[+] (IN)SECUREMagazine

06 | 2019
ISSUE 62

Modern threat landscape

What's your company's risk exposure?

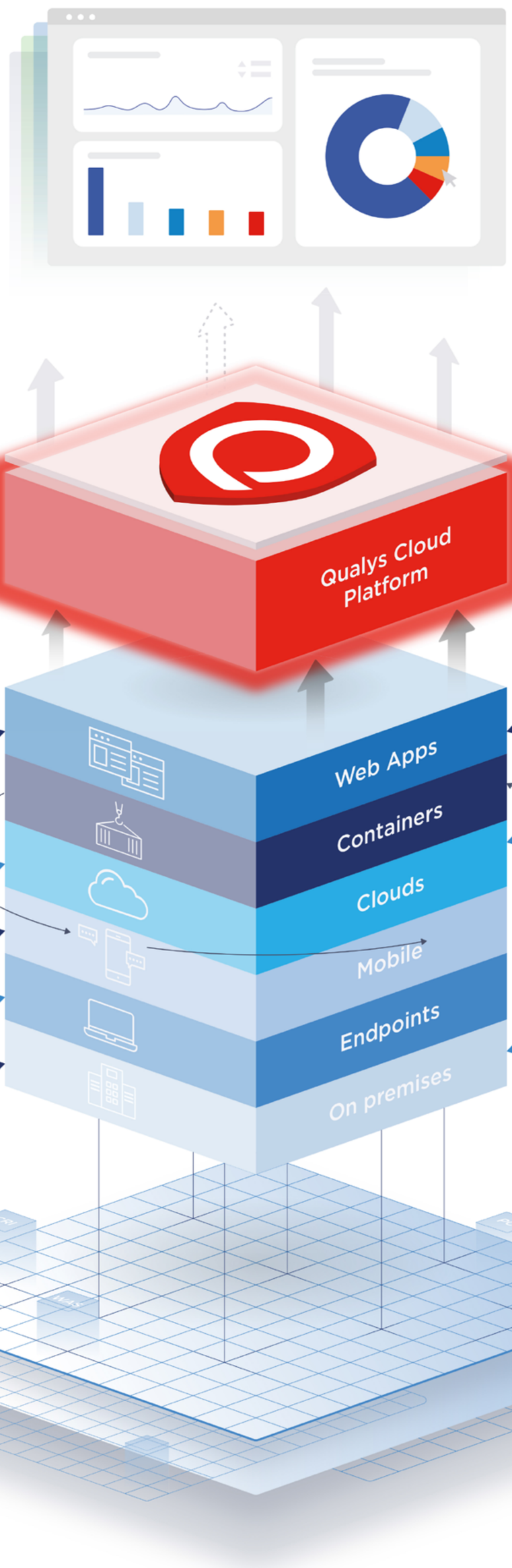
Building a modern data registry: Go beyond data classification

What happened to trust and transparency in cybersecurity?

One stack to secure your digital transformation.

THE POWER OF THE QUALYS CLOUD PLATFORM:

- 2-second visibility across all your global IT assets
- Continuous assessment of your security and compliance posture
- Identify zero-day vulnerabilities and compromised assets
- Automatically patch and quarantine assets
- See the results in one place, in real time
- Drastically reduce your spend



Try it free, unlimited scope, at qualys.com/trial

Qualys®

Table of contents

PAGE 04 — What's your company's risk exposure?

PAGE 08 — The modern threat landscape and expanding CISO challenges

PAGE 12 — Product showcase: Veriato Cerebral user & entity behavior analytics software

PAGE 15 — SECURITY WORLD

PAGE 23 — Building a modern data registry: Go beyond data classification

PAGE 31 — What happened to trust and transparency in cybersecurity?

PAGE 35 — Prioritising risks in a climate of geopolitical threats

PAGE 38 — INDUSTRY NEWS

PAGE 50 — An intelligence-driven approach to cyber threats

PAGE 53 — Is curiosity killing patient privacy? Combatting insider threats in the healthcare contact center

PAGE 57 — EVENTS

PAGE 58 — Protecting applications against DFA attacks

PAGE 60 — The SEC demands better disclosure for cybersecurity incidents and threats

Contributors

GARY E. BARNETT, CEO, Semafone
MIKE BURG, Director of Strategic Advisory, Alagen
SAM KERR, Senior Director of Product Management, Arxan
ROB SCOTT, CEO & President, Cygilant
DIMITRI SIROTA, CEO, BigID
MALCOLM TAYLOR, Director Cyber Advisory, ITC Secure
GRANT WERNICK, CEO, Insight Engines
GENE YOO, CEO, Resecurity

Visit the magazine website and subscribe at www.insecuremag.com

Mirko Zorz
Editor in Chief
mzorz@helpnetsecurity.com

Zeljka Zorz
Managing Editor
zzorz@helpnetsecurity.com

Berislav Kucan
Director of Operations
bkucan@helpnetsecurity.com

What's your company's risk exposure?

AUTHOR_ Mike Burg, Director of Strategic Advisory, Alagen

Capturing data is critical to effectively measuring your risk, but data collection alone is not a security metrics strategy.

Imagine the parents of a child who is allergic to peanuts looking at the information written on the wrapper of a candy bar. It would be excessive for them to study the calories, sugar content, physical size, weight, brand, number of followers on Instagram and look for an USDA Organic label. What really matters most is if it has peanuts in it. Without first establishing what metrics are important to your organization, you'll end up buried in numbers without any context or understanding to guide any meaningful analysis.

It's very important to clarify the context and assumptions being made when establishing your metrics strategy.

Harness the power of assumptions

Envision you're camping and your winter coat has a huge rip in it. How big is the risk of you suffering hypothermia? The answer depends. What month is it? Are you in Antarctica or Arizona? Do you also have a low-temperature-rated sleeping bag? This is context, and it's imperative. We can't conclusively identify a single component of risk when context and assumptions are undefined. We wouldn't know if events are significant, measurable, or repeatable.

> *Start with a goal for the security program. Next, determine what questions need to be answered to achieve the stated goal. Finally, determine what metrics would answer those questions.*

Security vulnerabilities within your organization may include weak database encryption, outdated operating systems, unpatched software or poor password hashing. Without the context (knowing the controls, the likelihood and impact of a security event, the prevalence of threats) you can't gauge risk effectively. Therefore, it's very important to clarify the context and assumptions being made when establishing your metrics strategy.

Focus on measurement principles

Simple decisions can make or break the effectiveness of execution. This is where we consider what's most important in how to take measurements to achieve accurate assessment. Focus on:

- Probability, not possibility - What's most likely to happen vs. everything that could happen?
- Relative accuracy, not precision - It's better to make estimates and achieve relative accuracy than aim for precision and be wrong.
- Objectivity - Subjective measuring leads to inconsistent results. Be as objective as possible.
- Calibrate for the human element - Humans are… humans. Plan for it.

Security metrics are business metrics

A winning security metrics strategy will always align with the business's goals and objectives. Only by considering these things can we pinpoint a security metrics strategy that accurately assesses the risk.

Let's start with what we can measure. Data can be divided into two categories: empirical, quantitative data and experiential, qualitative data.

There is often confusion between the two approaches. Each has its benefits, and neither is better nor worse than the other. They often answer different questions, so it's vital to choose the correct one for each query. Both may play an important role in the execution of your security metrics strategy.

A method I like to use for measurement is Goal-Question-Metric (GQM), an approach created by Victor Basili. Start with a goal for the security program. Next, determine what questions need to be answered to achieve the stated goal. Finally, determine what metrics would answer those questions.

Here's an example of how the GQM strategy works:

Imagine that a user browses to *mywebmail.wolf-in-sheeps-clothing.com* and inadvertently clicks on a malicious link embedded in the page. A malicious file is downloaded and installed on the user's computer. The infected computer utilizes the network for internal data exchange and begins to exfiltrate company PII to a command and control server at *mywebmail.wolf-has-your-data.com* on port 1234.

How can we use GQM to ascertain the vulnerability associated with this scenario?

Goal statement: Understand the risks of sensitive data loss from “crimeware” by analyzing the implementation of the security control set from the perspective of the end-user.

This is a well written goal statement as the objective is clear. That said, we can minimize subjective interpretation by defining a few terms.

Sensitive data:

- Company data labeled as “internal” or “confidential”
- Any company PII.

Crimeware:

- Opportunistic in nature, financial motivation
- Frequently affects consumers and is where “typical” malware infections will land.

Next, break down the scenario to determine what questions must be answered to achieve your goal. As a rule of thumb, you’ll want to think about and utilize industry recognized data where possible. You’ll also want to identify defensive security controls related to the scenario: OS patching, egress firewall rules, anti-virus, and administer rights all would make sense here.

> *Regardless of the desired metrics, when it comes to locating data to measure, there’s no shortage of potential sources.*

Appropriate simplification of the analysis enables us to move forward swiftly and not get lost in the minutiae that could make measurement unnecessarily complex.

Document assumptions:

- Security controls are effective/efficient
- Security controls are weighted equally
- Value of corporate data is weighted equally
- Time period over a year (frequency).

Once we have defined a goal and clarified the assumptions and potential components that relate to our scenario, we need to **determine the questions that need to be answered.** Our outcomes may include:

1_What type of devices are on the network?

2_Where does the sensitive data reside?

3_Who has access to the sensitive data?

4_How many devices are utilizing the current security control set?

5_How many crimeware help-desk tickets are there per year?

Now continuing down the framework, **what can we measure to answer the defined questions?**

1_Number and type of devices on the network

2_OS and distribution of devices on the network

3_Number and type of approved applications on workstations

4_Number and type of devices up-to-date on OS patches

5_Number of devices up-to-date on application patches

6_Number of active users and user accounts

7_Number of help-desk tickets associated with a "crimeware" event

Data sources & analytics: Quantifying risk

Regardless of the desired metrics, when it comes to locating data to measure, there's no shortage of potential sources. You might use Active Directory, DHCP, DNS, vulnerability scanners, OS/application patching servers, network/security devices, identity and access manager/authentication stores, etc.

Understanding an organization's risk is critical. Only with a well thought-out security metrics strategy will you avoid collecting irrelevant data and drawing questionable conclusions.

Utilizing the data gathered across all of your program goals, consider vulnerable asset value and loss probabilities to create a picture of overall risk. That's a book topic in its own right, but there are a few key guidelines to remember:

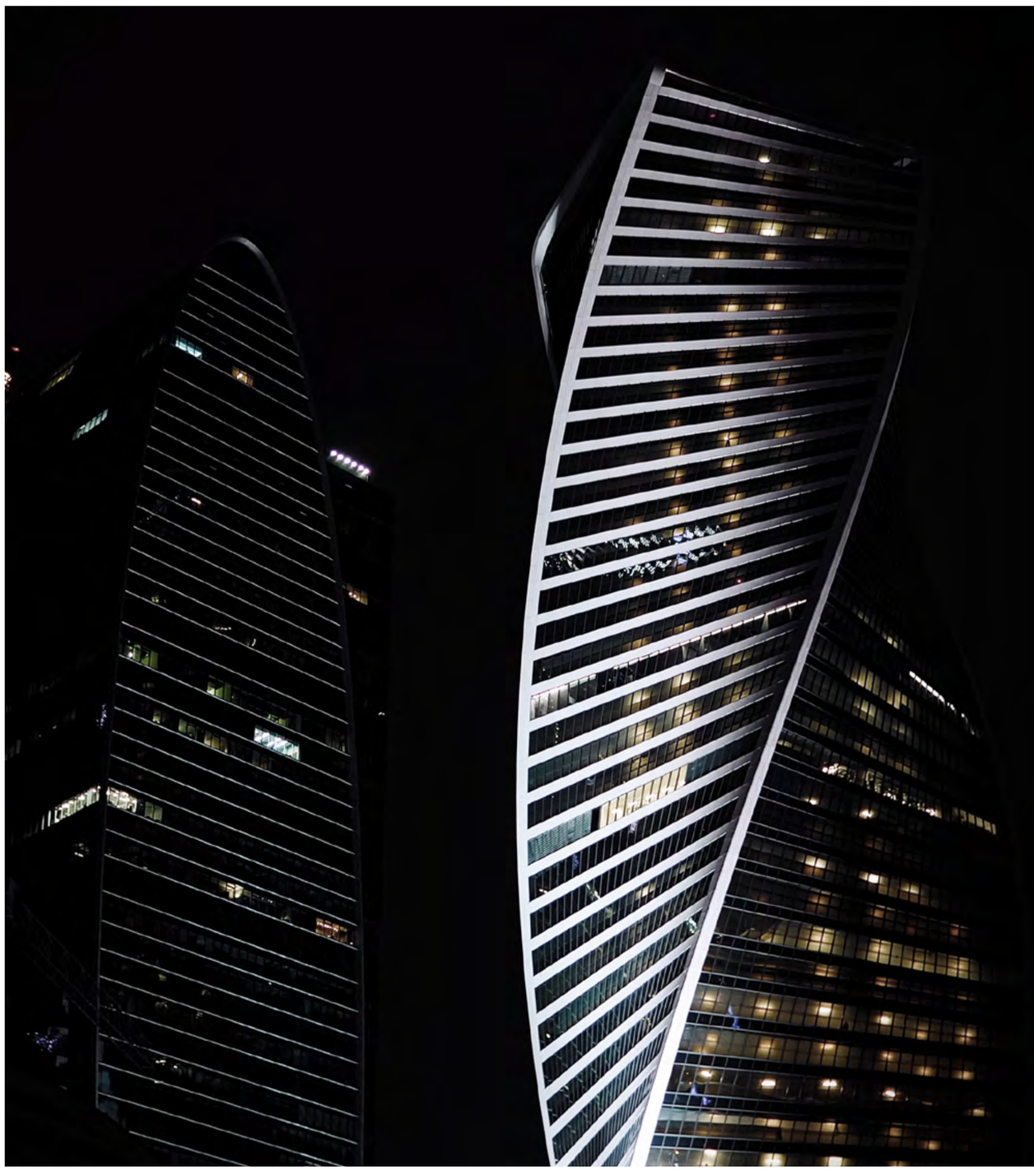
- Make your risk assessment scenario-based. This not only helps the focus remain on probable events, but also ensures that the right goals, corresponding questions, and appropriate metrics are considered.
- Ensure program-to-business alignment.
- Execute on a methodology for determining the nature and impact of the actual risk.
- Quantify risk with associated probable financial impact. This gives context to the risk assessment and can help guide any remediation strategy decisions.
- Prioritize security decisions and spend on empirical data. No longer are decisions made on gut feelings but are grounded in the findings of a more objective and repeatable process.

Building a winning security metrics strategy

Understanding an organization's risk is critical. Only with a well thought-out security metrics strategy will you avoid collecting irrelevant data and drawing questionable conclusions. Whether assessing risk on your own or with the help of external security specialists, utilizing a measurement framework ensures your data answers the critical questions about your security, and leads to meaningful analysis that can guide your security program.

Make the most of your measurements. Always check assumptions. Consider gauging implementation before sweating program efficiency. Use measurement principles and calibrate for the human element for metrics you can trust.

And if all of this feels overwhelming, start simple. This might seem like a lot, but understanding your company's risk exposure is critical, and you must start somewhere.



The modern threat landscape and expanding CISO challenges

AUTHOR_ Mirko Zorz, Editor in Chief, (IN)SECURE Magazine

Prior to starting Signal Sciences, its founders were running security at Etsy, and growing frustrated with existing legacy technology. So, they built their own.

For this interview with Andrew Peterson, CEO at Signal Sciences, we dig deep into hot topics such as modern CISO challenges and application security visibility. Prior to co-founding Signal Sciences, Andrew has been building leading edge, highly performing product and sales teams across five continents for +15 years with such companies as Google and the Clinton Foundation.

_ ***Information security has evolved quite a bit in the past decade. Based on your experience, what are the most significant security challenges for modern CISOs?***

CISOs have a huge responsibility to continually assess the security tools and processes they've put in place in their organizations to prevent a breach or cyber attack. That's a tall order in any organization: persistent attackers are constantly looking to find new vulnerabilities to exploit. With over 40% of all successful breaches caused by attacks at layer seven, the application layer, effective protection in production is no longer a "nice-to-have"—it's a must-have part of any security plan.

For this interview with Andrew Peterson, CEO at Signal Sciences, we dig deep into hot topics such as modern CISO challenges and application security visibility.

That said, the following challenges are the most relevant to embedding security within any organization's application development process to prevent an attack at the web layer:

Establishing visibility into how your apps are being attacked in production is paramount: you can't defend against what you can't see. It'd be great if developers made perfect code but the reality is no code is perfect or ever will be. So living with bugs and live vulnerabilities is the normal state for all security and engineering teams. Knowing where and how you're being attacked and if those attackers are succeeding is the only way you can mount an effective defense. Empower your team with this information so they can be proactive in responding to attacks before and as they occur.

A next-gen WAF or RASP like what we offer can protect web apps against account takeover, bad bots or business logic attacks where the attacker seeks to maliciously penetrate or otherwise leverage an app.

Security should be an enabler and not a blocker to development and operations teams. Once you establish reliable visibility into attacks, leverage it to help your teams prioritize their limited defensive resources instead of setting up security choke points in your SDLC. You're using tools like static and dynamic code testing and programs like bug bounty and penetration tests to generate lists of potential vulnerabilities and bugs. But instead of requiring developers to fix them immediately (which doesn't happen), evaluate where attackers are focusing their attacks and use that information to prioritize what bugs you ask your developers to prioritize. They'll more clearly see the need and urgency, you'll more effectively address real risks, and you won't be a blocker for launching new code. Everyone wins.

Leveraging the cloud and the opportunities to scale the business while securing the digital assets that will reside there is another issue many CISOs face. Whether you are transitioning legacy apps to the cloud or design and building cloud native apps, you'll need to put tooling in place to secure those applications that are the gateway to valuable data. The tool you choose for application security should also be flexible enough to protect apps run in legacy environments so you're not stuck with a point solution. While deploying apps to the cloud allows for scaling quickly, and thus serving a larger set of customers on an ongoing basis, it also widens the attack surface. A next-gen WAF or RASP like what we offer can protect web apps against account takeover, bad bots or business logic attacks where the attacker seeks to maliciously penetrate or otherwise leverage an app.

The fast-paced threat landscape is driving plenty of innovation in the cybersecurity industry, but businesses can struggle with the rate of technological change. What advice would you give to information security leaders that need to keep up with new developments but feel overwhelmed?

Industry news sources like Dark Reading and SC Magazine provide informed opinion and product reviews but can be limited in depth. I'd recommend subscribing to conversational style content like podcasts that can take the time to dig in on details and have the convenience benefit of being listened to at any time (commutes are my favorite). The Security Weekly podcasts hosted by Paul Asadoorian is a good example of high-value content that address specific subjects CISOs care about going beyond the surface level. Podcasts like Enterprise Security Weekly, Application Security Weekly and Risky Business are worth subscribing to and digesting for current trends and situations security teams have to deal with (disclaimer: myself and Zane Lackey of Signal Sciences have participated in these podcasts, but Paul has a variety of industry folks on to capture different point of views).

Outside of on-demand media sources, face-to-face meetups and local chapter meetings of industry groups like ISSA (Information Systems Security Association) can put a CISO in touch with folks with similar roles and concerns. We recently hosted the monthly ISSA-LA chapter meeting at Signal Sciences where a panel of experts shared their stories on how to establish security programs using the NIST and ISO frameworks.

Lastly, Gartner has a great tool for enterprise software evaluators and buyers called Gartner Peer Insights. It's like a Yelp for enterprise software where those who have evaluated not only the product but the organization behind the product leave reviews in their own words. We're in the web application firewall category and I'm glad to say we've done incredibly well by our customers as shown in those reviews.

We provide visibility into what's happening at the application layer wherever our customers deploy their apps.

_ *What do you see your customers most worried about and how do your products help address their concerns?*

It's a cliched word in security, but visibility into how and where adversaries will try to attack an organization's apps could mean the difference between a breach occurring and having to send out a breach notification: no CISO wants to do that. Those that have tried to use legacy WAF products repeatedly tell us they get little value from them—or that the maintenance burden does not justify such little return on the investment. In short, they want an appsec tool that both works and tells them what is happening so they either automatically block malicious requests or otherwise take action.

We provide visibility into what's happening at the application layer wherever our customers deploy their apps. We recently participated in the Cloud Native Security report where an astonishing 73% of the nearly 500 survey respondents said they lack actionable, real-time insight into threats and ongoing attacks in their production environments, including their apps in production.

We provide the necessary visibility at the application layer with both visual summaries and real-time alerts broadcast via popular DevOps tools like Slack and PagerDuty. We show the volume of attacks blocked and where in the app flow they are trying to maliciously manipulate customers' apps, APIs and microservices. For example, financial and e-commerce customers monitor key app interaction points like account registration, login and password resets. If traffic requests come from known-bad IP addresses or are associated with known indicators of compromise we collect from across our customer base, we can automatically block them. We can also alert customers on other request anomalies, log and alert on them and let the customer decide if they want to start blocking those as well.

_ *You say your Next-Gen WAF and RASP is designed to protect the modern web. How does it differ from other offerings out there?*

Legacy WAF offerings were not built for today's faster, more complex software development and deployment options. They offer protection, but due to the high maintenance and false positives, our customers who migrate from those legacy WAF offerings tell us they hardly run those products

We provide the best alternative to legacy WAF while offering the insights gained at the code layer with RASP.

in blocking mode in production. Our technology eliminates dependency on legacy WAF rules tuning while leveraging the code-layer instrumentation of RASP to gain detailed request and response data. We provide the best alternative to legacy WAF while offering the insights gained at the code layer with RASP.

The web application firewall market is very competitive. What makes the Signal Sciences WAF unique?

We designed and built our offering based on first-hand experience with legacy tools that didn't do what we needed them to do: protect the application where it resides without major maintenance overhead, all while providing the visibility I mentioned earlier. That's another problem with legacy WAF products: many are black boxes that tell you they found a matching pattern, but provide no context.

Our patented approach analyzes over 200 billion weekly production requests with no noticeable performance impact on the applications and APIs we help our customers protect.

At a high level, legacy WAF products were designed around static regexs—or pattern matching—to determine if a web request is good or bad. To expand the capabilities of a legacy WAF, the customer must dedicate full-time staff to developing, maintaining and testing rules on an ongoing basis to ensure they are still valid and work without breaking an app each time new code is released to production. And even with that dedicated person, the attack techniques vary over time, requiring an ever-growing ruleset. Now think about how many times per week and month a fully agile software team releases new code to production across various pieces of infrastructure—cloud, on-premise or a hybrid of the two—and you start to see the costly complexity required.

With Signal Sciences, there's none of that. We take a threshold approach to blocking so our customers can run our solution in full, automated blocking mode in production with virtually no false positives: 95% of our customers trust us to do just that.

With threshold blocking, we don't make a decision on each request like other legacy WAFs and RASP products, but instead look at suspicious payloads over time and with context to determine whether an actual attack is occurring. Our patented approach analyzes over 200 billion weekly production requests with no noticeable performance impact on the applications and APIs we help our customers protect.

Many of our customers tell us they do not dedicate a full-time staff person to our product. Instead, they rely on the out-of-the-box protection capabilities our technology provides that automatically protects their apps. Signal Sciences effectively becomes a reliable tool in their security arsenal dedicated to monitoring and detecting bad web requests and blocking them.

Our more advanced customers can utilize Power Rules that can be setup in our product console interface to provide more advanced protection. With Power Rules, they can enable rate-limiting rules around abusive behavior like content scraping and eliminate serving up content and resources to malicious users, potentially saving on infrastructure costs. And the same threshold-based approach can prevent malicious automated attacks via bots deployed to perpetrate application DDoS and account takeovers.

At the end of the day, we embed with our customers apps, APIs and microservices wherever they deploy them to provide this level of protection.

Product showcase: Veriato Cerebral user & entity behavior analytics software

When it comes to identifying and stopping insider data security threats, actionable insights into people's behaviors are invaluable. Employees involved in negative workplace events, contractors with access to critical systems and sensitive data, and departing employees all present elevated risks. Whether it's a true insider exfiltrating data, or hackers leveraging compromised credentials to become an insider, behavior patterns can indicate both emerging and immediate risks to your security.

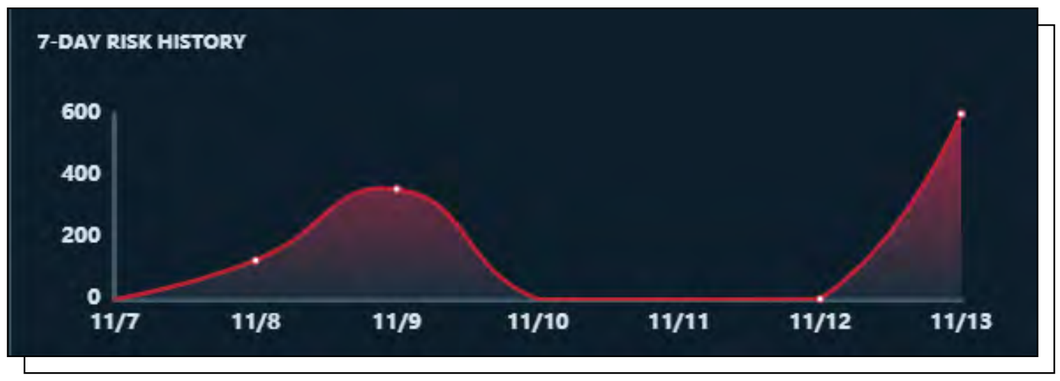
Veriato Cerebral user & entity behavior analytics (UEBA) software is a comprehensive threat detection solution that identifies risks and threats using a combination of machine learning, advanced statistical analysis and natural language processing to analyze both structured and unstructured data, and then automatically alerting the necessary stakeholders with videos and screenshots of the malicious-intent behaviors.

The result is an integrated view of normal, baseline behavior and anomalous activities, designed to augment traditional data loss prevention security measures and report upon findings to ensure 100% confidence when taking action.

Veriato Cerebral automatically builds and maintains user behavior baselines to discover normal patterns and process day-to-day variations.

Veriato Cerebral compares individual behavior patterns with group behavior patterns to determine commonalities and identify anomalous behaviors. Veriato Cerebral detects data movement anomalies including print patterns, email usage, and moving of information to shadow cloud-based apps and removable storage. It also watches for unusual log-in activity that indicates stolen credentials.

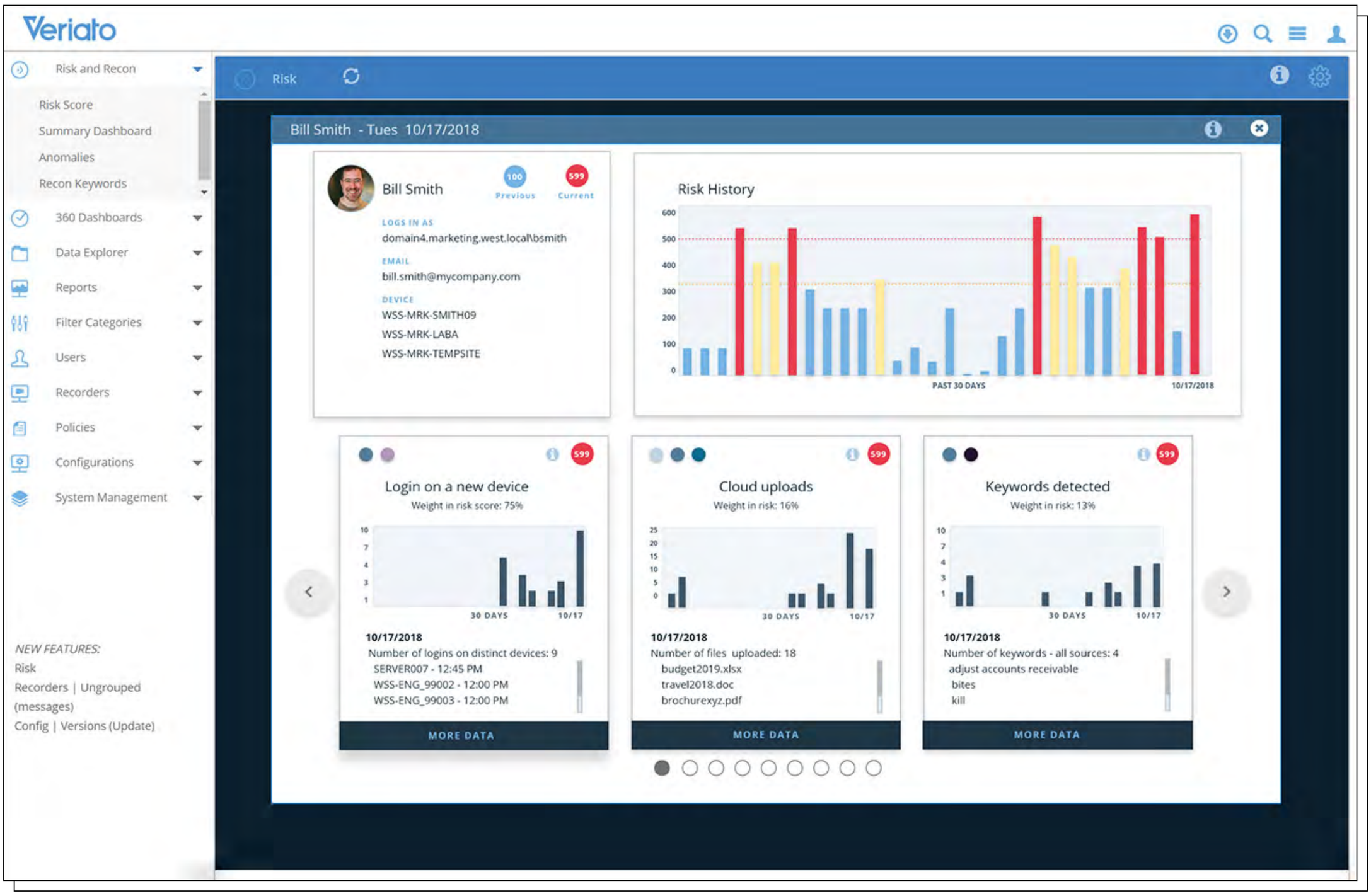
Alerts are generated when individuals deviate from their baseline behavior patterns, as compared with their historical selves, specific peer group, or a group of peers. Alert sensitivity can be adjusted easily.



When insiders attack, they most often do so from the endpoint. Veriato Cerebral employs an endpoint agent-based approach for continuous visibility.

Veriato Cerebral helps protect intellectual property, including source code and confidential business plans, by creating a system of record that supports best practices related to threats that exist when employees leave your organization.

Highly privileged user behavior is more closely inspected and monitored, even when in “normal user” mode. Veriato Cerebral evaluates behavior shifts in real time, so security teams can focus resources where they can be most effective.



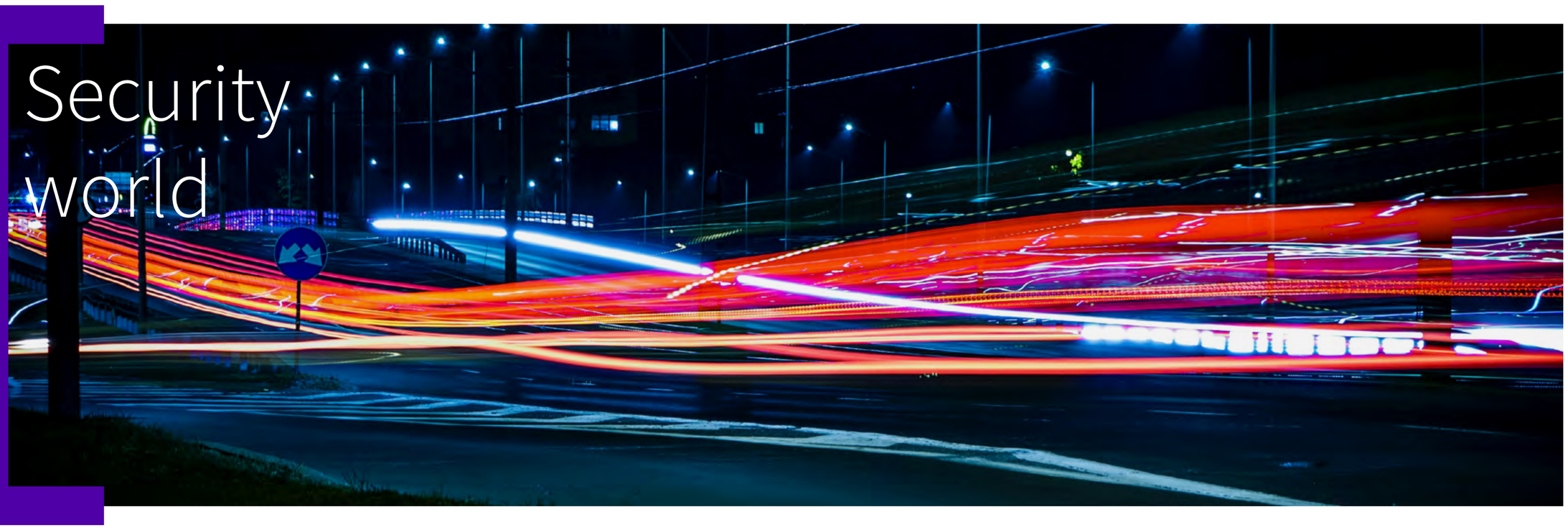
Veriato Cerebral creates a log of user activity to create early warning signs of attack, for rapid investigation and response. A distributed storage architecture keeps data secure and available without the expense and space needed for centralized storage.

Changes in the way people think, act and communicate often indicate insider activity. Veriato Cerebral analyzes your organization’s communications fabric for shifts in tone, intensity, pronoun usage and language patterns to help identify and prioritize threats.

Veriato Cerebral combines enhanced detection capabilities with deep, context-rich data for rapid, forensic-grade insight into what is occurring. The quantitative analysis is further supported by actual screenshots and playback video of the actions that raised flags in the first place.

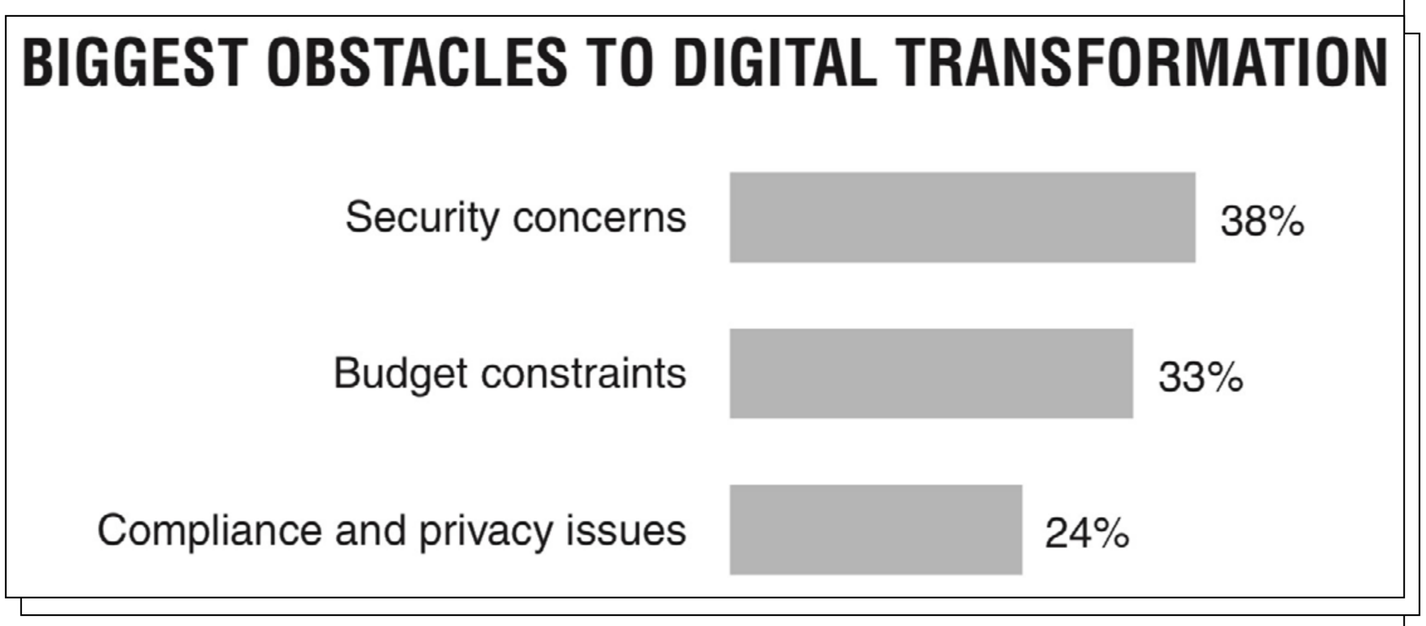
In today’s business world, people are your security perimeter. Protect yours by starting with a no-obligation Veriato Cerebral demo at https://www.veriato.com/products/cerebral-insider-threat-intelligence-platform

Security world



Traditional approach to data security hindering digital transformation initiatives

Security professionals who adopted a more traditional or reactive approach to their data protection and security program did not believe they would reach their digital transformation goals, according to a TITUS report.



The report, “The Vital Role of Security in Digital Transformation,” is based on a survey conducted by Market Strategies International of more than 600 IT decision makers at leading brands across a diverse set of industries in the United States, Canada and the United Kingdom.

The report highlights that more than nine out of 10 security professionals deploying a strategic approach to security believed their current efforts would address digital transformation needs within five years and that their organization would achieve its digital transformation goals in the next five years.

Most of these respondents held senior-level titles, with over half listing their title as Chief Information Security Officers (CISOs).

Conversely, only fifty percent of those leveraging a more traditional or conservative approach to their security initiatives believed their current efforts would address digital transformation needs in the next five years and that their organization would achieve its digital transformation goals in that same timeframe. While many of these respondents held more junior titles, a full third self-identified as CISOs.

How mainstream media coverage affects vulnerability management

Mainstream media is increasingly covering particularly dangerous, widespread or otherwise notable security vulnerabilities. The growing coverage has made more people aware of the risks and of the need to keep their various devices (software) up-to-date and, with the increased digitization of our everyday lives.

But among those people are also regulators and boards of directors who may demand their security teams do something about them immediately, even though they might be currently doing more important things than quickly patching a vulnerability that may or may not be critical to the company's security.

These urgent requests can sometimes be met and sometimes not. According to some of the CISOs and security analysts Tenable research analyst Claire Tills recently interviewed, when the security hole can be plugged easily, security teams might welcome the temporary disruption as an opportunity to score a quick "win" and show their value to the organization (even if the vulnerability is not critical).

But if the real risk of the vulnerability is lesser than it apparently seems, if there are no fixes or mitigations available, or if the patching process is expected to be difficult and time-consuming, enterprise security officers and their teams are in for a fight and a potentially great disruption of their activities and plans.

Most of the individuals canvassed by Tills used Meltdown and Spectre as an example of vulnerabilities that resulted in many headaches and derailments of vulnerability management programs. The news coverage was massive but not enough concrete information about the associated level of risk was available initially. Security teams first had to determine the risk involved, all the while being pressured to patch promptly. The patches were being released slowly and some were problematic.

Juggling all this while pushing back on the deadlines expected by higher-up executives and making them understand the real risk these vulnerabilities present to the company took a lot of effort. Still, there are positive aspects to all this: with every vulnerability that gains a high profile and gets noticed and forcefully prioritized by the higher-ups due to media coverage, defenders get better at evaluating the real risk of a vulnerability and communicating it to key stakeholders.

"While security teams are aware that media coverage is not an ideal measure of technical risk, they need to discuss their risk evaluation process with others. They also need to accept that the overall risk presented by a lower-severity vulnerability might require action," Tills noted.

Finally and most importantly, they must manage perceived risk and enable a measured response to vulnerabilities based on contextualization, rather than hype, she pointed out.

The largest breaches over the past three years have caused massive and irreparable damage

Publicly traded companies suffering the worst data breaches averaged a 7.5 percent decrease in stock price, a Bitglass report reveals.

Bitglass researched the three largest data breaches of publicly traded companies from each of the last three years in order to uncover cybersecurity trends and demonstrate the extensive damage that can be done by improper security. Among the incidents detailed in the Kings of the Monster Breaches report are the Marriott breach of 2018, the Equifax breach of 2017 and the Yahoo! breach of 2016.

The report explores the causes, repercussions and company responses for each of these preeminent breaches. Additionally, it recaps three of the most significant cybersecurity incidents that affected government agencies and private companies over the last three years.

The report's findings highlight the similarities between leading breaches and suggest that organizations have not been learning from the mistakes of their peers.

Key findings:

- The mean number of individuals directly affected by each breach was 257 million.
- To date, these breaches have cost their companies an average of $347 million in legal fees, penalties, remediation costs and other expenses.
- The average post-breach market cap decrease was $742 million (this excludes the outlier Facebook breach which lost $43 billion in market cap).
- It took an average of 46 days for the companies' stock prices to return to their pre-breach levels – Equifax's stock price still has yet to recover.

Companies investing in advanced forensic capabilities to identify attackers in greater detail

One in five companies are already using forensic investigations and other sophisticated methods to identify their attackers, like setting up honey pots and repositories of fake data to give attackers the idea they've hit real data while acting as a diversion tactic, according to Neustar.

Companies' growing investment in advanced forensic capabilities that can help identify attackers in greater detail is increasingly eclipsing what most law-enforcement agencies are willing to devote. 72 percent of respondents said their organization either already uses or would use honeypots or deception technology.

Furthermore, 71 percent of respondents would let hackers take the fake or booby-trapped document to gather counterintelligence – rather than shutting down an attack as soon as a bad actor engages with a deceptive file – in an effort to identify the thieves later or reveal information about the location, ownership and possible vulnerabilities of the hackers' machines.

Organizations face operational deficiencies as they deal with hybrid IT complexities

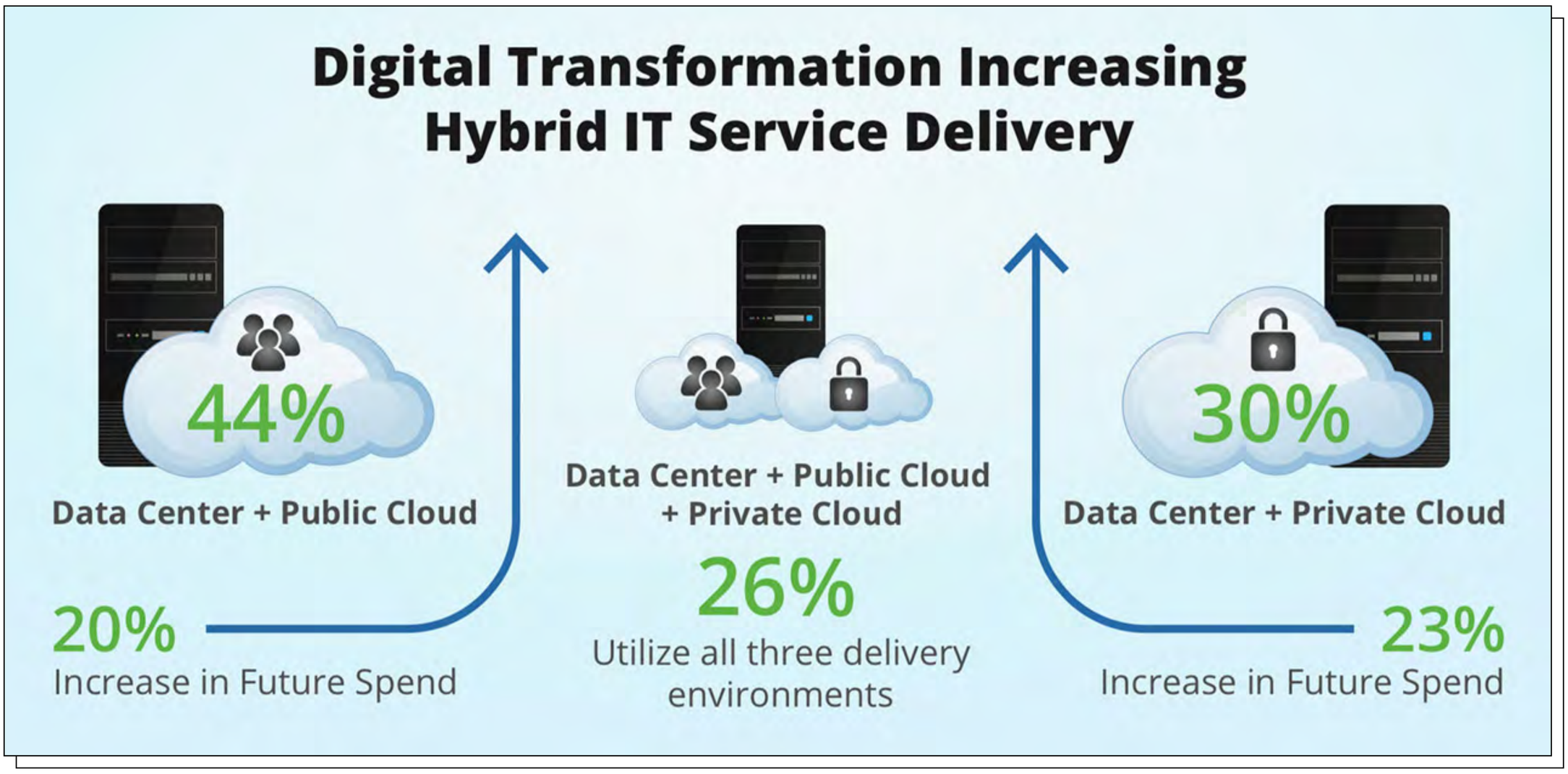
While enterprises are taking advantage of cloud computing, all enterprises have on-going data center dependencies, a Pulse Secure report reveals. One fifth of respondents anticipate lowering their data center investment, while more than 40% indicated a material increase in private and public cloud investment.

According to the "2019 State of Enterprise Secure Access" report, "the shift in how organizations deliver Hybrid IT services to enable digital transformation must also take into consideration empowering a mobile workforce, supporting consumer and IoT devices in the workplace, and meeting data privacy compliance obligations – all make for a challenging environment to ensure, monitor and audit access security.

"What was consistent across enterprise sizes, sectors, or location was that secure access for hybrid IT is a current and growing concern with cyber threats, requirements and issues emerging from many sources.

"The reporting findings and insights should empower corporate leadership and IT security professionals to re-think how their organizations are protecting resources and sensitive data as they migrate to the cloud," said Martin Veitch, editorial director at IDG Connect.

The survey found the most impactful incidents were contributed by a lack of user and device access visibility and lax endpoint, authentication and authorization access controls. Over the last 18 months, half of all companies dealt with malware, unauthorized/vulnerable endpoint use, and mobile or web apps exposures.



Most security pros have considered quitting due to a lack of resources

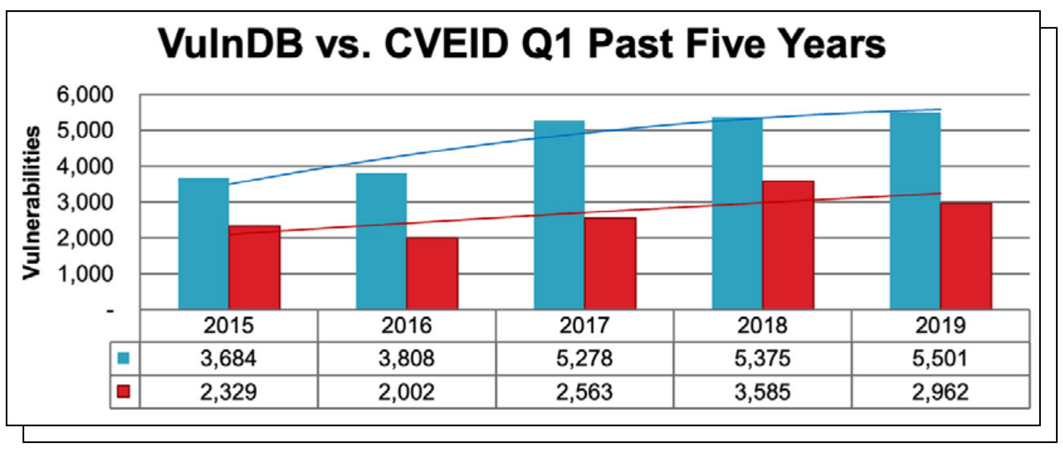
Companies are suffering from a lack of resources, both in terms of people and technology, and 72% have considered leaving their jobs for this reason, Censornet research reveals.

The survey found that security pros are not being helped by their security solutions. 65% want more technology but the average number of security products used is already 33% and 57% reported they are suffering from alert overload.

Ineffective cybersecurity technology was the joint second threat facing organizations, alongside unexpected/new cybersecurity threats such as new ransomware (both 47%). It was only beaten by cybersecurity staff shortages (50%). This makes bad technology a higher concern than human error (40%) and insufficient budget (41%).

"We can hardly be surprised that 74% of cybersecurity professionals describe themselves as "very busy", but it is worrying that technology isn't yet helping to solve the problem. In fact, it could be making it worse. The market has become saturated with point products – which is increasing cost and complexity and, as a consequence, reducing how effective they are," said Ed Macnair, CEO, Censornet.

Over half of all reported vulnerabilities in Q1 2019 have a remote attack vector



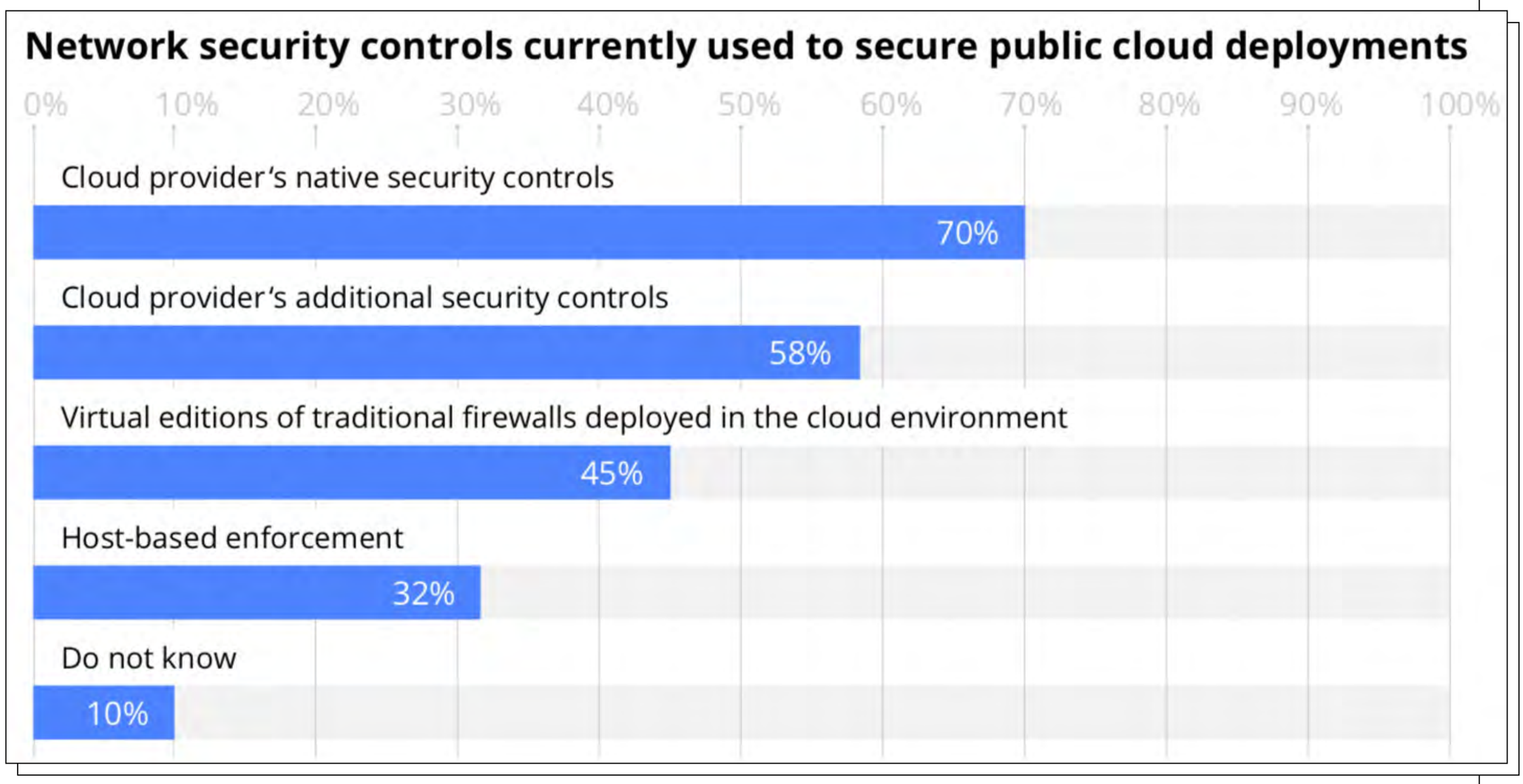
There were 5,501 vulnerabilities aggregated by Risk Based Security's VulnDB that were disclosed during the first three months of 2019. This represents a 1% increase over the same period in 2018, making this Q1 an all-time high. The results were released in the Q1 2019 Vulnerability QuickView Report. CVSSv2 scores of 9.0+, deemed critical issues, accounted for 14.0% of all published Q1 2019 vulnerabilities.

Risk Based Security's VulnDB published 2,539 (85%) more vulnerabilities than CVE/NVD in the first quarter. 45.8% of the vulnerabilities not published by NVD/CVE have a CVSS score of either 7.0 – 8.99 (high) or 9.0 – 10.0 (critical).

Just over half of all reported vulnerabilities in Q1 2019 have a remote attack vector followed by almost a third having a user-assisted or context-dependent attack vector. Unlike previous quarters, over 13% of the reported vulnerabilities require local access to a system or device.

While many are quick to dismiss local attacks as less risky, the increasing use of virtual technology and mobile devices may give an attacker a foothold on a device making local privilege escalation attacks more worrisome.

The security challenges of managing complex cloud environments



Holistic cloud visibility and control over increasingly complex environments are essential for successful deployments in various cloud scenarios, a Cloud Security Alliance and AlgoSec study reveals.

The survey of 700 IT and security professionals aims to analyze and better understand the state of adoption and security in current hybrid cloud and multi-cloud security environments, including public cloud, private cloud, or use of more than one public cloud platform.

"As companies of all sizes are taking advantage of the value of the cloud with its improved agility and flexibility, they are also facing unique new security concerns, especially when integrating multiple cloud services and platforms into an already complex IT environment," said John Yeoh, Global Vice President of Research, Cloud Security Alliance.

"The study findings demonstrate how important it is for enterprises to have holistic cloud visibility and management across their increasingly complex hybrid network environments in order to maintain security, reduce the risk of outages and misconfigurations, and fulfil audit and compliance demands."

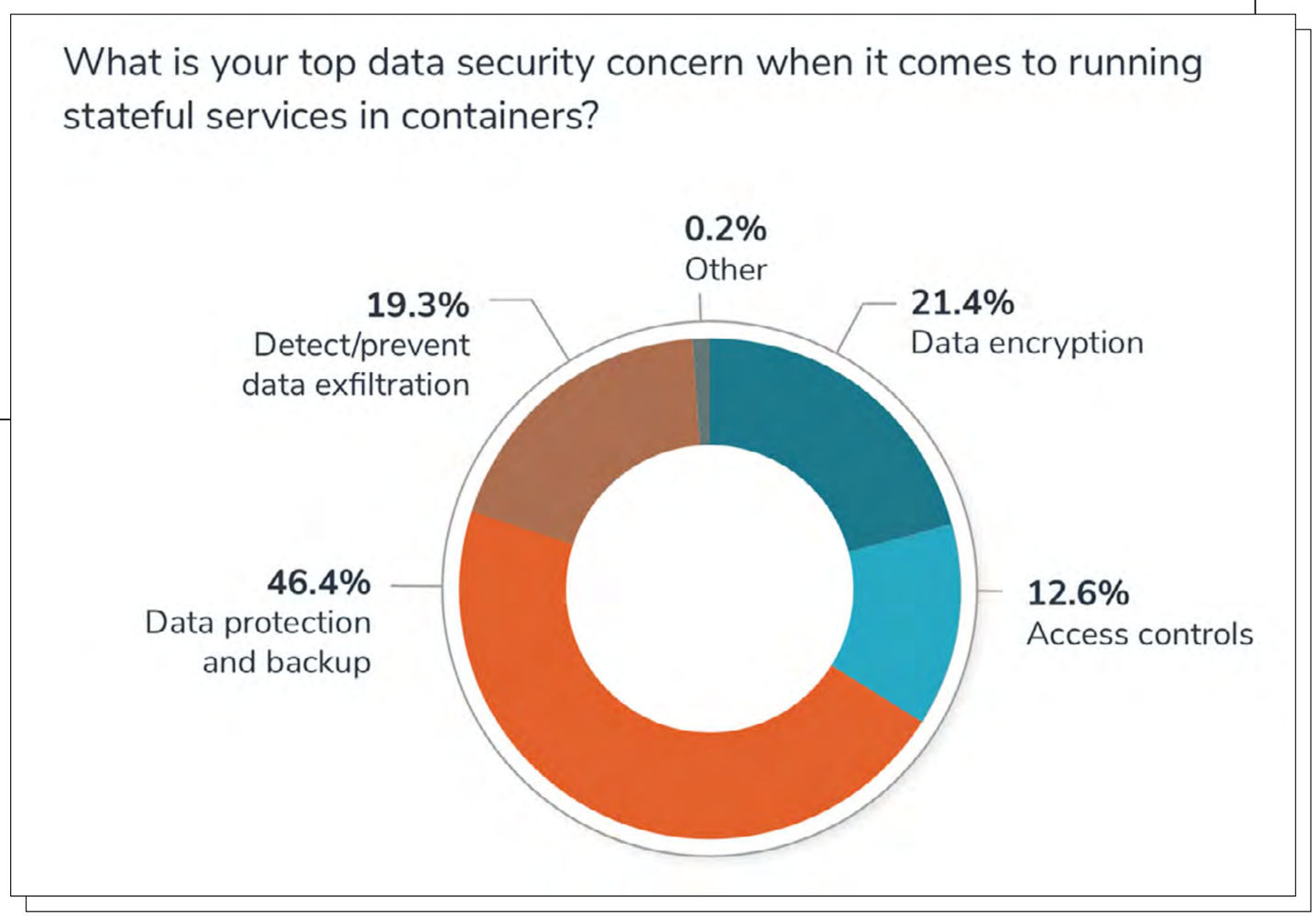
Companies increasingly investing in container adoption, security remains an issue

87 percent of IT professionals are now running container technologies, with 90 percent of those running in production and 7 in 10 running at least 40 percent of their application portfolio in containers — an impressive increase from two years ago, when just 67 percent of teams were running container technologies in production, a Portworx and Aqua Security survey reveals.

Yet despite their pervasiveness, containers aren't without hurdles: when asked to name their top challenges to container adoption, respondents most frequently cited security (51%), data management (40%) and cross-cloud/multiple cloud support (36%).

Other key findings:

- Organizations are making bigger investments in containers. In 2019, nearly one in five organizations is spending over $1 million annually on containers (17%). Compare this to just four percent in 2016.
- Data security tops the list of security challenges with a super majority of respondents (61%) listing this as their top security challenge, followed by vulnerability management (43%) and runtime protection (34%).
- For the third year in a row, increasing developer speed and efficiency is the primary driver of container adoption with 37 percent of respondents listing it as the top benefit.
- When asked which team bears the main responsibility for container security, most (31%) named the organization's security team, with a joint responsibility or DevSecOps in second place (24%). However, respondents' own roles influenced their answer, with 47 percent of DevOps respondents naming DevSecOps as the main owner and 54 percent of security respondents named security as the main owner.



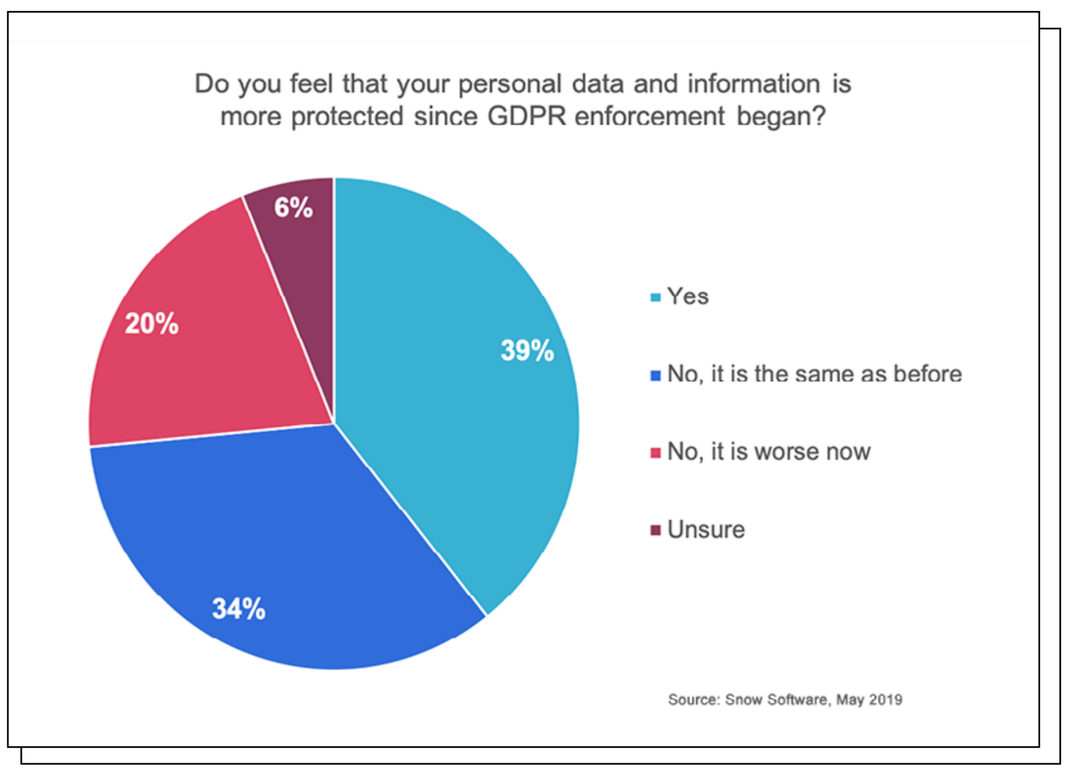
Most global workers noticed stricter policies at work as a result of GDPR

One year after GDPR went into effect, there are conflicting sentiments from the global workforce about whether the regulation has been effective, according to Snow Software.

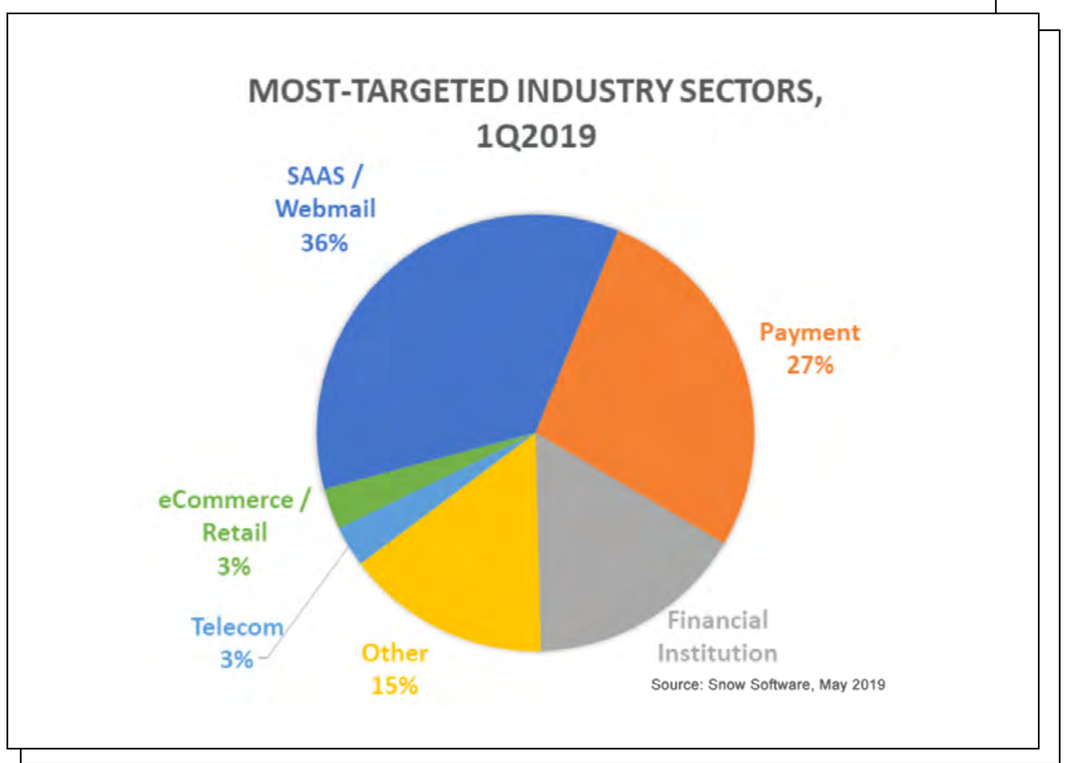
A new survey, which polled 3,000 professionals in the United States, Europe and Asia Pacific region, found that only 39% of respondents feel their personal data is better protected since GDPR enforcement began. Another 34% indicated that data protection seemed the same, while 20% are unsure and 6% actually believe their personal data is less protected than it was prior to enforcement.

This mixed response around the impact of GDPR likely reflects the complexity of educating the public on data regulations, as well as the difficulty that organizations still face in complying with the law.

According to the survey, 57% of global workers noticed stricter policies at work regarding the use of technology or customer data as a result of GDPR. Enforcement appears to have had the biggest impact in Europe, where 70% of respondents reported stricter policies, and at medium-sized businesses with 100 to 1,000 employees, where 65% of workers noticed policy changes.



Phishing targeting SaaS and webmail services increased to 36% of all phishing attacks



Users of Software-as-a-Service (SaaS) and webmail services are being targeted with increasing frequency, according to the APWG Q1 2019 Phishing Activity Trends Report.

The category became the biggest target in Q1, accounting for 36 percent of all phishing attacks, for the first time eclipsing the payment-services category which suffered 27 percent of attacks recorded in the quarter. Online SaaS applications have become fundamental business tools, since they are convenient to use and cost-effective. SaaS services include sales management, customer relationship management (CRM), human resource, billing and other office applications and collaboration tools.

“Phishers are interested in stealing logins to SaaS sites because they yield financial data and also personnel data, which can be leveraged for spear-phishing,” said Greg Aaron, APWG Senior Research Fellow.

Building a modern data registry: Go beyond data classification

AUTHOR_ Dimitri Sirota, CEO, BigID

Due to new privacy regulations - EU's Global Data Privacy Regulation (GDPR), the California Consumer Privacy Act (CCPA) and Brazil's General Data Protection Law (LGPD) - there is an increased urgency for organizations to understand what data they store and analyze. Security imperatives and pressure to extract more value from the information they store has also put pressure on companies to get data privacy right.

Historically, organizations invested in a variety of technologies to inventory their physical assets, but lacked adequate technology to find, map and inventory data assets.

Balancing the drive toward becoming a data-driven organization with the requirement of ensuring privacy-aware data governance has emerged as a crucial strategic concern.

After all, the challenge of becoming a data-driven organization extends beyond the practical considerations of how to automate the data pipeline and map data assets. They must also make sure that actions aimed at accessing, analyzing and sharing of their data are consistent with compliance, risk and privacy considerations.

Balancing the drive toward becoming a data-driven organization with the requirement of ensuring privacy-aware data governance has emerged as a crucial strategic concern. However, traditional data classification and cataloging tools simply lack the capabilities needed to find, map and inventory data assets accurately and efficiently at scale in the new age of GDPR and other privacy regulations.

> *A modern data registry cannot be a data warehouse – you'll simply be duplicating the data it maps and introducing limitations in scale.*

A data registry how-to

Enter the modern data registry. By taking a fresh approach to data discovery – focused on creating an inclusive list of what data is kept where and why – organizations can better meet data privacy, protection and governance requirements.

Organizations need to start with the basics. A modern data registry cannot be a data warehouse – you'll simply be duplicating the data it maps and introducing limitations in scale. Instead, organizations should build the registry in an index-like map, focusing on five key functionality and operational characteristics:

1_Content granularity: Privacy regulations require organizations to account for the data they collect – and that doesn't just mean knowing the type of data they collect. Companies need to know what data they have and who that data belongs to. Privacy is all about people, so knowing the "people" context of data is essential to meeting privacy requirements.

2_Usage context: Knowing what and whose data you have is a critical first step but creating a modern data registry with complete data intelligence means going further. This requires operational, technical and business knowledge, such as who can access this data, what applications are consuming the data, what third parties have access to the data, what is the purpose for collecting this data and does the organization have adequate consent to collect and process the data.

3_Data source coverage: A data registry that only covers unstructured files or relationship databases will not provide a complete data inventory. With the growing amount of data sources and applications used throughout the enterprise, organizations need to create a process that covers both unstructured file shares and structured databases, big data, cloud, NoSQL, logs, mail, messaging, applications and more.

4_Ability to scale: Organizations gather and analyze tens, if not hundreds, of petabytes of data. With increasing pressure to extract more value from data, that number is only increasing. A modern data registry needs to deliver an efficient index of data along with associated usage and must do it in a way that is scalable for a global enterprise.

5_Dynamic, not static: Once a data registry is created, organizations must anticipate that it will be changed and moved on a constant basis. Consequently, the registry must be able to self-update and accommodate any changes in near real-time to provide the clearest, most accurate picture of what data is kept where, when, and who it belongs to.

A new approach to building a data registry from data intelligence

Once the functional and operational foundation for a modern data registry is built, it is time to create a full accounting and inventory of your enterprise's distributed data assets. This requires data intelligence down to the discrete entity value – something not possible with metadata alone. Obtaining this level of data requires a hybrid approach to content discovery and contextualization, achieved by considering these four key requirements:

1_Entity Discovery and Resolution: In order to obtain the level of data intelligence necessary for privacy and protection use cases, organizations need a data discovery mechanism that can extract and resolve data entities based on data values – no matter if the data resides in structured, unstructured or semi-structured stores. Organizations also need to implement scanning systems that can disambiguate identical looking data based on context. For example, your system should be able to sperate a social security number from an account ID, even though they both may have the same value.

2_Entry Correlation and Contextualization: Privacy is about people. Period. To comply with privacy regulations, organizations need to account for their data and show correlation or association of data to a data subject. This must be reflected in a modern data registry. While essential for privacy, this can also provide a new level of understanding around the connectedness of data to high value identities like transactional IDs, account IDs and patent IDs.

3_Entity Classification by Type and Category: The approach to building a modern data registry must move past traditional classification tooling. Modern data registries should have entity-level granularity that requires more refined entity-level classification. If built with artificial intelligence or machine learning, this will expand how data is identified based on heuristics and inferred categorizations.

> *It cannot be said enough – the only way to comply with privacy regulations like GDPR and CCPA is if the organization can account for what data they hold and what individual the data belongs to.*

4_Metadata Capture and Cataloging: Even though pure-play metadata catalogs leave much to be desired from the registry standpoint, they still provide value because they can record where data categories can be found. This helps to both classify data entities correctly and identify where to prioritize deeper entity searches. The challenge lies in relying on human tags and annotations, since human error makes this data privy to inconsistencies. So, while technical metadata is important, you also need to capture operational and business context like access rights, purpose of use, or consent.

It cannot be said enough – the only way to comply with privacy regulations like GDPR and CCPA is if the organization can account for what data they hold and what individual the data belongs to.

A modern data registry looks beyond simply classifying and cataloging data to show the correlation and association of data to a data subject. Providing a new understanding of the connectedness of data to high-value identities no matter if they are located- in the data center or the cloud.

REPORT:

Infosecurity Europe 2019

Featuring analysts, policy experts and over 400 exhibitors, Infosecurity Europe took place in London in early June.

Renowned broadcaster Kate Adie CBE opened the first day of Infosecurity Europe 2019 with a keynote speech on Perspectives from the Frontline: Managing Risk & Building Resilience. In the session, the former BBC Chief News Reporter drew on her personal experiences reporting from war zones to provide fresh perspectives on risk, resilience and the security challenges facing organisations.

The event carried out the first in a series of daily visitor polls, which asked the question: Do you think it's likely there will be an attack on the UK's critical national infrastructure (CNI) this year? 70 percent of keynote attendees answered 'yes'.

On the second day, Jamie Bartlett, Senior Fellow and former Director of the Centre for the Analysts of Social Media, Demos and best-selling author delivered a session on Discovering the Digital Underworld: Privacy, the Dark Web, Tech & Democracy. He took his audience on a journey of discovery into how technology is changing society, from cybercrime and surveillance to privacy, data and democracy – including the Cambridge Analytica controversy.

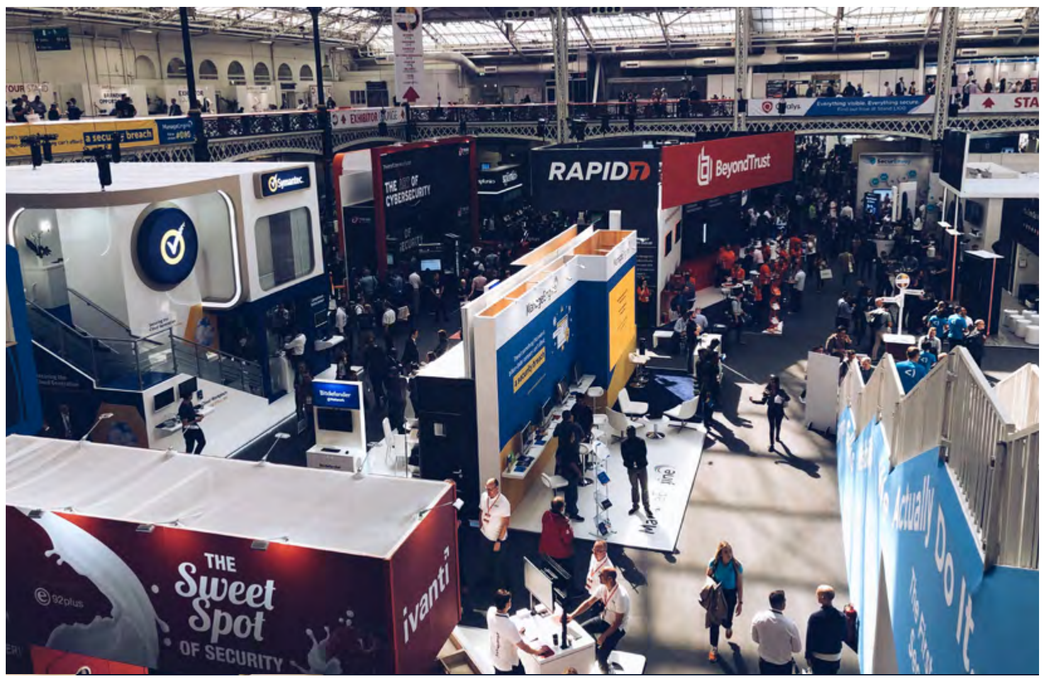
This session was followed by another high profile speaker, Dame Inga Beale, Former CEO, Lloyds of London, who presented on View from the Board: Managing Organisation Complexity & Risk. She gave attendees her perspective on the challenges of managing a complex organisation – including culture change, balancing history and innovation when delivering digital transformation, and communication between the board and information security function.

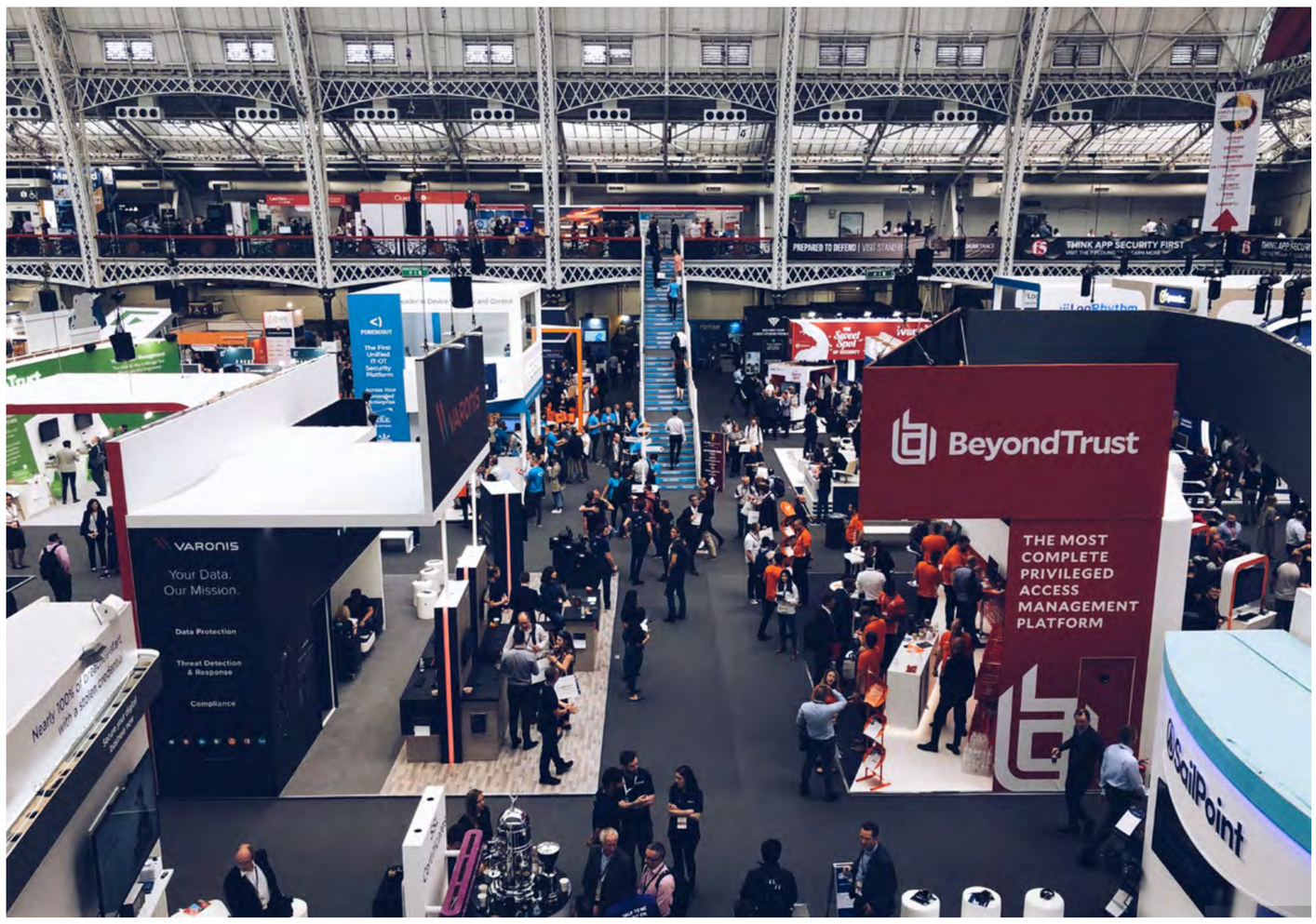
The second of Infosecurity Europe's daily visitor polls delved into this issue, asking keynote attendees the question: In 2019, have you experienced difficulties in getting investment from the board to secure legacy systems while embracing new technologies? 57 percent said that they had.

For the third and final day of Infosecurity Europe 2019 the future of information security, skills, people and innovation were the theme of the day. CEO of the National Cyber Security Centre, Ciaran Martin, returned to the show with a keynote speech on Defending the UK: The NCSC Vision for a more Secure UK. Ciaran discussed the need to 'focus on the fixes and not the fear' and glamorisation of cybersecurity. The future of tech such as 5G and IoT were also top of the agenda with Ciaran noting that we have the ability to see things coming and should prepare for the next phase of the internet.

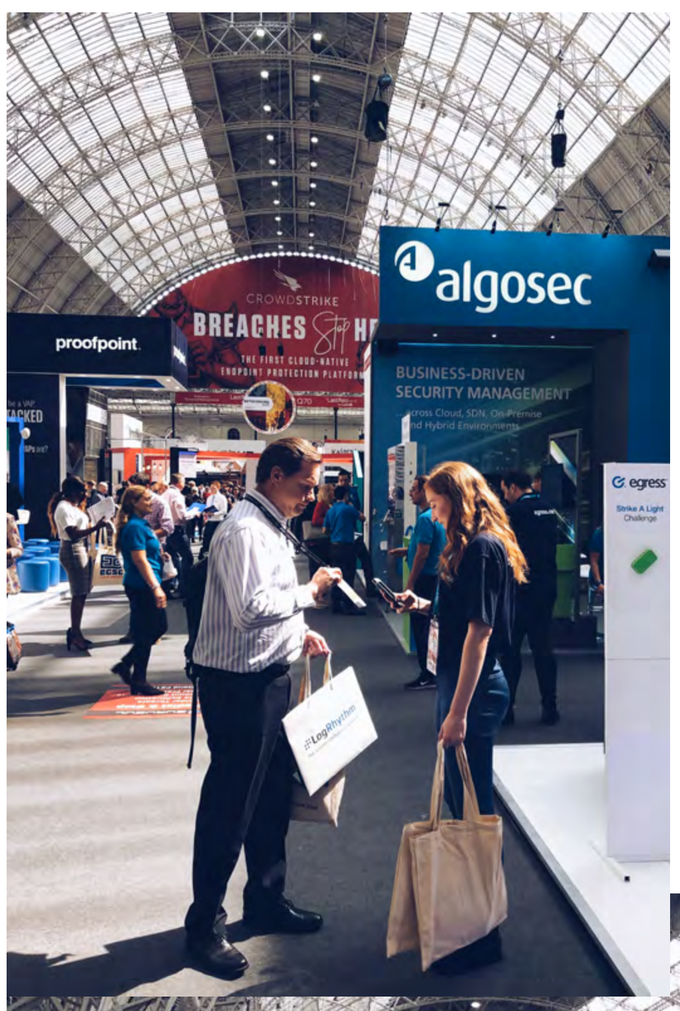
To coincide with the skills topic, the event carried out the third of its series of daily visitor polls, which asked the question: Are you confident the UK has enough cybersecurity-skilled professionals to meet the growing demands of an increasingly digital economy? 87% said that they were not confident.

#INFOSECURITY EUROPE 2019 gallery



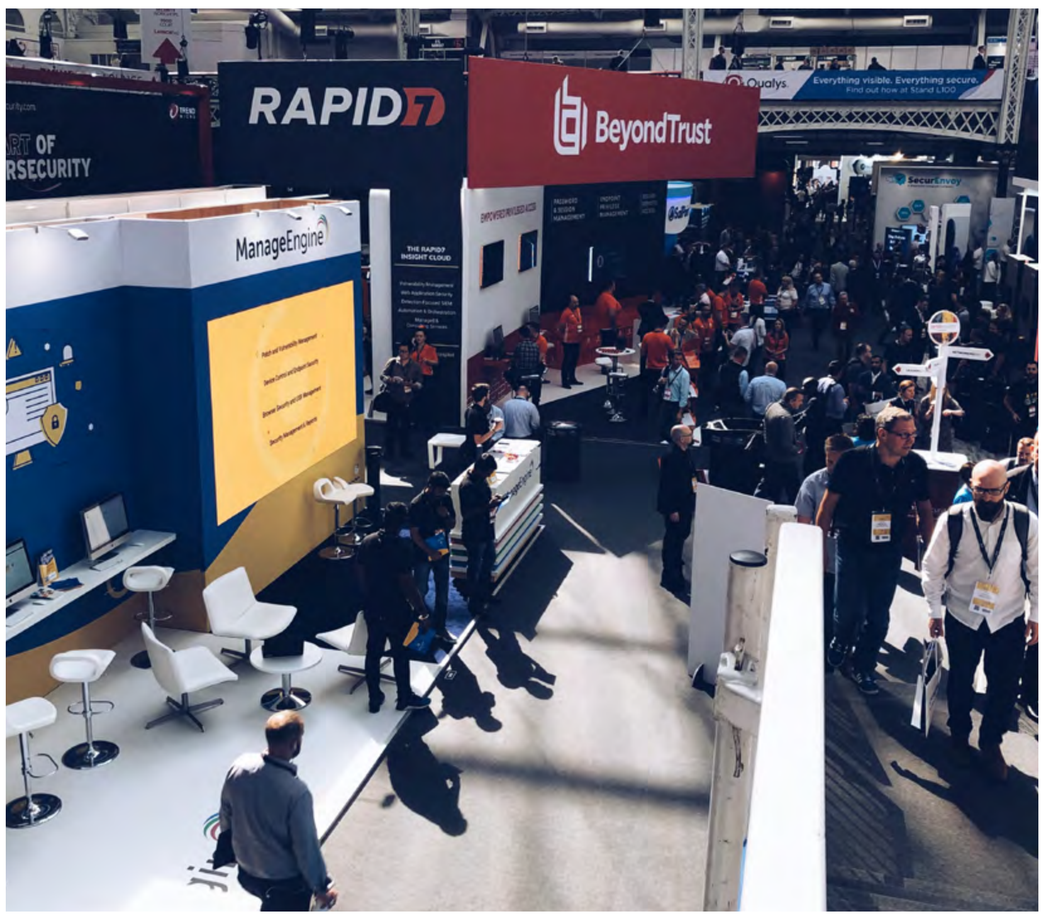

PREPARED TO DEFEND | VISIT STAND
THINK APP SECURITY FIRST
BeyondTrust
VARONIS
Your Data.
Our Mission.
Data Protection
Threat Detection
& Response
Compliance
THE MOST
COMPLETE
PRIVILEGED
ACCESS
MANAGEMENT
PLATFORM
SailPoint


CROWDSTRIKE
BREACHES Stop HERE
THE FIRST CLOUD-NATIVE
NETWORKING BAR


algosec
CROWDSTRIKE
BREACHES Stop HE
THE FIRST CLOUD-NATIVE
ENDPOINT PROTECTION PLATFORM
proofpoint.
BUSINESS-DRIVEN
SECURITY MANAGEMENT
egress
Strike A Light
Challenge


Cash Machine
Exit
TARGET YOUR DEVICE SECURITY


CROWDSTRIKE
BREACHES Stop HERE
THE FIRST CLOUD-NATIVE
ENDPOINT PROTECTION PLATFORM
Stand Q70
Carbon Black.
CYREN
Akamai
Intelligent Security
Starts at the Edge
25B
13B
300M
First to Detect, First to Protect.
Cyren.com


RAPID7
BeyondTrust
ManageEngine
Everything visible. Everything secure.

What happened to trust and transparency in cybersecurity?

AUTHOR_ Grant Wernick, CEO,
Insight Engines

IT and the business side need to work towards open lines of communication and shared responsibility across the organization to make cybersecurity not only a priority but a standardized part of daily operational procedures.

Today, we need proactive security measures that protect the organization responsibly, mitigate risk and adapt to an ever-changing threat landscape. This can only be truly achieved with transparency across the organization.

I've given presentations before where I've asked a room full of people to raise their hand if they are in charge of cybersecurity. I'll get a few raised hands from IT and Ops. Then I make the point that everyone's hand should be raised because today everyone plays a role in keeping their organization secure. Employees need to understand risk so they can make more informed decisions every time they go online and be aware of the consequences that being careless can carry.

IT and the business side need to work towards open lines of communication and shared responsibility across the organization to make cybersecurity not only a priority but a standardized part of daily operational procedures.

The marketing team has access to intellectual property. HR has access to sensitive personal data. Finance has access to data about the company's monetary health and funding longevity.
The security team needs to move beyond the mindset of "we protect everyone" and incorporate ways to empower people to protect themselves.

How did we get to be so closed off?

It's often said that the Internet was built on trust. When the basis of the Internet, ARPANET, was being developed, it was designed to connect academic institutions over a single network, so the basic idea was that the person on the other end would be a verified party. Therefore, not much thought was given to building in security.

Fast forward 30 years and everyone (and everything) is using the Internet for a myriad of services across the globe. Unfortunately, not all of those people can be trusted. The Internet was built on trust, but it's definitely not maintained on trust today.

> *To restore trust and transparency, organizations must first operate from a place of trust and transparency within themselves.*

People are increasingly distrustful of the Internet, which is no surprise given the daily announcements of new data breaches and especially high-profile mega breaches from household names such as Uber, Equifax, Marriott, and Yahoo. And those are just the one we hear about - the lack of transparency and attempted coverups further fuel doubt that cybersecurity is being taken seriously.

The loss of consumer trust and increasingly aggressive regulators setting record fines for data breaches are spurring the boardroom to take data security and data incident response seriously.

But to restore trust and transparency, organizations must first operate from a place of trust and transparency within themselves.

> *The gatekeepers of technical knowledge from information security and the clandestine nature of cybersecurity eventually came together to form security industry's current culture.*

Living in the shadows

As recently as ten years ago, cybersecurity wasn't a term that was used often. Corporations focused on information security – the preservation of confidentiality, integrity, and availability of information – as an operation under the IT department. You had a group of people with technical knowledge that communicated with those outside of their tribe only when they had to. There was no interaction or collaboration with the business side unless there was a problem that needed fixing. Remaining compliant was the main objective.

On the government side, intelligence agencies were well on the way of developing secretive tools, security concepts, risk management approaches and technologies for cybersecurity to deal with cyber-warfare, information warfare, critical infrastructure protection and other threats and vulnerabilities from cyberspace.

The gatekeepers of technical knowledge from information security and the clandestine nature of cybersecurity eventually came together to form security industry's current culture. For many years they embraced the secretive nature of their work and this is shown in how security has become a stand-alone part of the corporate IT organization, removed from the business side of the operation.

An increasingly complex world

In the early to mid-2000s, software really started (in the words of Marc Andreessen) "eating the world".

There was an explosion of data as online companies emerged faster and faster and traditional companies started building out their new digital identities. As most companies were slowly becoming IT companies, cybercrime flourished.

The barrier to entry to become a cybercriminal became lower and lower as hacking toolkits and exploits were being sold on the dark web, giving people with limited technical prowess the ability to pull of cybercrime activities. The rules of engagement between nation-states running cyberwarfare ops on each other blended into the private sector as evidenced by the North Korean hack against Sony Pictures in 2014. Suddenly, everyone and everything was fair game.

A siloed approach to security is no longer tenable.

Then, in 2016, corporate and government mandates started the move towards the cloud. The day-to-day of securing an organization became increasingly complex as organizations moved to hybrid clouds and multi-cloud platforms, distributing information broadly beyond the network perimeter by way of non-technical employees that neither have the time nor understanding to consider the security outcomes.

This is the world we live in today, but ticking off regulatory checkboxes and settling for the status quo of achieving compliance no longer solves the issue of non-stop, ever-evolving threats from every attack angle imaginable. A siloed approach to security is no longer tenable.

Opportunities for trust and transparency

Security and DevOps need to work closely together to develop processes where security is involved from the start so products and applications aren't being shipped with glaring vulnerabilities.

The first step is implementing a cybersecurity strategy that includes all stakeholders across the organization - from IT, security, and DevOps to all business units including financing, marketing and HR.

Then IT needs to work hand-in-hand with business unit owners to run regular workshops to educate them on the importance of security across the organization.

Thirdly, the board needs to be able to ask business risk related questions that get answered quickly by the security people in theorganization. They need to share a common language to have discussions about risks that affect the wellbeing of the enterprise.

Fourthly, security needs to start focusing on a hybrid world that isn't just about protecting the perimeter. We need to have open discussions about identity, endpoint and application security. The perimeter can no longer be the focus, and the responsibility for that should be accepted by the cloud vendors.

And the fifth point is this: security needs be removed from the realm of secrecy. Security is now a standard part of operating an organization and needs to be discussed openly as it is a critical success factor of ever operation. Openness, not secrecy, is the only way to move forward.

(ISC)²

2019 SECURITY CONGRESS

OCT. 28-30 | Walt Disney World Swan and Dolphin Resort | Orlando, Florida

If you attend just one industry conference in 2019, make it Security Congress. The agenda is packed with world-renowned speakers, training opportunities and interaction you won't capture anywhere else.

- Hear from visionary keynote speakers
- Build expertise with more than 100 educational sessions
- Gain an edge through CISSP, CCSP, Security Architecture and OWASP pre-conference training
- Meet cybersecurity professionals from around the globe
- Get current on the latest security trends

EARLY BIRD PRICING
THRU AUGUST 15

PLUS SAVE $50

When you use code: **HelpNet50**

Register Today

KEYNOTES

Captain "Sully" Sullenberger

William H. McRaven

Catherine Price

Erik Wahl

congress.isc2.org

Prioritising risks in a climate of geopolitical threats

AUTHOR_ Malcolm Taylor, Director Cyber Advisory, ITC Secure

One of the key reasons for the cyber threat landscape becoming more hostile is that the bar for entry into cyber crime has never been lower.

The cyber security landscape has become increasingly hostile in recent years, with a growing threat from common cyber criminals as well as the looming shadow of state-level geopolitical activity. Recent research commissioned by the UK government found that 32 percent of UK businesses have identified a breach or attack in the last 12 months and - it should be noted - many more have likely been compromised but lacked the capability to detect it.

One of the key reasons for the cyber threat landscape becoming more hostile is that the bar for entry into cyber crime has never been lower. There

is a growing awareness that you don't have to be a genius hacker to be a successful cyber criminal, and that even someone with minimal technical skill can go on the dark web and purchase a malware kit and a guide on how to use it.

Cyber crime also presents an attractively low-risk option for a criminal: there is a multitude of tools available for obfuscating identity and location and cases of arrest and trial are few and far between.

While we have seen more overt instances of cyber attacks mounted or directed by nation-states, this does not mean that the average organization should rush off to equip itself with defences against advanced state-level attacks.

Many high-profile breaches were also made possible by businesses making basic errors in setting up their infrastructure and cloud solutions – essentially leaving their doors wide open for even the most unskilled criminals.

Spreading state-level attacks

The cyber criminal community has enjoyed an increasing level of access to more advanced hacking tools. There have been a number of instances of state-level hacking tools being leaked online, such as the set of NSA exploits leaked by the Shadow Brokers group in 2017, which were subsequently used in the infamous NotPetya ransomware outbreak.

It has also become increasingly apparent that nation states sometimes outsource aggressive cyber activity to groups that were previously thought to be autonomous, such as the "Fancy Bear" group that allegedly has ties to the military intelligence agency of the General Staff of the Armed Forces of the Russian Federation (also known as "GRU").

This means that the average organization is now facing a greater level of attack sophistication and a larger number of potential adversaries. Most companies, however, are still not recognizing this risk.

How big a concern are geopolitical threats?

A great deal of attention was paid to nation-state cyberattacks this past year, particularly activity believed to be orchestrated by Russia's GRU in relation to the spying and poisoning scandals. China and North Korea have also frequently been accused of aggressive international cyber activity in recent years.

But while we have seen more overt instances of cyber attacks mounted or directed by nation-states, this does not mean that the average organization should rush off to equip itself with defences against advanced state-level attacks.

Intelligence agencies in most parts of the world are inhibited by significant legislation which bars corporate espionage, and even those without such limitations are still constrained by resources. Launching a targeted, high-level attack requires significant time and expertise, so state-level activity will only be commissioned against strategically important targets. Unless an individual or organization is involved in terrorism or serious crime or is in some way deemed political by certain actors, they will not be of interest to any intelligence agency. Even Russia, with its history of aggressive cyber activity, has been focused on gaining political advantage over economic gain.

There are some exceptions. China has frequently been accused of orchestrating cyber attacks for commercial espionage, with a recent case involving

attacks on universities in possession of intellectual property with military applications. However, rather than using secret state-level exploits, these attackers often use the same techniques and technology we see in common low-bar cyber-attacks.

Prioritizing risks

While the increased prominence of state-level attacks has served to increase awareness of cyber threats, it also frequently leads to skewed priorities that favour preparing for advanced attacks at the expense of the basics. For example, we have been approached by an increasing number of organizations asking about measures such as using military-level encryption to defend their assets from nation-state operatives, but most breaches occur because of basic failures such as weak passwords, exposure to simple phishing and poor patch management.

A common mistake for companies is basing their cyber strategy on perceived threats instead on their actual risk profile. In one instance we spoke with a company that was spending six figures on security annually but, on closer inspection, had left most of its essential data vulnerable.

At the heart of cyber security is risk management. This is the constant cycle of understanding threats and the dangers they present, making a decision on whether to fix issues or live with them, and then moving on to the next threat. While risk management has long been a core business activity, when it comes to financial and strategic issues organizations are still struggling to account for cyber risks in the same way. The complexity and use of esoteric language and unknown acronyms lead to cyber threats still being seen as “other” and not fitting in with the usual understanding of risk.

At the heart of cyber security is risk management. This is the constant cycle of understanding threats and the dangers they present, making a decision on whether to fix issues or live with them, and then moving on to the next threat

Getting started with cyber risk management

As with all risk management, the first step in managing cyber risks is to start with the basics. First and foremost, this means gaining an understanding of what the company’s most valuable assets are and identifying the security gaps that might expose them. An in-depth gap analysis will show what the company has done well and where it failed and - most important - what needs to change.

Once this has been established, they can start fixing the issues and closing the gaps. Some vulnerabilities will be near-instant fixes while others may take a year or more. Whatever the issue, the process needs to be highly organized and structured with objectives, deadlines and responsibilities.

This process will also help the company understand if it’s investing in the right things and prevent it from wasting money on costly and unnecessary advanced solutions at the expense of basic security hygiene.

Industry news

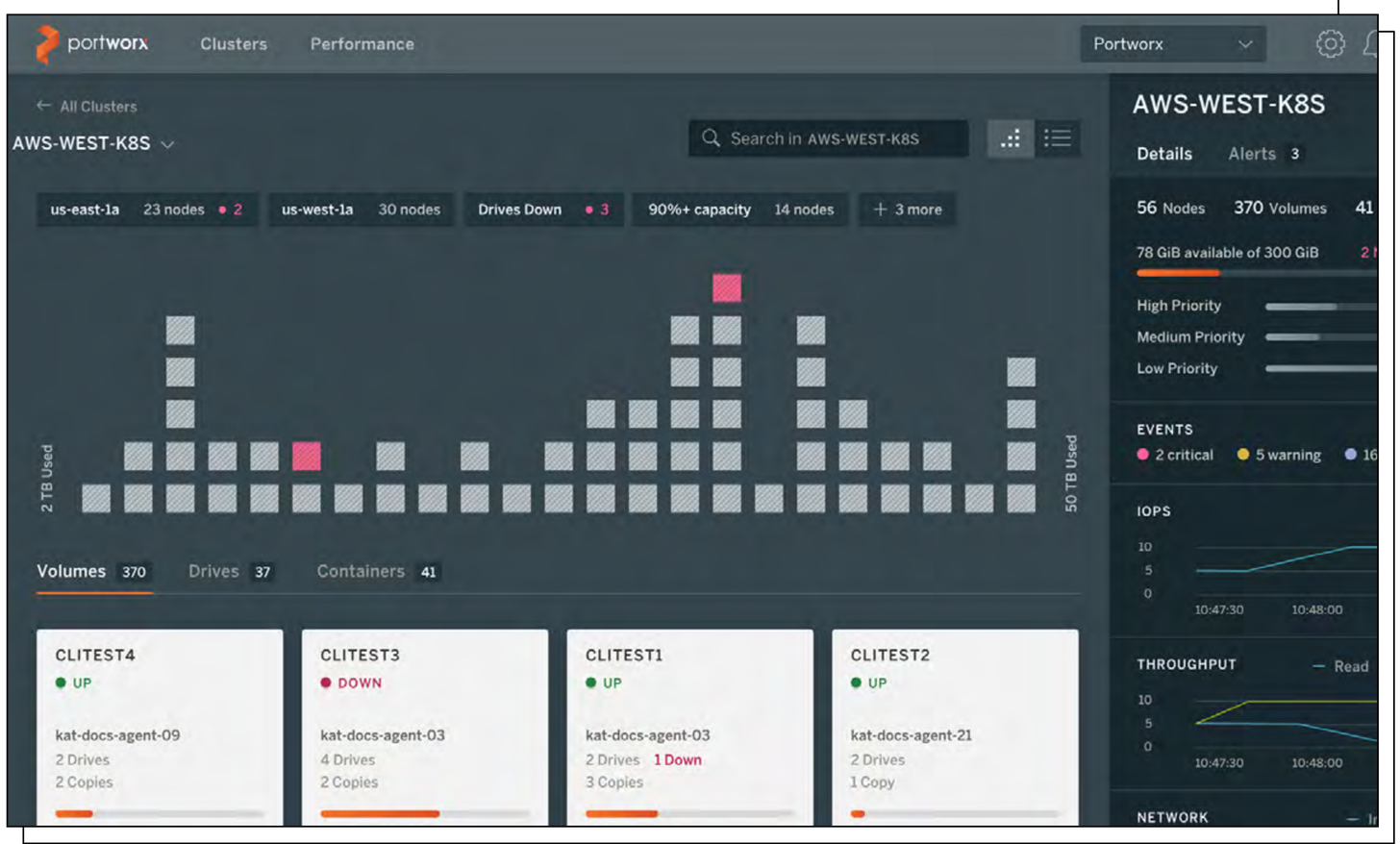
Portworx adds new backup and recovery features to its cloud-native storage and data management platform

Portwox announced Portworx Enterprise 2.2, an update to its cloud-native storage and data management platform with new features focused on security, data protection, and disaster recovery.

With this update, Portworx Enterprise provides a one-command backup and recovery experience for complex applications running on Kubernetes, giving enterprises more control over their mission-critical data.
With Portworx Enterprise 2.2, enterprises for the first time can easily back up entire Kubernetes applications to any S3-compatible object store, including data and Kubernetes objects, with a single command.
All data is backed up in its encrypted state using a key that only the customer controls, ensuring that bad actors never see the unencrypted data.

In the same way Portworx Enterprise backs up application data and application configuration, enterprises can now restore a Kubernetes application with a single command.

Restores are not limited to single containers: complex applications made up of multiple containers can be restored using Portworx Enterprise Group Snapshots, which create an application-consistent copy of distributed applications.



JASK launches a new Heads Up Display for security operations centers

JASK, the provider of the industry's first cloud-native SIEM platform, unveiled a first-of-its-kind Heads Up Display (HUD) for security operations centers (SOCs) based on cutting-edge scientific design principles and visualization concepts never before used in the cybersecurity industry.

Drawing inspiration from leading designers in science fiction and gaming as well as the latest user interface design concepts, the enhanced JASK ASOC platform offers maximal functionality on a single screen.

The new JASK ASOC platform design begins with the Insight Radar, a circular visualization that represents incoming alerts and events and draws the eye inward to where focus is needed first.

JASK correlates outer-edge records into an inner ring of signals (seen as a circular bar chart) and then leverages adaptive signal clustering to distill these down further into top-priority JASK Insights, seen as triangles. The right sidebar features charts giving additional information on what's happening in the customer environment in real time.

The left sidebar offers a high-level look at top-priority components the analyst needs to track, including what Insights are outstanding, how many devices are involved and what threats are still active.

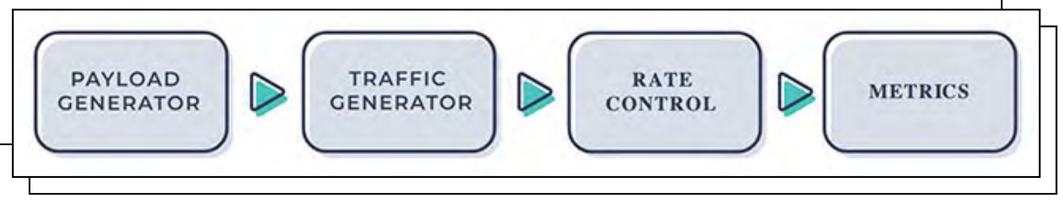
NS1 Flamethrower: Lightweight, open source DNS performance testing tool

NS1 released Flamethrower a lightweight, configurable open source tool for functional testing, benchmarking, and stress testing DNS servers and networks.

The tool supports IPv4, IPv6, UDP, TCP, DNS over TLS, as well as experimental support for DNS over QUIC. It has a modular system for generating the queries used in the tests, allowing for rich and realistic test scenarios that can plug into automation pipelines.

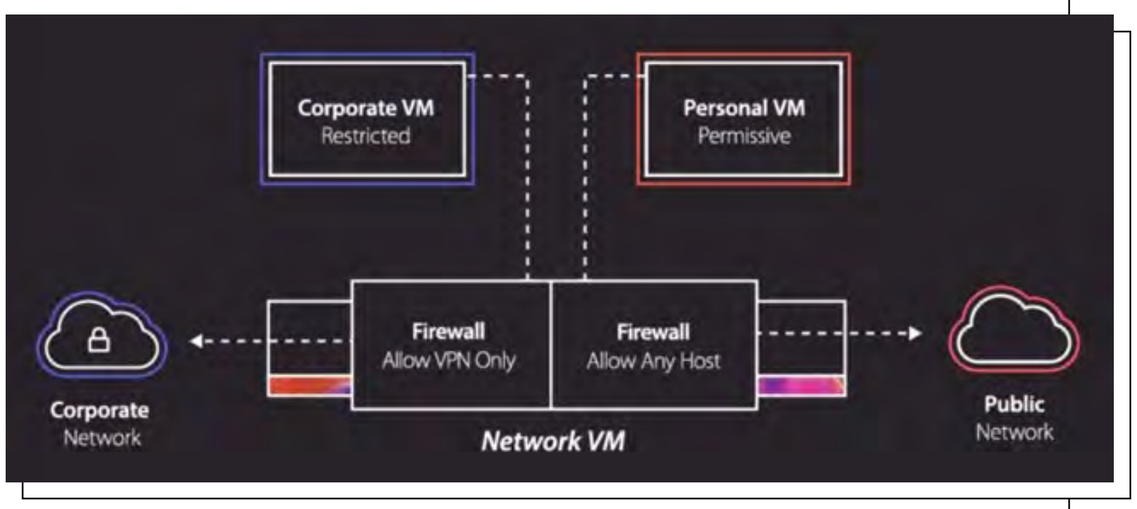
It simulates multiple concurrent clients and generates actionable metrics, including send and receive counts, timeouts, errors and data on minimum, maximum and average latency. The metric output format is suitable for ingestion into databases, such as Elastic, for further processing or visualization.

Flamethrower can adjust its queries per second flow over time, which is useful for generating a "signal" of traffic (e.g., a square wave) for calibrating time series metrics collection. It can also be used to mimic the surges in traffic an organization might see during a DDoS attack or stress test systems for failover, making it an ideal tool for wargaming and chaos engineering.



Trustwave unveils new database security scanning and testing software

Trustwave unveiled Trustwave DbProtect, new database security scanning and testing software that helps organizations better protect critical data assets hosted on-site or by major cloud service providers from advanced threats, configuration errors, access control issues, unauthorized privilege escalation, missing patches and more.
Trustwave DbProtect quickly discovers all databases and associated objects, users and enabled security features across an organization's entire footprint and chosen deployments including on-premises, hosted and hybrid cloud. It identifies data leakage, misconfigurations, access control issues, missing patches, unauthorized data modifications and other concerns that put organizations at risk for breaches and associated steep fines for non-compliance.
It delivers a single consolidated view of threats, vulnerabilities, perceived risks and compliance endeavors across the entire data environment. Using analytics, database administrators can drill down for views of each database or group of databases to run reports against an established baseline charting progress and operational efficiencies.



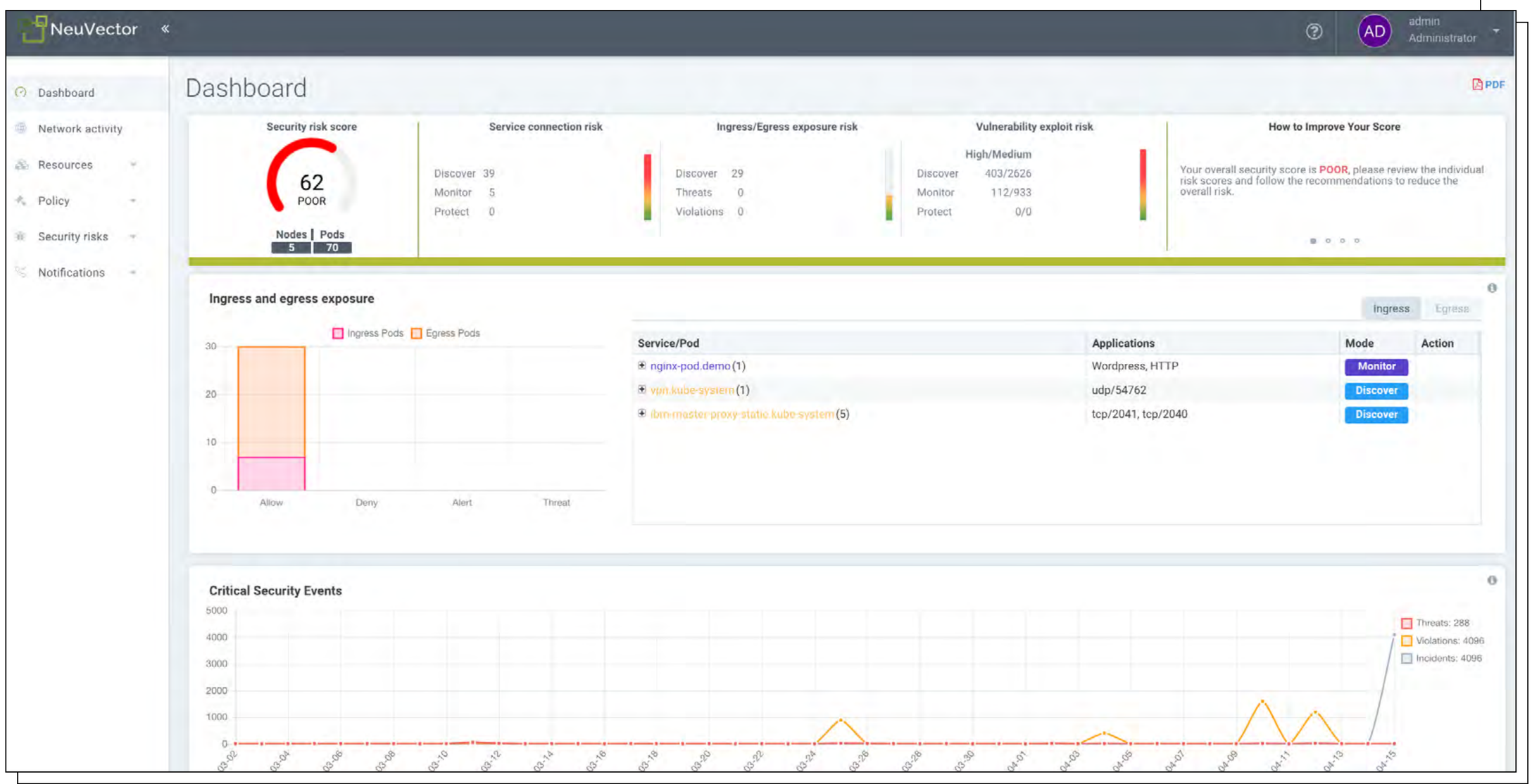
Hysolate 2.0 helps enterprises improve endpoint protection

Hysolate 2.0 makes it easier than ever to protect hundreds of thousands of endpoints from cyber threats while freeing end-users to access the resources they need to be productive.
The Hysolate Platform automatically transforms each physical end-user device into multiple, fully isolated environments.

These endpoints are built on top of a bare-metal hypervisor platform that sits below the device operating system (OS). Everything an end-user does happens in segregated local virtualized operating systems—for example, one that's locked-down and limited to sensitive resources and another for corporate day-to-day work, including email and Internet browsing.

These OS environments run locally, side-by-side on the same device. Applications and services automatically launch in the correct, designated environment, making the experience safe and seamless for end-users.

Advanced integration with Microsoft Active Directory, configuration management systems like Microsoft System Center Configuration Manager (SCCM), and Security Information and Event Management (SIEM) products, plus new role-based access control, let IT administrators leverage existing investments to quickly deploy Hysolate, seamlessly manage virtual endpoints and improve security posture of sensitive corporate assets.



NeuVector's new container risk assessment/visibility capabilities for security teams released

NeuVector announced new capabilities to help container security teams better assess the security posture of their deployed services in production.

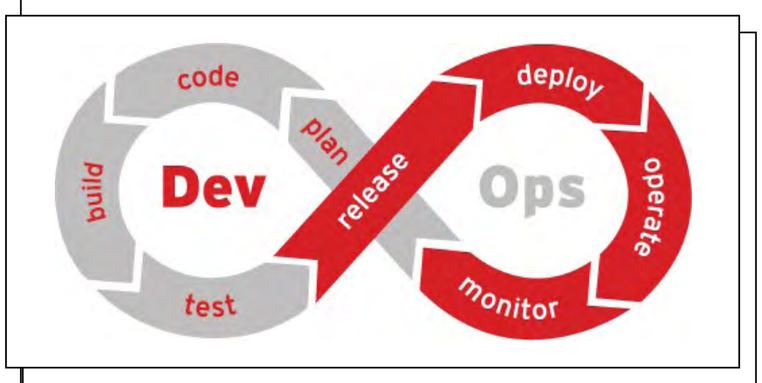
New dashboard widgets and downloadable reports provide security risk scores for the most critical run-time attack risks: network-based attacks and vulnerability exploits in containers. Specifically, NeuVector now delivers an intelligent assessment of the risk of east-west attacks, ingress and egress connections, and damaging vulnerability exploits.

An overall risk score summarizes all available risk factors and provides advice on how to lower the threat of attack – thus improving the score. The service connection risk score shows how likely it is for attackers to move laterally (east-west) to probe containers that are not segmented by the NeuVector firewall rules.

The ingress/egress risk score shows the risk of external attacks or outbound connections commonly used for data stealing or connecting to C&C (command and control) servers. Additionally, the vulnerability exploit risk combines run-time scan results for containers with the protection mode of the container.

If the container is protected by NeuVector's whitelist rules for network segmentation and process profiling, then there is a lower risk of a vulnerability exploit spreading or critically damaging the service.

Trend Micro unveils cloud-native security customized to the demand of DevOps



Trend Micro added container security capabilities to Deep Security to elevate protection across the entire DevOps lifecycle and runtime stack. Within the software build-pipeline, Trend Micro has extended its container image scanning to include pre-registry scanning, providing earlier detection of vulnerabilities and malware over and above scanning the trusted registry for any future threats.

Deep Security will now also scan for embedded secrets such as passwords and private keys and provide compliance and configuration validation checks, along with image assertion for digitally signed images.

At runtime of the container, Trend Micro has boosted container platform protection across Docker and Kubernetes. Deep Security has long ensured protection for the host and containers at runtime. This includes IPS rules, integrity monitoring to detect compromised instances of the platform, as well as log inspection.

To increase automation and decrease manual tasks, security and operations teams using Trend Micro can now use any command shell to execute the APIs. This additional option ensures full control of deploying policies, automation of monitoring, reporting and more.

LogRhythm launches a cloud -based version of its NextGen SIEM Platform

LogRhythm's launch of LogRhythm Cloud means customers can now enjoy the same full analyst experience as provided by LogRhythm's on-premise offering, while also realizing the efficiencies, cost savings and other benefits provided by a SaaS solution.

Because LogRhythm Cloud customers need significantly less time to deploy, administer and maintain the platform, they can spend more time using LogRhythm and benefitting from a platform specifically designed to reduce mean time to detect (MTTD) and mean time to respond (MTTR) at the lowest total cost of ownership (TCO).

With SOC efficiency more important than ever for maximizing the effectiveness of security teams and defeating cyberthreats before they harm the enterprise, LogRhythm delivers its SOAR capabilities as an integral set of capabilities across its product line. These capabilities include functionality such as incident response playbooks, case management, integrated threat intelligence feeds, and workflow automation – all of which are included in LogRhythm Cloud.

Alcide launches continuous security and hygiene scanner for Kubernetes and Istio

Alcide Advisor automatically scans for compliance, security and governance risks and vulnerabilities. It provides a single-pane view for all K8s-related risk, governance and compliance issues, including auditing, topology, network, policies scans and automated common vulnerabilities and exposure checks.

Integrated with the CI/CD pipeline, the monitoring enables DevOps teams to gain a deeper understanding and tighter control of their Kubernetes projects with a continuous analysis covering:

- Kubernetes CIS Benchmark
- Kubernetes vulnerability scanning
- Hunting misplaced secrets, or excessive secret access
- Workload hardening from Pod Security to network policies
- Ingress controllers for security best practices
- Kubernetes API server access privileges
- Kubernetes security best practices on AWS
- Kubernetes operators security best practices
- Istio security configuration and best practices

MistNet launches new threat detection and response platform using mist computing and edge AI

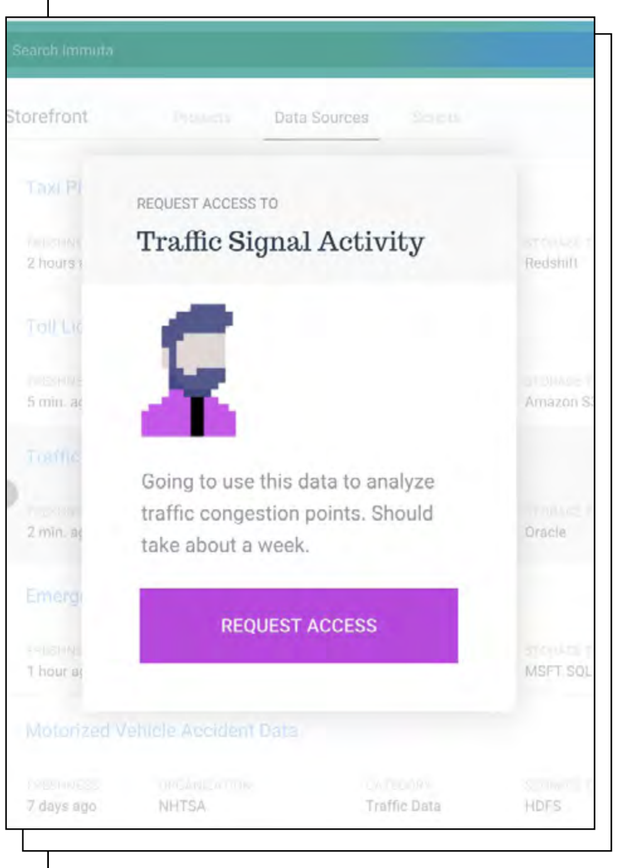
CyberMist breaks through the silos, monitoring users, hosts, OS internals, networks (LAN and WAN), public cloud resources, and IoT environments using distributed machine learning models to autonomously hunt and stop unusual and threatening activity in real-time, all while eliminating the backhauling of security data.

Unlike systems that focus only on network detection or endpoint detection, CyberMist provides full visibility by applying threat modeling techniques end-to-end across end user, host, OS, network, and cloud resources.

With TensorMist-AI, rather than backhauling security data to centralized compute resources for analytic processing, the system moves compute power to the data through its innovative use of mist computing technology, eliminating any data movement.

TensorMist-AI constructs a scalable security data analytics mesh that is geographically distributed in nature, yet maintains a centralized view and control function via the cloud.

Immuta releases new automated data governance platform with compliant collaboration features



Immuta announced Immuta Automated Data Governance Platform, which creates trust across security, legal, compliance and business teams so they can work together to ensure timely access to critical business data with minimal risks. Its automated, scalable, no code approach makes it easy for users across an organization to access the data they need on demand, while protecting privacy and enforcing regulatory policies on all data.

Its Automated Policy Inheritance feature eliminates the need for human intervention to manage policies across mashed up data sources. The Format Preserving Encryption and Reversible Masking features allow on-demand de-masking of sensitive data.

The Fingerprints feature eliminates any uncertainty about how downstream use could be impacted. It calculates the impact of data policy changes and provides visualizations to users of the statistical deviation. Together, with the Immuta Policy Inheritance feature, downstream users are notified about any changes and are provided details on how their use of the impacted data will affect them.

The Immuta platform ensures compliance with all major data regulations, and it is now interoperable with the Databricks Spark analytics engine, and cloud-based data warehouses Google Big Query and Snowflake.

SecBI extends its threat detection solution with automated response

SecBI, a disruptive player in cyber threat management, announced the extension of its agent-less, threat detection solution with automated response. Now SOCs and MSSPs can benefit from a comprehensive solution including detection, investigation, and automated response that delivers significant boosts in effectiveness and productivity.

Despite the intuitive coupling of automated response with advanced, machine-learning detection, the SOAR solutions available on the market typically fall short of offering both functionalities. Security operations using SecBI's automated detection and response solution will benefit from:

- Full scope detection of suspicious incidents
- Improved analyst productivity
- Instant coupling of detection with comprehensive response to threats
- Better prevention due to automatic delivery of information from response mechanisms

BigID new capabilities help enterprises scale responses to data access requests for privacy regulations

BigID, the leader in ML-driven personal data discovery and privacy, announced first-of-their-kind data access rights management features to help enterprises automate fulfillment of personal data access requests for privacy regulations like the California Consumer Privacy Act (CCPA).

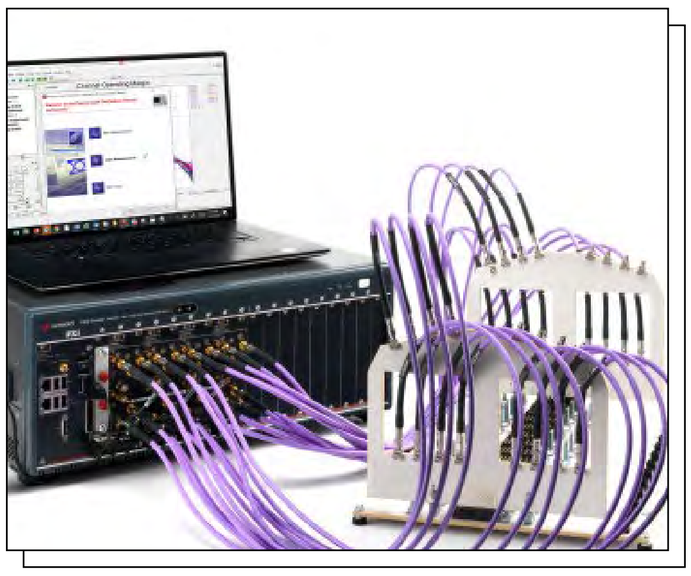
BigID pioneered the technology to help organizations find and inventory personal information by identity to fulfill privacy-driven personal data rights. The new advanced capabilities expand the company's market leadership in enterprise data access lifecycle management.

The new features include:

- Enhanced AI for identifying contextual personal data
- Smarter classification and correlation for connecting data to a person
- Expanded data coverage to more than 50 systems in the data center and cloud
- Enhanced data access management capabilities for analysts and operators
- New programmatic bulk processing capabilities for high volume requests
- Deep customization and summarization templates for tailored responses
- Enriched workflows for deletion, correction and portability
- Consent tracking and orchestration
- Automation for validating deleted data
- SDK integration with web and mobile data access request portals

Keysight Technologies unveils new integrated network analyzers

High-speed digital, wireless, aerospace and defense, and automotive companies need integrated active and passive components for devices such as cell phones, satellite communications, and 5G base stations, to increase performance and reduce size of end products. These highly integrated devices require highly integrated test solutions that address radio frequency (RF) test challenges while providing advanced functionality and performance. Keysight's new E5080B, P50xxA Series, and M980xA Series network analyzers deliver next generation features and performance in benchtop, USB, and PXI form factors. These new analyzers combine built-in pulse generators and modulators, spectrum analysis, and time domain analysis in a single instrument to save time by fully characterizing modern devices without the need for additional test hardware.



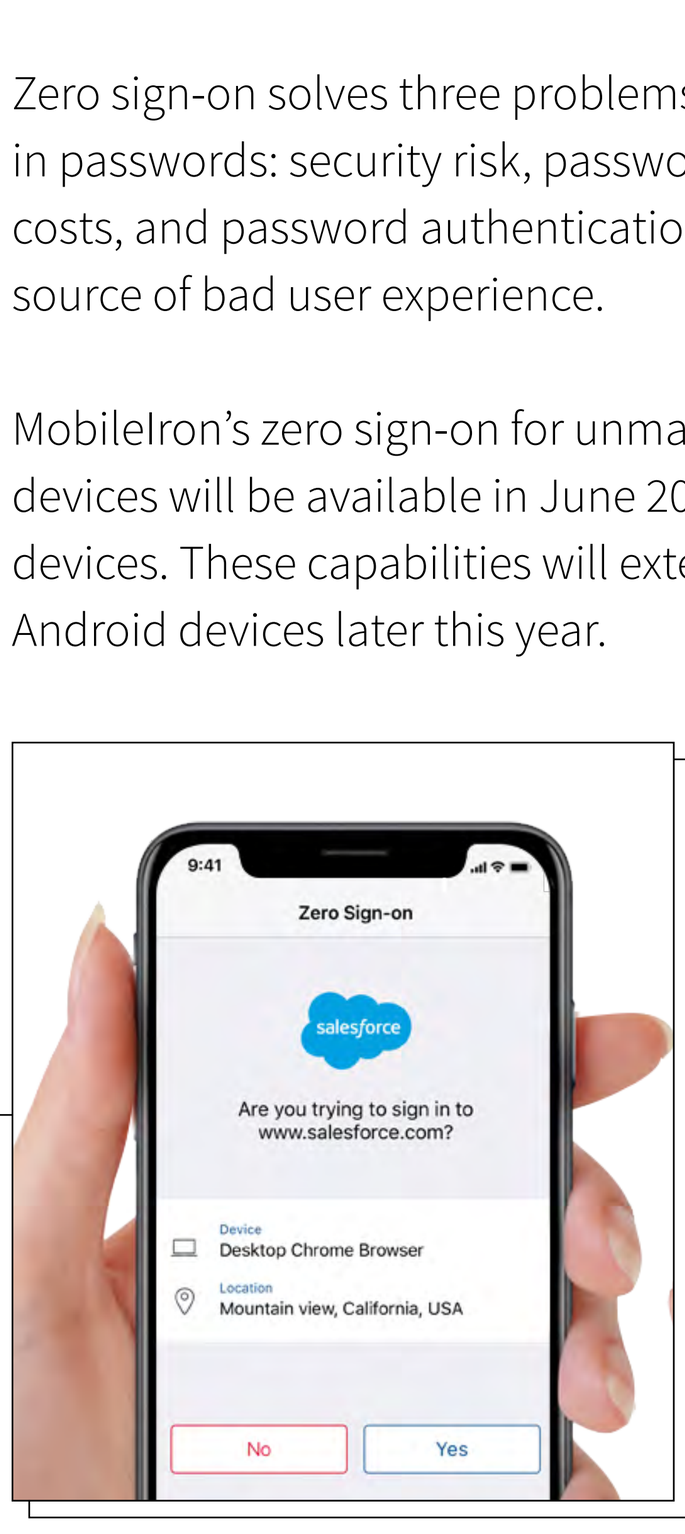
MobileIron introduces zero sign-on technology to eliminate passwords

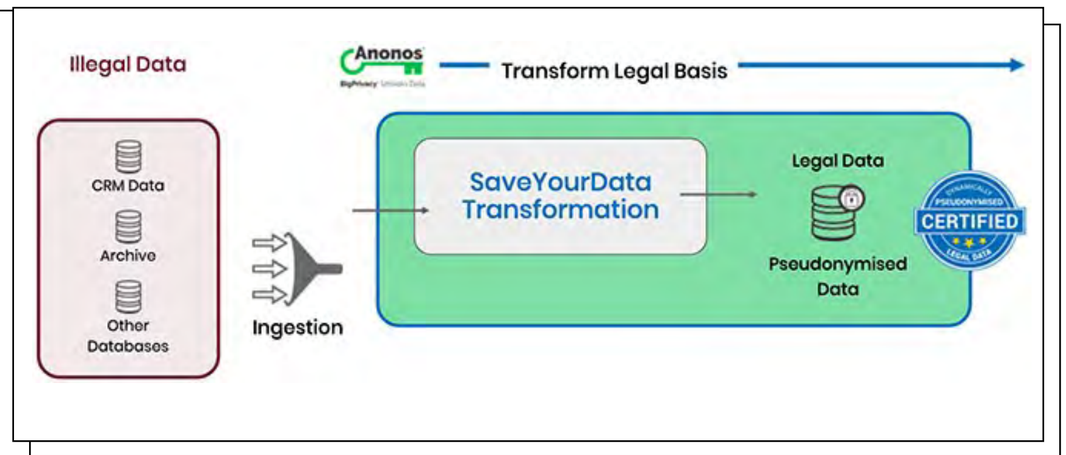
MobileIron introduced the industry's first mobile-centric, zero trust security platform, which allows for continuous enforcement and protection of data, both on the device and on the network, with comprehensive correlation between the critical signals for zero trust: user, device, apps, networks, and threats.

With mobile devices as your ID, organizations replace the password with a secure and frictionless alternative, ushering in a new era of user authentication. MobileIron is introducing a revolutionary zero sign-on experience built on the company's leading unified endpoint management (UEM) platform and powered by the MobileIron Access solution.

Zero sign-on solves three problems inherent in passwords: security risk, password-related costs, and password authentication as the source of bad user experience.

MobileIron's zero sign-on for unmanaged devices will be available in June 2019 on iOS devices. These capabilities will extend to Android devices later this year.





Anonos SaveYourData transforms pre-GDPR data into fully compliant data

Anonos launched SaveYourData, a software solution designed to allow companies operating under the EU GDPR to not only retain personal data collected before the law came into effect, but to also enable dynamic use of the data for analytics, machine learning, artificial intelligence and marketing activities.

Anonos SaveYourData transforms non-compliant consent-based pre-GDPR data into fully compliant data with a new legal basis that protects its long-term use for analytics, machine learning, artificial intelligence and marketing activities under legitimate interest processing.

SaveYourData is built around Anonos' patented dynamic pseudonymization technology which allows data use in a privacy-respectful manner. Using SaveYourData technology, data sets can be associated with dynamically generated pseudonyms that make innovative data use possible without exposing personal data to unauthorized re-identification. Anonos technology makes it possible under tightly controlled technical and organizational governance to enable data re-identification only for authorized purposes.

Anonos' patented technology and EuroPrivacy's certification of SaveYourData as fully compliant with GDPR pseudonymization requirements.

D3 operationalizes the MITRE ATT&CK framework, advancing its SOAR platform

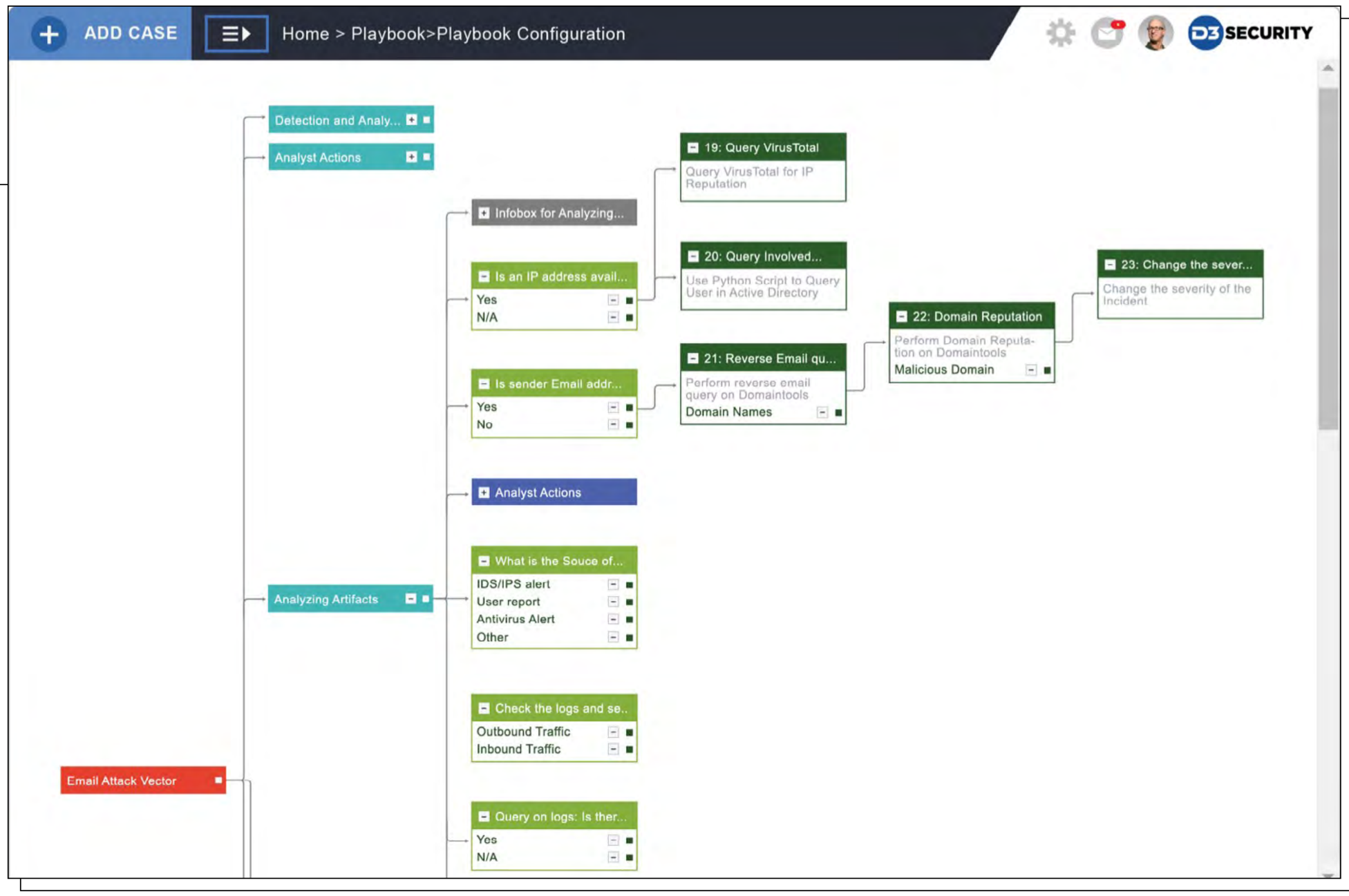
D3 Security has operationalized the MITRE ATT&CK framework, enabling the intelligent correlation of security events against the world's largest knowledgebase of adversary tactics and techniques.

D3's SOAR 2.0 treats events as links in a chain of adversarial intent, rather than as isolated occurrences.

When an event is ingested into D3, the system strips out IOCs and enters them into a kill chain discovery process, which identifies the ATT&CK techniques and tactics being used, and uses that information to search for correlated events. As more events are found, their IOCs and contextual data are entered back into kill chain discovery, continuously expanding the operator's view of the incident.

D3's SOAR 2.0 allows operators to predict adversary behavior based on patterns that MITRE has analyzed across their expansive knowledgebase of cyber attacks and threat indicators. This means that security teams do not need to search for needles in haystacks or hope that detection tools will catch every important event.

Instead, security operations and incident response teams can focus their efforts on the traces of attacks, techniques, and tactics that are highly correlated, prioritized, or in need of human attention.



Veeam Availability Orchestrator v2 to help orgs address operational, DR and data migration scenarios

Veeam Availability Orchestrator v2 expands its powerful orchestration and automation capabilities to a broader set of applications and VMs, helping organizations address a variety of operational and disaster recovery (DR) and data migration scenarios.

Other new features delivered in the release of Veeam Availability Orchestrator v2 include the ability to:

- More easily prove — and proactively remediate where necessary — service level agreement (SLA) attainment for internal and external compliance regulations and audits with enhanced reporting and compliance capabilities.
- Automatically leverage both backup and replica protection data for use cases beyond recovery verification, such as DevOps, patch and upgrade testing, analytics and more.
- Empower business units, application owners and operations teams with their own secure access to orchestration planning and testing resources

Endace launches new platform for monitoring in 10GbE networks

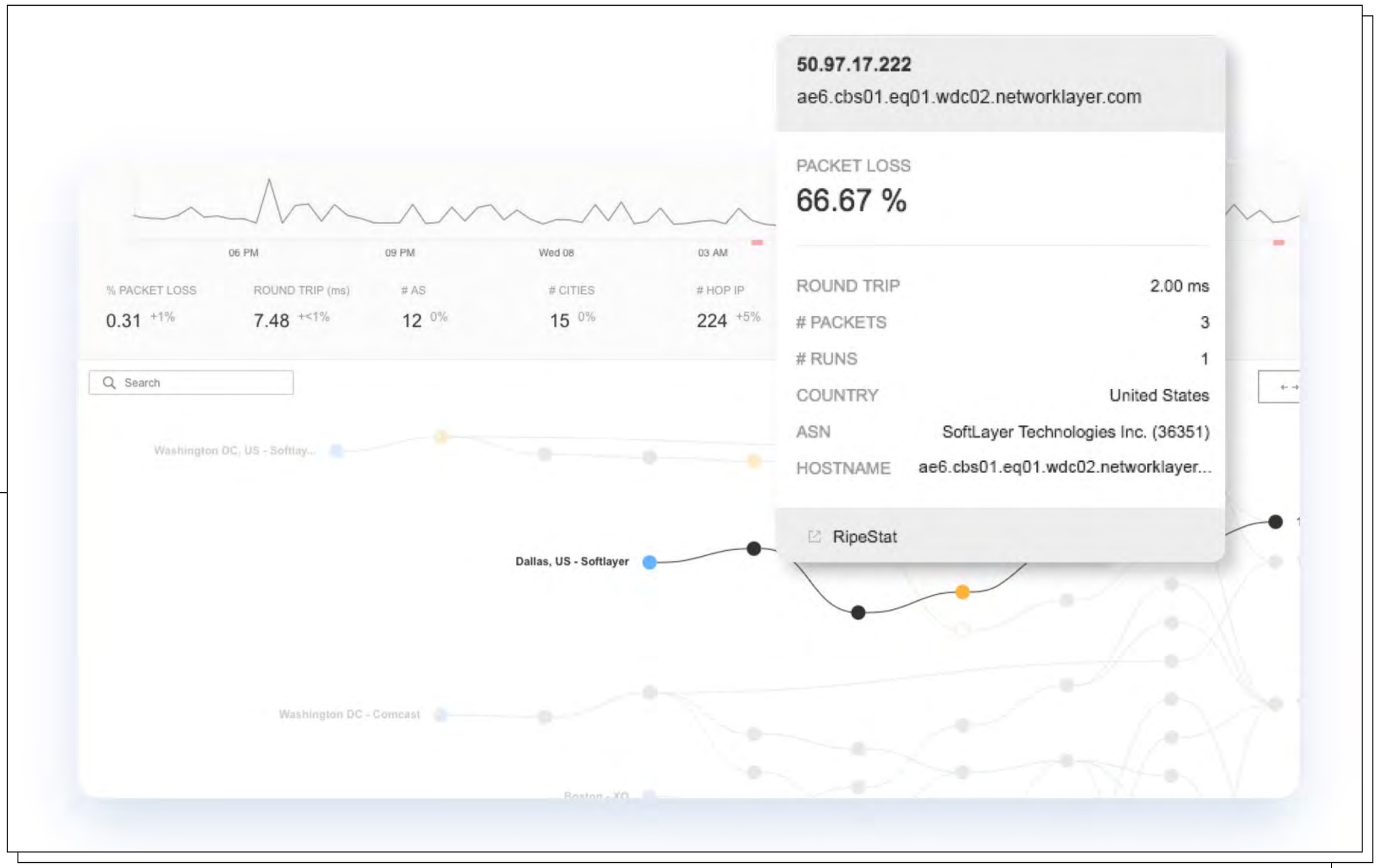
Endace launched its new EndaceProbe 8200 Series Analytics Platform for monitoring in 10GbE networks.

The new 8200 Series combines 100% accurate packet capture with deep storage capacity, rapid search capability and impressive hosting density in a very compact 2RU footprint. This modular approach allows customers to continually and cost-effectively expand their monitoring infrastructure.

With 360 terabytes of effective packet storage and write-to-disk speed of 15Gbps, the 8200 Series is an ideal building block for growing networks, allowing customers to easily scale packet capture speed, storage capacity and hosting capability as network bandwidth consumption increases over time.

The 8200's powerful hosting environment enables easy deployment of multiple security and performance analytics solutions from Endace's industry-leading Fusion partners, as well as from open source projects.

The EndaceProbe's modular design lets customers stack or group multiple EndaceProbes together to form a network-wide packet capture and analytics infrastructure. This centrally managed, centrally searchable infrastructure allows them to



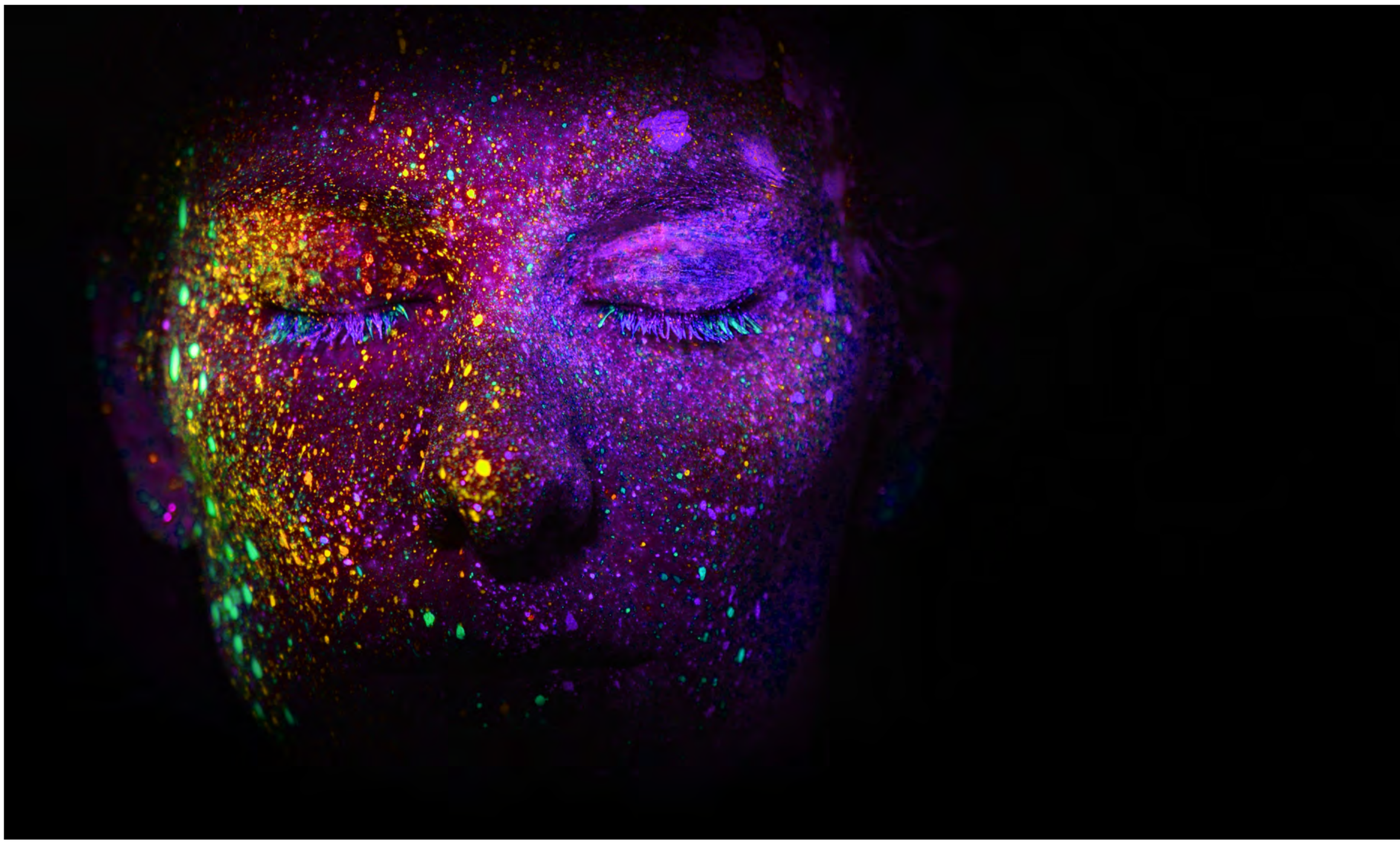
Catchpoint's new monitoring platform offers continuous visibility into all network dependencies

Catchpoint introduced Internet Intelligence, which shows a network's impact on the end user experience by continuously monitoring network health and network paths to private, public or hybrid clouds, CDNs, and other distributed IT architecture.

This far-reaching visibility isolates degradations across broadband, transit, last mile and wireless ISP networks that could negatively impact end users. It also reduces mean-time-to-detect and offers the ability to adjust network peering to optimize delivery speeds.

The Catchpoint Node Network's 800 IPv4 and IPv6 vantage points in 200 cities powers this capability.

With its vast geographic footprint, continuous monitoring via broadband and transit ISPs, and with monitoring agents on the world's leading dedicated internet providers such as Verizon, Comcast, Level3, China Telecom, and China Mobile, Catchpoint can pinpoint transit degradations to a specific ISP or peering point.



An intelligence-driven approach to cyber threats

AUTHOR_ Gene Yoo, CEO, Resecurity

In the age of big data, it is easy to think that only machines can detect a signal amid the noise. While it's true that big data tools can discover signals that might not be obvious, they can also create their own kind of noise in which the true signal — a true threat — can be lost.

> *Research indicates that less than 1% of reported anomalies represented actual threats and figuring out which detected threats constitute those dangerous few is exhausting, anxiety-inducing work.*

That's a problem anyone dealing with traditional security monitoring systems over the past few years has come to recognize. Threat detection systems have become extremely good at detecting anything that looks anomalous but, as the number of detected anomalies keeps going up, the number

of actual threats is still a small fraction of those. Research indicates that less than 1% of reported anomalies represented actual threats and figuring out which detected threats constitute those dangerous few is exhausting, anxiety-inducing work.

The need for human, contextualized intelligence

What security professionals suffering from alert fatigue need is threat intelligence that has already been vetted and contextualized by human beings. Big data and AI tools provide an abundance of data and they can identify events and activities of concern, but most security professionals within an enterprise have neither the training nor the time to make sense of the raw information. They need threat intelligence that has already been sifted, analyzed and contextualized, a "finished intelligence" that is "actionable" to their organizations.

> *Human intelligence teams can bring insight to the interpretation of raw intelligence that no machine can.*

That's where human intelligence professionals and threat hunting teams come into play. These professionals detect a different kind of threat than those detected by big data and AI tools. If machine tools excel at detecting individual trees, human intelligence professionals excel at understanding the character of the forest. They can detect code phrases and double meanings in dark web conversations that machine tools may not detect (until they've been trained to do so). They can consider the motives of threat actors and the connections that bind them. They can examine the actions of these actors, even actions that are ostensibly benign, and occasionally detect a plan in those activities long before a machine can detect an exploit resulting from those actions.

Augmenting intelligence for a more focused response

I'm not suggesting that human intelligence professionals and threat hunting teams replace the monitoring and detection systems. Instead, they can augment and enhance the raw intelligence captured by these powerful machine tools. Human intelligence teams can bring insight to the interpretation of raw intelligence that no machine can. They can connect clues with the glue of experience and contextual understanding, which no machine yet does.

The challenge of acting on augmented intelligence

There's one problem with gaining access to this kind of augmented intelligence: few organizations are in a position to use it effectively. The defensive infrastructure of most organizations is still cluttered with old walls erected to stop older threats, and the work of tuning those defenses remains a serious challenge.

Security personnel within an organization need deeper insight into the hardware, software and services informing the organization's infrastructure. Finished intelligence is going to provide much more focused information about which organizations are at risk, at which points of vulnerability, and for what reason. A new threat may take advantage of a vulnerability in firmware on a certain class of IoT device, for example, but a security team can only act upon that information if they know that they have those devices in their IoT estate and at what release level their firmware is.

What enterprise security professionals need is a way to operationalize this finished threat intelligence. They need tools that can provide deep insight into the hardware, software and processes informing the operational ecosystem of the enterprise, including

its endpoints, networks, clouds, IoT devices, supply chains and more. Moreover, they need tools that can enable them to make changes to any element in that ecosystem in a streamlined and orchestrated manner.

> *An intelligence-driven approach to cyber threats requires movement on two fronts simultaneously.*

Better threat intelligence creates an opportunity for an enterprise to mount a proactive cyber defense, but without an ability to operationalize that threat intelligence, the enterprise may not be able to launch the defense effectively in advance of the impending attack. With tools to operationalize this threat information, an organization can respond quickly and effectively to protect its people, data and processes — even its brand and reputation — from any emerging cyber threat.

Moving forward

An intelligence-driven approach to cyber threats requires movement on two fronts simultaneously.

We need to continue to gather and analyze threat data aggressively. Finished intelligence that has been vetted and contextualized by human intelligence experts and threat hunting teams can be passed on to the security professionals within an organization. The latter can then proactively implement the appropriate precautions to protect the enterprise against the real threats in the environment.

Is curiosity killing patient privacy? Combatting insider threats in the healthcare contact center

AUTHOR_ Gary E. Barnett, CEO, Semafone

The digitization of healthcare is changing the face of fraud. With the advent and growth of electronic health records (EHRs), online patient portals and virtual clinics, a wealth of sensitive medical information is available across multiple digital channels and while hackers and cybercriminals pose a massive risk to this information, it's not just "outside" fraudsters you should be concerned about.

Almost 60 percent of healthcare data breaches originate from insiders.

Insider threats are increasingly putting patient data at risk. Employees within a healthcare organization can often access a patient's protected healthcare information (e.g., medical history) or personally identifiable information (e.g., social security number, payment card data) without a valid reason. Despite the numerous laws and industry standards designed to protect patient data – the Health Insurance Portability and Accountability Act (HIPAA), the Payment Card Industry's Data Security Standard (PCI DSS), the new EU General Data Protection Regulation (GDPR) – data breaches in the healthcare industry continue to occur at a rate of more than one per day in the US. Though employees can lose their jobs, their professional licenses or even face prison time for inappropriately accessing or sharing a patient's data, the temptation to snoop often proves too great. In fact, almost 60 percent of healthcare data breaches originate from insiders.

Sometimes the temptation for an unsolicited peek at medical records arises because the patient is a celebrity. For example, late actress Farrah Fawcett's cancer diagnosis was leaked to the *National Enquire*r by an employee of the UCLA Medical Center – *before* Fawcett had a chance to personally tell her family or even process the devastating news herself. Similarly, when Michael Jackson passed away, unauthorized

staff, including contractors and medical students, accessed his death certificate more than 300 times. More recently, NFL player Jason Pierre-Paul suffered a hand injury that necessitated the amputation of one of his fingers. While he was in the hospital, two employees leaked his medical information to ESPN – a potentially career-altering blow right when he was negotiating a $60 million contract with the New York Giants.

Many large healthcare systems are the size of a small city and there are numerous factors that can contribute to cases of insider fraud or compound the risks of a potential data breach.

It's not only celebrities who must worry about the privacy of their PHI, though. Private citizens also fall victim to healthcare data breaches. Cases can be as innocent as a concerned friend or neighbor curious to know why their acquaintance has checked into the hospital, or more nefarious in nature, such as a disgruntled former friend or ex-lover seeking revenge. In other cases, the patient's healthcare data is used for identity theft or fraud. For example, UMass Memorial Healthcare recently agreed to pay $230,000 to resolve a lawsuit when two employees inappropriately accessed patients' data and used the information to open credit card and cell phone accounts. In fact, one in five healthcare provider employees admit they would be willing to sell confidential patient data – a truly shocking statistic.

Though human curiosity will never go away, the right training, tools and technology can help healthcare organizations mitigate the risks posed by insiders and better protect their patients' personal information.

Now, all this is not to say that employees in the healthcare industry are bad. In fact, most are loyal and honest. However, many large healthcare systems are the size of a small city and there are numerous factors that can contribute to cases of insider fraud or compound the risks of a potential data breach.

I recently spoke with Phil Fasano, CEO and co-founder of Bay Advisors, LLC, and former executive at Kaiser Permanente and AIG. He mentioned that when he worked at Kaiser in the early 2000s the organizations had more than 300,000 employees, including some 60,000 to 80,000 temporary staff – contact center workers, custodians and administrative staff – working on any given day. With that many people, there will unfortunately be somebody with ill intentions at some point. Individuals employed in temporary roles or those where turnover is high may not be as familiar with compliance regulations or may be more tempted to violate the rules because they figure they will be long gone before they get caught.

Cost of a data breach

The fallout from a data breach can be disastrous for a healthcare organization. HIPAA violations can lead to fines that range anywhere between $100 and $50,000 per violation or per record. And breaches in PCI DSS compliance – for example, failure to adequately secure patients' payment card information in the healthcare contact center or billing and collections department – can range from $5,000 to $500,000 per month. For repeated offences, the payment card brands can even revoke the right of the healthcare organization to process transactions using their cards. And these costs don't even begin to consider the damage done to a healthcare organization's brand reputation when a data breach occurs and patients no longer believe their provider or insurer is adequately protecting their personal information.

Though human curiosity will never go away, the right training, tools and technology can help healthcare organizations mitigate the risks posed by insiders and better protect their patients' personal information. Here are a few best practices you can implement *today*:

Best practices for securing patient data from your curious employees

- **Background checks** – I cannot stress enough the importance of conducting thorough background checks on all employees, even temporary staff and contractors. Many organizations skip this step, but there should be no exceptions and no excuses. Background checks can be critically important in identifying individuals who should not be allowed to work in roles that have access to PHI, payment card information or any other type of sensitive data.
- **Compliance training** – All employees with access to any type of sensitive data – whether patient medical histories or billing and payment information – should undergo thorough data security and privacy compliance training. At a minimum, they should be trained on the relevant requirements for HIPAA, GDPR and PCI DSS. Employees should have their training refreshed at least annually.
- **Limit access to sensitive data** – Healthcare organizations should enforce the principal of least privilege user access (LUA) on all computer systems. LUA states that an employee should only have the minimum level of access necessary to do their jobs. For example, an agent in the health system's contact center needs access to some patient information in order to accept payments or schedule appointments; but they should not be able to access the patient's private medical history or pull up their information when they are not on the line with the patient.
- **Segment networks** – Healthcare providers should segment their networks not only to strengthen data security, but also to ease regulatory compliance. For example, with a segmented network, the healthcare provider need only worry about PCI DSS compliance on the portions of the network where payments are processed and transmitted. By accepting payments on dedicated terminals that are separate from ordinary business activities like email, the healthcare provider can limit the scope of compliance for PCI DSS and HIPAA alike, potentially saving tens of thousands of dollars and many man hours in compliance program costs.
- **Break the glass** – Healthcare organizations should adopt "break the glass" solutions that alert appropriate staff if an employee views sensitive patient data unnecessarily or asks the employee to re-enter their password when accessing confidential information or the records of a high-profile patient. Some even use sophisticated pattern recognition to automatically flag suspicious activity, such as when an employee who views tens of thousands of patients records a month, when his peers typically only view a few thousand. The growth of technologies like machine learning are making these solutions more sophisticated and available to healthcare providers of all sizes.
- **Don't keep data you don't need** – No one can hack data you don't hold. In addition to segmenting their networks, healthcare organizations should, when possible, keep sensitive data out of their IT and computer systems in the first place.

Ultimately, protecting the confidentiality of PHI, PII and sensitive payment card data is part of the responsibility of healthcare providers, as an extension of the Hippocratic Oath to respect the privacy of patients. That includes securing patients' medical records and cardholder data from both inside and outside threats, whether their intent is malicious or simply curiosity. By adopting best practices and technologies healthcare providers can ensure their patients' privacy, and trust, remains intact.

Is Your Security More WTF than WAF?

Level Up Your Protection with Blocking That Doesn't Break Your App.

Signal Sciences next-gen web application firewall and runtime application self-protection are built to protect the modern web.

Find out how at **signalsciences.com**

Signal Sciences

Events

(ISC)2 Security Congress 2019

October 28-30, 2019
Walt Disney World Swan and Dolphin Resort, Orlando, FL, USA
http://congress.isc2.org/d/pbqql6?RefID=helpnet

(ISC)2's 2019 Security Congress will unite industry colleagues from around the globe for three days of education, best-practice sharing and networking in a variety of formats.

With more than 100 tactical, focused learning opportunities, this event will advance a global perspective and vision as our premier conference for cybersecurity professionals.

With hands-on learning opportunities like CISSP, CCSP, Security Architecture and CISO 2-day training courses, Career Center, and a Networking Night at House of Blues, this is the conference to add to your must-attend list. (ISC)2 members are eligible for special discounted pricing and will earn CPEs.

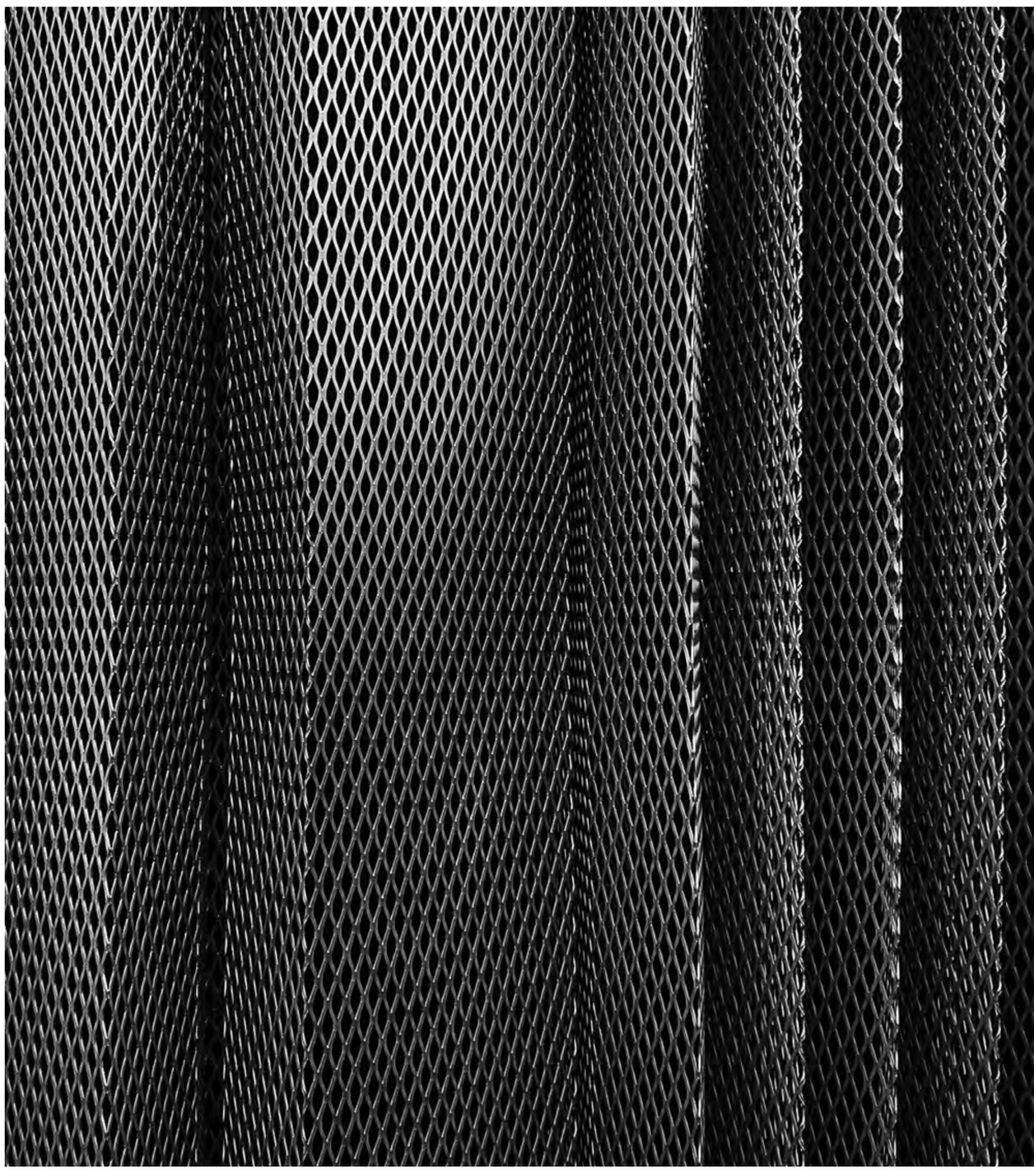
HITB+CyberWeek

October 12-17, 2019
Abu Dhabi, UAE
https://cyberweek.ae

Hack In The Box (HITB), known for its cutting-edge technical talks and trainings in computer security, is launching its biggest global event to be held in Abu Dhabi, UAE from 12-17 October 2019. HITB+CyberWeek will bring together the world's top thinkers and cyber security experts to share their latest knowledge, ideas and techniques among security professionals but also students.

HITB+CyberWeek will feature:

- World's top 25 Capture the Flag teams competing in a new style of attack and defense contest featuring a record-breaking prize pool of US$100,000
- The best bug hunters and ethical hackers competing in an all-new coordinated bug bounty contest with US$1.5 million to be won
- New challenge for Artificial Intelligence (AI) enthusiasts with US$100,000 in prize money to develop future cyber security tools using machine learning
- Growing knowledge and nurturing capabilities with a Capture the Flag competition for high school and university students, bringing the winners of Belgium and Germany's Cyber Security Challenge to Abu Dhabi for the finals



Protecting applications against DFA attacks

AUTHOR_ Sam Kerr, Senior Director of Product Management, Arxan

2001 was an exciting year for cryptography: the new Advanced Encryption Standard (AES) specification was finalized, making a mathematically secure and performant encryption algorithm available to the public. Designed to replace older cryptographic algorithms that were starting to show weaknesses in their math and to be vulnerable to the increasing computing power available to attackers, AES put the power back in the hands of those trying to protect their data. Attackers quickly recognized that brute force attacks and attacks on the math of AES were going to be ineffective and that they needed a new approach.

Attackers inject faults in different parts of the app until they find a place where a fault changes the output of a crypto operation in a specific way.

What is Differential Fault Analysis?

With the first research paper on the topic published in 2002, Differential Fault Analysis, or DFA, is an attack technique that is designed to recover cryptographic keys from apps by injecting "faults" into the app's crypto code at runtime and observing changes in the app's behavior. A fault is essentially flipping a bit inside an internal calculation and observing what changes. Faults can be injected in a variety of ways, such as varying power levels in hardware devices or changing bits of memory in software.

Attackers inject faults in different parts of the app until they find a place where a fault changes the output of a crypto operation in a specific way. Based on how the crypto operation's output changes, DFA and some math can allow crypto keys to be recovered. Once those keys are recovered, any data encrypted with them is at risk.

Originally, DFA was an an attack primarily against hardware devices, where machine code was not readily available for attackers to view. The software case was much more straightforward, since crypto keys were usually clearly visible inside the app code, which disassemblers could easily display. For a long time, if a piece of code was doing cryptography, it was kept in a secure environment to prevent attackers from looking at it and find the used keys.

This has changed dramatically: consumers today have many apps on their mobile phones, desktop computers, smart TVs, and even automobiles. Because attackers could now simply look at the code in the app, apps needed protection for their cryptographic routines and keys. White-box cryptography was introduced in 2002 to address this exact concern.

> *DFA is no longer purely an attack limited to academia or high-end security labs.*

White-box cryptography was introduced to make it possible to provide secure cryptographic implementations in apps where attackers can manipulate the code and data at will. White-box cryptography is a way to get the same output for a given input as a normal cryptographic implementation, but the internals of how it is done are completely different from a standard crypto implementation. This makes it very difficult for an attacker to understand what is happening. Because of the difficulty they had understanding white-box crypto implementations, building off the success in hardware, attackers began to use DFA as a technique against white-box cryptography in software implementations.

Defense against DFA attacks

DFA is becoming more common. Various security researchers speak about DFA attacks at conferences, they implement hardware and software DFA attacks, and publish how-tos. DFA is no longer purely an attack limited to academia or high-end security labs. Real-world attacks are occurring and, with the proliferation and weaponization of the attack code, the frequency of reported attacks is increasing.

As DFA advances in effectiveness and commonality, it is imperative to ensure that your defenses against it are keeping pace and are still able to protect the cryptographic routines inside your app. There are several steps you can take to ensure that you are doing as much as possible to defend against DFA attacks.

The first is ensuring that you are using a modern white-box cryptography implementation which is designed to defend against DFA and is tested against the latest versions of the attack. Because the attacks grow in sophistication over time, is important to use a white-box implementation that is actively developed to keep pace with new attacks.

Secondarily, you should ensure that your application is using app shielding to make it more difficult for attackers to mount a DFA attack in the first place. Applications with obfuscation make it difficult for attackers to understand where to inject faults and applications that can recognize when they are under attack can immediately take action to stop the attack before it progresses.

As companies increasingly rely on networked systems and on the Internet, cybersecurity threats have grown. Companies that fall victim to a successful cyberattack incur substantial costs for remediation, including increased costs tied to cyber-protection, lost revenues, legal actions and more. All of these costs can impact the riskiness and value of a public company's stock.

The SEC demands better disclosure for cybersecurity incidents and threats

AUTHOR_Rob Scott, CEO & President, Cygilant

In February of 2018, the SEC issued a Commission Statement and Guidance that spelled out principles that public companies should follow in making disclosures about cybersecurity dangers and attacks.

Given the frequency, magnitude and cost of cybersecurity incidents, the US Securities and Exchange Commission (SEC) has stated that it is "crucial for public companies to inform investors

about relevant cybersecurity risks and incidents in a timely fashion."

In February of 2018, the SEC issued a Commission Statement and Guidance that spelled out principles that public companies should follow in making disclosures about cybersecurity dangers and attacks. This guidance expands on a previous SEC staff guidance released in 2011 and addresses two new topics:

1_Cybersecurity disclosure policies
2_The application of insider trading prohibitions in a cybersecurity context

The following are the five key issues the SEC outlines in the guidance. (Note that this discussion is for information only. For personalized compliance recommendations, please consult a lawyer.)

1_Materiality

In the past, when companies filed disclosures required by the Securities Act of 1933 and the Securities Exchange Act of 1934, they may have disclosed cybersecurity risks and incidents on a periodic basis or when issues became "material"—significant enough to disclose—delaying disclosure when an incident was still under investigation.

> *The SEC advises companies to avoid generic disclosures and tailor them to their particular cybersecurity risks and incidents.*

The 2018 guidance lowers the threshold for disclosure. Companies should now disclose "known trends and uncertainties," says Brian V. Breheny, a partner who heads the SEC Reporting and Compliance Practice at Skadden, Arps, Slate, Meagher & Flom LLP. "If something is reasonably likely to result in a material impact on the company, you should give investors an early warning."

In determining what is material, the guidance suggests that companies consider the nature, extent and potential magnitude of the event and the harm such incidents could cause. Companies should disclose enough information so that statements are not misleading and correct prior disclosures that later prove to be untrue. On the other hand, the SEC does not intend for companies to make disclosures detailed enough to compromise their cybersecurity efforts.

2_Types of security risks that must be disclosed

Item 503 (c) of Regulation S-K (of US Securities Act of 1933) and Item 3.D of Form 20-F (which must be submitted by "foreign private investors") require companies to disclose the most significant factors that make investments in their securities speculative or risky. The new guidance recommends that companies include cybersecurity risks and incidents in these disclosures. The SEC advises companies to avoid generic disclosures and tailor them to their particular cybersecurity risks and incidents.

When David J. Lavan, Partner at Dinsmore & Shohl LLP and former special counsel in the Division of Corporate Finance at the SEC, works with clients, some key risk factors he considers include:

- What industry is the company in? Some industries are subject to more cybersecurity threats than others. Finance, healthcare, retail and utilities are far more likely to be attacked than construction, for example.
- Has the company had any cyber-related incidents? What type of incidents have they had?
- Do they have data about their customers? Employees? Agents? Deposit holders? Policy holders?
- What information does the company store or transmit? Personally identifiable information? Healthcare info? Proprietary info? Info in the public domain?
- What regulations is the company required to comply with? NYDFS? GDPR? CCPA?
- Is there anything in the contract with the company hosting the client's data or providing cloud services that might impact other companies storing information in that facility?
- Does the company have business recovery procedures in place?
- Does the company have insurance? How does this affect the company's ability to recover from a cybersecurity incident? Disclosing this in the 10K helps investors understand who is responsible for cyber-related operational risk.
- Does the board understand its disclosure responsibility?
- Does the company understand how to perform cyber-related risk reporting? Can they report fast enough for the risks to be considered properly by the company's disclosure committee?
- Are the security risks changing? Has there been an uptick in clients getting pinged even if no one's getting through?

3_Disclosure policies and procedures

The Guidance encourages companies to adopt comprehensive cybersecurity policies and procedures and regularly assess their sufficiency and compliance. The assessment should include the efficiency of the company's disclosure controls and procedures related to cybersecurity risk.

"Cybersecurity incident teams should be well coordinated with disclosure compliance and other non-IT professionals within the company. Disclosure controls and procedures should ensure that relevant information about cybersecurity risk is collected and documented in a timely fashion and that it is reported to the appropriate personnel to assess its materiality," N. Peter

Rasmussen, Senior Legal Analyst at Bloomberg Law, explains.

"Companies are under cyberattack all the time. Whether these ongoing risks become material and whether they need to be disclosed are different questions," Breheny notes. "The issue is whether individuals involved in cybersecurity are elevating issues that come up quickly enough and to the right people to determine whether something needs to be disclosed."

If the company's controls and procedures fail to ensure that information about a cyber incident is properly raised for timely disclosure and the company made the certifications anyway, the CEO and CFO could be at risk for enforcement action.

The company's CEO and CFO must certify the controls. If the company's controls and procedures fail to ensure that information about a cyber incident is properly raised for timely disclosure and the company made the certifications anyway, the CEO and CFO could be at risk for enforcement action.

4_Role of officers and the board

Item 407(h) of Regulation S-K and Item 7 of Schedule 14A requires companies to disclose the board of directors' role in overseeing company risks, including how the board administers its oversight function and the effect this has on the board's leadership structure. With the 2018 guidance, the SEC emphasizes the board's role in monitoring and overseeing cybersecurity risk. The guidance implies that cybersecurity is clearly a board-level concern and not just a matter for the tech department.
La Fleur C. Browne, Associate General Counsel and Assistant Secretary, Church & Dwight, says her firm's board has a disclosure committee that regularly evaluates what needs to be included in disclosure statements. "Different people might view materiality differently. When the guidance first came down, our disclosure committee met with our IT department to review the guidance, discuss the types of threats they see, and explain that they should let the committee know what's going on. IT has committed to report any cybersecurity incidents to the disclosure committee, which in turn determines whether the issue is material and should be disclosed."

The head of IT now attends Church & Dwight Disclosure Committee meetings to provide updates on cybersecurity so the committee can have informed discussions. The disclosure keeps the CEO and CFO informed about what IT is seeing and whether it's material to the company. Our board also has a cybersecurity item on the agenda of every board meeting and has a deep dive discussion about cyber security at least once a year."

5_Insider trading

Finally, the 2018 Guidance requires companies/directors to comply with laws regarding insider trading in connection with information about cybersecurity risks and incidents. Companies should have well-designed policies and procedures to prevent insider trading based on cybersecurity risks and incidents.

Overall, in light of the 2018 Guidance, Rasmussen notes that it's fair to say that we can expect the SEC will take a closer look at cybersecurity disclosures by public companies. "Issuers must anticipate the questions the SEC will have. And the SEC has indicated that it will emphasize risk factor disclosures, the timely disclosure of cyber incidents, insider trading controls and the effectiveness of the company's data security policies and internal accounting controls. We can expect to see greater enforcement activity based on inadequacies in these areas of disclosure."