrased, mapped to the software development lifecycle activities that they support. Beneath the current feature list, expected enhancements are included as well.

ACTIVITY: TEST

Discovery of Backdoors
Method: Automated, *Responsibility*: Finite State

CVE Identification
Identifies Common Vulnerability Enumeration identifiers associated with identified software packages.
Method: Automated, *Responsibility*: Finite State

Cryptographic Settings
Identifies poorly configured cryptographic settings, e.g., standardized host key files.
Method: Automated, *Responsibility*: Finite State

Cryptographic Variables
Identifies hard-coded cryptographic material in firmware images, e.g., private keys, authorized key files.
Method: Automated, *Responsibility*: Finite State

Exploit Mitigations
Identifies binary safety features to determine if they have been disabled to protect against malicious attacks.
Method: Automated, *Responsibility*: Finite State

Hard-Coded Credentials
In addition to highlighting vulnerability, this feature aids in discovery of backdoors.
Method: Automated, *Responsibility*: Finite State

Software Composition Analysis (SCA)
Finite State Software composition analysis (SCA) analyzes first- and third-party/open source software. It detects operating system(s), software packages, versions, and software license usage. This information is used to create a software bill of materials based on automated analysis of processes installed and/or running on IoT devices.
Method: Standard, *Responsibility*: Finite State

Software License Usage
Automated SCA includes identification of software licenses in use.
Method: Automated, *Responsibility*: Finite State

Static Application Security Testing
Static application security testing (SAST) identifies previously unknown 0-day memory corruption as well as patterns of vulnerabilities in first- and third-party code.
Method: Automated, *Responsibility*: Finite State

Supply Chain Risk Analysis
Finite State conducts research on software and hardware vendors in order to assess and summarize intelligence on third-party product provenance.
Method: Process, *Responsibility*: Finite State

Unsafe Function Calls
Identifies first- and third-party unsafe legacy functions like C strcpy.
Method: Automated, *Responsibility*: Finite State

Vulnerability Identification
Identifies all known vulnerabilities in the software bill of materials, including third-party binaries and the operating system.
Method: Automated, *Responsibility*: Finite State

Vulnerability and Risk Correlation
Correlates information from the vulnerability database about the risk from known exploit data.
Method: Automated, *Responsibility*: Finite State

ACTIVITY: RELEASE

SBOM Security Report
The SBOM Report, accompanied by the Full Security Report, will include all identified Vulnerability Information in industry-standard presentation; for example, Common Vulnerability Enumeration (CVE) and Vulnerability Exploitability (VEX), in Excel, PDF, and JSON (coming soon).
Method: Automated, *Responsibility*: Manufacturers

Software Bill of Materials Report
The SBOM information includes components, licenses, copyrights, and security reference in Software Package Data Exchange® (SPDX®) format, an open standard for communicating SBOM. It should be regenerated with each product release.
Method: Automated, *Responsibility*: Manufacturers

ACTIVITY: PROCURE

Device Risk Diagram
A graphical depiction of the Finite State Automated Product Security Assessment. The risk scores are relative to all other firmware analyzed by Finite State, so it is an industry-comparative score. An absolute security scoring model is expected in a subsequent release. Device owners may use this diagram to compare the security of similar products. manufacturers may use it to compare their security performance to that of other manufacturers.
Method: Standard, *Responsibility*: Shared

Finite State Automated Product Security Assessment
Finite State includes the ability for both the manufacturer and the device owners to assess IoT product security in the course of business risk management processes, and to share information related to IoT asset security in standard reports and/or exports. The manufacturer is expected to use these reports to self-assess and demonstrate the strength of its product, and the device owner is expected to review this assessment prior to procurement.
Method: Standard, *Responsibility*: Shared

APPENDIX A CONTINUED

ACTIVITY: UPDATE

Update Software Bill of Materials
With each release, the SBOM is updated to include more information and analysis, so device owners should rerun and review the Finite State Automated Product Security Assessment.
Method: Procedure, *Responsibility*: Device Owner

ACTIVITY: MONITOR

Vulnerability Verification
Finite State has emulation capabilities that are automated and can be extended to verify the presence of known vulnerabilities in binaries. These are employed in dynamic application security testing (DAST), a method of testing code in operation. Manufacturers should use vulnerability verification to ensure that new releases do not include known vulnerabilities, and assets owners should periodically run this report to ensure that their own installations remain free of known vulnerabilities.
Method: Automated, *Responsibility*: Shared

EXPECTED ENHANCEMENTS

ACTIVITY: CODE

Issue Management Integration
Import/export Finite State findings/issues to develop JIRA tickets.
Method: Automated, *Responsibility*: Manufacturers

ACTIVITY: BUILD

CI/CD Build Integration
Automated security analysis of build artifacts and system images capability for continuous integration and continuous delivery processes.
Method: Automated, *Responsibility*: Manufacturers

ACTIVITY: TEST

Absolute Security Score
A graphical depiction of the Finite State Automated Product Security Assessment currently displays a comparative score relative to all other firmware analyzed by Finite State. An absolute security scoring model a corresponding diagram is a planned enhancement. Device owners may use this diagram to assess device security. Manufacturers may use it to target their efforts to improve security.
Method: Standard, *Responsibility*: Shared

ANALYST REPORT

ATTACK SURFACE MANAGEMENT: THE FIRST LINE OF DEFENSE AGAINST RANSOMWARE

EDWARD AMOROSO

Ransomware attacks continue to cause problems for businesses despite many efforts to reduce the risk. The technique known as attack surface management is discussed and shown to provide an effective first line of defense against malicious ransomware campaigns.

INTRODUCTION

One of the most significant recent cyber security issues involves ransomware attacks by malicious actors who demand payment from victims before seized files will be unlocked. Despite the ease with which criminals have been able to perform such attacks, the defensive community has had considerable difficulty responding to ransomware, and even more difficulty preventing such attacks.

In contrast, one of the most significant security advances involves management of the so-called attack surface of an organization. Although technically not a new concept, so-called attack surface management (ASM) has improved sufficiently to handle an increasingly virtual and distributed network edge. This is good news, since many organizations now operate decentralized cloud-oriented networks. ASM is well-suited to this approach.

In this report, we make the case that ASM is well-suited as a first line of defense against ransomware attacks. We illustrate how the necessary steps that malicious actors must take to engage in ransomware can be identified and mitigated using ASM controls. This should be good news for enterprise teams, especially because ASM solutions are readily available from commercial vendors to address a wide variety of attacks.

UNDERSTANDING RANSOMWARE ATTACKS

Ransomware is an attack that involves malicious control of a target victim's data with the threat of either public disclosure or blocked access if some ransom fee is not paid. The extortion is usually carried out through encryption of victim files, which allows the malicious actor to withhold the decryption keys until payment is received — almost always using some anonymous, untraceable digital currency.


TLP:WHITE

FBI FLASH

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

25 AUG 2021

Alert Number
MC-000150-MW

The following information is being provided by the FBI, with no guarantees or warranties, for potential use at the sole discretion of recipients in order to protect against cyber threats. This data is provided to help cyber security professionals and system administrators guard against the persistent malicious actions of cyber actors. This FLASH was coordinated with DHS-CISA.

This FLASH has been released TLP:WHITE. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

Indicators of Compromise Associated with Hive Ransomware

Figure 1. Typical Ransomware Advisory From FBI[1]

Most of the time, ransomware is accomplished through simple means, such as through content attachments or URL redirection in a phishing attack, but some attacks, such as WannaCry, were carried out via worm methods that did not rely on users clicking on links or attachments. In either case, the incidence of ransomware has stubbornly remained high, with organizations such as the FBI reporting losses of nearly $30M in 2020.[2]

OVERVIEW OF ATTACK SURFACE MANAGEMENT

Early enterprise teams learned quickly that so-called scanning of the local network offered desirable visibility into applicable security posture. This included data on what was connected to the network, what services were being offered by systems on that network, and where the external entry and exit gateways were located. Many successful vendors grew significantly through provision of enterprise scanners.

More recently, however, with the proliferation of SaaS and cloud-based applications and with the trend toward zero trust access to workloads in a work-from-anywhere arrangement, organizations have had to rethink their organizational boundaries. What has resulted is a new concept known as an attack surface, which is defined as the collective access points where enterprise resources can be reached.

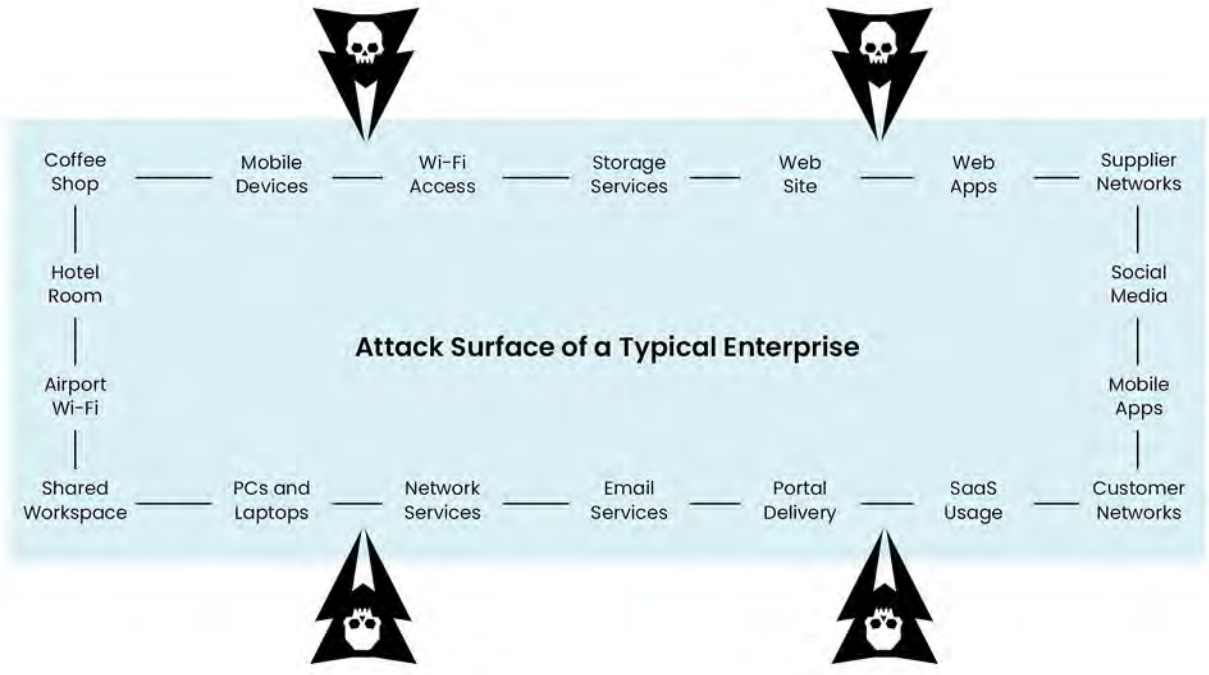


Figure 2. Typical Enterprise Attack Surface

To handle the security aspects of protecting an attack surface, a discipline known as attack surface management (ASM) has emerged. This method includes advanced capabilities to obtain visibility into the attack surface through discovery, to ensure policy enforcement through controls, and to address cyber threats through mitigation and response functions. Many commercial vendors now offer ASM solutions.

PREVENTING RANSOMWARE WITH ASM

While it might seem obvious, according to the discussions above, that enterprise teams should rely on ASM to reduce the ransomware threat, this connection has not been sufficiently made by practitioners or the analysts who influence security methodologies. This situation must change, if only because most other methods to reduce ransomware risk have not worked — and ASM is well-suited to a concept known as Ransomware Ops.

Understanding RansomwareOps

While it is often believed that ransomware is a singular event that occurs when someone clicks or downloads malicious content, the reality is that ransomware attacks involve a series of steps by malicious actors. This can include many of the offensive tasks commonly associated with advanced persistent threats (APTs) such as reconnaissance, scanning, access, privilege gain, lateral traversal, and so on.

It is thus more accurate to view a ransomware campaign in the context of this series of attack steps, which we refer to here as RansomwareOps. This might seem to present a greater challenge, since so many more attack steps are included, but the reality is that these various stages of a campaign offer cyber defenders with multiple opportunities to detect the attack and to take steps to either prevent or detect what is happening.

MITRE Attack Model

An excellent model that can be used to understand how RansomwareOps are performed comes from the security research team at MITRE. Their ATT&CK framework has been particularly useful across the defensive cyber security community, and it comes with an underlying model of how an adversary will typically operate. As suggested above, ransomware campaigns will resemble other types of attack approaches, so the MITRE model is highly relevant.[3]

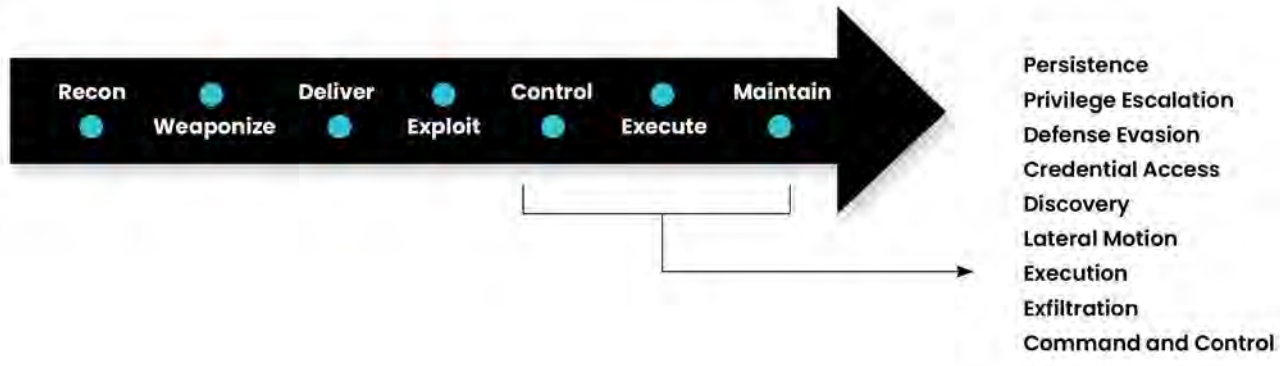


Figure 3. MITRE Attack Campaign Model

The goal of using an attack model such as from MITRE is that it helps to identify where specifically a security control might be placed to prevent a given campaign from proceeding. For example, in theory, if it is possible to stop the earlier steps such as recon and weaponization, then the likelihood of success for later steps such as execution and maintenance should be significantly reduced.

ASM Solution Approaches
The protection of an attack surface can be done either through a collection of point solutions, each designed to address some aspect of surface exploitation, or through an integrated platform, generally offered from a commercial provider. Our emphasis here will be on the use of a commercial ASM platform, but the requirements listed below can be addressed locally using whatever controls are deemed appropriate. The security requirements that should be considered essential to any ASM solution include the following three protection tasks:

ASM Task 1: Identification – The first step in establishing an ASM scheme involves discovering exactly what constitutes the attack surface. This should start with well-known and IT-managed devices and systems but must extend to include unmanaged infrastructure, as well as any shadow IT services being used. Shadow IT represents a significant challenge because it is so easy for employees and business units to engage directly with cloud and SaaS providers.

Most ASM identification solutions are based on a comprehensive program of testing, scanning, probing, and assessment. Penetration testing, including automated support, is an especially good method for identifying subtle attack surface components that might not be otherwise recognized. Red, blue, and purple team engagements are also excellent approaches to help create an accurate view of the targetable attack surface.

ASM Task 2: Prioritization – The second step in implementing ASM involves prioritizing how discovered attack surface elements are protected. Such elements include every component shown in Figure 2 (see above) and must factor in the relative importance of each component to the mission of the organization. For example, companies with heavy dependence on third-party suppliers will have to prioritize accordingly.

Most ASM prioritization includes data on the relative intensity of vulnerabilities found on a targeted attack surface. In the best case, the ASM discovery will include identification of entry and exit points, as well as estimates of the vulnerabilities for these devices. Both factors would then contribute to prioritization. For example, a storage service essential to the business, but that includes a vulnerability, would be prioritized for rapid mitigation.

ASM Task 3: Protection – The third step in the ASM solution lifecycle involves taking steps to mitigate whatever security issues have been identified and prioritized. As with all security protections, this can include prevention, detection, or response tasks consistent with models such as NIST 800-53.[4] Such protections will also swing widely between solutions for suppliers, mobile devices, cloud services, and on and on. Each will require different control.

Most ASM protections are now evolving from the physical perimeter controls used previously to more distributed, virtualized protections. Thus, whereas a prior generation of security teams might have addressed the attack surface by tightening some firewall rules, present-generation security teams must engage in more tailored security tasks targeting a much wider assortment of attack surface

Most ASM prioritization includes data on the relative intensity of vulnerabilities found on a targeted attack surface. In the best case, the ASM discovery will include identification of entry and exit points, as well as estimates of the vulnerabilities for these devices. Both factors would then contribute to prioritization. For example, a storage service essential to the business, but that includes a vulnerability, would be prioritized for rapid mitigation.

ASM Task 3: Protection – The third step in the ASM solution lifecycle involves taking steps to mitigate whatever security issues have been identified and prioritized. As with all security protections, this can include prevention, detection, or response tasks consistent with models such as NIST 800-53.[4] Such protections will also swing widely between solutions for suppliers, mobile devices, cloud services, and on and on. Each will require different control.

Most ASM protections are now evolving from the physical perimeter controls used previously to more distributed, virtualized protections. Thus, whereas a prior generation of security teams might have addressed the attack surface by tightening some firewall rules, present-generation security teams must engage in more tailored security tasks targeting a much wider assortment of attack surface

Figure 4. ASM Solution Lifecycle

We do not address here many practical considerations in selecting an ASM solution, including installation, maintenance, and budget. The cost to procure and install an ASM platform is particularly important, especially if the goal is to avoid ransomware payment. Balancing the cost to prevent with the cost to respond is thus an important return on investment (ROI) task that should be performed at some point by the enterprise security team. (TAG Cyber can assist security teams desiring this type of ROI analysis.)

Role of ASM in Stopping RansomwareOps

ASM turns out to offer an excellent means for mapping exploitable entry and exit points in an enterprise to the offensive steps one would expect to find in a ransomware attack campaign. The key observation is that ransomware finds its way into an enterprise via offensive actions that exploit the attack surface. No ransomware attack occurs without touching an attack surface in some way. In this respect, it is an excellent first line of defense against ransomware.

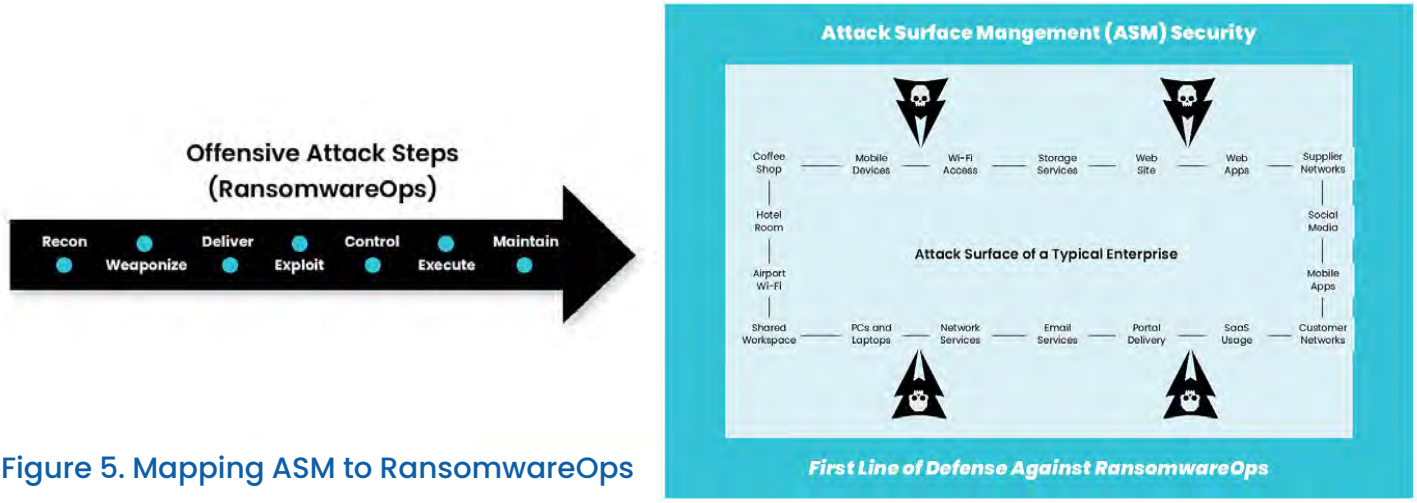


Figure 5. Mapping ASM to RansomwareOps

This implies that the best security methodologies for avoiding ransomware must include focus on the ASM. This can be done in a piecemeal manner with controls for each aspect of ASM, perhaps from different vendors, open-source software, or internal development teams. It can also be supported through a commercial ASM solution, which has the advantage of providing more uniform coverage, reporting, and alerting about ASM-related protection issues.

PROPOSED RANSOMWARE ACTION PLAN FOR ENTERPRISE

Enterprise teams are advised to initiate a management action plan immediately to address the security threats to their attack surface. While action plans will vary from one organization to another based on local preferences, threats, and infrastructure, most proposed plans will include the following major tasks, which draw from the information and recommendations presented throughout this report:

Task 1: Inventory of Current ASM-Related Solutions
The organization is advised to include a comprehensive identification of all current and ongoing ASM-related tasks. This includes finding any scanning processes, inventory tasks, penetration testing projects, or other activities that are directly related to reducing attack surface risk. This baseline task is important because organizations can build on existing solutions (if available) to optimize their target ASM process at the lowest cost.

Task 2: Creation of ASM Requirements
Any baseline ASM solutions found in Task 1 can be combined with an assessment of enterprise security risk to create a comprehensive set of requirements. These requirements should include the functional controls necessary for ASM (which can be combined into a vendor request for proposal (RFP) document), but they should also include practical issues, such as budget and procurement constraints (e.g., vendor country of origin).

Task 3: Selection of Suitable Commercial ASM Provider
The third task (which can be performed in parallel with the other tasks) involves the selection of one or more ASM commercial vendors to support the program. While some advantages exist in working with multiple vendors, the TAG Cyber team recommends that buyers consider working with a vendor supporting comprehensive ASM coverage. Enterprise teams can contact TAG Cyber for assistance with this rationalization and selection task.[5]

[1] *https://www.ic3.gov/Media/News/2021/210825.pdf*

[2] *https://en.wikipedia.org/wiki/Ransomware*

[3] *See https://www.mitre.org/sites/default/files/publications/16-3713-finding-cyber-threats%20with%20att%26ck-based-analytics.pdf.*

[4] *https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final*

[5] *TAG Cyber provides a Research as a Service (RaaS) platform which enterprise teams can use to self-serve useful information and to reach tiered support experts who can assist with non-operational security tasks such as vendor selection.*

TAG CYBER

ANALYST REPORT

ACHIEVING DEVOPS SECURITY THROUGH VISIBILITY AND MANAGEMENT: AN INTRODUCTION TO THE SYSDIG PLATFORM

EDWARD AMOROSO

Visibility and management of cloud infrastructure provides important controls necessary to achieve DevSecOps. Key security protections include run-time views of identity entitlements as well as levels of privilege and permissions usage. The Sysdig platform is shown to implement these cyber security capabilities for cloud-native software environments.

INTRODUCTION

For many years, software applications were hosted in private data centers protected by corporate firewalls. Coded in a monolithic manner, these applications were often easy to manage because they had few dependencies other than front-end interfaces and back-end databases. This is not to say that they were bug free. In fact, such applications were typically riddled with exploitable flaws due to crude coding practices and bad programming languages.

More recently, software applications have come to be coded in a more containerized manner, usually orchestrated with tools such as Kubernetes and managed using automated techniques such as infrastructure-as-code to define and control the computational environment. While this allows for the reuse of existing modules, which reduces costs and increases flexibility, it also increases the number and types of dependencies that must be identified and managed.

In this report, we outline the cyber security issues that emerge in these modern DevOps environments with emphasis on the types of identities used by cloud-native applications. This includes threats related to permissions, entitlements, and enforcement of which users have been granted access to which cloud resources.

The commercial Sysdig[1] platform is introduced and shown to effectively implement advanced controls for these DevOps-related threats.

SECURITY ISSUES IN DEVOPS

One of the most challenging aspects of modern DevOps is the rapid pace of change for software applications. Where previously, it might have been expected that a given application would be modified only occasionally or not at all (e.g., early mainframe applications), the modern software engineer must deal with an on-going demand for new features, upgrades, fixes, and enhancements. The pace of such change is sometimes measured in hours.

This on-going update process drives the need for security engineers to design controls that can keep up with the changes. Automation is the only reasonable choice, especially for non-trivial applications, and when such controls are integrated into DevOps, the enhanced DevSecOps designation is often used to describe the resulting software development lifecycle (SDLC). Not all development teams have made this transition, but many have.

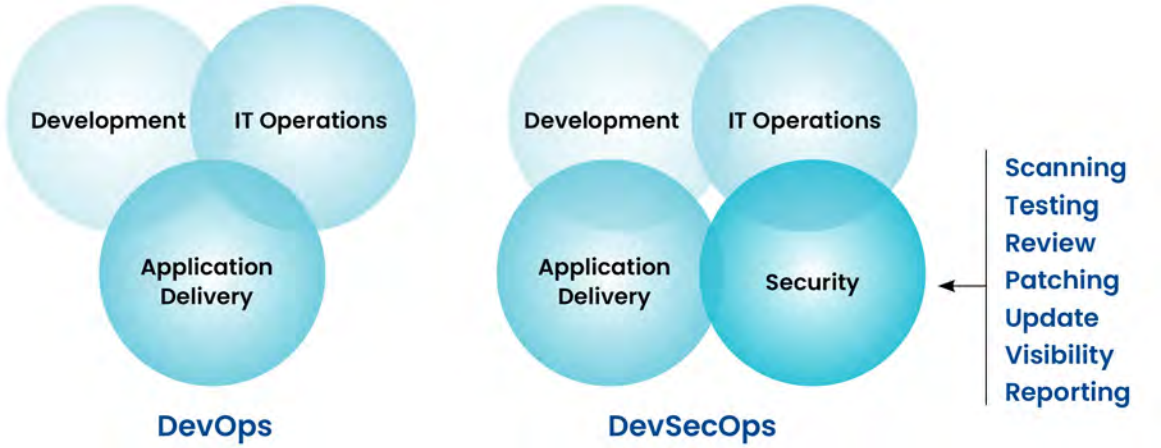


Figure 1. DevOps versus DevSecOps

The security threats that emerge in modern DevSecOps can be mapped to all phases of the SDLC process. For example, malicious insertions might be introduced during coding updates – and this requires controls to deal with rogue developers. At the other end of the DevOps process, malicious actors might degrade an application in production environments through their access to the underlying run-time system. This must also be mitigated.

The result is that security engineers have now realized that the best underlying framework for identifying and addressing security threats to applications is the broad DevOps lifecycle. This is good news because it covers all aspects of potential attacks, but it is also challenging news because the breadth of DevOps coverage demands that many different types of cyber security controls be deployed and administered.

VISIBILITY AND MANAGEMENT IN DEVOPS

Legacy applications have been protected in traditional data centers using a range of cyber controls that can be viewed roughly as preventive, detective, or reactive. All these security controls depend on the ability to achieve visibility into both static and dynamic aspects of the applications. This includes identifying software configurations and observing software behavior. Comparison to an expected profile can then drive insight into determining security posture.

Traditional cyber security controls also depend on the ability to manage the application and its associated run-time environment. This is done with familiar security methods such as endpoint controls, security information and event management (SIEM), next generation firewall (NGFW) and so on. Frameworks such as NIST 800-53 provide application and security teams with guidelines on how such controls should be arranged in the typical corporate data center.

With the shift to multi-cloud, however, these controls also shift. Thus, rather than using a scanner to probe monolithic apps in a physical data center, modern environments involve containerized workloads, orchestrated with Kubernetes, and secured through modern methods such as cloud security posture management (CSPM), secure access service edge (SASE), and endpoint detection and response (EDR).

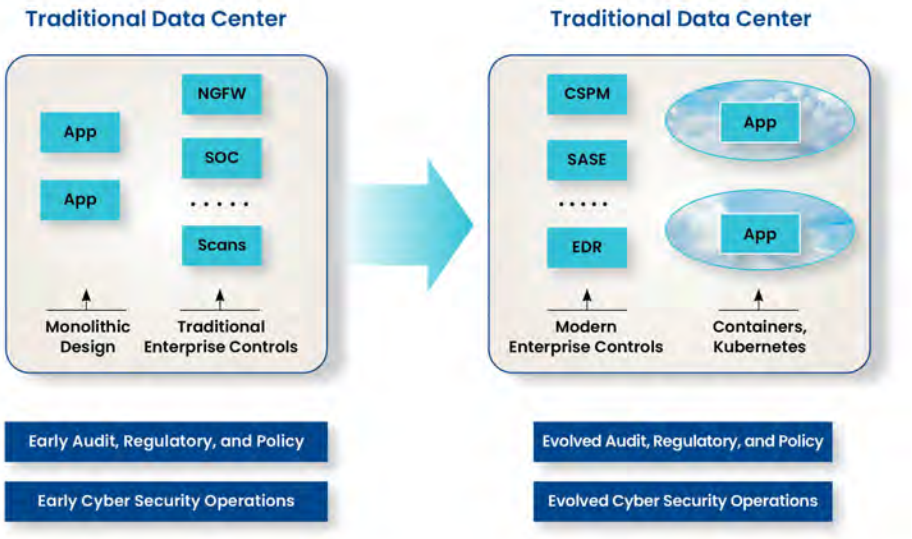


Figure 2. Shift in Controls from Legacy Data Center to Public Multi-Cloud

Security engineers have typically categorized modern cloud security controls into two main groupings: Controls that collect data for posture visibility, and controls that take mitigation action to prevent threats. Such combination of active and passive security results in an effective means for optimizing security posture – but deployment can be challenging. Combining the best open-source tools with commercial support requires selecting the right mix of partners.

Perhaps the greatest change that comes with the shift to multi-cloud is that both active and passive controls for hosted apps in multi-cloud environments have had to evolve. In the next section, we will examine a commercial platform from Sysdig that was designed with this shift in mind. The goal is to create an evolved architecture that can support both compliance and cyber security obligations for the modern enterprise.

OVERVIEW OF SYSDIG PLATFORM

The commercial Sysdig DevOps platform was developed for modern software development environments that are using containers, Kubernetes, and hybrid cloud infrastructure. The platform is built on an open-source tool called Falco[2], which provides run-time detection, and an open-source tool called Prometheus[3], which provides application and Kubernetes monitoring. Sysdig combines these open-source tools with commercial support capability.

Sysdig Secure Architecture

The Sysdig platform includes a front-end agent that is integrated into the host environments in which containers and orchestration are performed. This front-end feeds metadata, event, and other information to the Sysdig Engine, which in turn provides event information to the security information and event management (SIEM) platform and notification to workflow. Sysdig APIs support integration with additional tools including open-source capabilities.

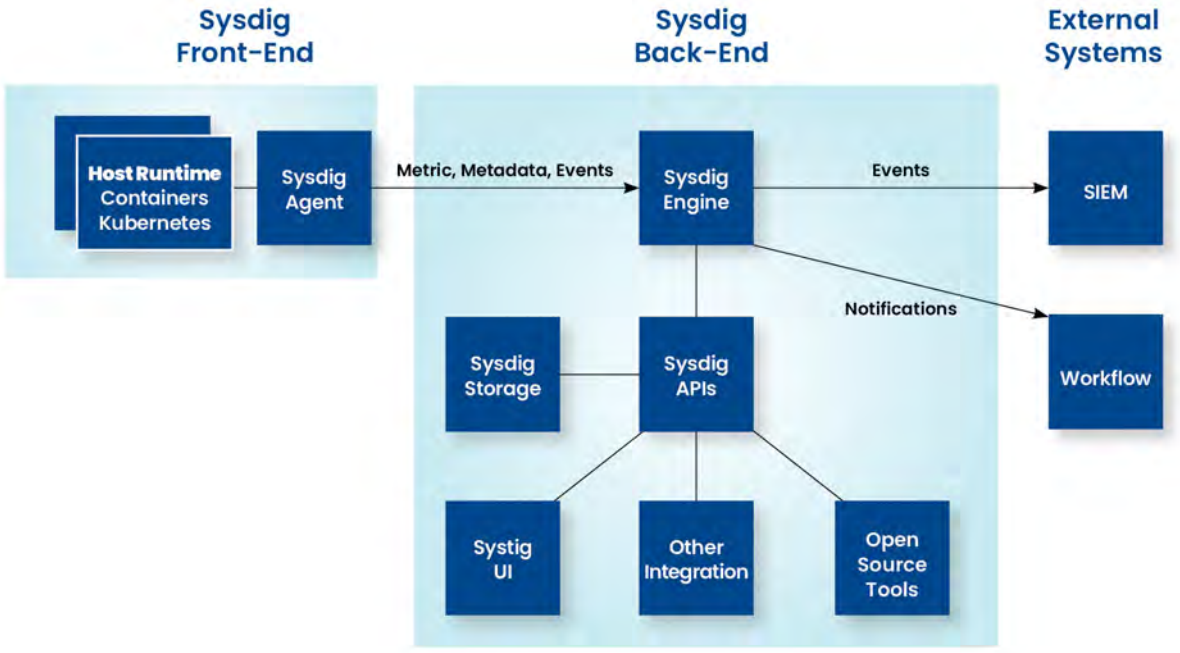


Figure 3. Sysdig Architecture

The Sysdig platform includes a combination of major subsystems, features, and tools that are arranged in a flexible manner to support a variety of different local software process configurations. The way these functions work is that they integrated directly into the DevOps workflow to provide an accurate source of what is happening at a low level with the software.

- *ContainerVision* – This function supports deep visibility into containers, networks, applications, and systems by accessing system call activity. The objective is to support incident response and troubleshooting during DevOps.
- *ImageVision* – This function scans CI/CD pipelines and registries for vulnerabilities and misconfigurations. The objective is to block vulnerabilities and monitor for new CVEs in advance of production.
- *CloudVision* – This function consolidates cloud activity from logs such as AWS Cloudtrail into a single view. The objective is to support alerting on configuration changes to permissions, AWS buckets, and other cloud resources.
- *ServiceVision* – This function provides context for Kubernetes and cloud service metadata to support dashboards, metrics, and security status reporting. This also supports identifying the correct team to resolve a vulnerability quickly.

In addition, the Sysdig platform integrates with open-source tools that are widely used for troubleshooting cloud application and low-level software issues.

- *Cloud Custodian* – The open-source CloudCustodian rules engine is designed to reside within a workload environment to offer asset discovery and static configuration insights into assets such as cloud APIs across accounts in AWS, GCP, and Azure. CloudCustodian identifies misconfigurations such as exposed AWS S3 Buckets and validates compliance.
- *VulnDB* – The Sysdig vulnerability scanner uses its VulnDB resource[4] which includes details on thousands of vulnerabilities to provide inline scanning for workloads such as AWS Fargate or Amazon Elastic Container Repository (ECR). This scanning support is also essential for both cyber threat avoidance and cloud compliance reporting.
- *Falco* – The open-source Falco tool is used in the context of a Sysdig Secure deployment to help investigate vulnerabilities and threats from users, workloads, or services in the local environment. Falco provides cloud activity logs that offer context for the overall Sysdig Secure protection.

Sysdig Capabilities

The Sysdig platform provides DevOps teams with a variety of important security capabilities for their workload applications hosted in AWS, GCP, and Azure. These capabilities, which include asset discovery, cloud security posture management, and threat detection, are not only useful for avoidance of cyber threats during the entire software process, but also for establishing compliance in hybrid multi-cloud environments using data rich reporting screens.

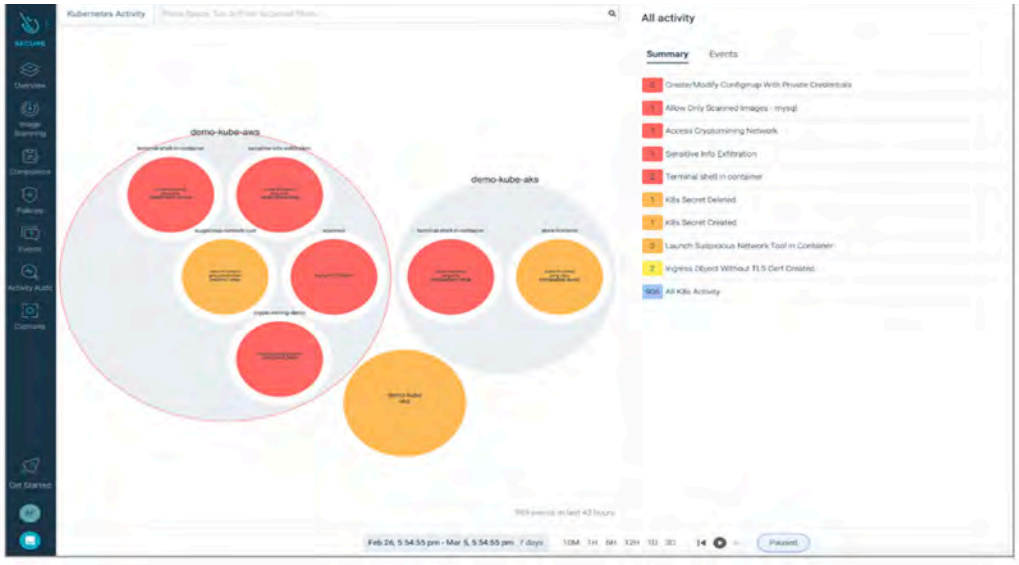


Figure 4. Sample Sysdig Reporting Screen

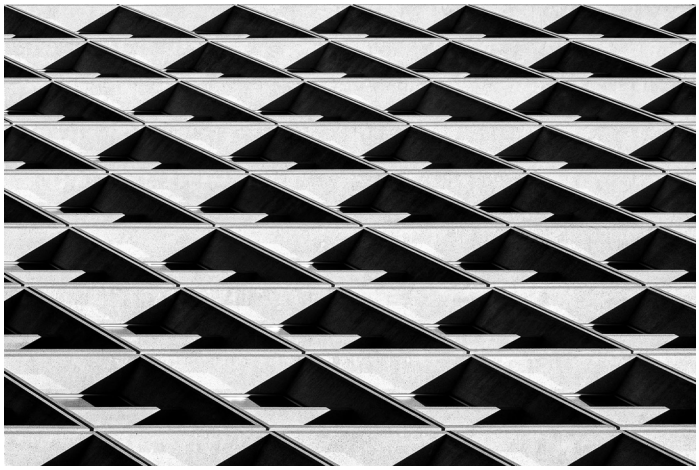
PROPOSED ACTION PLAN

For DevOps teams who seek to improve the cyber security of their runtime environment, it is recommended by the TAG Cyber analyst team that the following management steps be initiated immediately:

Step 1: Inventory Current SDLC Security
It is useful to review existing security tools being used to secure the current DevOps environment. This should include both functional capabilities as well as any procedural controls. Particular attention should be placed on whether effective metrics can be derived from these existing security capabilities.

Step 2: Review Security and Compliance Requirements
The next step is to review existing and expected security and compliance requirements. This will differ between different business sectors and sizes of the organization. Regulatory environments will have particularly intense security and privacy requirements in emerging hybrid cloud infrastructure.

Step 3: Review Commercial and Open-Source Options
The third step is to systematically review options for improving DevOps security using both open-source tools such as Falco and Prometheus and commercial solutions such as the Sysdig platform outlined in this report. TAG Cyber analysts are always available to assist with such commercial solution review and selection.



DISTINGUISHED VENDORS

TAG CYBER

DISTINGUISHED VENDORS

Q 1 2022

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

Abnormal

Abnormal Security protects organizations from the email attacks that matter most so they can focus on other business initiatives. Abnormal integrates with Microsoft or Google in minutes, with no disruption to the mail flow to protect you from business email compromise, supply chain fraud, account takeovers, ransomware, and other advanced email attacks.

AaDya

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

allot

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

ARISTA

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

TAG CYBER DISTINGUISHED VENDORS

2022

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

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

CyCognito provides an SaaS platform that goes beyond external attack surface and vulnerability management to continuously monitor, detect and remediate risk in an organization's IT ecosystem. Founded by veterans of national intelligence agencies, CyCognito prioritizes threats based on their business impact in order to preempt security breaches and eliminate exposure.

CyberGRX standardizes third-party cyber risk management, allowing for insights, risk prioritization, and smarter decision making across your vendor ecosystem. Driven by sophisticated data analytics and automation, real-world attack scenarios, and real-time threat intelligence, CyberGRX provides comprehensive and ongoing analysis of vendor portfolios so customers can effectively manage their cyber risk reputation.

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

Efani is a secure mobile service with an encrypted SIM Card that protects cell phone accounts from potential SIM Swap vulnerabilities, eavesdropping and location tracking. Using rigorous identify verification and offering 24/7 tech support, Efani defends potential victims from phone hacking and cybercrimes by delinking personal information and encrypting data.

TAG CYBER DISTINGUISHED VENDORS

2022

Elisity helps companies redefine security and access in a world of cloud, mobility, and connected devices. Its platform, Elisity Cognitive Trust, combines zero-trust network access and an AI-enabled software-defined perimeter, allowing enterprises to proactively protect their data and assets while ensuring secure access to any application or device, by any user, from anywhere.

Fortinet offers advance threat protection through an integrated mesh platform security fabric that provides consistent surveillance across extended digital attack surfaces and deployments. Used by a wide range of industries from health care to finance, Fortinet ensures seamless interoperability, visibility and control, and guarantees network, application, platform and endpoint security.

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

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

Immersive Labs is a unique cybersecurity human training platform that goes beyond generic training and certification to prepare companies internally for emerging cyber threats. Using myriad crisis simulations, gaming and creative role playing, Immersive provides practical and relevant content, teaching personnel how to become expert detectors and mitigators of cyber risk.

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

TAG CYBER DISTINGUISHED VENDORS

2022

RISKIQ®

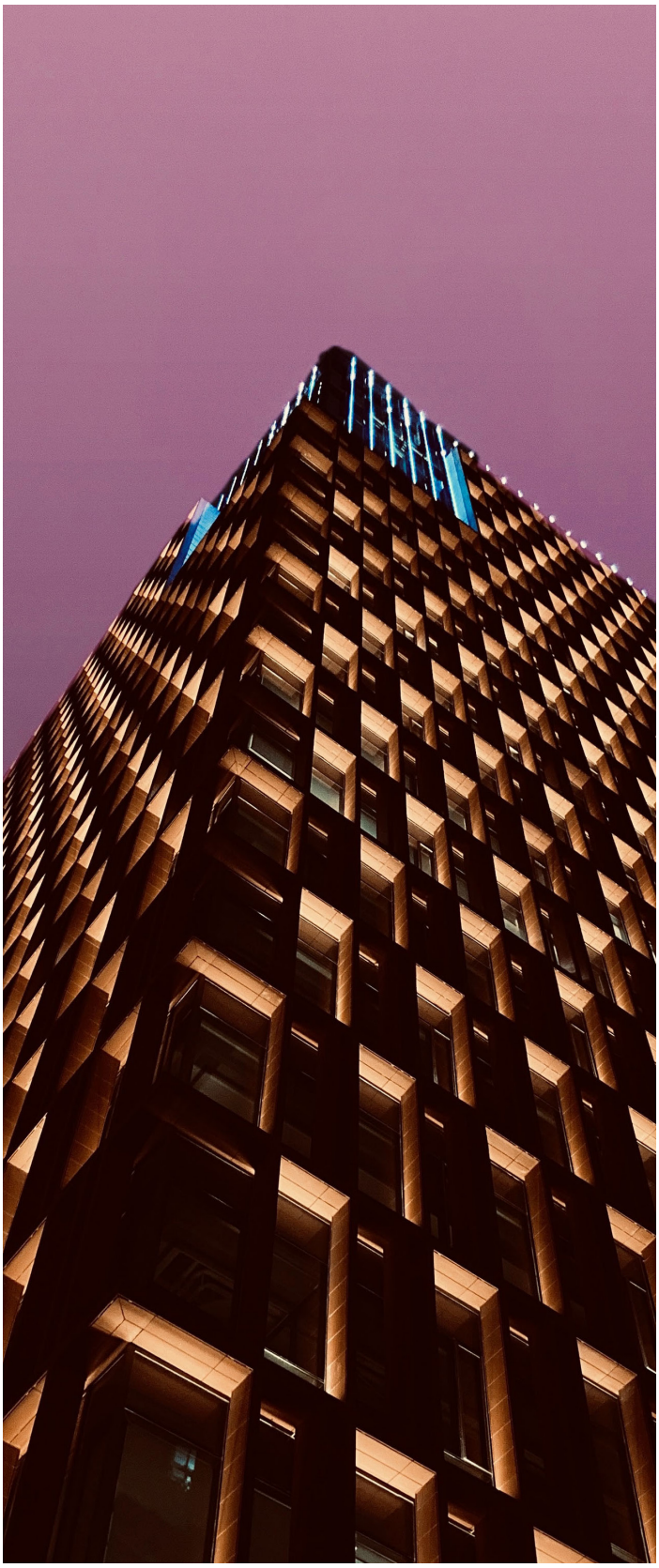
RiskIQ maps threat intelligence on a global scale through multiple automated discovery and continuous scanning platforms that secure an enterprise's attack surface. Composed of former NSA and intelligence officers, the RiskIQ Service team delivers precision-focused monitoring of a company's digital security, mitigating exposure by fingerprinting, detecting and thwarting cyber risk.

ivanti

Ivanti protects IT landscapes from cloud to edge with Ivanti Neurons, a cloud-based platform that finds, repairs and protects all devices automatically wherever teams are located, giving companies the ability to streamline management by modernizing a VPN deployment and transforming into a Zero Trust design, thereby achieving fast vulnerability remediation.

semperis

Semperis is an identity driven protection platform with a multipronged Active Directory Protect and Recover approach. True to their mission to be "Always Ready," Semperis continuously monitors hybrid systems for exposure indicators and is able to restore operations in record time if a ransomware or wiper attack infiltrates domain controllers.



TAG CYBER DISTINGUISHED VENDORS

2022

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

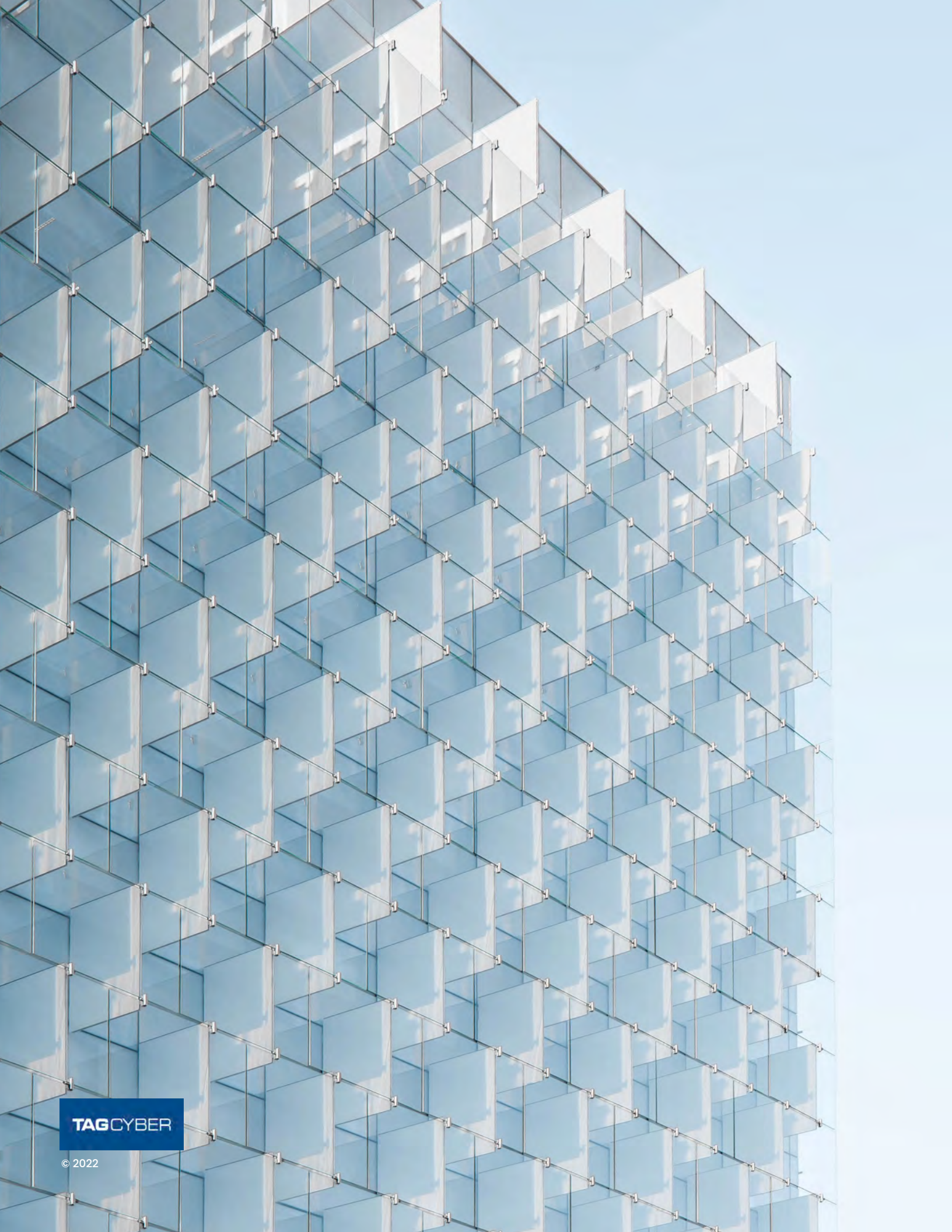
Sysdig is a software-as-a-service platform built on an open-source stack. Its Secure DevOps Platform provides security that lets clients confidently run containers, Kubernetes, and cloud services — allowing them to secure their build pipeline, detect and respond to runtime threats, continuously validate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

Tracker Detect protects every enterprise application against insider threats using a nine step TrackerIQ process which includes detection of anomalies via a patent pending activity flow clustering engine. The platform's seamless integration provides unmatched accuracy with activity flow analytics, allowing for automatic, swift and accurate detection and response to any application.

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

Varonis uses Metadata Framework technology for transparent, continuous collection and analysis of information within a company's data stores and perimeter devices. Constructed by cybersecurity experts with expertise in advanced analytics, the Varonis all-in-one Data Security Platform uses automation to massively reduce risk and sophisticated detection that monitors every file to preempt cyber and ransomware attacks.

Replacing standard firewalls with state-of-the-art, hardware enforced products, Waterfall Security Solutions protects major global infrastructure control systems from sophisticated ransomware attacks. Waterfall's Unidirectional Security Gateways enable IDS sensors and security monitoring systems to connect simultaneously to both IT and OT networks, with no risk of compromise to utility or rail industry power grids.



TAG CYBER