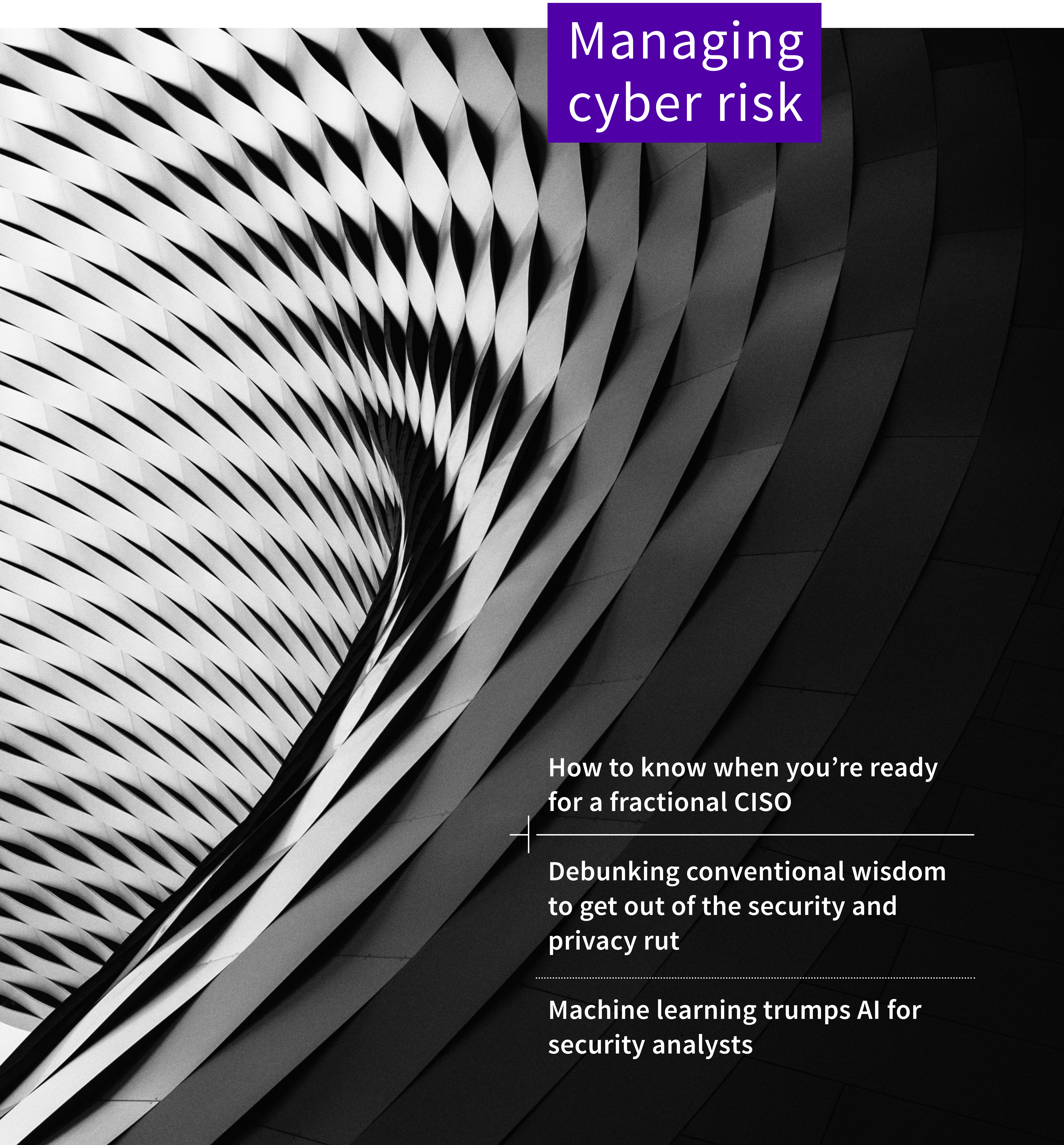
[+] (IN)SECURE Magazine

02 | 2019

ISSUE 61



Managing cyber risk

How to know when you're ready for a fractional CISO

Debunking conventional wisdom to get out of the security and privacy rut

Machine learning trumps AI for security analysts

(ISC)²

SECURE SUMMIT / EMEA

ENRICH ENABLE EXCEL

EARLY BIRD REGISTRATION OPEN

15–16 April 2019 | World Forum, Hague

The 2019 (ISC)² Secure Summit EMEA will bring together 400+ cybersecurity professionals over two days.

Based on the theme of Enrich. Enable. Excel., our summit provides a highly interactive educational programme that tackles today's current concerns.

This is the perfect opportunity to enhance your skills and meet with peers from all levels of practice and across a range of industries to discuss common challenges.

Surround yourself with a trusted support network of colleagues, and career mentors and advisors, join a Chapter or get involved in other initiatives.

Keynote Speaker

Felicity Aston

MBE, British Polar Explorer
Scientist, Author

Pre-Summit
Workshop Day Open to
All Conference Attendees
14 April, 2019

REGISTER ON

securesummits.isc2.org

Discount available for (ISC)² members, Chapter members and students.

#ISC2Summits

Table of contents

Contributors

MIKE BURG, Director of Strategic Advisory, Alagen
JON FIELDING, EMEA Managing Director, Apricorn
DEAN SYSMAN, CEO, Axonius
KEITH BROMLEY, Sr. Manager, Solutions, Keysight
MENY HAR, VP of Products, Siemplify
ANDREA LITTLE LIMBAGO, PhD, Chief Social Scientist, Virtru
BRENDAN PATTERSON, VP of Product Management, WatchGuard Technologies

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

How to know when you're ready for a fractional CISO

AUTHOR_Mike Burg, Director of Strategic Advisory, Alagen

Many companies eventually find themselves in the following situation: they're growing, their technology, infrastructure and teams are expanding, perhaps a M&A is on the horizon, and the board is asking pointed questions about security. It's usually at this point that a business starts to notice fissures in the walls of what once felt like a tightly locked structure. New challenges in operations, culture, and security begin to arise.

Inevitably, when a company hits this phase of growth, the question of hiring a CISO comes up. Should you pull the trigger? Maybe. But maybe not.

A CISO is a big and important role for today's technology, healthcare, financial, and other regulated industries. Hiring a CISO means your organization has hit a point of scale where security is a top priority and needs to become more a part of the culture and the leadership.

Before you hire an expensive recruiter, spend months interviewing candidates and add a hefty new line to your budget, consider a fractional CISO. It's an option that could provide you with the security leadership you need while affording the most intelligent use of resources.

The benefits of a fractional CISO

Fractional CISO providers can be chosen to deliver the exact skills you require, exactly when you require them.

Consider an organization that is struggling to achieve and maintain PCI compliance for a complex environment. Beyond security expertise, the organization requires a PCI compliance veteran who understands the program-building and transformation journey ahead. Moreover, they require a proven business advisor, one who can educate management, guide investment decisions and build the coalitions necessary to ensure lasting success. The importance of introducing a seasoned strategist at this stage cannot be overstated. However, as you would imagine, these individuals are in short supply, and their premium rates would be wasteful expenditures as long-term resources.

A fractional CISO can be the best answer for a growing company that needs leadership and strategy, is heading into unknown or uncomfortable regulatory compliance waters, but isn't quite ready to pull the trigger on a full-time hire.

A fractional CISO can also have a keen eye for resourcing, creating efficiencies by leveraging external relationships and assessing in-house talent to ensure all levels of work will be performed by the best SME for the job. Whether delivering board-level messaging, guiding compliance fulfillment or simply developing security policies, fractional CISOs meet the unique demands of a growing business and its emerging security program.

The right time to make the hire

CISOs are often reactive hires. Major breaches and regulatory compliance pressures have been the driving forces to launch many security programs. Whatever the trigger, there is almost always a specific outcome required in a short amount of time.

Concurrently, this is when a company learns that their existing resources don't have the right leadership to address the security challenges at hand. Many times, organizations struggle to meet these needs by propelling a senior engineer into the ranks of leadership, only to later realize that they were not prepared for the work they were required to take on. In these instances, it quickly becomes obvious that a different kind of leader and strategy is necessary.

Particularly in these fledgling security programs, fractional CISOs are game-changers in helping emerging leaders span the void between technical know-how and business acumen. Whether operating independently or mentoring and up-leveling existing talent, the fractional CISO can help you jumpstart your security program and implement a program framework capable of serving you well into the future.

What to expect from a fractional CISO

Typically, the person in this role has been in the industry for many years, has had previous exposure to many security scenarios and has skillfully maneuvered his or her way through compliance audits that send many of us running in the opposite direction. Your fractional CISO is there to lead.

He or she will also bring a sophisticated level of visibility to the security program. A hot topic right now is the quantification of security risk. CEOs and boards want this assessed in financial terms. The fractional CISO should have the experience and knowledge to answer this particular call.

A fractional CISO can be the best answer for a growing company that needs leadership and strategy, is heading into unknown or uncomfortable regulatory compliance waters, but isn't quite ready to pull the trigger on a full-time hire. The fractional CISO can deliver the right mix of security leadership, strategic blocking and tackling, and can help optimize and mature your overall security program.

Debunking conventional wisdom to get out of the security and privacy rut

AUTHOR_Andrea Little Limbago, PhD, Chief Social Scientist, Virtru

Given the unprecedented rate of technological change, the dizzying news cycle, and an always-on social media mentality, it may be surprising to learn that when it comes to security and privacy, we are actually deep in a rut.

Faced with seemingly daily news stories of mega-breaches and unauthorized selling or sharing of personal data, the general public is overwhelmed with the contradictory feelings of defeatism and anger. Congressional hearings and legislative proposals have attempted to raise awareness of data privacy and security but, to date, little progress has been made. And all the while the security industry continues to advocate for "best practices" that even experts have trouble following consistently.

This rut persists largely due to conventional wisdom that has been taken as gospel but which, upon closer inspection, is blocking any technological or legal innovation in data security and privacy.

We see this same mentality dominating the social media business model, which takes for granted that ad-based revenue is the only possible business model. Dr. Zeynep Tufekci recently eloquently rejected this conventional wisdom, providing counter examples and alternative regulations to force a reimagining of revenue streams that are not dependent on the vast data collection behind an ad-based business model. We similarly must overturn the conventional wisdom that deters data privacy and security.

Here are four beliefs that must be debunked by the big tech and security communities in order to make meaningful progress towards a society that values and protects data privacy:

1_Data privacy protections hinder innovation

The conventional wisdom most embedded within the tech and business community is that data protection hinders innovation. This was a theme during the debate over the recently passed California Consumer Privacy Act (CCPA). However, this myopic perspective signals a general disconnect with the state of cybersecurity and attacks by criminals and nation-states on American corporations.

By some accounts, the intellectual property stolen from U.S. companies through digital means constitutes “the greatest transfer of wealth in history.” Intellectual property is at the core of innovation, and it is being plundered at historically unprecedented rates measured in the trillions of dollars. As a recent United States Trade Representative report highlighted, China alone is responsible for “unauthorized access to intellectual property, trade secrets, confidential business information, technical data, negotiating positions, and sensitive and proprietary internal business communications.” The lack of persistent, useable data protection tools and the absence of national privacy legislation are already hindering American innovation.

With trillions of dollars and the intellectual property that serves as the backbone of our economic prosperity and national security lost, we need to view data privacy and security as core to innovation, not a hindrance.

> *Corporate breaches extend well beyond personal secrets and target very specific and lucrative PII in addition to intellectual property.*

2_Data privacy is irrelevant if you have nothing to hide

Conventional wisdom also holds that data protection and privacy aren’t relevant for those who have nothing to hide. Even if you have somehow avoided social media, e-commerce and any tangential connection to corporate proprietary data, there’s still a good chance your financial, health, and personally identifiable information (PII) have been compromised. Corporate breaches extend well beyond personal secrets and target very specific and lucrative PII in addition to intellectual property.

After the Marriott breach, China is now considered to be the biggest threat to individual privacy. Having amassed consumer data - including social security numbers, birth dates, income and addresses - from the Office of Personnel Management, Anthem, and now potentially Marriott (to just name a few sources), consumers are direct victims when it comes to corporate attacks. You can even assess how much of your personally identifiable information has been stolen across all of the most high-profile breaches.

3_There is an inherent trade-off between security and convenience

Of course, data protection has historically been so cumbersome that even those who do take data privacy seriously find security “best practices” too difficult to implement. Conventional wisdom holds that an inherent trade-off must exist between security and convenience and has left us with the sage advice to avoid clicking on links and to memorize lengthy and complex passwords and change them often.

> *Finely tuned regulation is required to prompt innovation and safeguard privacy. This yet again turns conventional wisdom on its head, as thoughtful regulations can be the conduit for innovation in an industry so deeply muddled in unsustainable best practices.*

It is mind-blowing that this has been the state of security for so long. Also, data privacy and security best practices have disrupted business workflows, ignored user experience, and have been obscured within lengthy, esoteric terms of agreements for far too long. There are signs that this is slowly changing, but usable security must become a core part of development instead of being accessible to only the most sophisticated users.

4_Self-regulation is sufficient for securing data

Unfortunately, it does not seem like market forces will push data privacy out of its rut. As Apple’s Tim Cook recently noted, when it comes to privacy, “we have to admit when the free market is not working.” While self-regulation was once deemed sufficient for data privacy, there is finally an agreement that some regulation is necessary to protect data privacy.

Finely tuned regulation is required to prompt innovation and safeguard privacy. This yet again turns conventional wisdom on its head, as thoughtful regulations can be the conduit for innovation in an industry so deeply muddled in unsustainable best practices.

U.S. legislation has also been stalled for years, but 2019 may finally see some progress toward federal data privacy and security legislation. Driven by global forces such as the European Union’s General Data Protection Regulation and shifting domestic public opinion in favor of some form of data protection, Congress is feeling the pressure to do something about data privacy. This would be a welcome change, but lessons must be learned from existing efforts to ensure data protection legislation focuses on transparency, control, accountability, and feasibility.

Under the proper incentive structures - combining both carrots and sticks - regulations could provide the much- needed spark to elevate innovation in an industry that continues to spend billions of dollars with little progress to show for it.

The digital landscape is only growing in complexity. New technologies are infringing on data integrity and the proliferation of cyber capabilities and threat actors continue to expand without limitations on targets or impact. We must get out of the current rut in our approaches to data privacy and finally make concrete legal and technological progress that prioritizes data privacy as a fundamental right, as well as an economic and national security imperative.

Security world

Should enterprises delay efforts to remediate most vulnerabilities?

Companies today appear to have the resources needed to address all of their high-risk vulnerabilities. The research demonstrates that companies are getting smarter in how they protect themselves from today's cyber threats, improving operational efficiency and resource allocation, while best managing risk.

Cybersecurity researchers from Kenna Security and Cyentia Institute analyzed 3 billion vulnerabilities managed across 500+ organizations and 55 sources of external intelligence. They then took a deep dive into the realities of remediation using anonymized data from a sample of 12 enterprises that were selected to cover a range of industries, sizes, and remediation strategies.

They found that:

- Organizations have closed 70 percent of the critical vulnerabilities on their systems, but they still aren't as efficient as they could be. Out of the 544 million high-risk vulnerabilities, organizations remediated 381 million, leaving 163 million open.
- The data shows that organizations remediated a total of over 2 billion vulnerabilities, indicating that enterprises have the resources to address the vulnerabilities that pose the greatest risk. This can be accomplished by implementing remediation strategies that prioritize resources to tackle all of the 544 million high risk vulnerabilities first, only moving on to the 2.9 billion lower risk vulnerabilities afterward.

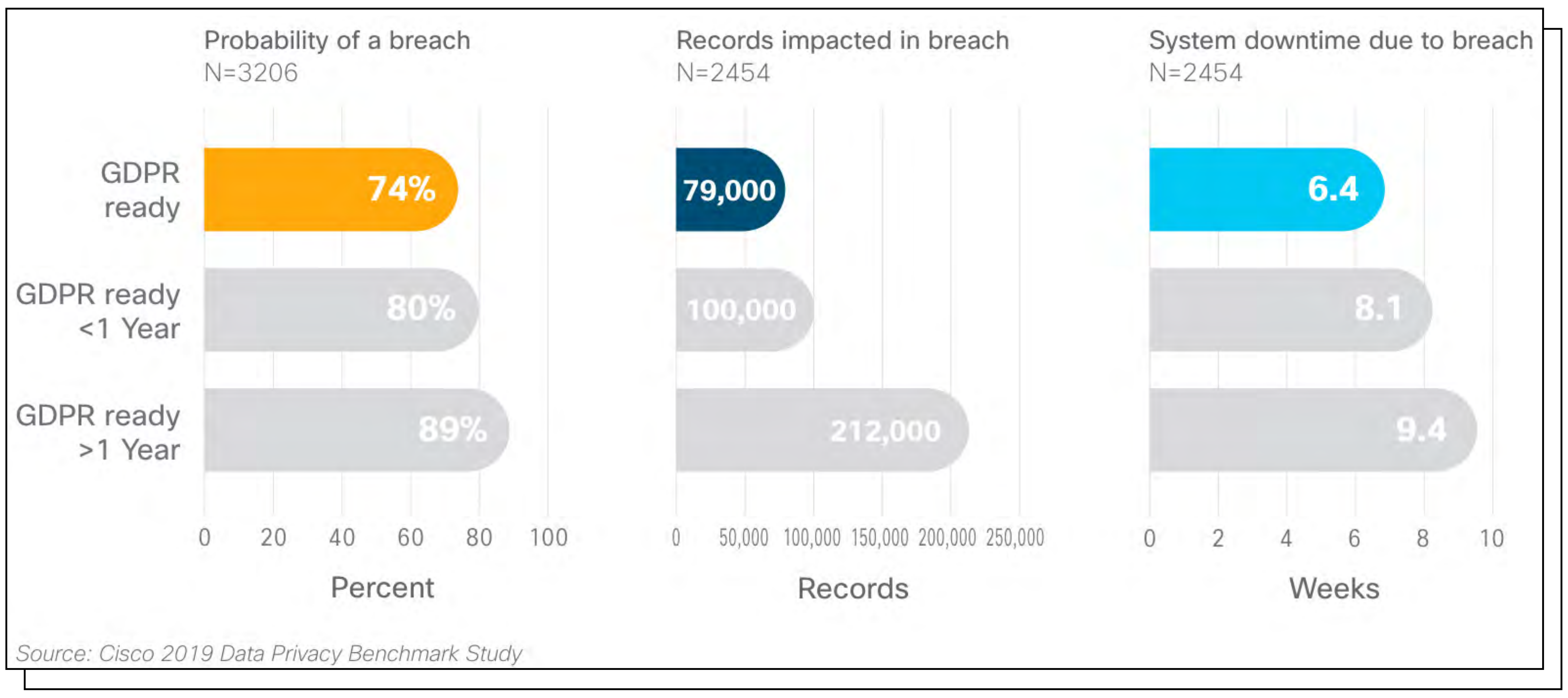
Enterprises are struggling with cloud complexity and security

The rush to digital transformation is putting sensitive data at risk for organizations, according to the 2019 Thales Data Threat Report – Global Edition with research from IDC. As organizations embrace new technologies, such as cloud deployments, they are struggling to implement proper data security.

According to the report, nine out of 10 respondents are using, or will be using, some type of cloud environment, and 44% rated complexity of that environment as a perceived barrier to implementing proper data security measures. In fact, this complexity is ahead of staff needs, budget restraints and securing organizational buy-in.

GDPR-ready organizations see lowest incidence of data breaches

Organizations worldwide that invested in maturing their data privacy practices are now realizing tangible business benefits from these investments, according to Cisco's 2019 Data Privacy Benchmark Study. The study validates the link between good privacy practice and business benefits as respondents report shorter sales delays as well as fewer and less costly data breaches.



Source: Cisco 2019 Data Privacy Benchmark Study

"This past year, privacy and data protection importance increased dramatically. Data is the new currency, and as the market shifts, we see organizations realizing real business benefits from their investments in protecting their data," said Michelle Dennedy, Chief Privacy Officer, Cisco.

Customers are increasingly concerned that the products and services they deploy provide appropriate privacy protections. Those organizations that invested in data privacy to meet GDPR requirements experienced shorter delays due to privacy concerns in selling to existing customers: 3.4 weeks (vs. 5.4 weeks for the least GDPR-ready organizations). Overall the average sales delay was 3.9 weeks in selling to existing customers, down from 7.8 weeks reported a year ago.

GDPR-ready organizations cited a lower incidence of data breaches, fewer records impacted in security incidents, and shorter system downtimes. They also were much less likely to have a significant financial loss from a data breach.

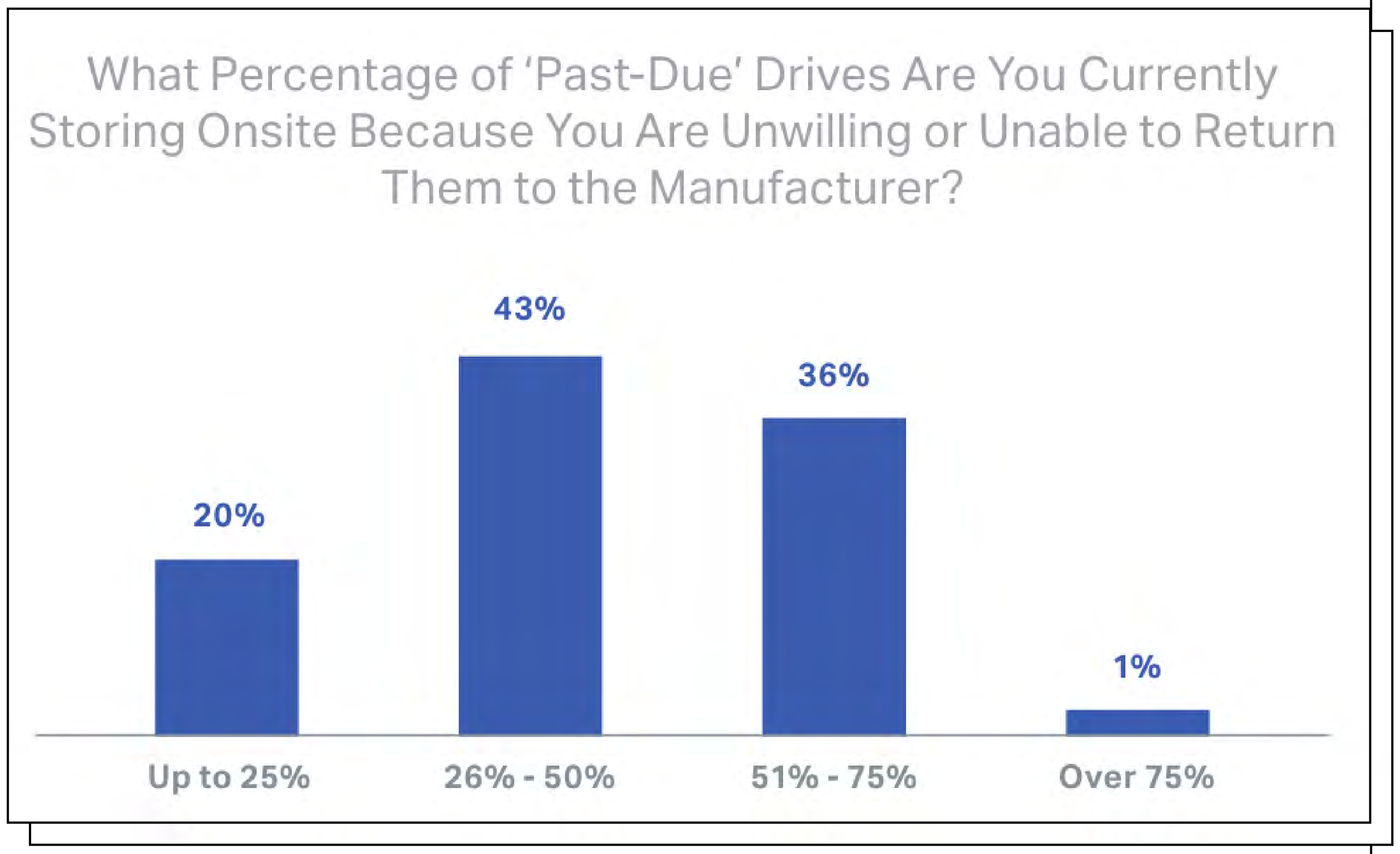
Reimagining risk management to mitigate looming economic dangers

In a volatile market environment and with the edict to "do more with less," many financial institutions are beginning efforts to reengineer their risk management programs with emerging technologies in the driver's seat, a new survey by Deloitte Global has revealed.

Seventy percent of the financial services executives surveyed said their institutions have either recently completed an update of their risk management program or have one in progress, while an additional 12 percent said they are planning to undertake such a renewal effort.

A big part of this revitalization will be leveraging emerging technologies, with 48 percent planning to modernize their risk infrastructure by employing new technologies such as robotic process automation (RPA), cognitive analytics, and cloud computing.

Organizations waste money storing useless IT hardware

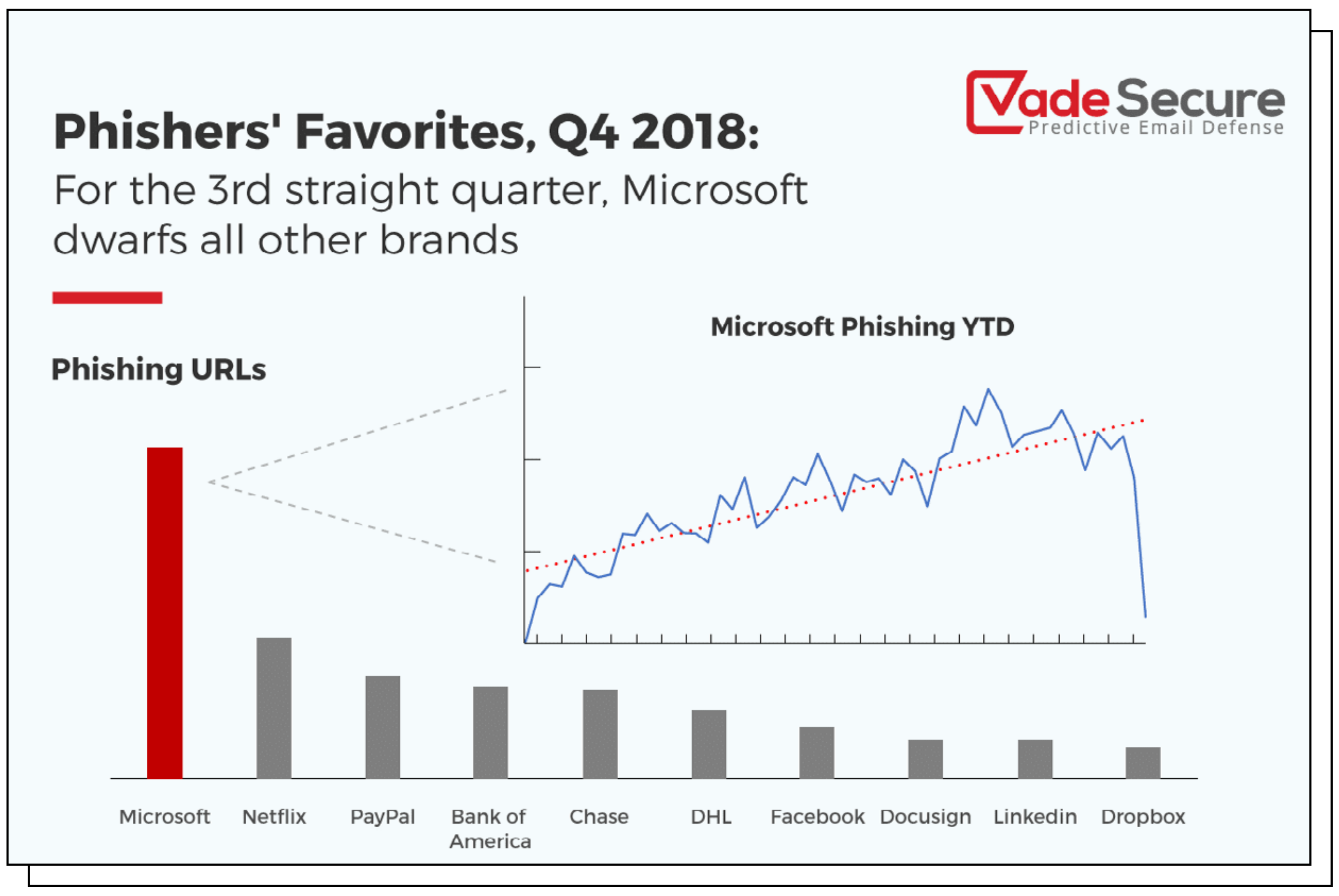


A survey of 600 data center experts from APAC, Europe and North America reveals that two in five organizations that store their data in-house spend more than $100,000 storing useless IT hardware that could pose a security or compliance risk.

Astonishingly, 54 percent of these companies have been cited at least once or twice by regulators or governing bodies for noncompliance with international data protection laws. Fines of up to $1.5 million could be issued for HIPAA violations due to storing data past its retention date, with that number multiplied by the number of years each violation has been allowed to persist.

Blancco's study, The High Cost of Cluttered Data Centers, produced in partnership with Coleman Parks, reflects the extent in which global organizations are paralyzed by fear of reputational damage. This is primarily the risk of sensitive data that is stored on old IT hardware of being breached or misused. Put simply, organizations are opting to spend vast sums of money storing these devices, contrary to data protection laws and regulations, rather than entrusting them to data erasure experts for wiping before reuse.

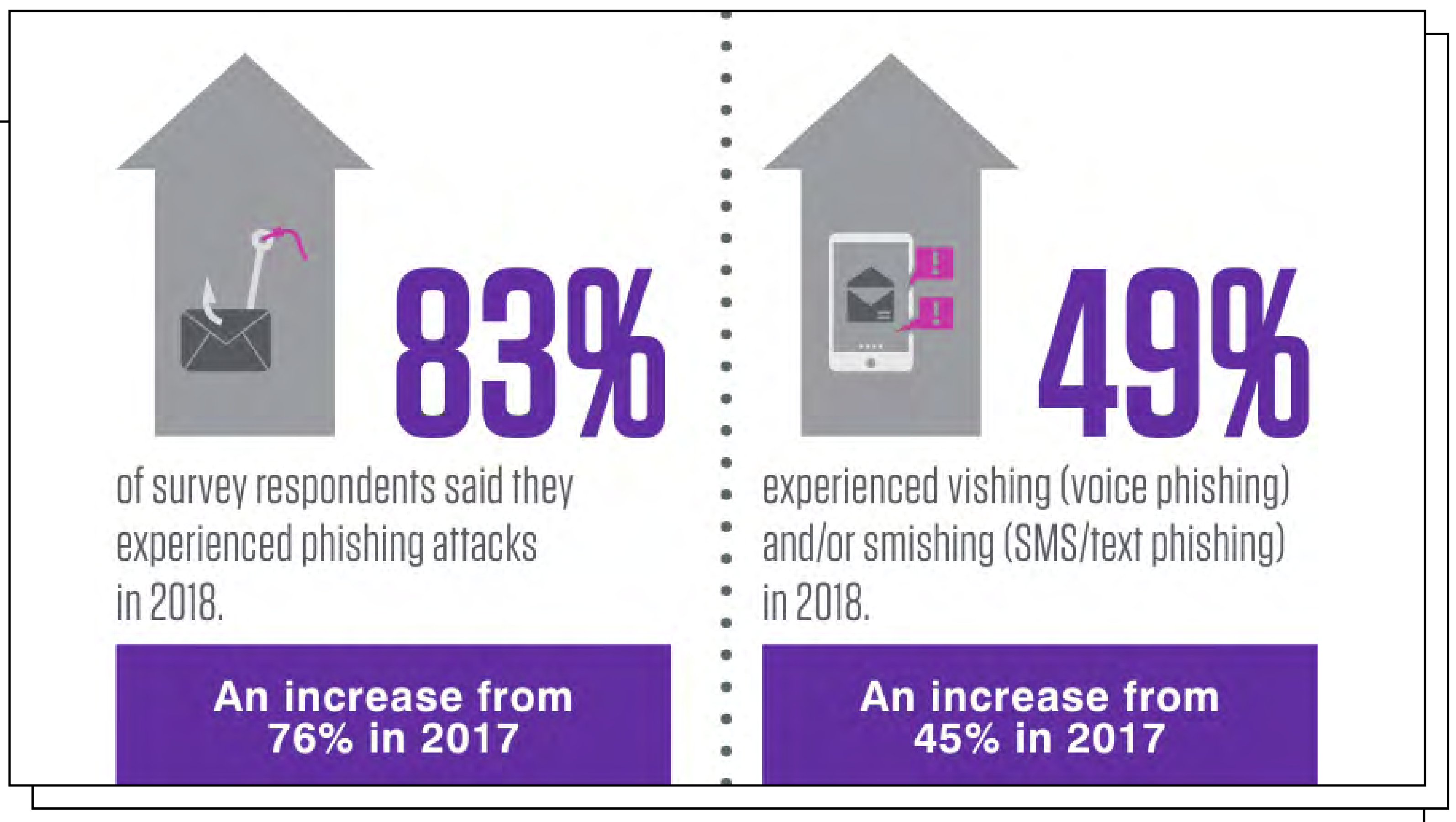
Microsoft remains the most impersonated brand, Netflix phishing spikes



Although Microsoft remains the top target for phishers, Netflix saw an incredible surge in December 2018, making it the second most impersonated brand in Q4 2018, according to Vade Secure.

Microsoft remains the #1 impersonated brand, receiving more than 2.3 times the number of phishing URLs than Netflix. One credential can provide hackers with an entry point to all of the apps under the Office 365 platform—as well as the files, data, contacts, etc., stored in them – meaning that they can use these legitimate accounts to conduct insider attacks on colleagues or spear phishing attempts targeting business partners. These types of multi-phased attacks have been steadily increasing over the past year and show no signs of slowing down.

83% of global respondents experienced phishing attacks



Proofpoint analyzed data from tens of millions of simulated phishing attacks sent over a one-year period, along with nearly 15,000 cybersecurity professional survey responses, to provide an in-depth look at state of global phishing attacks.

Overall, 83 percent of global information security respondents experienced phishing attacks in 2018, up from 76 percent in 2017, and nearly 60 percent saw an increase in employee detection following security awareness training. In addition, more organizations were affected by all types of social engineering attacks year over year. For the first time, compromised accounts bypassed malware infections as the most commonly identified impact of successful phishing attacks.

"Email is the top cyberattack vector and today's cybercriminals are persistently targeting high-value individuals who have privileged access or handle sensitive data," said Joe Ferrara, general manager of Security Awareness Training for Proofpoint. "As these threats grow in scope and sophistication, it is critical that organizations prioritize security awareness training and establish a people-centric strategy to defend against threat actors' unwavering focus on compromising end users."

Cybercrime could cost companies trillions over the next five years

Companies globally could incur $5.2 trillion in additional costs and lost revenue over the next five years due to cyberattacks, as dependency on complex internet-enabled business models outpaces the ability to introduce adequate safeguards that protect critical assets, according to Accenture.

Based on a survey of more than 1,700 CEOs and other C-suite executives around the globe, the report — Securing the Digital Economy: Reinventing the Internet for Trust — explores the complexities of the internet-related challenges facing business and outlines imperatives for the CEO's evolving role in technology, business architecture and governance.

Cybercrime from a wide range of malicious activities poses challenges that can threaten business operations, innovation and growth, and expansion, ultimately costing companies trillions of dollars. The high-tech industry faces the highest risk, with more than $753 billion hanging in the balance, followed by the life sciences and automotive industries, with $642 billion and $505 billion at risk, respectively.

Risk managers see cybersecurity as the biggest threat to business

Sword GRC canvassed almost 150 risk managers from highly risk-aware organizations worldwide for their opinions. Overall, cybersecurity was seen as the biggest risk to business by a quarter of organizations.

In the UK, Brexit and the resulting potential economic fallout was cited as the biggest risk to business by 14% of risk managers. The most notable regional variation was in the US where 40% of organizations see cybersecurity as the most threatening risk.

The most lucrative opportunities for business were the benefits and efficiencies achieved by harnessing technology, followed by expansion into new markets or sectors.

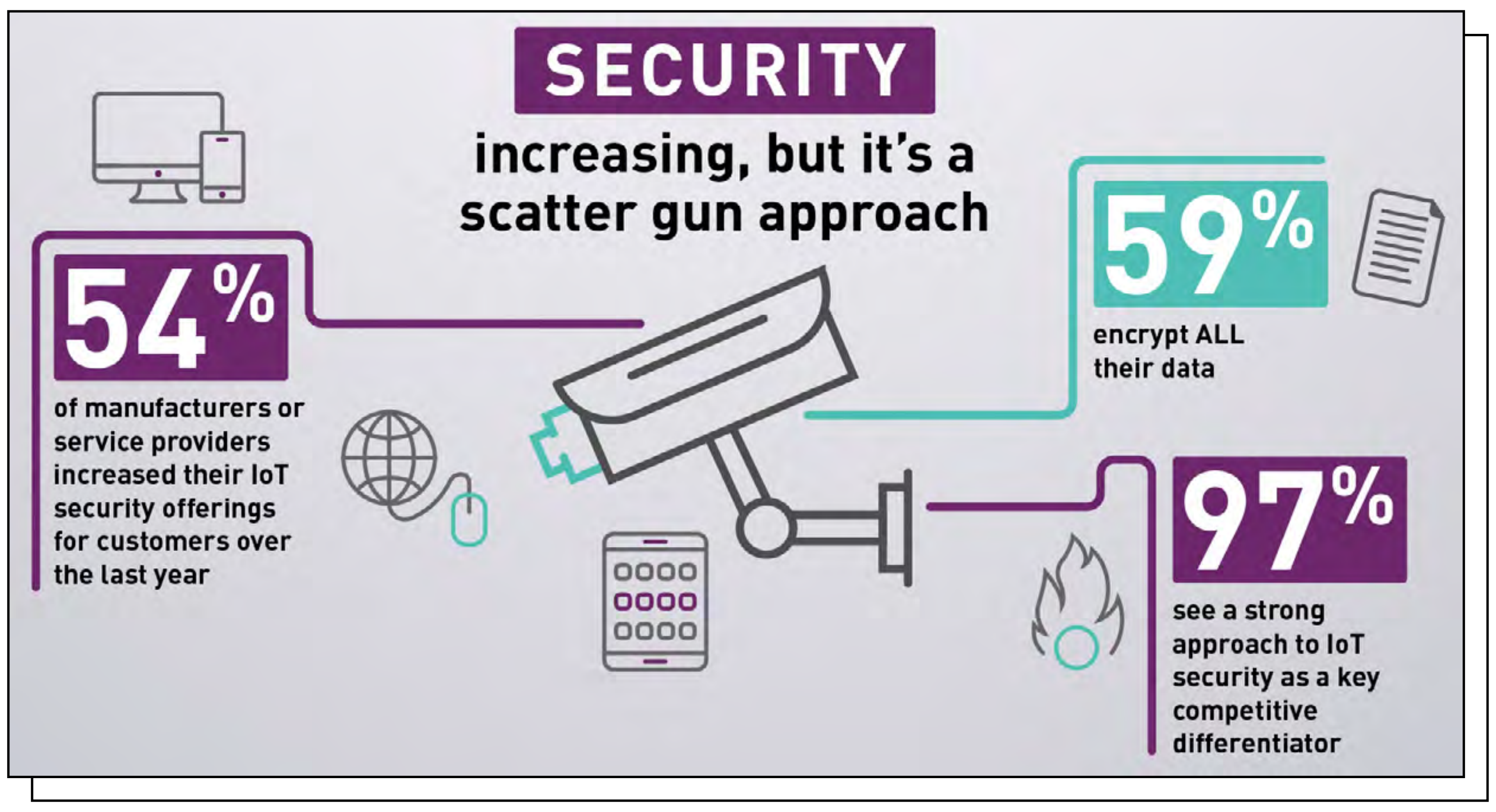
Risk managers were also asked about their acknowledgement and preparations for Black Swans (an event that is highly unlikely to materialize but if it did, would have a substantial impact). In both the US and UK, a major terrorist attack on the business is seen as the most likely Black Swan (UK 29% and US 35%), however, in Australia/New Zealand, only 13% of risk managers thought that one was likely.

Companies still struggle to detect IoT device breaches

Only 48% of businesses can detect if any of their IoT devices suffers a breach, according to Gemalto. This comes despite companies having an increased focus on IoT security:

- Spending on protection has grown (from 11% of IoT budget in 2017 to 13% now)
- Nearly all (90%) believing it is a big consideration for customers
- Almost three times as many now see IoT security as an ethical responsibility (14%), compared to 4% a year ago.

With the number of connected devices set to top 20 billion by 2023, businesses must act quickly to ensure their IoT breach detection is as effective as possible.

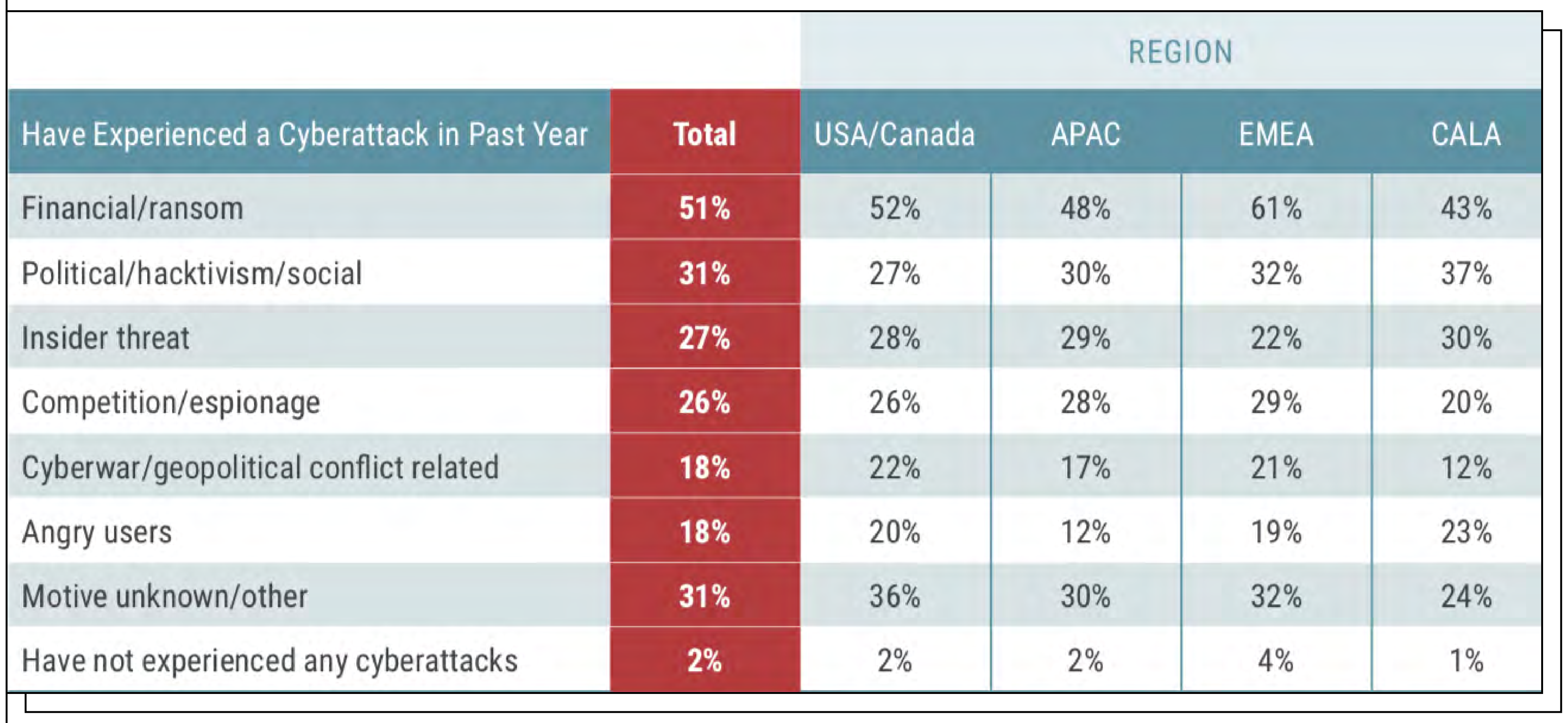

SECURITY
increasing, but it's a scatter gun approach
54%
of manufacturers or service providers increased their IoT security offerings for customers over the last year
59%
encrypt ALL their data
97%
see a strong approach to IoT security as a key competitive differentiator

Surveying 950 IT and business decision makers globally, Gemalto found that companies are calling on governments to intervene, with 79% asking for more robust guidelines on IoT security, and 59% seeking clarification on who is responsible for protecting IoT. Despite the fact that many governments have already enacted or announced the introduction of regulations specific to IoT security, most (95%) businesses believe there should be uniform regulations in place, a finding that is echoed by consumers, 95% of which expect IoT devices to be governed by security regulations.

The costs of cyberattacks increased 52% to $1.1 million

Radware has released its 2018-2019 Global Application and Network Security Report, in which survey respondents estimate the average cost of a cyberattack at $1.1M. For those organizations that calculate (versus estimate) the cost of an attack, that number increases to $1.67M.

The top impact of cyberattacks, as reported by respondents, is operational/productivity loss (54%), followed by negative customer experience (43%). What's more, 45% reported that the goal of the attacks they suffered was service disruption. 35% said the goal was data theft.



		REGION			
Have Experienced a Cyberattack in Past Year	Total	USA/Canada	APAC	EMEA	CALA
Financial/ransom	51%	52%	48%	61%	43%
Political/hacktivism/social	31%	27%	30%	32%	37%
Insider threat	27%	28%	29%	22%	30%
Competition/espionage	26%	26%	28%	29%	20%
Cyberwar/geopolitical conflict related	18%	22%	17%	21%	12%
Angry users	18%	20%	12%	19%	23%
Motive unknown/other	31%	36%	30%	32%	24%
Have not experienced any cyberattacks	2%	2%	2%	4%	1%

While the cost of attack mitigation continues to rise, so does the number of organizations under attack. Most organizations have experienced some type of attack within the course of a year, with only 7% of respondents claiming not to have experienced an attack at all. 21% reported daily attacks, representing a significant rise from last year (13%).

Not only are attacks becoming more frequent, they are also more effective: 78% of respondents hit by a cyberattack experienced service degradation or a complete outage, compared to 68% last year. Even with these numbers, 34% of respondents do not have a cybersecurity emergency response plan in place.

New requirements for the secure design and development of modern payment software

The PCI Security Standards Council (PCI SSC) published new requirements for the secure design and development of modern payment software.

The PCI Secure Software Standard and the PCI Secure Lifecycle (Secure SLC) Standard are part of a new PCI Software Security Framework, which includes a validation program for software vendors and their software products and a qualification program for assessors. The programs will be launched later in 2019.

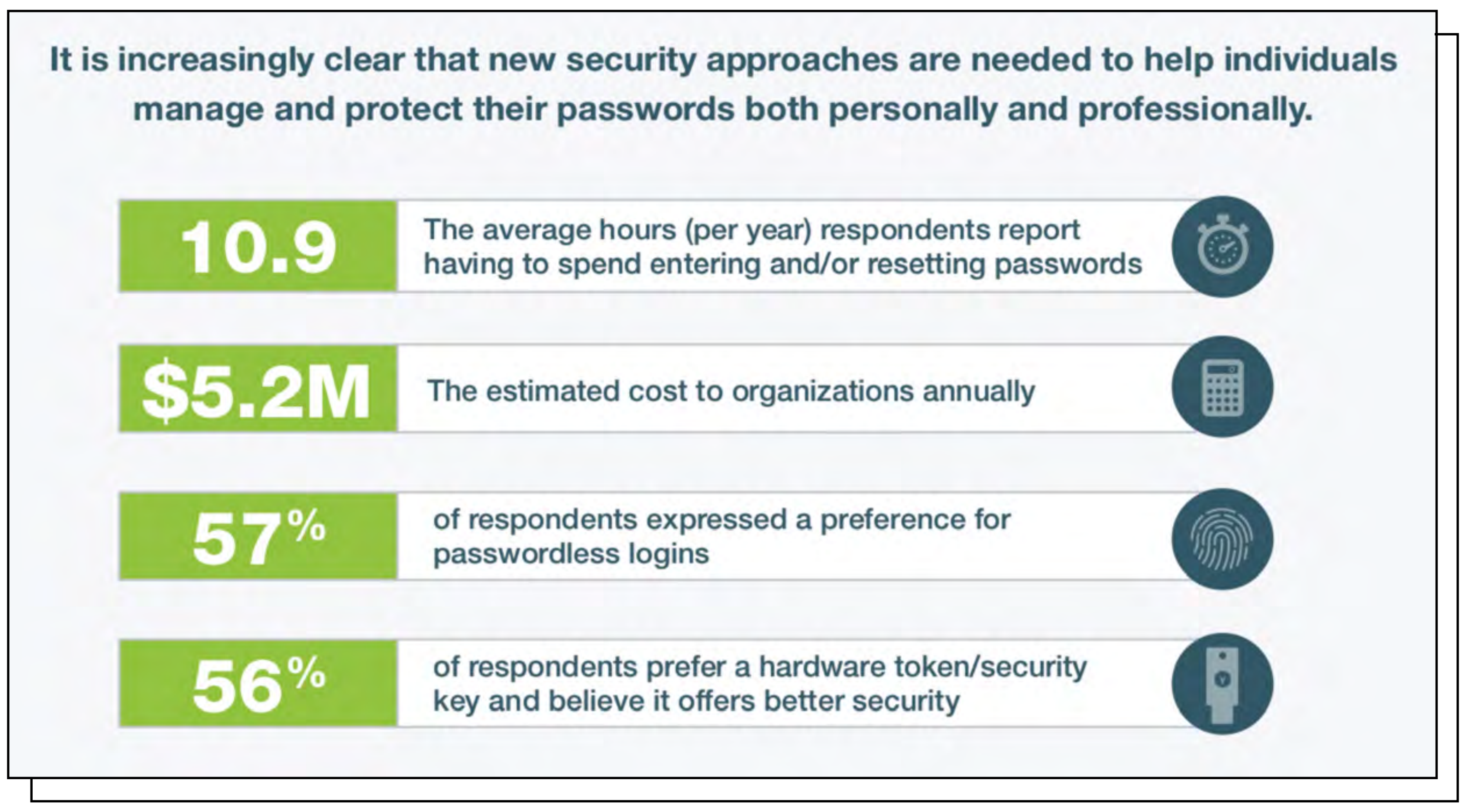
"Innovation in payments is moving at an incredible pace. Each advancement provides the industry the opportunity to develop applications more quickly and efficiently than before and to design software for new platforms for payment acceptance," said PCI SSC Chief Technology Officer Troy Leach. "The new PCI Secure Software Standard and PCI Secure SLC Standard support this evolution in payment software practices by providing a dynamic way for developers to demonstrate their software protects payment data for the next generation of applications."

How privacy and security concerns affect password practices

Yubico announced the results of the company's 2019 State of Password and Authentication Security Behaviors Report, conducted by the Ponemon Institute, who surveyed 1,761 IT and IT security practitioners in the United States, United Kingdom, Germany and France.

As cyberattacks become more prevalent, vulnerabilities created by poor password and authentication practices lead to attacks such as phishing. More than half of respondents (51 percent) say they have experienced a phishing attack in their personal life, while 44 percent of respondents have experienced a phishing attack at work. However, while phishing attacks are occurring on a frequent basis, 57 percent of respondents who have experienced a phishing attack have not changed their password behaviors.

Almost half of respondents (47 percent) say their companies are most concerned about protecting customer information and 45 percent of respondents say they are most concerned about protecting employee information.



It is increasingly clear that new security approaches are needed to help individuals manage and protect their passwords both personally and professionally.

10.9	The average hours (per year) respondents report having to spend entering and/or resetting passwords
$5.2M	The estimated cost to organizations annually
57%	of respondents expressed a preference for passwordless logins
56%	of respondents prefer a hardware token/security key and believe it offers better security

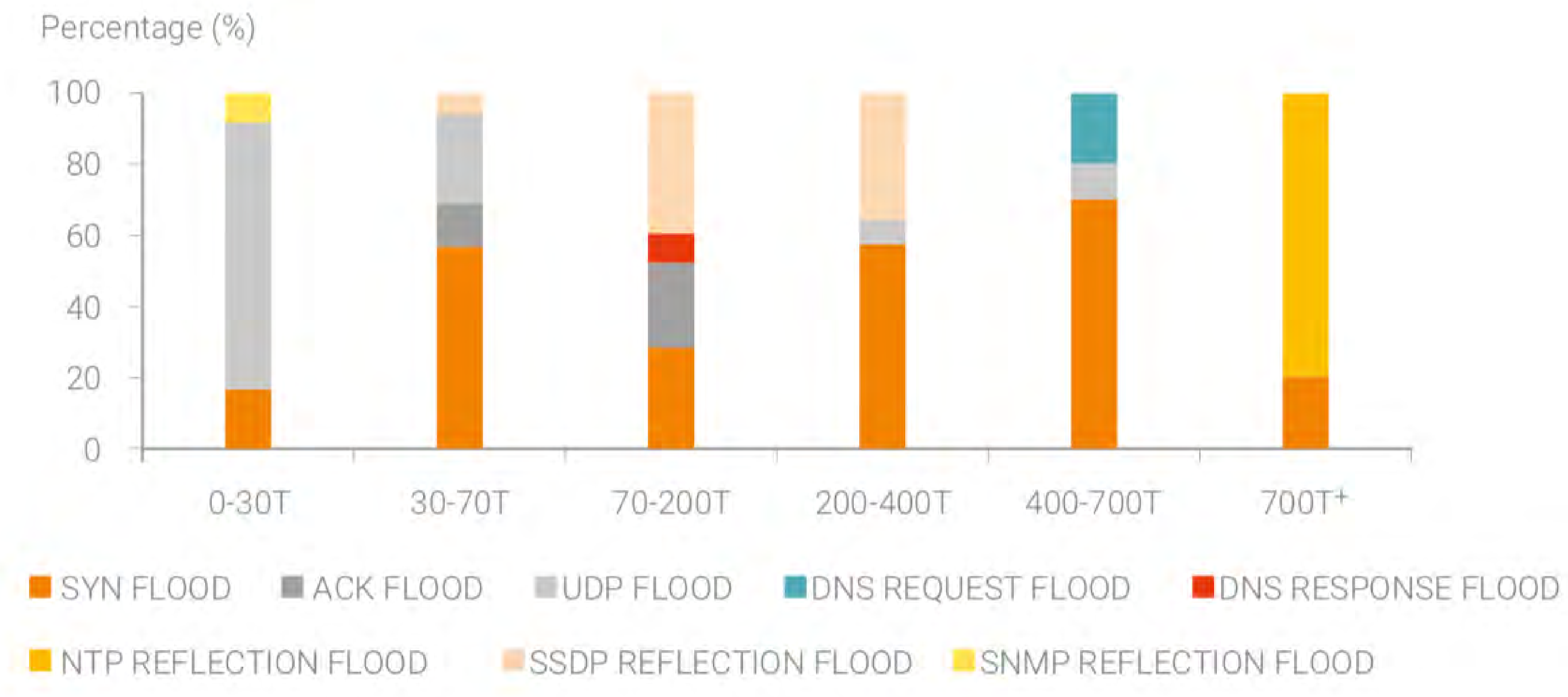
The biggest cybersecurity challenge? Communicating threats internally

IT executives responsible for cybersecurity feel a lack of support from company leaders, and 33 percent feel completely isolated in their role, according to Trend Micro.

IT teams are under significant pressure, with some of the challenges cited including prioritizing emerging threats (47 percent) and keeping track of a fractured security environment (43 percent). The survey showed that they are feeling the weight of this responsibility, with many (34 percent) stating that the burden they are under has led their job satisfaction to decrease over the past 12 months.

"As cyber-attacks increase in volume and sophistication, accountability needs to be shared. No business can afford for the IT function to be an island, because it will inevitably buckle. This means shifting the mindset from cybersecurity being a standalone initiative to a shared responsibility across an organization,“ said Bharat Mistry, Principal Security Strategist, Trend Micro.

Researchers analyze DDoS attacks as coordinated gang activities



IP Gang Attack-Type Classification against Attack Volume Size

In a new report, NSFOCUS introduced the IP Chain-Gang concept, in which each chain-gang is controlled by a single threat actor or a group of related threat actors and exhibit similar behavior among the various attacks conducted by the same gang. By studying the historical behavior of the 80 gangs identified in the report, NSFOCUS built several unique gang profiles to analyze their preferred attack methodologies and how to develop a better defense system against future attacks.

Key findings:

- These gang members, though only a tiny fraction (2 percent) of all the attackers, are responsible for a much larger portion (20 percent) of all the attacks.
- Most of the gangs have fewer than 1,000 members, but NSFOCUS also sees one gang with more than 26,000 members.
- Reflection flood attacks are the dominant attack methods favored by the gangs, specifically in high-volume attacks due to their great amplification factor.
- Gangs typically do not operate at their full potential capacity. However, knowing their maximum attacking power is very important in planning the defense against them.
- The top attacker source region are European countries. Asian countries, as well as North America, also contributed a significant amount.

Global IT spending to reach $3.8 trillion in 2019, up 3.2% from 2018

“IT is no longer just a platform that enables organizations to run their business on. It is becoming the engine that moves the business,” says John-David Lovelock, research vice president at Gartner. “As digital business and digital business ecosystems move forward, IT will be the thing that binds the business together.”

With the shift to cloud, a key driver of IT spending, enterprise software will continue to exhibit strong growth, with worldwide software spending projected to grow 8.5 percent in 2019. It will grow another 8.2 percent in 2020 to total $466 billion. Organizations are expected to increase spending on enterprise application software in 2019, with more of the budget shifting to software as a service (SaaS).

How accepting that your network will get hacked will help you develop a plan to recover faster

AUTHOR_Keith Bromley, Sr. Manager, Solutions, Keysight

Protecting the corporate network from ever-evolving security threats is an intense and extremely stressful job. For a security team, a 99 percent success rate is still a complete failure: that one time a hacker, piece of malware, or DDoS attack brings down their organization's network (or network availability) is all that matters. It's even more frustrating when you consider that an attacker can spend less than $1,000 USD on a computer and malware and bring down a network that you have spent millions of dollars on state-of-the-art equipment to protect.

So, what's the solution to that problem? It comes down to two things: prevention and acceptance. Security teams must continue to prevent security attacks while also accepting the reality that the network will eventually get breached.

This doesn't mean accepting the role of victim. The concept of network security resilience is focused on answering the following question: "How can I make our network more resilient in order to limit the damage that a bad actor or malware can do in the future?"

According to a 2018 study conducted by Ponemon Institute, the average length of time it takes organizations to identify a data breach is 197 days. A 2018 Trustwave report revealed that over half of victimized companies never discover the breach themselves.

Aiming for resilience

A successful implementation of network security resilience relies on making a fundamental shift in both security strategy and mindset. Organizations cannot expect to see the benefits if they don't embrace change. However, change is easier said than done, as many security engineers, architects and CIOs are caught up in a philosophy that is primarily focused on prevention.

To start the shift towards resilience, you must embrace three simple tenets:

- Accept the network security resilience concept
- Accept the belief that you can make real changes
- Commit to making the change.

First, security teams need to accept that it is not a question of "if", but "when" your network will be breached. While prevention should always be a key security architecture goal, a resilient strategy focuses on recognizing the breach, investigating the breach, and then remediating the damage as quickly as possible.

While the concept is straightforward, setting aside some of the security budget for resilience instead of spending it all on upgrading defenses might, at first, be difficult. If budget is truly a problem, you might have to put together a plan to convince your CIO or CISO that the security of your company's personally identifiable information (PII) is at risk and that you need some extra budget to minimize that risk.

According to a 2018 study conducted by Ponemon Institute, the average length of time it takes organizations to identify a data breach is 197 days. A 2018 Trustwave report revealed that over half of victimized companies never discover the breach themselves. Instead, they are informed of it by law enforcement, business partners, customers, or someone else. Verizon's 2018 Data Breach Investigations Report notes that 87 percent of breaches occur in just minutes, meaning that finding and responding to breaches quickly is vitally important. Therefore, a rapid response can have an effect and limit the exfiltration of some, or maybe even all, personally identifiable data. Limiting this data exfiltration is what will limit the cost of a breach because it limits the company's liability – no data loss means no fines and no public reporting of the incident.

Invest in the right set of capabilities that let you know that you have, in fact, been breached and implement those capabilities so that you may know it in a reasonable amount of time.

The second step toward network security resilience is to overcome any pessimism in order to make a positive change in this area. Some people get caught up in the mindset that there is nothing they can do that will be effective, so why waste the time. This mindset is often cleared up once a breach happens, PII is stolen, the company is faulted for their lack of prevention techniques, fines are imposed by government agencies (like the FTC and HHS departments in the United States) and lawsuits are filed against the company. Unfortunately, a mindset change at this point is too late.

> *Unfortunately, security teams will never achieve full peace of mind. There will always be new hackers, new malware and new security threats to a network.*

The implementation of changes to the network that can increase resiliency is definitely possible. If the average length of time from intrusion to detection is 197 days, then there are definitely some "low hanging fruit" improvements that can be made to reduce it.

The third thing that organizations must do is to act on the change. There are always new tools to implement, but you need to make a "planned" start. The reason I say planned is that while there are several things security teams can do, they need to follow through on the new processes. Some activities require less effort than others, if implemented correctly.

For instance, application intelligence with geolocation can be used to expose indicators of compromise. Consider the example that there is someone in Eastern Europe accessing your FTP server in Dallas and transferring data back to the Eastern Europe location. If you have no authorized users in that geographic area, there is a good chance that your network has been compromised and you should act immediately. However, you need the setup and inspection of that data to be easy in the first place. This typically requires some sort of dashboard that can quickly and easily expose the relevant information - no log file inspections, no physical correlation of data points on your points, etc. Any manual activities like those will slowly kill the use of any resilient tactics, unless you have the staff for this kind of activity.

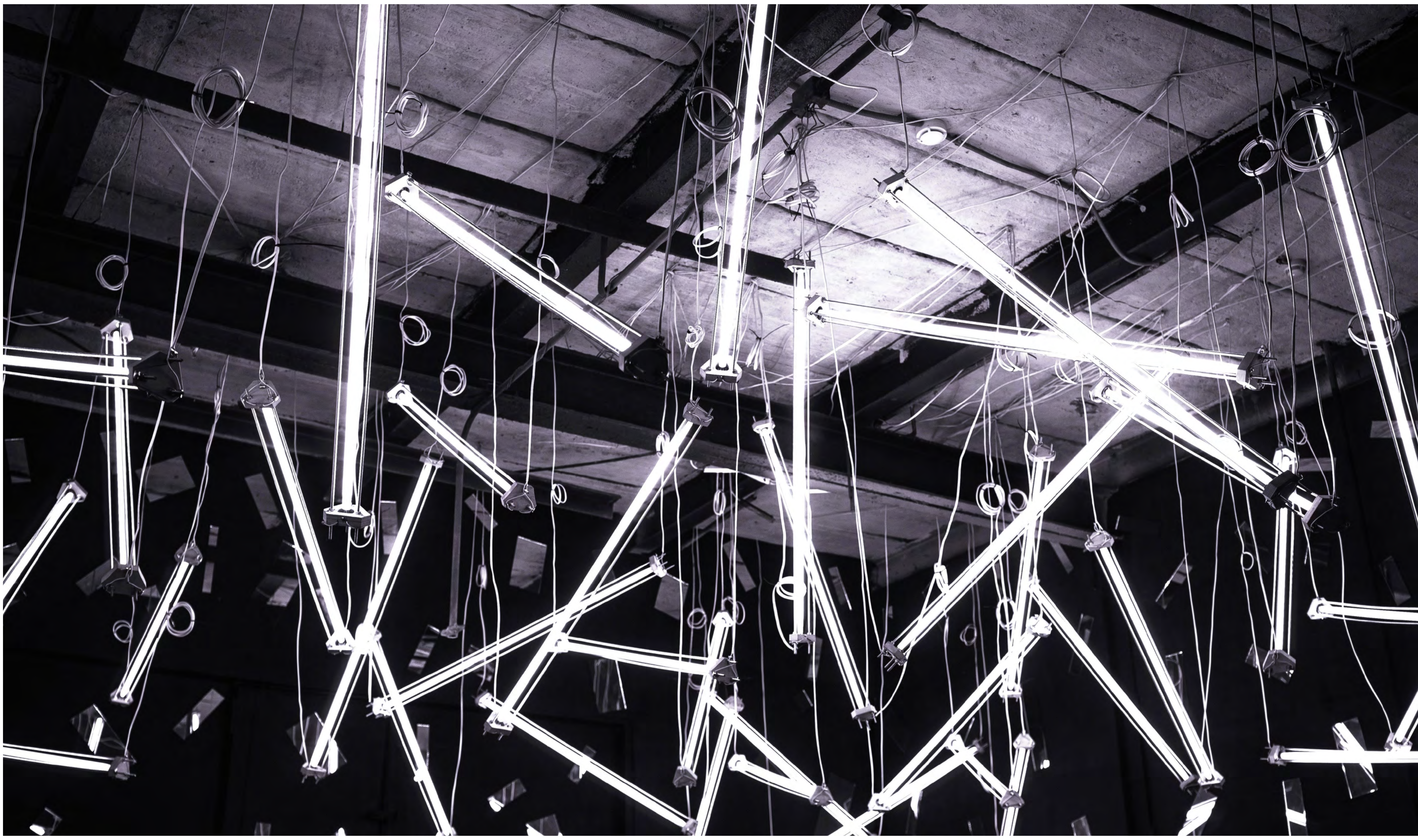
Another simple tactic is the use of a threat intelligence gateway that blocks the exfiltration of data to known bad IP addresses. The trick here is that you need a gateway that has constant updates that are easy to load. This gives you a formidable defense that does not consume an exorbitant amount of your time.

When you put these things together, you have a solid approach. Invest in the right set of capabilities that let you know that you have, in fact, been breached and implement those capabilities so that you may know it in a reasonable amount of time. Six months is not reasonable and even one month is probably too long. At the same time, you do not have to know within seconds or minutes (although that would be very nice). You pick that interval.

Conclusion

Network security resilience is all about trying to minimize corporate risk and the cost of a breach. The intent is to create a solution that identifies indicators of compromise and gives you actionable information to get the network back up and running as fast as possible after a breach has occurred.

Unfortunately, security teams will never achieve full peace of mind. There will always be new hackers, new malware and new security threats to a network. But by adopting a strategy focused on network security resilience, you'll be prepared for breaches and you'll limit the damage they can do.



Four differences between the GDPR and the California Consumer Privacy Act

AUTHOR_Jon Fielding, EMEA Managing Director, Apricorn

By passing the California Consumer Privacy Act (CCPA), which goes into effect on January 1, 2020, the Golden State is taking a major step in the protection of consumer data. The new law gives consumers insight into and control of their personal information collected online. This follows a growing number of privacy concerns around corporate access to and sales of personal information with leading tech companies like Facebook and Google.

> *The CCPA is a strong step in the right direction for the U.S. However, it does not go as far as European Union's General Data Protection Regulation (GDPR), which went into effect May 25, 2018.*

The bill was signed by Governor Jerry Brown hours after it was unanimously approved by the State Assembly and Senate. The law will ultimately result in strict control of consumer data usage from corporate entities, as well as major fines for tech companies that do not comply with it.

With the CCPA, Californian consumers will have the right to:

1_Know what personal information companies are collecting about them

2_Know what commercial purposes their information is collected for

3_Know which third-party businesses their personal information is shared with

4_Refuse the sale of their information

The CCPA is a strong step in the right direction for the U.S. However, it does not go as far as European Union's General Data Protection Regulation (GDPR), which went into effect May 25, 2018.

> *CCPA fines are applied per violation (up to a maximum of $7,500 USD per violation), are uncapped and there are apparently no sanctions for non-compliance.*

The GDPR unifies data privacy laws across Europe while protecting and empowering EU citizens' data privacy. It also impacts every company that processes or controls EU citizens' data, regardless of location, which means that the GDPR is legally binding for U.S. businesses with global operations, international sites or even remote workers.

It remains to be seen what the final version of the CCPA will look like and how closely it may resemble the GDPR. With that said, it's important for companies to be in complete compliance with both sets of laws.

Although the CCPA appears to be like the GDPR, there are four main differences between the two laws.

The businesses that must comply

The GDPR applies to all businesses that process data of EU citizens, irrespective of their location or size. The CCPA is slightly narrower in its scope: it only applies to California-based businesses with a revenue above $25 million USD or those whose primary business is the sale of personal information. (The latter criterion is a nod to the Facebook/Cambridge Analytical scandal.)

Financial penalties

The GDPR mandates penalties for non-compliance and/or data breach, which can reach up to 4% of the company's annual global turnover or 20 million euros (whichever amount is greater), with the commitment that administrative levies will be applied proportionately.

CCPA fines are applied per violation (up to a maximum of $7,500 USD per violation), are uncapped and there are apparently no sanctions for non-compliance. The violation is only considered at the point of breach (many would say too late), whereas GDPR can apply a sanction where a company is deemed to be at risk of a breach or not behaving responsibly. In addition, CCPA allows for the consumer to sue the business for violation.

Consumer rights

Both regulations endow the consumer with specific rights such as the right to have information deleted or accessed.

> *Under both regulations, if a company suffers a breach but the data is encrypted (unintelligible to unauthorized users), some of the company's obligations are reduced.*

The GDPR is specifically focused on all data related to the EU consumer/citizen whereas the CCPA considers both the consumer and household as identifiable entities and, in some cases, only considers data provided by the consumer as opposed to data sourced or purchased from third parties. It is important that businesses test their processes to ensure they can accommodate these rights.

Enactment and enforcement

Before the CCPA goes in effect in 2020, it may get more descriptive. In its current form, it looks like it was created in reaction to recently publicised instances of misuse of personal data. In comparison, the GDPR was adopted in April 2016 and became enforceable on May 25, 2018.

Although the California Consumer Data Privacy law is not as comprehensive as the GDPR, it's the first step to protecting consumer data. California pioneered tech innovation and is now paving the way for consumer privacy. This new law gives consumers more protection and understanding of how their data is being collected and used, which ultimately gives them control of their data.

Other states are expected to follow California's lead and it will be interesting to see which state will be next.

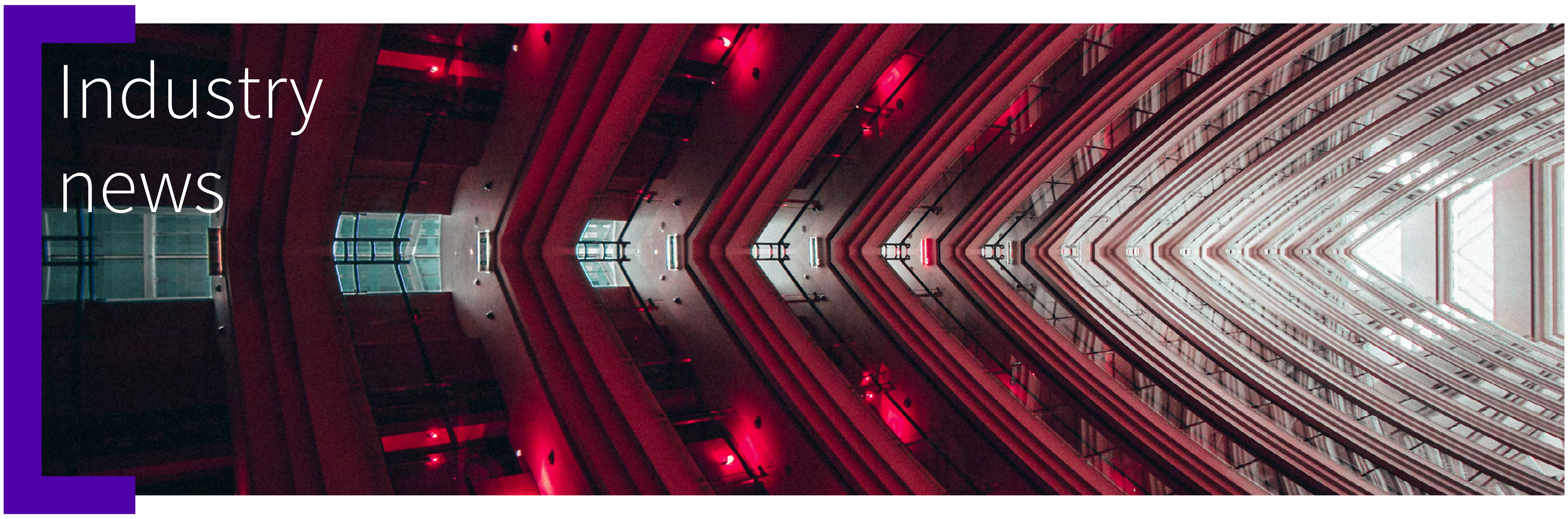
The use of encryption is addressed in both laws

The good news is that both laws call for data encryption, making this an essential privacy protection component for businesses. If breached data is encrypted, companies have a level of protection against unauthorized access and some reduction in liability by default.

GDPR's Article 32 is focused on encryption. The regulation doesn't prescribe any specific technologies, and Article 32 is the first and only technical recommendation provided within the whole set of articles (99 in all).

Under both regulations, if a company suffers a breach but the data is encrypted (unintelligible to unauthorized users), some of the company's obligations are reduced. For instance, in that case the organization is not required to notify everyone affected by the incident.

Industry news



Varonis Data Security Platform 7.0 released

Version 7.0 of the Varonis Data Security Platform features new cloud and threat detection and response capabilities: new event sources and enrichment, threat intelligence to Varonis security insights, and playbooks that arm customers with incident response plans right in the web UI – making it easier for customers to follow responses to security incidents.

“This new release of the Varonis Data Security Platform speaks to the fact that too many modern organizations are combatting a lack of perimeter visibility, in-house expertise, proactive incident response, and the requirement for a cyber-resilient strategy – creating prime targets for attackers,” said Peter Evans, chief marketing officer, Optiv.

VDOO releases runtime protection agent for connected devices

VDOO’s end-to-end platform facilitates security and trust for IoT devices throughout the entire device lifecycle — from security analysis to implementation, certification and post-deployment security enablement.

The VDOO Vision Analysis Platform is a web-based service that performs analysis of a device’s firmware and determines its security gaps and requirements. Following the analysis of the device, the VDOO platform offers guidance for vendors to implement the identified requirements. Once security features have been implemented, the platform validates this, and provides a physical and digital certification to communicate the device’s security standing to the world.

Dragos updates its asset identification, threat detection, and response platform

The Dragos Platform is designed for extreme visibility of ICS assets and threats, built upon its DPI capabilities. DPI capabilities enable protocol analysis for contextual depth, providing greater accuracy and speed in the identification of thousands of assets. This fine-grained characterization, akin to fingerprinting a device, enables more accurate assessments of normal or abnormal usage and communication patterns necessary for automated asset identification and threat detection.

In addition to its existing DPI capabilities, Dragos Platform 1.4 further supports asset visibility with new geographical map views to locate and understand industrial assets.

Quali introduces SaaS cloud management platform CloudShell Colony for accelerating DevOps

Quali unveiled CloudShell Colony, a software-as-a-service (SaaS) cloud management platform for DevOps. CloudShell Colony automates DevOps environments all the way from development to production, while allowing IT and project managers to govern the use of cloud resources from a single pane of glass.

This announcement follows the recent news highlighting Quali's $22.5 million Series-C funding round in December 2018. CloudShell Colony initially being released as controlled availability (CA) software equips DevOps teams, developers and testers with reusable application environments on public clouds such as Amazon Web Services, Microsoft Azure with support for Kubernetes deployments. Quali is providing varying levels of the solution based on company size.

Symantec introduces advanced EDR tools and fully-managed service

Enterprise IT and Security Ops teams are increasingly challenged to investigate and respond to advanced and emerging threats with available resources and staff. Symantec's MEDR service harnesses the power of EDR 4.0 to improve incident response, threat hunting and forensics, fortifying teams with investigation expertise and threat intelligence from a world-class team of Symantec SOC analysts.

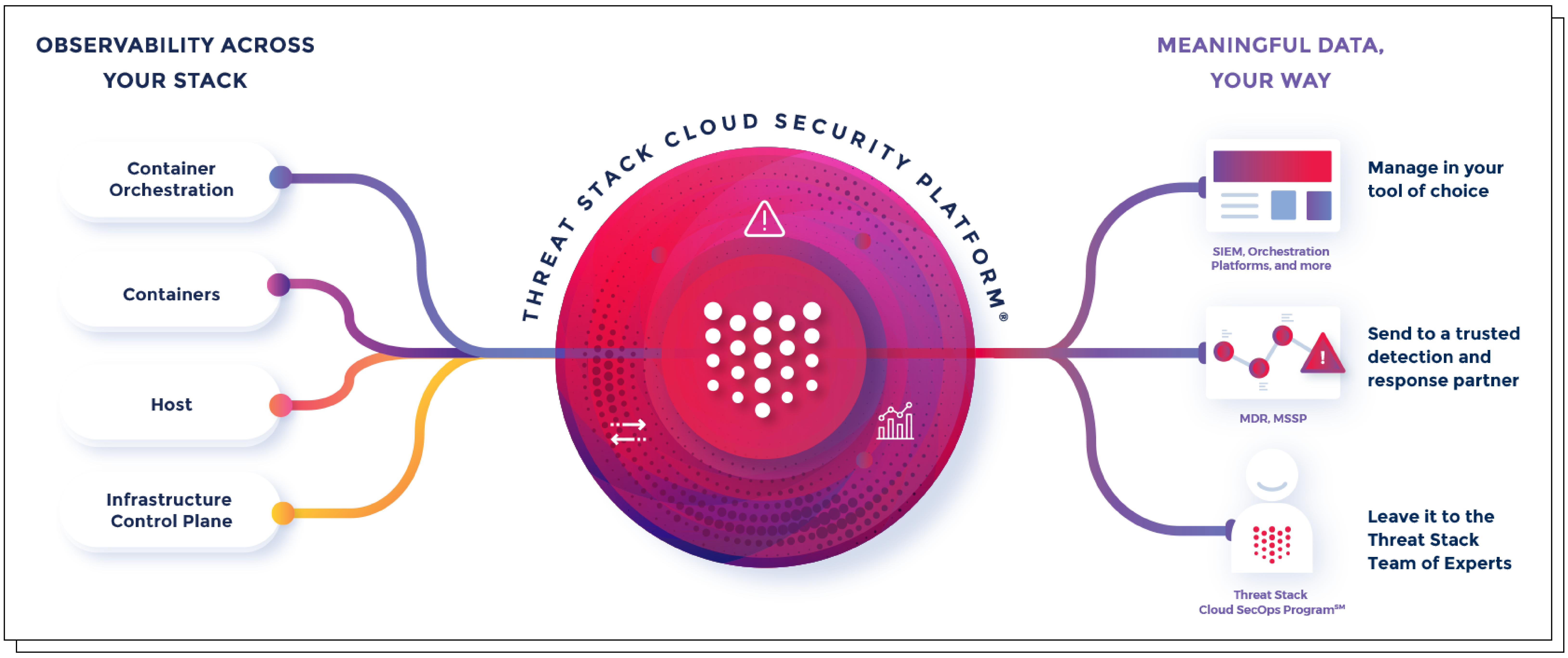
Symantec MEDR detects stealthy attacks and expertly examines suspicious activity for faster incident validation and response. A powerful combination of Symantec EDR 4.0, the SOC technology platform, and the Global Intelligence Network, allows Symantec analysts to provide 24x7 expertise. Managed threat hunting, remote investigations, and endpoint containment enable security teams around the world to stay ahead of threats.

API cybersecurity solution from Ping Identity protects organizations against API threats

Ping Identity has made several updates to PingIntelligence for APIs, its AI-powered API cybersecurity solution. These latest enhancements include an AI-based cloud trial, the ability to detect new types of attacks, support for Splunk environments, and additional integration with API gateways.

"Ping is helping organizations protect against a landscape of cybersecurity threats, including those against API infrastructures. Many of the recent API abuses and attacks took months and years to detect, further reinforcing the need for IT leaders to build API-security focused teams," shared Bernard Harguindeguy, CTO, Ping Identity.

Threat Stack announces new API for streamlined DevOps and security workflows


OBSERVABILITY ACROSS YOUR STACK
Container Orchestration
Containers
Host
Infrastructure Control Plane
THREAT STACK CLOUD SECURITY PLATFORM®
MEANINGFUL DATA, YOUR WAY
Manage in your tool of choice
SIEM, Orchestration Platforms, and more
Send to a trusted detection and response partner
MDR, MSSP
Leave it to the Threat Stack Team of Experts
Threat Stack Cloud SecOps Program℠

Threat Stack released a new comprehensive API that will give customers the ability to create, deploy, augment, and tune security rules directly within their existing DevOps and security tools.

Threat Stack customers will now be able to seamlessly manage and configure the Threat Stack Cloud Security Platform without a separate interface, reducing context switching within workflow tools, while leading to more actionable alerts and reducing alert fatigue.

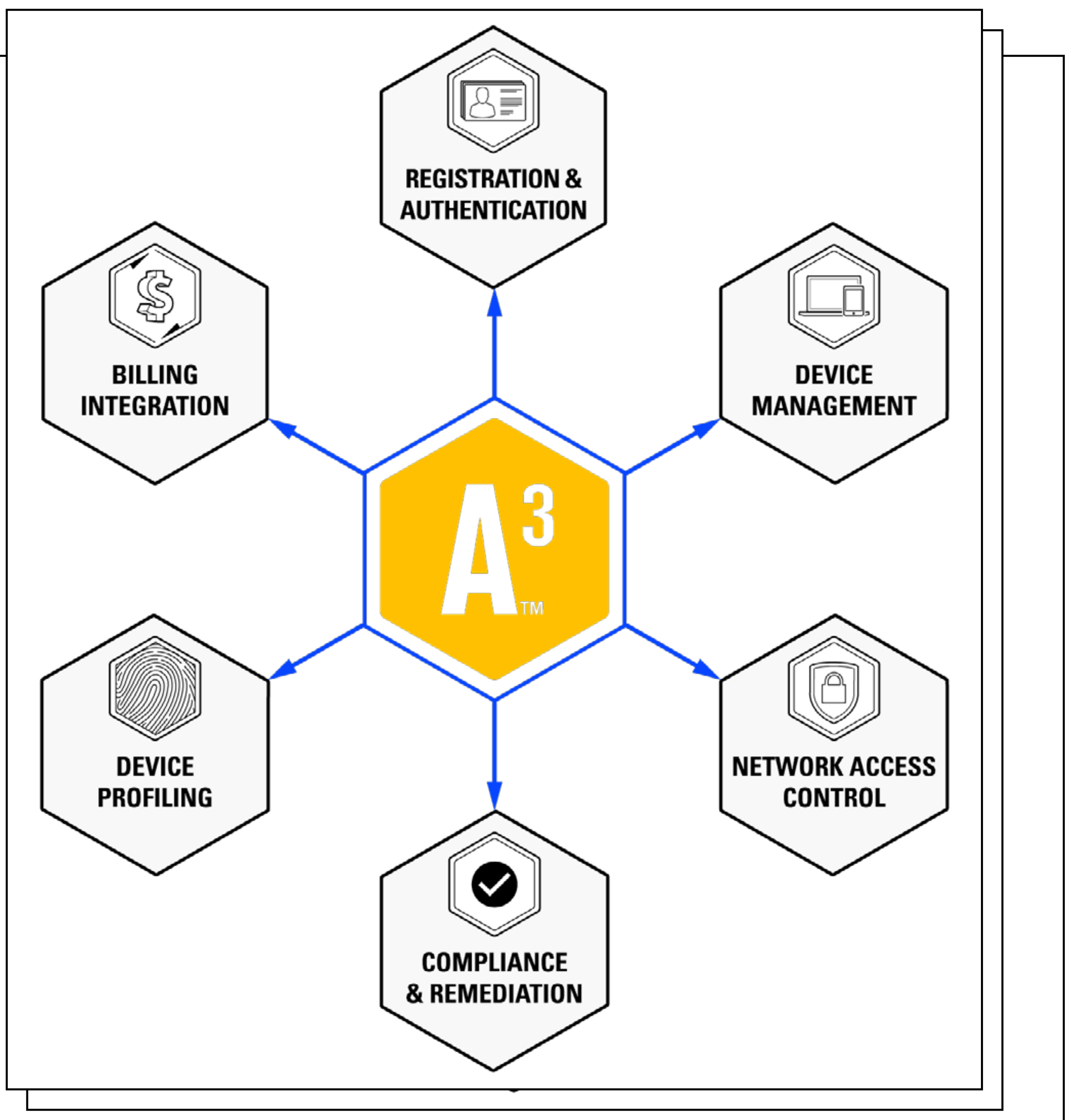
The new comprehensive API will allow for the suppression and dismissal of alerts from existing tools, drastically streamlining incident response workflows and reducing the mean time to response (MTTR). The ability to disable and enable rules programmatically will also enable Threat Stack customers to conduct system maintenance without interrupting DevOps and Security teams or increasing the number of false positive alerts. Threat Stack is enabling DevOps and security teams to reduce the number of tools needed to secure their cloud infrastructure.

NICE Actimize announces IFM-X platform powered by augmented intelligence

NICE Actimize released IFM-X, its next-generation Integrated Fraud Management (IFM) platform that leverages automation and machine learning to optimize effectiveness while reducing the total cost of implementing and operating an enterprise fraud risk management system.

By utilizing NICE Actimize's IFM-X, financial institutions will be able to integrate data into their fraud detection systems and utilize analytics, while optimizing fraud operations efficiency.

Aerohive announces cloud management for its A3 Secure Access Management solution



Aerohive Networks released the cloud management for its A3 Secure Access Management solution. A3 brings an approach to Corporate, BYOD, Guest, and IoT client device onboarding, authentication, and network access control (NAC).

First launched in May 2018 as an on-premises solution, Aerohive now introduces a new deployment option for A3 with cloud-based monitoring and, expected in Q2, configuration for all customer sites, while localized tasks like device onboarding and access-control enforcement will be executed by on-site enforcement nodes.

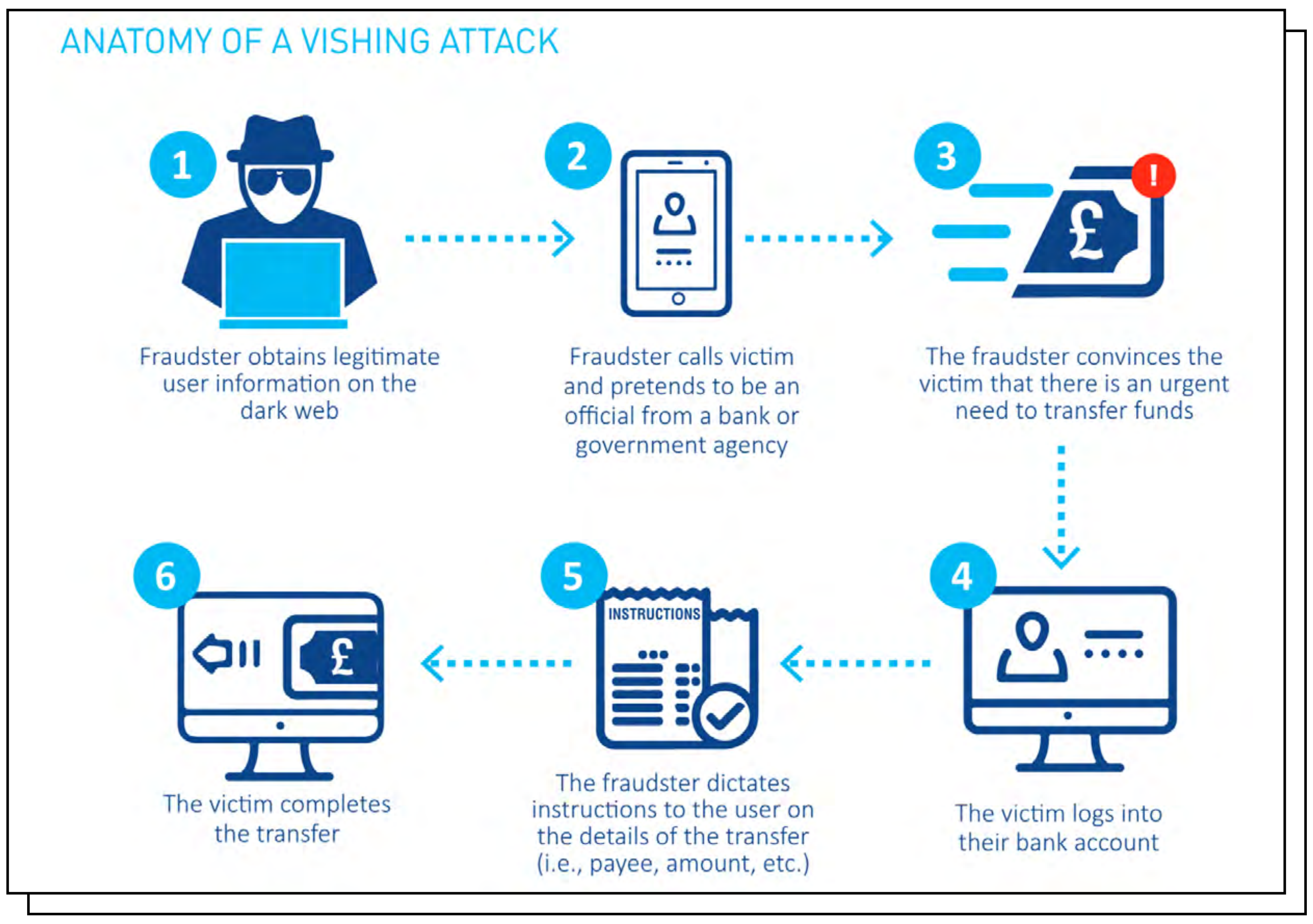
Like A3 itself, its cloud management is vendor-agnostic and fully supports Aerohive and non-Aerohive networks alike. In addition, the latest release of A3 includes simplification of key installation and operational tasks, such as a complete A3 platform cluster that can be installed in 6 clicks, as opposed to traditional solutions that require tedious, lengthy CLI-based configuration procedures for the same task. With the A3 cloud-management option, Aerohive continues to execute on its roadmap to simplify the Secure Access Management space.

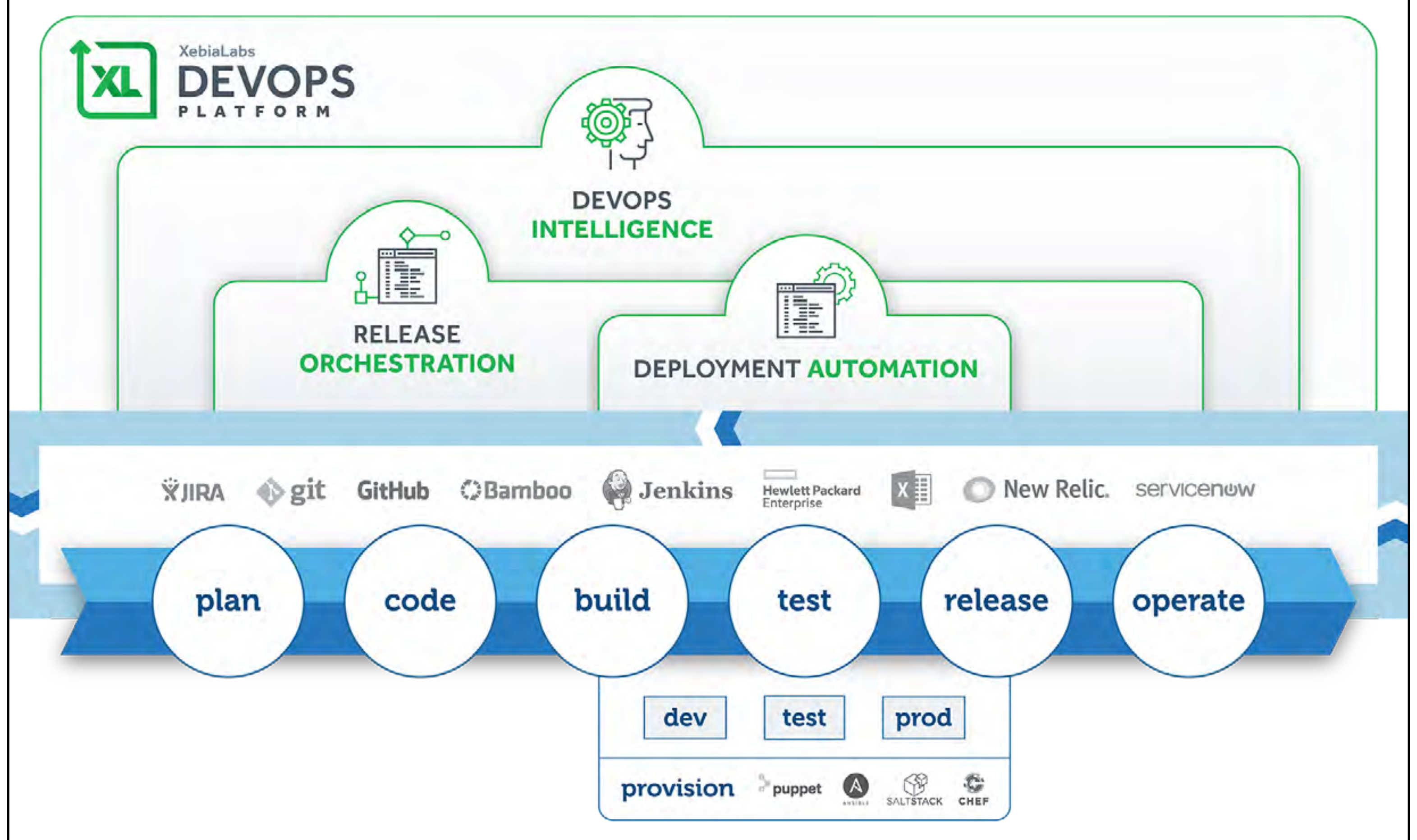
BioCatch launches new behavioral biometrics offering to combat vishing

BioCatch has introduced a new offering to help protect consumers from phone scams known as vishing, a type of Authorized Push Payment (APP) fraud, in response to the growing vishing epidemic.

Vishing, which involves fraudsters impersonating bank or other officials to trick victims into transferring funds, has become the fastest growing social engineering scam in the United Kingdom. UK Finance reported that in the first half of 2018, nearly 4,000 UK banking customers lost an average of £9,000 each due to vishing scams.

BioCatch detects changes in known user behavior that suggest the victim is under the influence of a criminal, unwittingly taking instruction to conduct fraudulent money transfers. Leveraging 39 patented advanced data science and AI techniques and 25 more with patents pending, BioCatch analyzes the user’s online interactions and generates behavioral insights.


ANATOMY OF A VISHING ATTACK
1
Fraudster obtains legitimate user information on the dark web
2
Fraudster calls victim and pretends to be an official from a bank or government agency
3
£
The fraudster convinces the victim that there is an urgent need to transfer funds
4
The victim logs into their bank account
5
INSTRUCTIONS
The fraudster dictates instructions to the user on the details of the transfer (i.e., payee, amount, etc.)
6
£
The victim completes the transfer



XebiaLabs launches new DevOps risk and compliance capability for software releases

The XebiaLabs DevOps Platform provides a single pane of glass for technical and business stakeholders to track the release chain of custody across the end-to-end CI/CD toolchain, from code to production. And, with visibility into security and compliance issues, teams can take action to ensure that release failure risks, security vulnerabilities, and IT governance violations are resolved early in the software delivery cycle.

According to Derek Langone, CEO of XebiaLabs: “To effectively manage software delivery at enterprise scale, DevOps teams need a way to accurately manage and report on the ‘chain of custody’ and other compliance requirements throughout the software delivery pipeline. It’s also vital for them to have visibility into the risk of release failures or security issues as early in the release process as possible. That’s when development teams can address issues the quickest without impacting the business.”

Bluetooth enhances support for location services with new direction finding feature

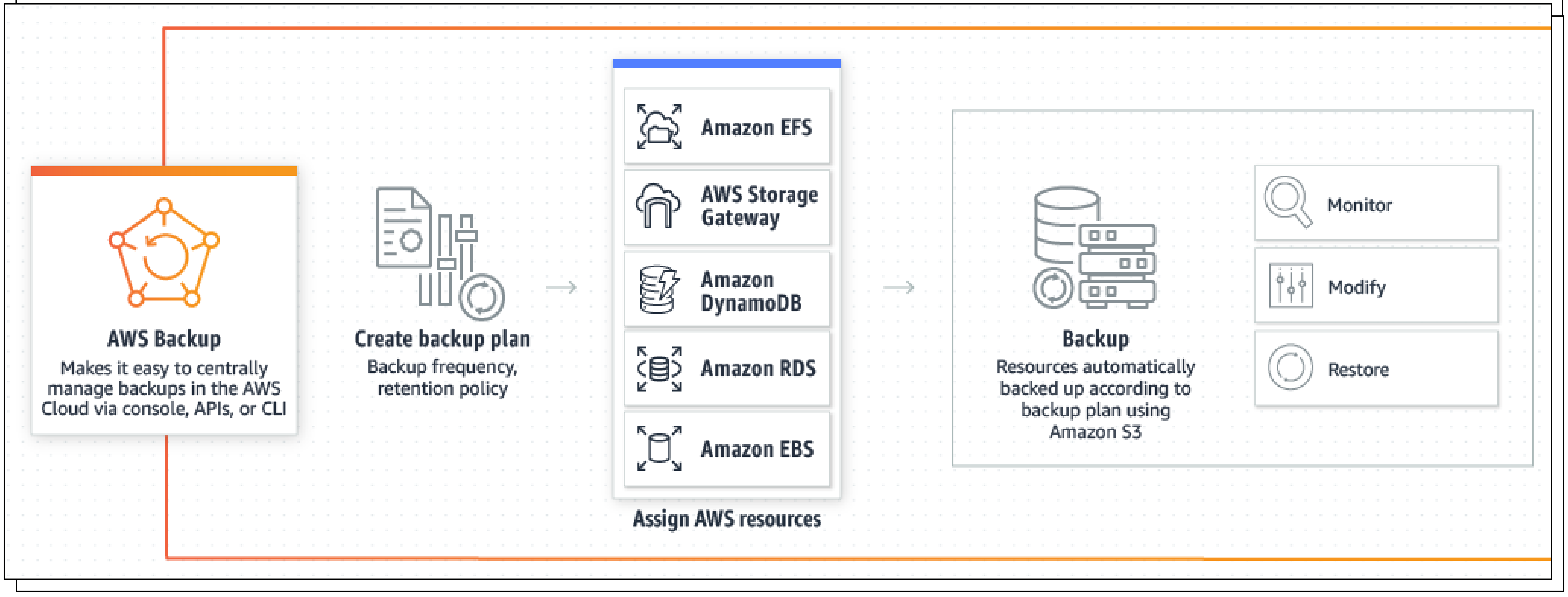
The Bluetooth Special Interest Group (SIG) today announced a new direction finding feature that holds the potential to significantly enhance the performance of Bluetooth location services solutions. The new feature allows devices to determine the direction of a Bluetooth signal, thereby enabling the development of Bluetooth proximity solutions that can understand device direction as well as Bluetooth positioning systems that can achieve down to centimeter-level location accuracy.

Bluetooth location services solutions generally fall into two categories: proximity solutions and positioning systems. Today, proximity solutions use Bluetooth to understand when two devices are near each other and approximately how far apart the are. They include item finding solutions such as personal property tags, as well as point-of-interest (PoI) information solutions like proximity marketing beacons. By including the new direction finding feature, Bluetooth proximity solutions can add device direction capability. For example, an item finding solution could not only let a user know when a personal property tag is nearby, but also in what direction, greatly enhancing the user experience.

Amazon Web Services announces AWS Backup

Amazon Web Services released AWS Backup, a backup service that makes it faster and simpler for customers to back up their data across AWS services and on-premises, helping customers meet their business and regulatory backup compliance requirements.

AWS Backup removes the need for custom solutions or manual processes by providing a centralized place to manage backups across AWS. With just a few clicks in the AWS Management Console, customers can create a policy that defines how frequently backups are created and how long they are stored. Customers can then assign these policies to their AWS resources, and AWS Backup handles the rest by scheduling backup actions for the assigned AWS resources, orchestrating across AWS services, and managing their retention period.


AWS Backup
Makes it easy to centrally manage backups in the AWS Cloud via console, APIs, or CLI
Create backup plan
Backup frequency, retention policy
Amazon EFS
AWS Storage Gateway
Amazon DynamoDB
Amazon RDS
Amazon EBS
Assign AWS resources
Backup
Resources automatically backed up according to backup plan using Amazon S3
Monitor
Modify
Restore

Pulse Secure launches new vADC Community Edition to help developers build smarter applications

Pulse Secure launched a new Community Edition of its software-based virtual Application Delivery Controller (vADC) to help application developers create application solutions with lower costs and time to market.

Pulse vADC Community Edition integrates easily with common DevOps tools for automated provisioning and orchestration, such as Kubernetes, Terraform, Puppet and Chef, making it easy to start building secure and scalable applications from day one.

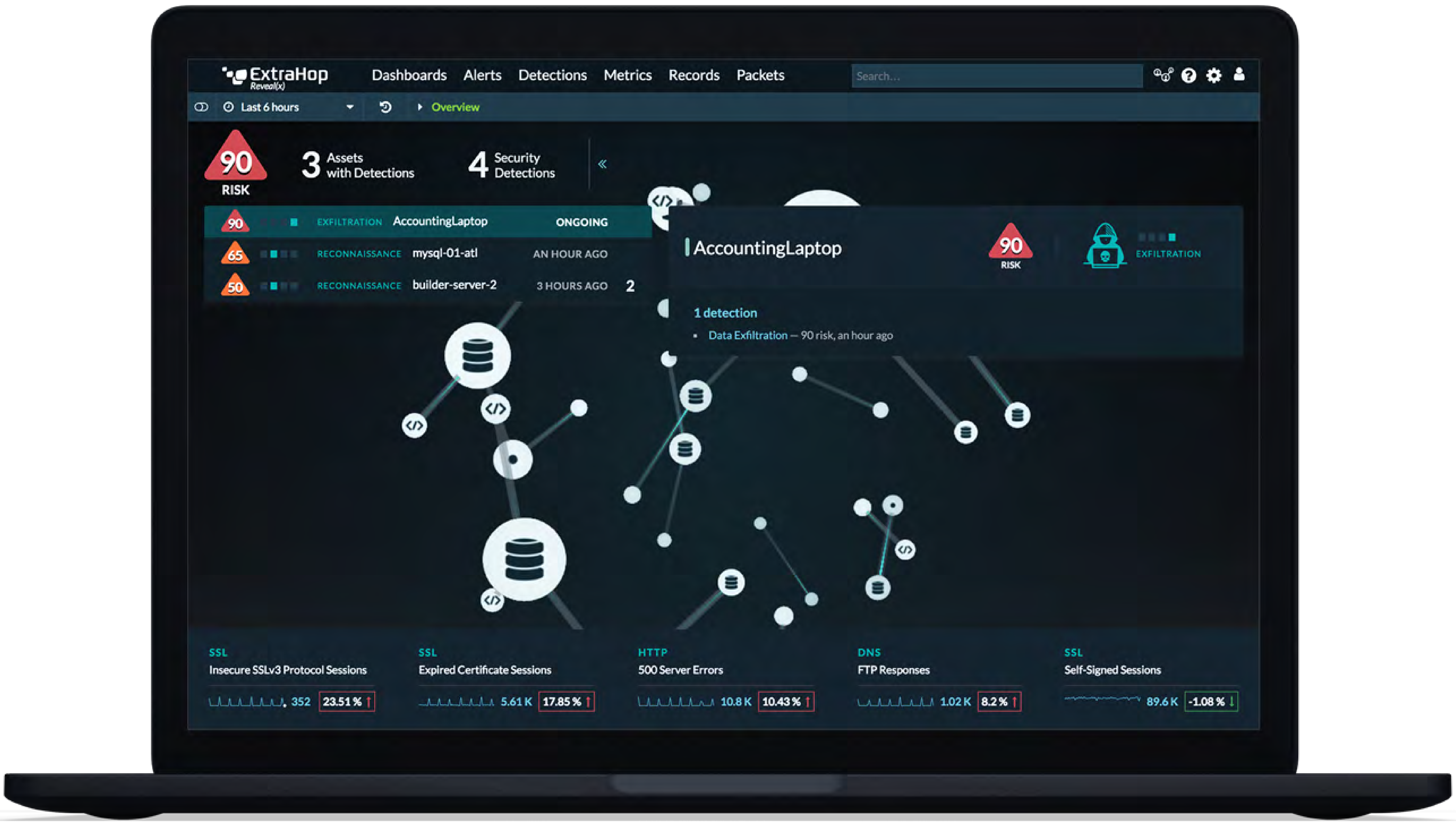
“Pulse Secure vADC Community Edition is a free, full-featured application delivery controller that can be used in production scenarios which allows developers and enterprises to accelerate cloud application deployment by removing the hurdle of procurement and tooling. Pulse Secure is setting the benchmark for try before you buy that competitors will have to follow,” said Mike Fratto, senior analyst at 451 Research.

ExtraHop turns security analysts into threat experts with Reveal(x) winter 2019

ExtraHop released new capabilities designed to help Security Operations Center (SOC) and Network Operations Center (NOC) teams identify and safeguard critical assets, detect late-stage and insider threats, and transform security analysts into threat experts with streamlined investigation workflows.

The winter 2019 release of ExtraHop Reveal(x) improves SOC and NOC analyst productivity through contextual discovery of the enterprise attack surface, full-spectrum detection, and one-click guided investigation for incident response.

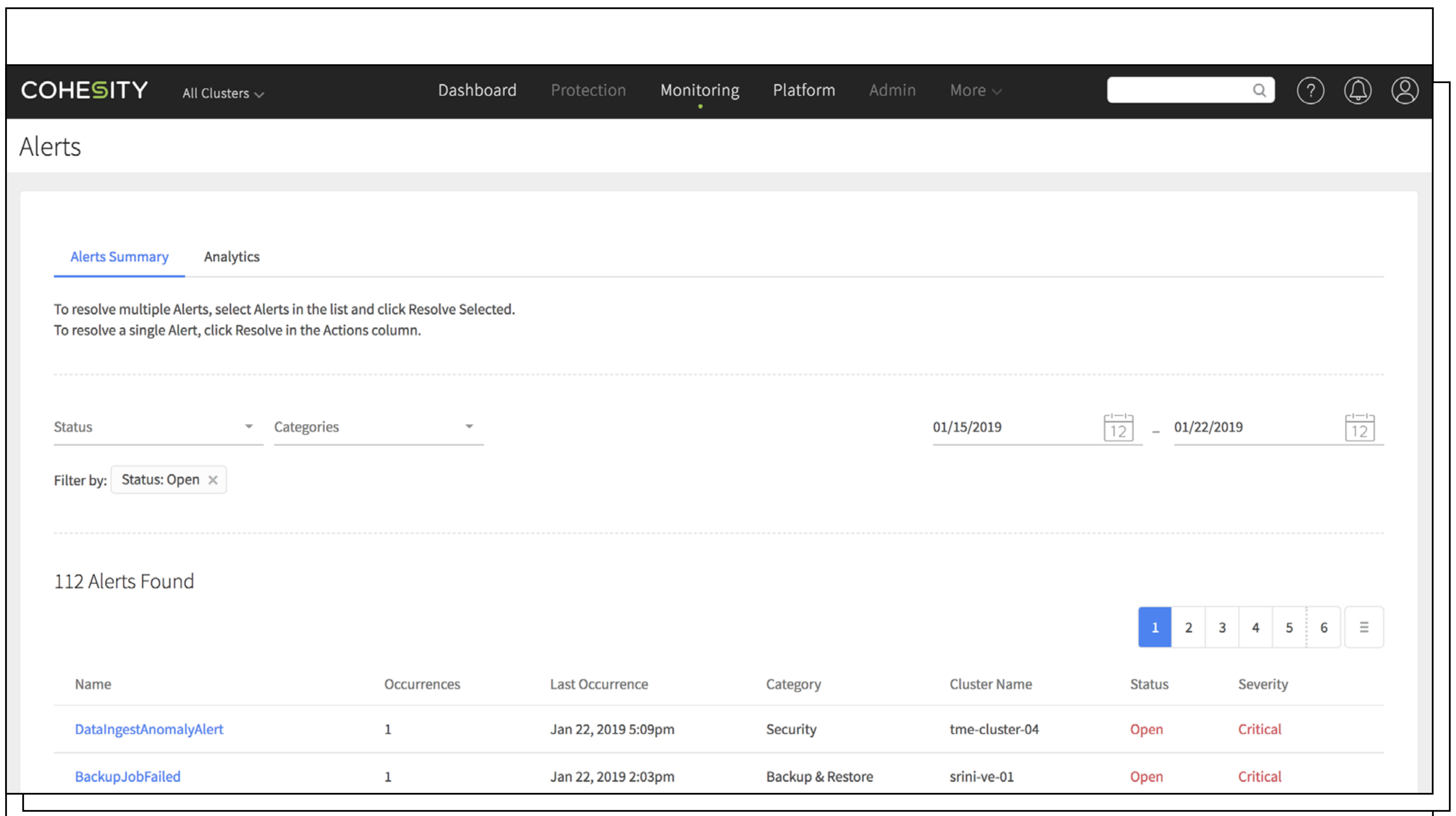
Detections incorporate device and user context to identify known and unknown threats using an array of machine learning, rule-based, and custom techniques. Detections incorporate suggested next steps and are made actionable through clear evidence, enabling front-line analysts to validate, close, or escalate prioritized events with confidence. Senior analysts get detail on users and devices to support rogue device detection, insider threat investigations, threat hunting, and forensics.


ExtraHop Reveal(x)
Dashboards
Alerts
Detections
Metrics
Records
Packets
Search...
Last 6 hours
Overview
90 RISK
3 Assets with Detections
4 Security Detections
90 EXFILTRATION AccountingLaptop ONGOING
65 RECONNAISSANCE mysql-01-atl AN HOUR AGO
50 RECONNAISSANCE builder-server-2 3 HOURS AGO 2
AccountingLaptop
90 RISK
EXFILTRATION
1 detection
Data Exfiltration — 90 risk, an hour ago
SSL Insecure SSLv3 Protocol Sessions 352 23.51 %
SSL Expired Certificate Sessions 5.61 K 17.85 %
HTTP 500 Server Errors 10.8 K 10.43 %
DNS FTP Responses 1.02 K 8.2 %
SSL Self-Signed Sessions 89.6 K -1.08 %

HITRUST expands to deliver “One framework, one assessment approach” globally

HITRUST’s integrated programs and services offers global companies a path to meet the requirements of multiple standards from the European Union’s GDPR and the Fair Information Practice Principles (FIPPs) to the NIST Framework for Improving Critical Infrastructure Cybersecurity in the U.S. as well as requirements like HIPAA and the Federal Financial Institutions Examination Council.

These latest developments will allow organizations operating in Europe and Asia to use HITRUST’s programs and services to address their data protection requirements and manage their third-party risk with one assessment. To support its growth in Europe, HITRUST will be conducting educational sessions through its Community Extension Program to provide organizations with key information and resources necessary to facilitate better risk management practices.



To resolve multiple Alerts, select Alerts in the list and click Resolve Selected.
To resolve a single Alert, click Resolve in the Actions column.

112 Alerts Found

Name	Occurrences	Last Occurrence	Category	Cluster Name	Status	Severity
DataIngestAnomalyAlert	1	Jan 22, 2019 5:09pm	Security	tme-cluster-04	Open	Critical
BackupJobFailed	1	Jan 22, 2019 2:03pm	Backup & Restore	srini-ve-01	Open	Critical

Cohesity backup solution prevents, detects, and responds to ransomware attacks

Cohesity released the Cohesity Anti-Ransomware Solution, a series of new capabilities available for the latest version of Cohesity DataPlatform that combats ransomware attacks. This solution offers the set of capabilities of any modern-day backup vendor with a multi-layered approach that can prevent, detect, and if necessary, respond to attacks.

“Legacy backup solutions are ineffective against today’s ransomware attacks, which have become a top concern for almost every organization,” said Raj Rajamani, vice president of product management, Cohesity. “Real protection requires an integrated approach that combines proactive defense measures, intelligent monitoring, and the power to restore massive amounts of data immediately.”

5 reasons why asset management is a hot topic in 2019

AUTHOR_Dean Sysman, CEO, Axonius

Sometimes buzzwords are good predictors of what organizations see as priorities in a given year. If you surveyed both the revenue-generating and security functions of enterprises in 2019, you would hear two terms often repeated: “digital transformation” and “zero trust”.

While the two terms may seem at linguistic odds, the idea that organizations must embrace the digital age to drive growth and operate more efficiently while simultaneously maintaining adequate information security makes sense. It won’t be easy, though, as there’s a persistent problem that has to be solved before reconciling those two initiatives.

The march toward the digital promised land

While definitions vary, digital transformation can be boiled down to the application of technology in every business function to crush inefficiency.

Enterprises are ripe with examples of staggering inefficiencies. For example, a 2017 survey by the Credit Research Foundation revealed that nearly half of all business payments are made by paper check. Baffling, to be sure, but the good news is that businesses are recognizing that it's time to make a change. In fact, a recent survey from AppDirect found that nearly 80% of companies are in the process of strategizing and implementing their digital transformation initiatives.

The war against manual business processes is certainly a net positive, but it isn't waged without security challenges. The concept of digital transformation is about more than just onboarding technologies: with every new asset, user or device added, enterprises are continuously and increasingly introducing new risks.

Open the digital floodgates, yet trust no one

At the same time businesses rush to employ new technologies, the security function is embracing a new model that challenges the traditional approach to keeping information secure: Zero Trust.

While traditional information security approaches used the castle-and-moat analogy that focused on defending a perimeter and assumes anything on the inside is safe, the Zero Trust model makes no assumption based on position relative to perimeter.

Just because a user or asset has made it onto the corporate network it does not automatically mean they should be trusted. Employing the Zero Trust model means verifying anything and everything trying to connect to the organization's systems before granting access.

Two excellent aspirations, one nagging issue: Asset management

The business wants to use technology to increase speed, efficiency and growth. Security wants to interrogate every asset, device and user at all times to be sure all access is appropriate.

Both are noble ambitions, but there's one issue that must be solved first before either of these initiatives can succeed: asset management.

Asset management is the Toyota Camry of cybersecurity. In a landscape of solutions using AI, machine learning, deception and other sci-fi sounding technologies, getting a credible inventory of all laptops, desktops, servers, VMs, cloud instances, users, and so on, is decidedly unsexy. But despite the lack of luster, understanding all assets and how they adhere to the overall security policy is the only way organizations can both embrace digital transformation while continuously validating whether assets, users, and devices should be granted access.

Here are five reasons why asset management is necessary for achieving digital transformation and Zero Trust.

1_A staggering number of devices

With Gartner Research projecting that the number of connected things will reach 14.2 billion in 2019 and 25 billion by 2021, managing this increasing number of connected assets, devices and users is quickly becoming an urgent security priority for CISOs, CIOs, and frankly, organizations everywhere.

More recent trends like BYOD, mobile devices, remote work and the cloud have led to a significant shift in the way organizations think about which devices they're responsible for securing. In a world where any device has access to corporate information, the sheer number of devices security teams are tasked with identifying and securing is astounding. As organizations continue to grow, it's no longer possible or scalable to ensure that every device or cloud instance is covered by the security solutions required by the corporate security policy.

2_A growing attack surface and opportunistic cyber criminals

The rise in the number of assets means that enterprises across the globe continue expanding their attack surface. Most of the high-profile breaches we hear about today are a result of inadequate cybersecurity asset management. Whether it's an unpatched Apache server, a public-facing Amazon bucket or a smart fish tank in a casino, organizations are often breached when an attacker can find an easy way into the environment, which frequently happens by exploiting an asset that isn't accounted for or does not adhere to security policy.

3_Too many tools with not enough answers

New products, solutions, and services are introduced to the market every day, and as a result, companies purchase and onboard a myriad of products to secure a variety of different assets. The problem is that instead of making life easier and more secure, the sheer volume of these devices ends up creating silos of information, making it more difficult for security teams to answer basic questions about their security posture like "How many Windows hosts do I have?" and "Are they adhering to our security policy?".

> *Considering the ever-expanding attack surface and talent gap, CISOs don't want to use scarce, highly-trained resources to take on manual, tedious tasks like inventorying every asset. This problem is multiplied when the assets are siloed and distributed across a variety of products, tools, and solutions.*

4_The inevitable march to the cloud

The cloud is fast, cheap and scalable, which is why 85% of companies have adopted and utilized cloud infrastructure moderately or extensively in the past year. Unfortunately, the security solutions once used for on-premise devices don't always translate to the cloud.

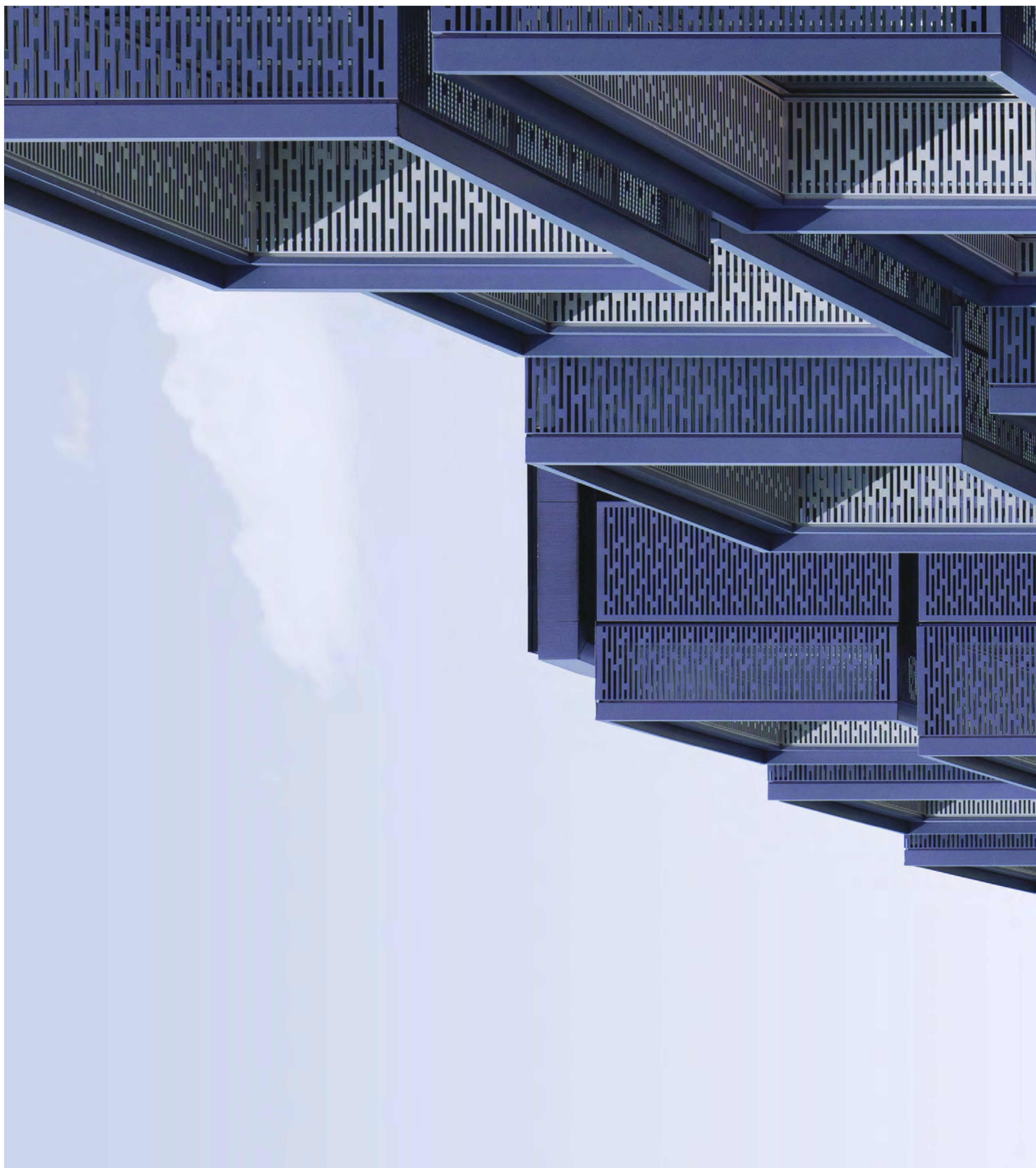
5_Too much work, too few resources, never enough time

Although the number of connected devices, assets, and users is increasing, skilled security professionals are in short supply, expensive, and overworked.

Considering the ever-expanding attack surface and talent gap, CISOs don't want to use scarce, highly-trained resources to take on manual, tedious tasks like inventorying every asset. This problem is multiplied when the assets are siloed and distributed across a variety of products, tools, and solutions.

We're at a time in cybersecurity where despite all of the advanced technologies available to businesses, the industry has yet to solve the old and unsexy problem of asset management for cybersecurity.

As long as digital transformation continues on, this age-old problem worsens. If your organization is onboarding or deploying new technologies, there's no better time to develop, optimize and strategize cybersecurity asset management.



Machine learning trumps AI for security analysts

AUTHOR_Meny Har, VP of Products, Siemplify

Machine learning is currently one of the biggest buzzwords in cybersecurity and the tech industry in general, but the phrase is often overused and misapplied, leaving many with their own, incorrect definition.

So, how do you cut through all the noise to separate fact from fiction? And how can this tool be best applied to security operations?

What is machine learning?

Machine learning (ML) is an algorithm that gives the software applications it is applied to the ability to autonomously learn from its own environment, then improve operations based on the data collected. It does this without much human supervision or being specifically programmed to do so.

The technology makes it possible to analyze terabytes of data and discern patterns that would otherwise be missed. People often think that machine learning stops at summarizing data and finding patterns for humans to extrapolate from those patterns, but that's not correct. ML goes beyond just summaries and rather uses the data to make predictions for the future.

Some examples of machine learning are more obvious than others. When Netflix recommends a new show for you to watch, that suggestion is based on data it collected from what you previously watched.

Machine learning is used for much more than human convenience, though. For example, global energy giants General Electric (GE) and Beyond Petroleum (BP) announced a partnership to deploy machine learning across their wells and oil rigs, stating, "the oil well software will harvest information from sensors monitoring vibrations, temperature, pressure and other well properties.

It will store, contextualize and visualize the data, and provide the right BP workers with real-time insights.”

> *Machine learning is an analyst’s secret weapon and an increasingly essential asset to have in your toolkit. Machine learning provides SOC analysts with the focus and insights to work smarter, not harder.*

Machine learning and artificial intelligence aren’t synonymous

One of the biggest misconceptions regarding machine learning is that it can be referred to interchangeably with artificial intelligence (AI). While the idea of machine learning is a subset of AI, the two are different. AI is a blanket term for the simulation of human intelligence processes by machines, while machine learning is a way to use the concept of AI, but requires very little guidance from humans, aside from the initial algorithm.

Machine learning and security operations

Many are concerned about the malicious use of machine learning and some studies predict an “arms race” of sorts when it comes to this technology. While no one can accurately predict the future of machine learning and its use by both good and bad actors, there are two major areas where security operations teams should apply it today.

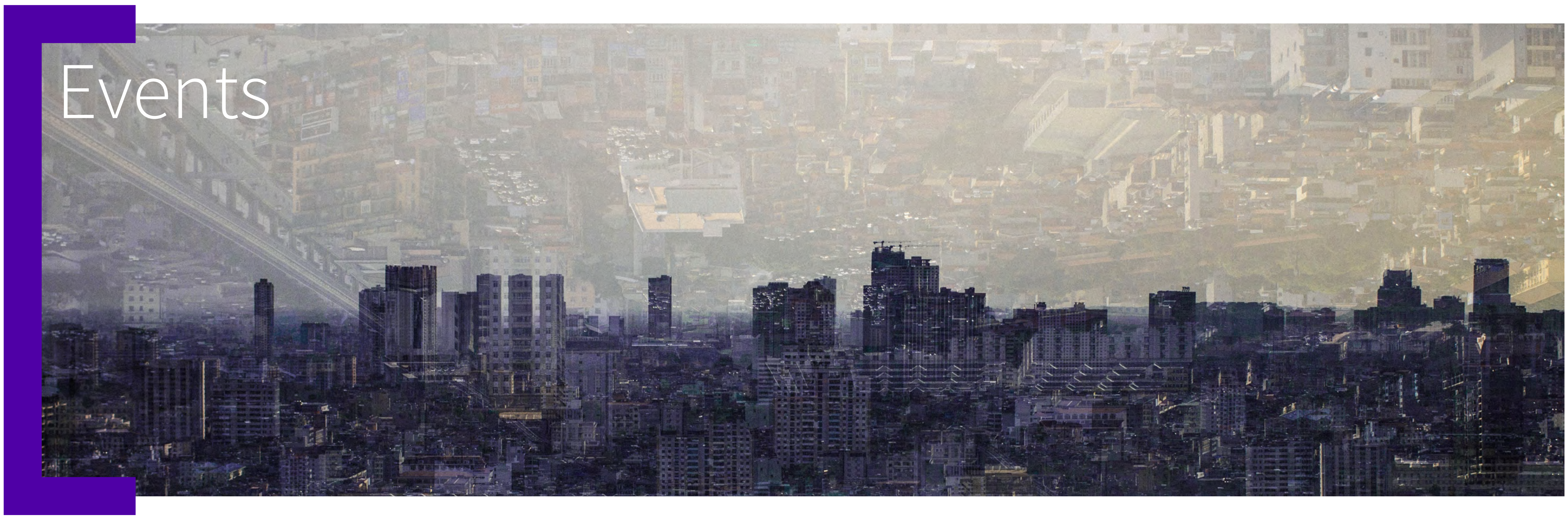
First and foremost, machine learning can significantly improve a security operations center’s (SOC’s) detection abilities. Much like the Netflix example, machine learning can help detect new threats based on past malicious activity. While it may take an analyst several hours to manually go through logs to identify a potential threat and cross-reference it with past incidents, machine learning can enable your systems to do this in an instant, leaving the analyst with more time to spend on investigation and remediation activities.

The second major benefit is in the realm of prioritization. Most security teams are inundated with far more alerts than they can reasonably manage and investigate. Wading through rows of data to determine which alerts are most pressing is tedious and time-consuming. By learning from past alerts and events, machine learning can prioritize alerts for security analysts, illuminating those that are most critical and putting them at the top of the queue for triage and remediation.

This same principle can also be applied in prioritizing resources within the SOC. Let’s say you have an analyst that is hyper-efficient at addressing malware alerts. Utilizing machine learning, your systems can learn to automatically assign the most critical malware alerts to this particular analyst, ensuring that they will be addressed as quickly and effectively as possible. In this way, machine learning becomes a powerful operations enabler, streamlining resource and people management for maximum efficiency and impact.

Analysts’ secret weapon

Machine learning is an analyst’s secret weapon and an increasingly essential asset to have in your toolkit. Machine learning provides SOC analysts with the focus and insights to work smarter, not harder. At the end of the day, security operations are all about preventing threats and neutralizing them as fast as possible. Machine learning uses data to better enable teams to do just that.



Events

RSA Conference 2019

March 4 – 8, 2019
Moscone Center, San Francisco
https://www.rsaconference.com/helpnet-us19

Looking for cybersecurity intel? Your search starts and stops here, at RSA Conference 2019. A hub for innovation, industry experts and up-and-coming talent alike, RSAC 2019 is where the world talks security. And security talks back. From expert-informed keynotes, enlightening seminars, and interactive exhibitions, the agenda is filled with critical discussions on today's trends, challenges and forward motion.

HITBSecConf2018 – Amsterdam

April 9 – 13, 2019
NH Grand Krasnapolsky, Amsterdam
https://conference.hitb.org/hitbsecconf2019ams/

The 9th annual HITB Security Conference features six 3-day technical training courses followed by a 2-day triple track conference, a Capture the Flag competition, technology exhibition with an expanded area covering AI and blockchain related entities, a space for EU hackerspaces, a lock picking village, car hacking and hardware related exhibits plus our CommSec track - a free-to-attend track of 30 and 60 minute talks.

(ISC)^2 Secure Summit EMEA

April 15 – 16, 2019
The World Forum, The Hague
http://helpnet.pro/v0rq

This event will welcome hundreds of the best minds in cybersecurity from across EMEA. Presentations come from every level of practice and are selected for their ability to provoke thought. Front-line practitioners and administrators can find themselves sitting beside and talking to specialists, senior managers and CISOs. It's a dynamic that contributes to the development in our profession's understanding and curation of good practice.

Considering an SD-WAN Deployment? The best solution may already be in your network

AUTHOR_Brendan Patterson, VP of Product Management, WatchGuard Technologies

When the internet goes down, business stops. Every business today relies on cloud applications to run day-to-day operations, including CRM applications like Salesforce, engineering collaboration tools such as JIRA and Confluence and office productivity tools like Office 365.
IT departments need to deliver high-quality, reliable links for all applications that are core to the company's business operations.

> *Businesses are excited about SD-WAN technology because it presents an opportunity to curtail the costs associated with expensive multiprotocol label switching (MPLS) solutions, moving traffic to public internet lines and often using secure VPN solutions to communicate between sites.*

To meet this demand in a cost-effective way, businesses are looking to one of the hottest topics in networking right now: software-defined wide-area network (SD-WAN). In fact, analysts predict this market will grow to $2.5 billion by 2022.

Businesses are excited about SD-WAN technology because it presents an opportunity to curtail the costs associated with expensive multiprotocol label switching (MPLS) solutions, moving traffic to public internet lines and often using secure VPN solutions to communicate between sites. Network links without assured or guaranteed service can now be used to deliver business class services, including Voice over IP and video applications.

But with a crowded and growing market, what type of SD-WAN solution should companies look for and how will they affect the businesses' overall security?

As with any emerging technology, there's no shortage of new vendors making bold claims about their product capabilities, and every vendor's definition of the technology varies in order to match what they can deliver. That's why it's crucial for businesses to truly understand what SD-WAN is and what it isn't before embarking on a new deployment. Surprisingly, in many cases firewall appliances are now able to provide SD-WAN services as well as network security in a single appliance.

The 4 key characteristics of SD-WAN

There are several important features and capabilities that should be included in any SD-WAN solution.

These include:

1_The use of software to manage connections over different link or connection types – MPLS, cable modem, DSL, 4G and links from different ISPs. Every SD-WAN service should offer dynamic path selection between these different links based on predefined policies set to align with business priorities. They should test circuit performance in real time, measuring packet loss, latency, and jitter to determine if the line meets the acceptable level of quality for its application traffic.

2_Traffic management for applications. For example, they should be able to guarantee 10 Mbps for all Salesforce traffic.

3_Secure VPN capabilities for site-to-site tunnels with full IKEv2 level encryption or TLS level transport. When internet connections are used, businesses need to ensure that all data is private and none of the traffic can be viewed by third parties.

4_"Zero-touch" deployment options that allow SD-WAN appliances to be delivered to remote locations and configured automatically by simply powering on and connecting to the internet. This ease of deployment aspect is critical, as technical staff and network engineers are scarce and businesses need to quickly deploy cloud solutions as they roll out new hybrid WAN architectures to distributed sites.

> *If you are already running an NGFW or UTM in your network, evaluate it against the four key characteristics of SD-WAN outlined in this article. You may be pleasantly surprised to learn that it already meets most or all of these capabilities*

SD-WAN is typically delivered by placing a routing appliance or physical box in a branch location. Some SD-WAN solutions provide additional security capabilities like antivirus services or web content inspection. In certain instances, the solution is even offered by the telecom carrier as part of a monthly managed service. This is somewhat ironic since these are also the same organizations that sell expensive MPLS solutions.

SD-WAN solutions should not introduce new security risks or vulnerabilities

Another important point to consider is who will be installing the SD-WAN solution. Is it an experienced managed service provider than understands the security of your network and will take the time to understand your needs, or is it a telecom provider looking to add some extra dollars to an existing sale?

There are some common security pitfalls to be aware of when introducing a new SD-WAN capability:

- An inexperienced operator may install SD-WAN routing devices behind a next-gen firewall or UTM and bypass the firewall that is already in place for some or all traffic. This would be a major security vulnerability because it could expose the internal networks to public access, bypassing all malware inspection at the UTM.
- The security capabilities offered with the SD-WAN may offer a false sense of security for customers. Does the solution only rely on simple signature-based detections to find malware passing through the network? Advanced and evasive threats can easily circumvent basic antivirus solutions. This is why it’s critical to have layered, advanced security services like behavioral-based and artificial intelligence-enabled antivirus as a part of the overall SD-WAN solution deployed at remote sites.
- Managed SD-WAN solutions may claim to offer some basic firewall services, but they can also take days to respond to simple requests to implement or change basic rules. For example, if an application no longer needs to have a port open, a company should be able to immediately implement a change that no longer exposes it.

UTMs may offer an effective, economical SD-WAN solution

The solution to a problem can often be found directly under your nose! For many years, next-generation firewalls (NGFWs) and Unified Threat Management (UTM) solutions have evolved to consolidate network and security functions onto a single appliance strategically located at the network perimeter.

If you are already running an NGFW or UTM in your network, evaluate it against the four key characteristics of SD-WAN outlined in this article. You may be pleasantly surprised to learn that it already meets most or all of these capabilities.

Plus, if your UTM offers SD-WAN and critical security functionality in a single appliance, that removes the need to purchase, deploy and manage multiple appliances. Next, compare the level of security offered by your UTM appliance against that of the pure SD-WAN solutions you might be considering.

Many new SD-WAN providers are novices in the security space, so the level of protection they offer may not meet your requirements.

SD-WAN adoption will continue at a rapid pace of the foreseeable future. As you consider the best approach for your organization, take a second look at your security appliance. You may find that the best option for your SD-WAN deployment has been there all along.