CYBEREDGE GROUP

2019 Cyberthreat Defense Report

North America | Europe
Asia Pacific | Latin America
Middle East | Africa

« Research Sponsors »

PLATINUM

CODE42 · DXC.technology · Gigamon · imperva

GOLD

aqua · LOOKINGGLASS · Recorded Future · StackRox

SILVER

ARCTIC WOLF · BANDURA CYBER · ctera · {disruptOps} · edgeworx solutions · illusive

Table of Contents

Introduction

CyberEdge's annual Cyberthreat Defense Report (CDR) has garnered considerable media attention and accolades over the last five years. It's unlike any research report in the IT security industry. Rather than supplying statistics on specific cyberattacks and data breaches (which many of our sponsors do quite well), we provide deep insight into the minds of IT security professionals.

Now in its sixth year, the CDR has become a staple among IT security leaders and practitioners by helping them gauge their internal practices and security investments against those of their peers – now across 17 countries and 19 industries. Simply put, there is no other report of its kind.

CyberEdge would like to thank our Silver, Gold, and Platinum research sponsors without whose continued support this report would not be possible.

Top Five Insights for 2019

As always, our latest CDR installment yields dozens of actionable insights. But the following are the top five takeaways from this year's report – at least in our eyes:

1. **Security analytics poised for success.** 2019 could well be known as the year that security analytics hit its stride. The greatest inhibitor to IT security's success is contending with too much security data. Our research participants identified security analytics as the most-wanted security management and operations technology for 2019.

2. **Application development migraines.** For the second consecutive year, IT security organizations struggle with application development and testing more than any other security process. And application containers are, once again, the Achilles' heel of IT security organizations.

3. **Ransomware on the rise.** Last year's ransomware stats were ugly. This year's stats are even uglier. The percentage of organizations victimized by ransomware is up, the percentage of organizations paying ransoms is up, and the percentage that lost data by refusing to pay ransoms is up, as well.

4. **Machine learning garners confidence.** More than 90% of IT security organizations have invested in machine learning (ML) and/or artificial intelligence (AI) technologies to combat advanced threats. More than 80% are already seeing a difference.

SURVEY DEMOGRAPHICS:

- **Responses received from 1,200 qualified IT security decision makers and practitioners**
- **All from organizations with more than 500 employees**
- **Representing 17 countries across North America, Europe, Asia Pacific, the Middle East, Latin America, and Africa**
- **Representing 19 industries**

5. **Web application firewalls rule the roost.** For the second consecutive year, the web application firewall (WAF) claims the top spot as the most widely deployed app/data security technology.

About This Report

The CDR is the most geographically comprehensive vendor-agnostic study of IT security decision makers and practitioners. Rather than compiling cyberthreat statistics and assessing the damage caused by data breaches (other researchers do a great job there), the CDR surveys the perceptions of IT security professionals, gaining insights into how they see the world.

Specifically, the CDR examines:

- The frequency of successful cyberattacks in the prior year and optimism (or pessimism) for preventing further attacks in the coming year
- The perceived impact of cyberthreats and the challenges faced in mitigating their risks
- The adequacy of organizations' security postures and their internal security practices
- The organizational factors that present the most significant barriers to establishing effective cyberthreat defenses
- The investments in security technologies already made and those planned for the coming year
- The health of IT security budgets and the portion of the overall IT budget they consume

Introduction

By revealing these details, we hope to help IT security decision makers and practitioners gain a better understanding of how their perceptions, concerns, priorities, and defenses stack up against those of their peers in other countries and industries. Applied constructively, the data, analyses, and findings can be used by diligent IT security teams to shape answers to many important questions, such as:

- Where do we have gaps in our cyberthreat defenses relative to other organizations?
- Have we fallen behind in our defensive strategy to the point that our organization is now the "low-hanging fruit" (i.e., likely to be targeted more often due to its relative weaknesses)?
- Are we on track with both our approach and progress in continuing to address traditional areas of concern, while also tackling the challenges of emerging threats?
- How does our level of spending on IT security compare to that of other organizations?
- How are other IT security practitioners thinking differently about cyberthreats and their defenses, and should we adjust our perspective and plans to account for these differences?

Another important objective of the CDR is to provide developers of IT security technologies and services with information they can use to better align their solutions with the concerns and requirements of potential customers. The net result should be better market traction and success for solution providers – at least those that are paying attention – along with better cyberthreat protection technologies for all the intrepid defenders out there.

The findings of the CDR are divided into four sections:

Section 1: Current Security Posture

The security foundation an organization currently has in place and the perception of how well it is working invariably shape future decisions about cyberthreat defenses, such as:

- Whether, to what extent, and how urgently changes are needed
- Specific types of countermeasures that should be added to supplement existing defenses

Our journey into the depths of cyberthreat defenses begins, therefore, with an assessment of respondents' perceived effectiveness of their organization's investments and strategies relative to the prevailing threat landscape.

Section 2: Perceptions and Concerns

In this section, our exploration of cyberthreat defenses shifts from establishing baseline security postures to determining the types of cyberthreats and other obstacles to security that concern today's organizations the most. Like the perceived weaknesses identified in the previous section, these concerns serve as an important indicator of where and how organizations can best improve their cyberthreat defenses going forward.

Section 3: Current and Future Investments

Organizations can ill afford to stand still when it comes to maintaining effective cyberthreat defenses. IT security teams must keep pace with the changes occurring around them – whether to the business, technology, or threat landscapes – by making changes of their own.

With respondents' perceptions of the threat landscape and the effectiveness of their organization's defenses as a backdrop, this section sheds light not only on the security technologies organizations currently have in place, but also on the investments they plan to make over the coming year.

Introduction

Section 4: Practices and Strategies

Mitigating today's cyberthreat risks takes more than investing in the right technologies. You must ensure those technologies are deployed optimally, configured correctly, and monitored adequately to give your organization a fighting chance of not making tomorrow's front page news.

In this section, we assess best practices IT security professionals embrace for combatting today's threats. We also gauge adoption of leading-edge technologies and ascertain how they're used.

Navigating This Report

We encourage you to read this report from cover to cover, as it's chock full of useful information. But there are three ways to navigate through this report, if you are seeking out specific topics of interest:

- **Table of Contents.** Each item in the Table of Contents pertains to specific survey questions. Click on any item to jump to its corresponding page.
- **Research Highlights.** The Research Highlights page showcases the most significant headlines of the report. Page numbers are referenced with each highlight so you can quickly learn more.
- **Navigation tabs.** The tabs at the top of each page are clickable, enabling you to conveniently jump to different sections of the report.

Contact Us

Do you have an idea for a new topic that you'd like us to address next year? Or would you like to learn how your organization can sponsor next year's CDR? We'd love to hear from you! Drop us an email at research@cyber-edge.com.

Research Highlights

Current Security Posture

- **Attack success redux.** The percentage of organizations affected by a successful cyberattack ticked up from 77% to 78%, despite last year's first-ever decline (page 7).
- **Pessimism spike.** Nearly two-thirds of IT security professionals believe a successful cyberattack is imminent in 2019 (page 8).
- **Container security woes.** For the second year, application containers edge mobile devices as IT security's weakest link (page 9).
- **Application development headaches.** For the third year, app development and testing is the security process organizations struggle with the most (page 10).
- **Cyberthreat hunting inhibitors.** The greatest challenge is implementing and integrating cyberthreat hunting technologies (page 11).
- **Worsening skills shortage.** 84% of organizations are experiencing an IT security skills shortage, up from 81% last year (page 12).

Perceptions and Concerns

- **Cyberthreat trifecta.** Malware, spear phishing, and ransomware top the list of cyberthreat concerns for the third consecutive year (page 13).
- **Funding ransomware.** Ransomware attacks are rising, and so are the number of ransom payers (page 14).
- **Security data avalanche.** IT security professionals can't keep up with growing mountains of security data (page16).
- **Old dogs, new tricks.** More than half of organizations are re-training existing IT staff to tackle cloud security challenges (page 18).
- **Glass half full?** Nearly four in five respondents believe their scanning and patching efforts have improved, but is it enough? (page 19).

Current and Future Investments

- **Security's slice of the pie.** On average, IT security consumes 12.5% of the overall IT budget (page 20).
- **Record-setting security budgets.** The average security budget is going up by 4.9% in 2019 (page 22).
- **Network security's top picks.** Advanced malware analysis, next-gen firewalls (NGFWs) and deception solutions are the top network security technologies planned for acquisition in 2019 (page 24).
- **Defender of endpoints.** Containerization / micro-virtualization heads the list of endpoint security technologies respondents plan to acquire in 2019… again (page 26).
- **Ruling the app/data security roost.** For the second consecutive year, WAF is the most widely deployed app/data security technology (page 28).
- **Most-wanted security technology.** Advanced security analytics tops 2019's most wanted list not only for the security management and operations category, but also for all technologies in this year's report (page 30).
- **Burgeoning biometrics.** Biometrics bubbled to the top as the most sought-after identity and access management technology for the coming year (page 32).
- **Bringing the heat for advanced threats.** More than four in five respondents believe ML and AI technologies are making a difference in the battle to detect advanced cyberthreats (page 34).

Practices and Strategies

- **Unsolved SSL decryption puzzle.** Decrypting SSL/TLS network traffic so that it can be inspected for threats remains a persistent challenge for nearly three in four organizations (page 36).
- **TIPping the security scales.** Enterprises are sourcing threat intelligence platforms (TIPs) to improve cyberthreat detection and validate security alerts (page 37).
- **Sourcing strategies for security analytics.** Purchasing a standalone product to complement an existing SIEM is the top approach for adding security analytics to an organization's cyberthreat defenses (page 38).
- **Flying high with SOAR.** Forward-leaning organizations are adopting security orchestration, automation, and response (SOAR) solutions to accelerate SecOps tasks (page 39).
- **MSSPs to the rescue.** Nine of 10 organizations are leveraging managed security service providers (MSSPs) to offload at least one IT security function (page 40).

Section 1: Current Security Posture

Past Frequency of Successful Cyberattacks

How many times do you estimate that your organization's global network has been compromised by a successful cyberattack within the past 12 months? (n=1,137)

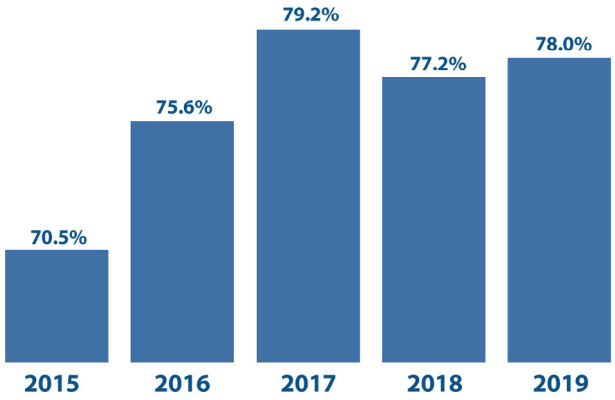

Figure 1: Frequency of successful attacks by year.

"Unfortunately, that glimmer of hope has vanished because successful attacks are, once again, on the rise."

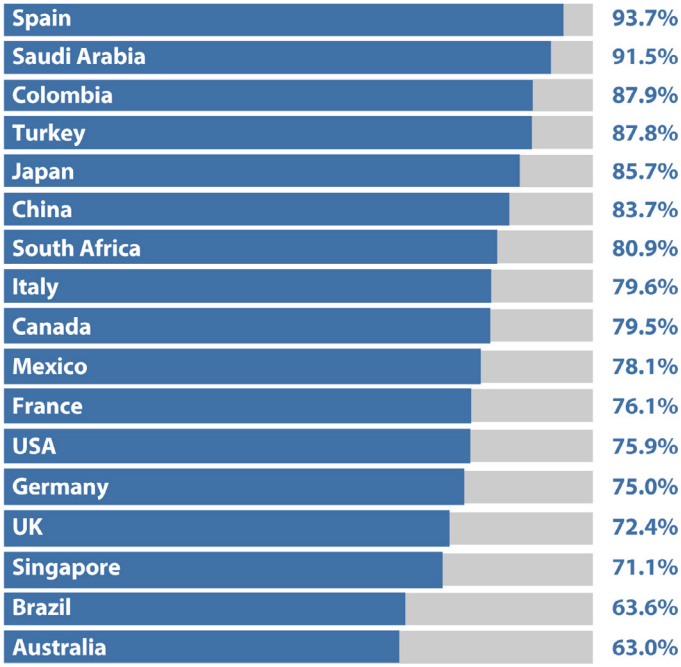

Figure 2: Percentage compromised by at least one successful attack in the past 12 months.

Last year, we expressed cautious optimism after witnessing the first-ever decline in successful cyberattacks in our report's five-year history. Unfortunately, that glimmer of hope has vanished because successful attacks are, once again, on the rise. Last year, 77.2% of respondents reported a successful cyberattack. This year, that figure rose to 78.0% (see Figure 1). Furthermore, the portion of respondents reporting more than 10 successful attacks has also expanded, from 9.0% to 9.4%.

Analyzing the data regionally (see Figure 2), we can report a couple of bright spots. First, the cyberthreat climate in Mexico has dramatically improved. Last year, Mexico was hardest hit of all countries, with 93.9% of respondents reporting successful attacks. This year, Mexico is in the middle of the pack at 78.1%. Unfortunately, another Spanish-speaking country, Spain, has taken over as hardest hit, with 93.7% of respondents reporting successful attacks. As in Mexico, the situation has improved down under: Australia is revealed to be the least targeted, with only 63.0% of respondents reporting successful attacks – down from 66.7% last year.

Of the seven key industries tracked in this report, telecom & technology (81.2%) is the industry hardest hit in this year's report, followed by education (80.0%) and retail (79.2%). Healthcare (69.1%) is the least-targeted industry this year.

Dissecting the data by headcount, mid-size enterprises with 5,000-9,999 employees were affected the most (88.0%) by successful cyberattacks. They felt the impact considerably more than the largest (more than 25,000 employees; 73.9%) and the smallest (500-999 employees; 66.7%) organizations.

Section 1: Current Security Posture

Future Likelihood of Successful Cyberattacks

What is the likelihood that your organization's network will become compromised by a successful cyberattack in 2019? (n=1,153)

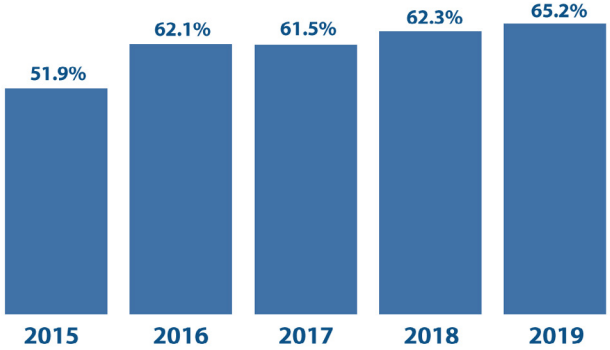

Figure 3: Likelihood of being successfully attacked in the next 12 months.

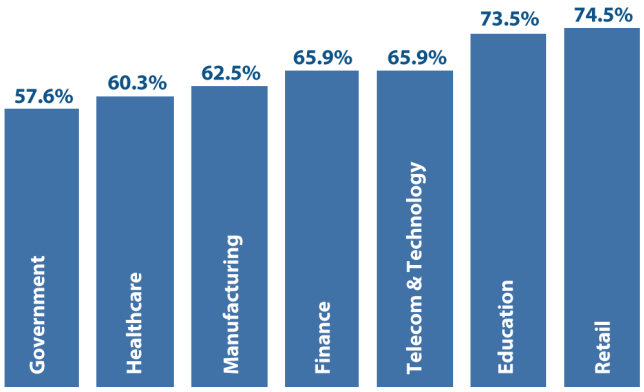

Figure 4: Percentage indicating compromise is "more likely to occur than not" in the next 12 months.

People, in general, embrace optimism over pessimism. Time magazine surveyed 801 Americans in 2013 asking them if they felt they were, in general, more optimistic or pessimistic by nature. 50% identified as optimistic while only 4% identified as pessimistic, with the balance somewhere in between. Although this survey is now six years old, we believe it still applies today.

However, after being inundated with sophisticated cyber-attacks over the past decade, IT security professionals tend to be more pessimistic as it pertains to the likelihood of their organizations being compromised by one or more cyber-attacks in the coming year. And frankly, they have every right to be.

In last year's report, 77.2% of respondents reported successful cyberattacks in the preceding year. Despite this sour reality, only 62.3% felt a successful attack was likely in the coming year. This pattern continues: while 78% reported successful attacks this year, only 65.2% expect the same in 2019 (see Figure 3).

Let's ponder this further: 78.0% were victimized last year, but only 65.2% feel they're likely to be victimized again this year. That means 12.8% have reason to believe things are getting better. But why? Here are a few plausible explanations:

- Security budgets in 2019 set a record for the highest single-year increase in our report's six-year history, at 4.9% (see page 22).
- Despite being inundated with security data (see page 16), organizations are investing heavily in security analytics in 2019 (see page 30).
- More than four in five respondents believe that innovative new ML and AI technologies are making a difference in the battle to detect advanced cyberthreats (see page 34).

Other notable findings from this year's report include:

- The percentage of respondents considering it "not likely" that their organization will be breached in the coming year held fairly steady, with only a slight decrease from 12.8% in 2018 to 12.6% for 2019.
- Geographically, China (91.9%), Turkey (85.7%), and Mexico (84.4%) are the most pessimistic in the coming year. Respondents in Australia (48.0%) like their chances.
- Of the seven key industries tracked in this report, retail (74.5%), education (73.5%), and telecom & technology (65.9%) employ the most pessimistic IT security profes-sionals. Surprisingly, government (57.6%) respondents are the most bullish, despite numerous high-profile government data breaches around the world (see Figure 4).

Section 1: Current Security Posture

Security Posture by IT Domain

On a scale of 1 to 5, with 5 being highest, rate your organization's overall security posture (ability to defend against cyberthreats) in each of the following IT components: (n=1,191)

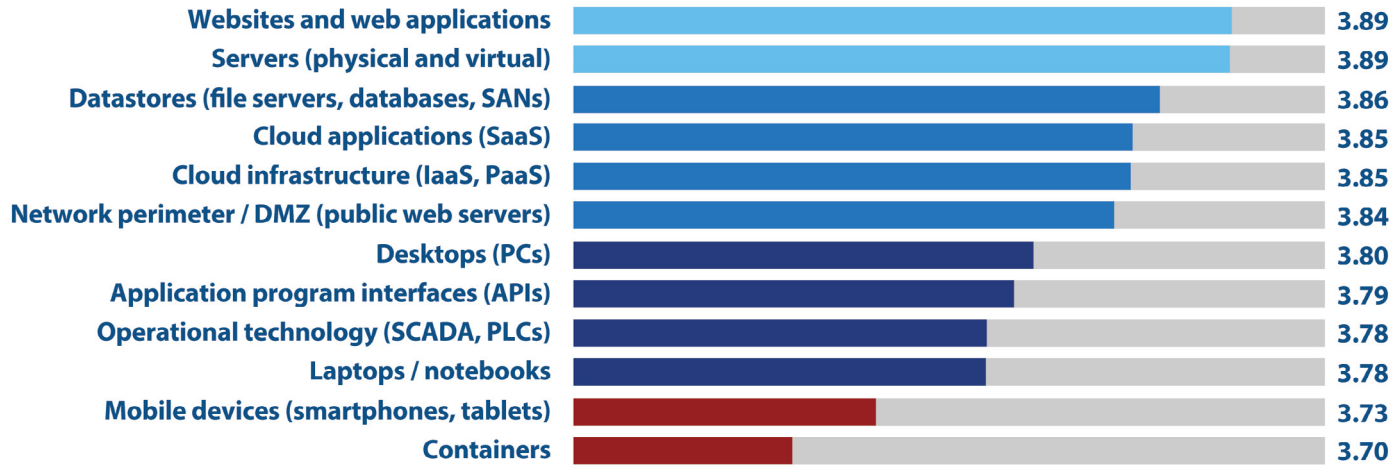

Figure 5: Perceived security posture by IT domain.

Defending today's complex networks against an ever-evolving climate of advanced cyberthreats is no easy task. And, of course, some IT components are easier to defend than others.

For the past six years, we've asked our research participants to rate their ability to defend cyberthreats against various classes of IT components. The results are, once again, fairly understandable.

Traditional IT components such as websites, physical and virtual servers, and datastores are largely static. That means it's easier to keep them up-to-date with patches and easier to detect inbound cyberthreats targeting them (see Figure 5). However, it is more challenging to secure other types of IT components:

- Newer IT components – such as application containers and operational technology (OT) devices – are harder to protect because corresponding cyberthreats are still emerging and experience with related defenses remains low.
- Devices that are infrequently connected to the corporate network – such as smartphones, tablets, and laptops – are more difficult to keep up-to-date with the latest patches and threat signatures.

"Newer IT components – such as application containers and operational technology (OT) devices – are harder to protect because corresponding cyberthreats are still emerging and experience with related defenses remains low."

An interesting footnote: on a scale of 1 to 5, with 5 being highest (i.e., most secure), the average rating for IT components in both 2018 and 2019 is 3.82 – precisely the same to the hundredth of a point. So, although some IT components are perceived as slightly easier to secure in 2019 as compared to last year (e.g., mobile devices – from 3.67 to 3.73), this result is offset by another group of IT components that are perceived as slightly more challenging to secure in 2019 (e.g., datastores – from 3.95 to 3.86).

Section 1: Current Security Posture

Assessing IT Security Functions

On a scale of 1 to 5, with 5 being highest, rate the adequacy of your organization's capabilities (people and processes) in each of the following functional areas of IT security: (n=1,189)

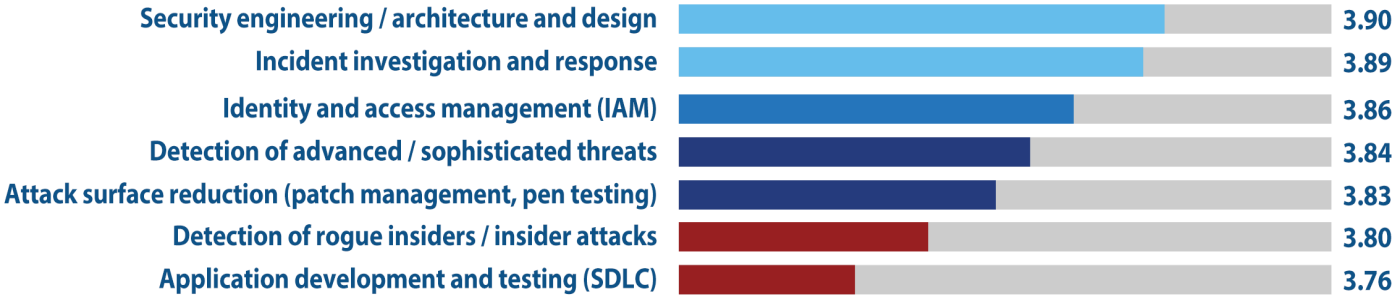

Figure 6: Perceived adequacy of functional security capabilities.

In the previous section, we asked our research participants to rate their confidence about securing various classes of IT components. In this section, we asked a similarly structured question: how they rate the adequacy of their organization's internal security processes.

For the third straight year, application development and testing is the Achilles' heel of IT security organizations. This finding aligns perfectly with the corresponding result in the prior section, as application containers are the most challenging IT component to secure. Thankfully, IT security vendors are continuing to add innovations to the following DevSecOps tools that should help to automate the application development and testing process:

- Static application security testing (SAST)
- Software composition analysis (SCA)
- Dynamic application security testing (DAST)
- Mobile application security testing (MAST)

The next two most-challenging processes swapped positions from last year's report, despite achieving scores that changed by only the slightest of margins. Detection of rogue insiders achieved the second-worst position and attack surface reduction achieved third-worst position. With regard to the latter, a silver lining from this year's CDR is that our respondents believe that their vulnerability management and patch management capabilities have improved over the past 12 months, resulting in faster patching and diminished attack surfaces (see page 19).

"For the third straight year, application development and testing is the Achilles' heel of IT security organizations."

On another sour note, identity and access management (IAM) fell from first position last year (3.94) to the middle of the pack this year (3.86) – the largest rating drop of the eight IT security processes. But on the bright side, respondents continue to be bullish about their user security awareness / education capabilities (3.90), despite the assertion that security awareness among employees is still a major concern (see page 16).

Section 1: Current Security Posture

Cyberthreat Hunting Inhibitors

On a scale of 1 to 5, with 5 being highest, rate how each of the following inhibit your organization from achieving effective threat-hunting capabilities: (n=1,189)

Figure 7: Inhibitors to achieving an effective cyberthreat hunting program.

Last year, we asked our research participants whether they felt their respective organizations had invested adequately in cyberthreat hunting solutions. Although four in five respondents (81.7%) felt their employers had invested adequately, that means one in five (18.3%) was not confident in this regard. Given the sophistication of today's advanced threats and the numerous advancements in modern cyber-threat hunting technology, this result is disconcerting.

This year, we delved a little deeper into the topic. We asked respondents to rate potential inhibitors to their organization's cyberthreat hunting endeavors. The results were insightful.

First, the top cyberthreat hunting inhibitor pertains to the challenge of implementing and/or integrating threat-hunting tools and technologies (3.38) (see Figure 7). Perhaps this is an opportunity for cyberthreat hunting software vendors to distinguish themselves by offering new (or improved) APIs to streamline integration efforts. And it's certainly an opportunity for these vendors and their respective channel partners to offer expert consulting to assist their customers with installing and configuring their cyberthreat hunting solutions.

Second, a lack of skilled threat-hunting personnel (3.31) is also a significant concern for our respondents. This goes hand in hand with the aforementioned integration challenge when organizations lack the expertise and manpower to properly install and configure sophisticated threat-hunting platforms. It also underscores the growing shortfall in skilled IT security personnel, as highlighted in the next section.

On the other end of the spectrum are the threat-hunting solutions themselves. Potential lack of third-party validation (3.25) and lack of effective solutions (3.27) are of least concern.

"The top cyberthreat hunting inhibitor pertains to the challenge of implementing and/or integrating threat-hunting tools and technologies."

Section 1: Current Security Posture

The IT Security Skills Shortage

Select the roles/areas for which your organization is currently experiencing a shortfall of skilled IT security personnel. (Select all that apply.) (n=1,165)

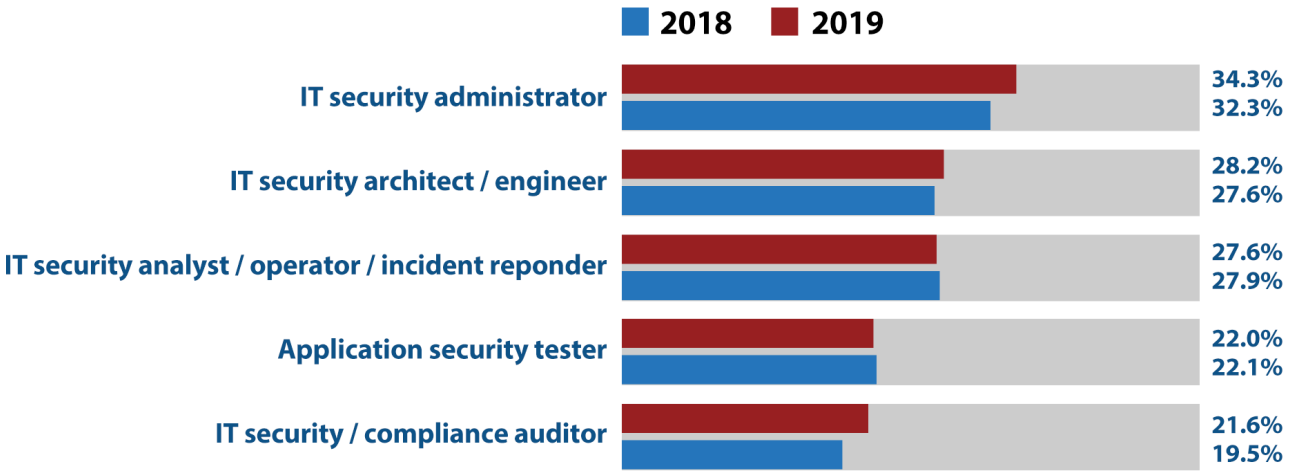

Figure 8: Cybersecurity skills shortage by role.

One of the most significant challenges facing virtually every IT security organization is finding and retaining top-notch talent. In fact, it's been one of the top three overall inhibitors to IT's success in the war against cyberthreats in each of the past three years of this report – and it remains in the top three this year (see page16).

Last year, we reported that 80.9% of organizations were experiencing a shortage of qualified IT security talent. This year, we're sad to report this figure has risen to 84.2%.

However, some IT security positions are more difficult to recruit for than others (see Figure 8). For the past two years, it's been most challenging to recruit IT security administrators (34.3%) and IT security architects and engineers (28.2%), likely because these are typically higher-level positions requiring extensive experience and broad expertise. Recruiting IT security / compliance auditors is the least challenging (21.6%), perhaps because hands-on technical expertise is less important.

Other findings of interest include:

- Brazil (65.6%), Germany (74.3%), and Australia (76.1%) remain the least impacted by the cybersecurity skills shortage, while Japan (94.0%) struggles the most again this year, followed by Saudi Arabia (91.8%) and Singapore (90.0%).
- Education (91.3%) is, once again, the industry most affected by the IT skills shortage, while government (81.8%) and healthcare (81.9%) organizations appear to be the least affected (see Figure 9).
- The IT security skills shortage varies little by organization size, both in overall level of impact and impact by role.

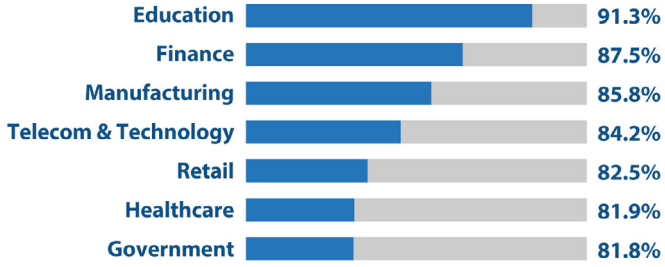

Figure 9: Percentage affected by the cybersecurity skills shortage.

Section 2: Perceptions and Concerns

Concern for Cyberthreats

On a scale of 1 to 5, with 5 being highest, rate your overall concern for each of the following types of cyberthreats targeting your organization. (n=1,193)

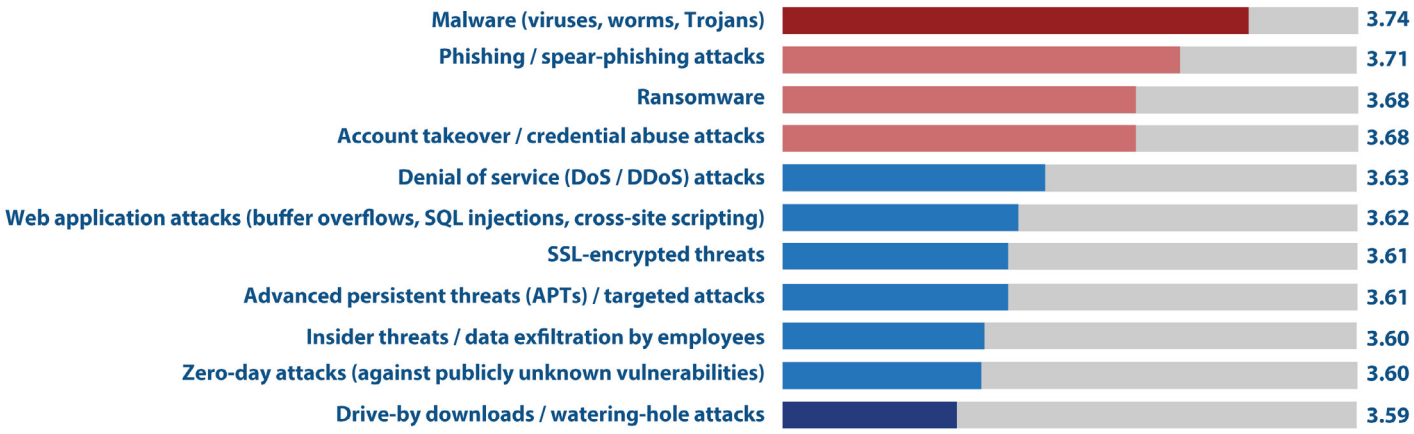

Figure 10: Relative concern for cyberthreats by type.

We witnessed some of the largest high-profile data breaches on record in 2018, including Marriott Starwood hotels (500 million records), Under Armour (150 million records), Google+ (52.5 million records), Panera (37 million records), and Facebook (30 million records). What do these cyberattacks and hundreds more have in common? Malware.

Although other types of threats are responsible for data breaches too, malware leads the pack. It has claimed the top spot on the list of cyberthreats causing the greatest concern in five of the last six years, including this one (see Figure 10). Also no surprise, phishing / spear-phishing attacks and ransomware occupy the second and third positions, as they've done in the preceding two years.

Interestingly, drive-by downloads / watering-hole attacks, zero-day attacks (against publicly unknown vulnerabilities), and insider threats (data exfiltrated by employees) are of least concern to our research participants. Zero-day attacks, in particular, fell from 5th position last year to 10th position this year. Despite the hype from many security vendors – especially those that specialize in detecting advanced threats without signatures – zero-day attacks are but a rounding error in comparison to the successful data breaches resulting from known, unpatched vulnerabilities.

One tiny glimmer of hope from this year's results is the second consecutive decline in overall concern for cyberthreats. Remembering that respondents were asked to rate their concern for each type of threat on a scale of 1 to 5, with 5 being highest, we averaged together all the ratings for each year and created what we call a Threat Concern Index (see Figure 11) – a barometer for cyberthreat concern on the whole.

Between 2014 and 2017, our Threat Concern Index rose considerably, from 3.10 to a peak of 3.84. But since then, it's declined to 3.66 in 2018 and 3.64 in 2019. Okay, it only dropped by two-hundredths of a point from last year, but as IT security professionals, we're just happy that the needle is moving in the right direction.

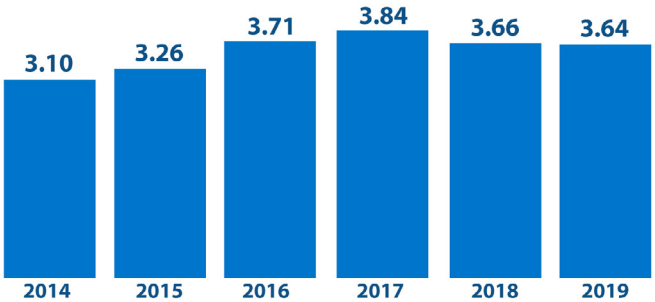

Figure 11: Threat Concern Index depicting overall concern for cyberthreats.

Section 2: Perceptions and Concerns

Responding to Ransomware

If victimized by ransomware in the past 12 months, did your organization pay a ransom (using Bitcoins or other anonymous currency) to recover data? (n=1,164)

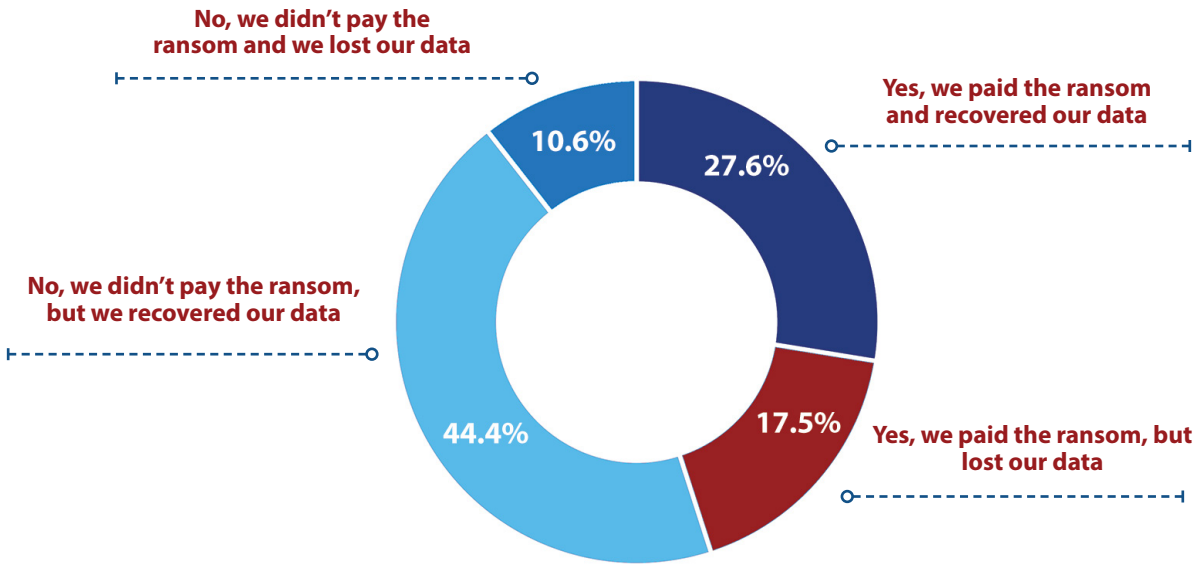

Figure 12: How victims responded to ransomware.

Despite diminishing press coverage on WannaCry, NotPetya, and Bad Rabbit, ransomware is still alive and well. Once again, we asked our research participants whether their employers were victimized by ransomware last year and, if so, whether they paid the associated ransoms. And, if they did pay the ransom, whether they got their data back.

Figure 12 and Table 1 depict the key results. Unfortunately, most of it is bad news.

To summarize:

- The percentage of organizations victimized by ransomware ticked up this year, from 55.1% to 56.1%.
- The percentage of victimized organizations that paid associated ransoms rose considerably this year, from 38.7% to 45.0%.
- The percentage of victimized organizations that refused the ransoms and subsequently lost their data increased this year, from 13.1% to 19.2%.

	2018	2019
Percentage of organizations victimized by ransomware	55.1%	56.1% ↑
Percentage of victimized organizations that paid ransom(s)	38.7%	45.0% ↑
Percentage of victimized organizations that refused ransom(s) and lost their data	13.1%	19.2% ↑
Percentage of victimized organizations that paid ransom(s) but lost their data	50.6%	38.8% ↓

Table 1: Key ransomware statistics.

Section 2: Perceptions and Concerns

Frankly, we're befuddled by the notion that more ransom refusers are losing their data as compared to a year ago. Why aren't more organizations leveraging automated backup solutions? If an end user's laptop, for example, is compromised by ransomware, the IT department should simply re-format the hard disk, re-image the laptop, and restore the user's data from backup. This isn't rocket science, people!

The only bright note regarding ransomware in this year's report is the increase in ransom payers who successfully recovered their data – from 49.4% last year to 61.2% this year. Perhaps these cybercriminals read the press coverage from our 2018 Cyberthreat Defense Report and decided it would be in their best long-term interests to return compromised data to their respective owners.

Other notable findings include:

- Saudi Arabia (87.8%), Turkey (74.0%), and China (68.7%) top the list of countries most affected by ransomware (see Figure 13). Japan (37.8%), Australia (39.6%), and France (44.4%) are least affected.
- Of the seven key industries tracked in this report, the ones most affected by ransomware include retail (59.2%) and telecom & technology (57.7%). The least-affected industries are government (40.6%) and manufacturing (43.3%).
- Once again, mid-size enterprises with 5,000 to 9,999 employees (66.0%) are most affected by ransomware, while smaller organizations with 500 to 999 employees (47.8%) are least affected.

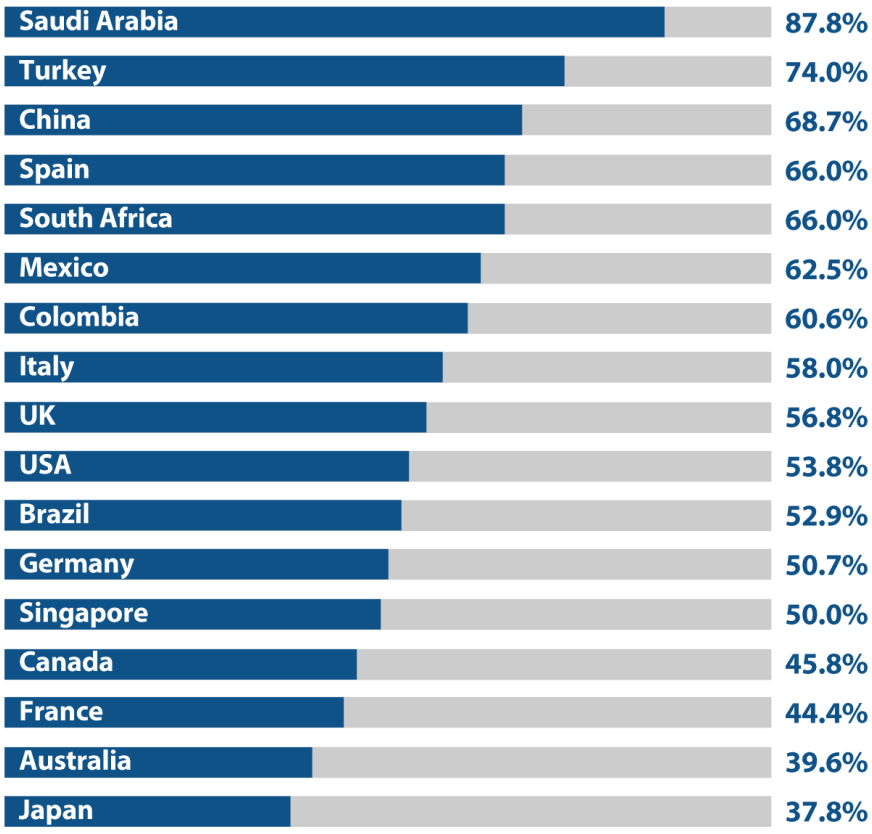

Figure 13: Percentage affected by ransomware in the past 12 months.

Section 2: Perceptions and Concerns

Barriers to Establishing Effective Defenses

On a scale of 1 to 5, with 5 being highest, rate how each of the following inhibit your organization from adequately defending itself against cyberthreats. (n=1,187)

Figure 14: Inhibitors to establishing effective cyberthreat defenses.

Each year, we ask respondents to tell us what's inhibiting them from defending their respective organizations against cyberthreats. In other words, what's standing in their way?

During the most recent four of the six years we've asked this question (2016-2019), the same three responses have been at the top: low security awareness among employees, lack of skilled personnel, and too much data to analyze. However, the last response had never bubbled up to number one – until this year (see Figure 14).

Too much data to analyze achieved 3rd place in 2017, 2nd place in 2018, and now 1st place in 2019. This bodes well for IT vendors and service providers that offer security analytics capabilities, as their solutions can help IT security organizations cut through the noise of literally millions of security events generated by a typical enterprise security infrastructure.

Another related challenge is the strain that increasingly high volumes of data place on an organization's security tools/infrastructure. As such, solutions that help prioritize and optimize the distribution of different types of security data to the appropriate tools are an important consideration too -- one with the potential not only to help contain security infrastructure costs, but also improve security visibility overall.

"Too much data to analyze ranked 1st place in 2019. This bodes well for IT vendors and service providers that offer security analytics capabilities."

Section 2: Perceptions and Concerns

Low security awareness among employees and lack of skilled personnel tied for second place this year. In fact, since too much data to analyze is just two one-hundredths of a point higher, we can really think of this as a three-way tie for first.

At the bottom of the list of concerns are lack of effective solutions available in the market (3.09), too many false positives (3.14), and lack of budget (3.15). We certainly know from conducting this study year after year that lack of IT security budget is rarely of major concern (see page 16).

Last year, we created a new chart called the "Security Concern Index" (see Figure 15). We averaged together all the inhibitor ratings for each year in an attempt to gauge the overall concern for security inhibitors. Think of this as a way to determine how stressed out security professionals are about the obstacles standing in the way of doing their jobs.

Although 2019 technically represents the fifth consecutive year of increases to the Security Concern Index, the score for 2019 is only one one-hundredth of a point higher than in 2018 – 3.18 in 2018 versus 3.19 in 2019. So, let's just call it a wash.

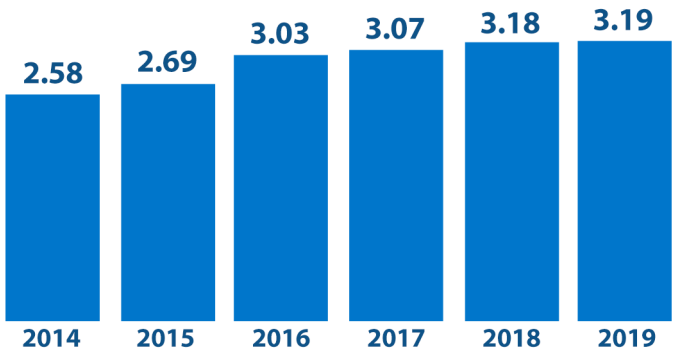

Figure 15: Security Concern Index, depicting average ratings among security inhibitors.

Section 2: Perceptions and Concerns

Addressing Cloud Security Needs

How is your organization planning to address its cloud security needs? (Select all that apply.) (n=1,152)

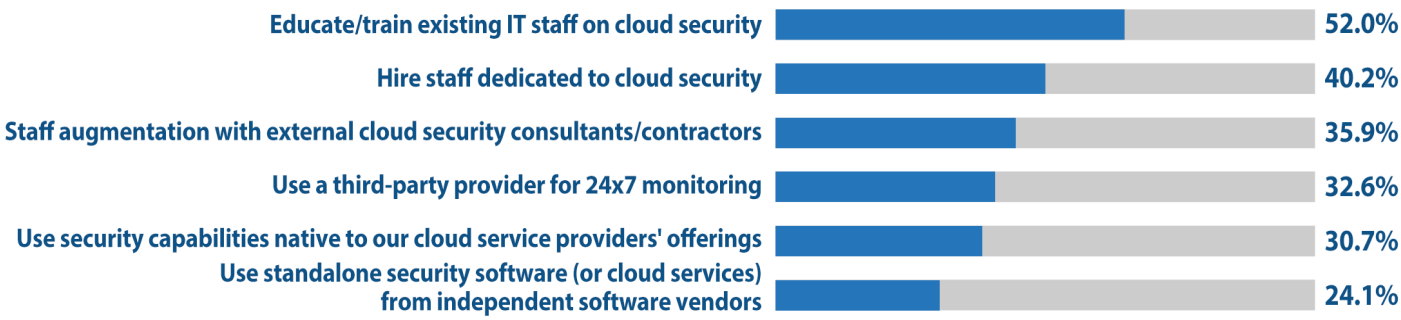

Figure 16: Addressing cloud security needs.

Last year, we asked our research participants to identify their most significant cloud security challenges. We learned that maintaining data privacy, controlling access, and monitoring for threats were the three most significant challenges.

This year, we asked respondents a different cloud security question: how they're planning to address their cloud security needs. Their responses were insightful (see Figure 16).

It's clear that respondents understand how difficult it is to recruit new IT security talent. We've seen that time and again in this year's (see page 16) and prior years' reports. Thus, the top strategy to address cloud security needs is to train existing IT staff on cloud security (52.0%). Beyond that, responding organizations will attempt to hire new staff dedicated to cloud security (40.2%), but if that fails, they'll augment their cloud security staff with external consultants / contractors (35.9%).

Fewer respondents intend to rely on standalone security software (or cloud services) from independent software vendors (24.1%) or the security capabilities native to cloud service provider offerings (30.7%).

Other notable findings:

- The countries most likely to train existing IT staff on cloud security are Turkey (69.4%) and China (68.0%).
- The countries most confident in their ability to hire new staff to service their cloud security needs are Singapore (54.2%) and Mexico (51.5%).
- The countries most likely to augment their cloud security staff with consultants and contractors are Brazil (66.7%) and Japan (46.7%).
- Cloud security staffing strategies do not vary significantly by industry or organization size.

Section 2: Perceptions and Concerns

Vulnerability Patching Challenges

Describe your agreement with the following statement: "Our vulnerability management and patch management capabilities have improved over the past 12 months, resulting in faster patching." (n=1,183)

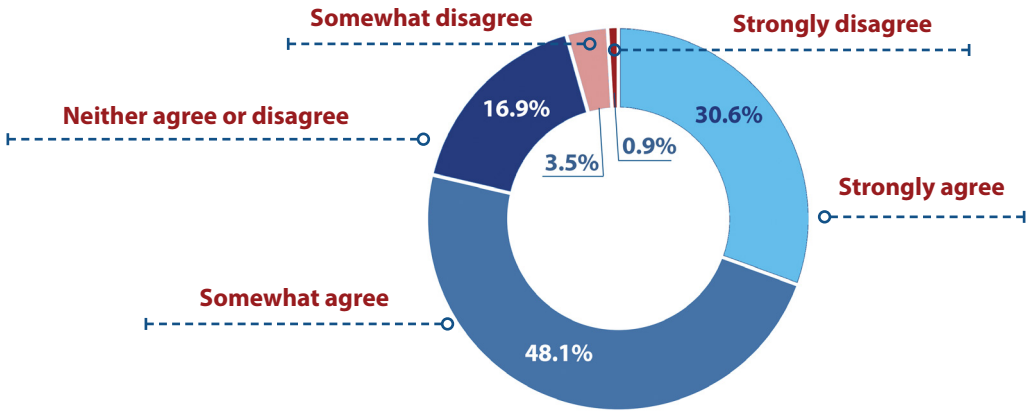

Figure 17: Confidence in improved vulnerability management and patch management capabilities.

We know from a plethora of third-party research studies that the vast majority of data breaches caused by malware correspond to vulnerabilities that have been publicly known for a year or longer. So, last year we asked our research participants what is preventing their organizations from patching systems more quickly. Top responses were infrequent windows to take production systems offline for patching and lack of qualified personnel.

This year, we asked whether respondents felt their vulnerability management and patch management capabilities had improved over the preceding 12 months. At first glance, the results are promising (see Figure 17).

Nearly four in five respondents (78.7%) felt their organization had made improvements in its vulnerability management and patch management endeavors over the preceding 12 months. Of course, this also means that one in five (22.3%) is not confident whether progress has been made. In today's cyberthreat climate, this does not bode well.

"Nearly four in five respondents (78.7%) felt their organization had made improvements in vulnerability management and patch management."

Stepping onto a proverbial soap box for a moment, we commend organizations that invest in the latest and greatest technologies designed to detect advanced threats. But we also feel that too many organizations overlook the arguably greater need to reduce their attack surfaces by eliminating the vulnerabilities that these cyberthreats are designed to exploit. In other words, if you eliminate your infrastructure's vulnerabilities, then cyberthreats designed to exploit those vulnerabilities are rendered harmless.

Thus, we encourage our readers to consider new policies, processes, and technologies designed to help mitigate risk by reducing the network's attack surface. Scan and patch often.

Other notable findings:

- The countries most confident their vulnerability management and patch management capabilities have improved are Brazil (94.1%) and Turkey (91.8%). The least confident are Japan (51.1%) and Australia (69.4%).
- Of the seven key industries referenced in this report, the most-confident ones are healthcare (81.9%) and telecom & technology (81.4%). The least-confident industries are education (70.0%) and retail (71.7%).
- Confidence in improved vulnerability management and patch management capabilities does not vary significantly by organization size.

Section 3: Current and Future Investments

IT Security Budget Allocation

What percentage of your employer's IT budget is allocated to information security (e.g., products, services, personnel)? (n=1,136)

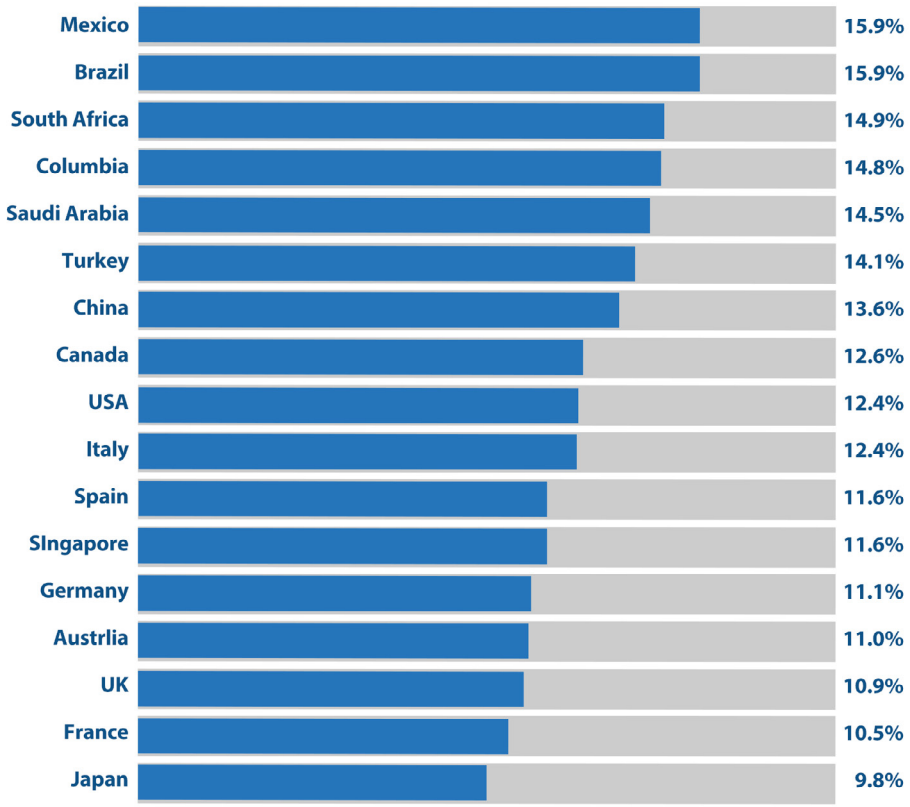

Figure 18: Mean percentage of IT budget allocated to security, by country.

Same as last year, we asked our respondents to tell us the specific percentage of their employer's overall IT budget that is allocated to information security. With this approach, we're able not only to identify an accurate mean level of spending, but also to group responses into ranges (e.g., 6%-10%, 11%-15%, and 16%-20%) for comparison with prior years' findings.

"The mean percentage of the IT budget currently being allocated to information security is 12.5% globally – an increase of 0.4% from a year ago."

Section 3: Current and Future Investments

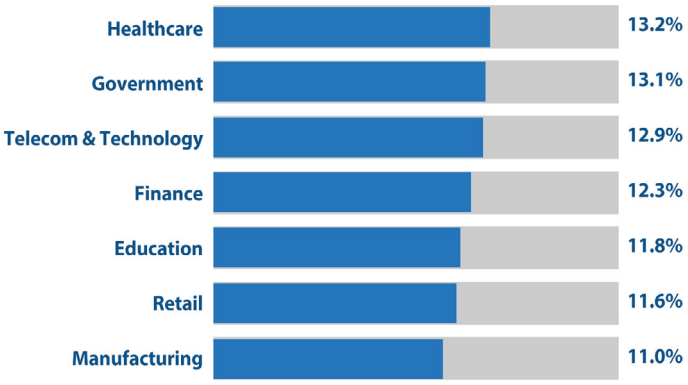

Figure 19: Mean percentage of IT budget allocated to security, by industry.

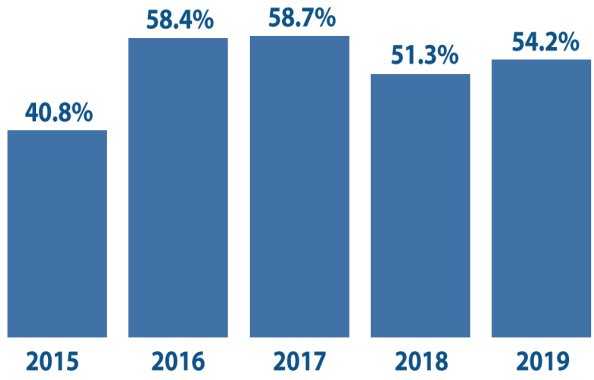

Figure 21: Percentage spending 11% or more on security.

Our results this time around indicate that the mean percentage of the IT budget currently being allocated to information security is 12.5% globally – an increase of 0.4% from a year ago. Figure 18 depicts mean security spending by country, Figure 19 by industry, and Figure 20 by organization size (i.e., employee count).

Figure 21, in turn, compares the percentage of organizations designating 11% or more of their overall IT budgets to information security for the past five years. As you can see, after a first-ever drop in this metric last year, it has now nudged upward again – from 51.3% in 2018 to 54.2% in 2019.

Given a prevailing security climate characterized by relatively few publicized (major) breaches, a quiescent compliance landscape, and not so many flashy new security technologies coming on the scene, the reversals for both of these metrics could be considered a bit surprising.

Figure 20: Mean percentage of IT budget allocated to security, by organization size.

Plausible explanations, however, include: (a) the potential that our findings are simply oscillating around some sort of steady-state result (e.g., ~12% for mean budget allocation and ~55% for those spending more than 11% on security); and (b) a significant increase in spending on security personnel and/or automation and response solutions to help fill gaps in these areas.

It's also important to keep in mind that these metrics are relative. Although InfoSec certainly remains a top-of-mind issue for most organizations worldwide, we have no way (at least within the confines of this report) to account for fluctuations in importance – and, therefore, budget allocation – across all the other areas of IT.

Other notable findings:

- Turkey (2.6%), Colombia (2.1%), and China (1.9%) had the greatest year-over-year increases in mean IT budget allocated to InfoSec, while budgets in France (-1.0%) and the United Kingdom (-0.6%) contracted the most.
- With mean allocation increases of 0.8% and 1.3%, respectively, healthcare (13.2%) and government (13.1%) organizations now spend the greatest percentage on security among the big 7 industries, while retail (11.0%) has slipped to the bottom.
- Although larger organizations (10,000+ employees) continue to spend a greater slice of their IT budget pie on security (13.0%), their smaller counterparts are narrowing the gap (12.2%, up from 11.7% a year ago).

Section 3: Current and Future Investments

IT Security Budget Change

Do you expect your employer's overall IT security budget to increase or decrease in 2018? (n=1,147)

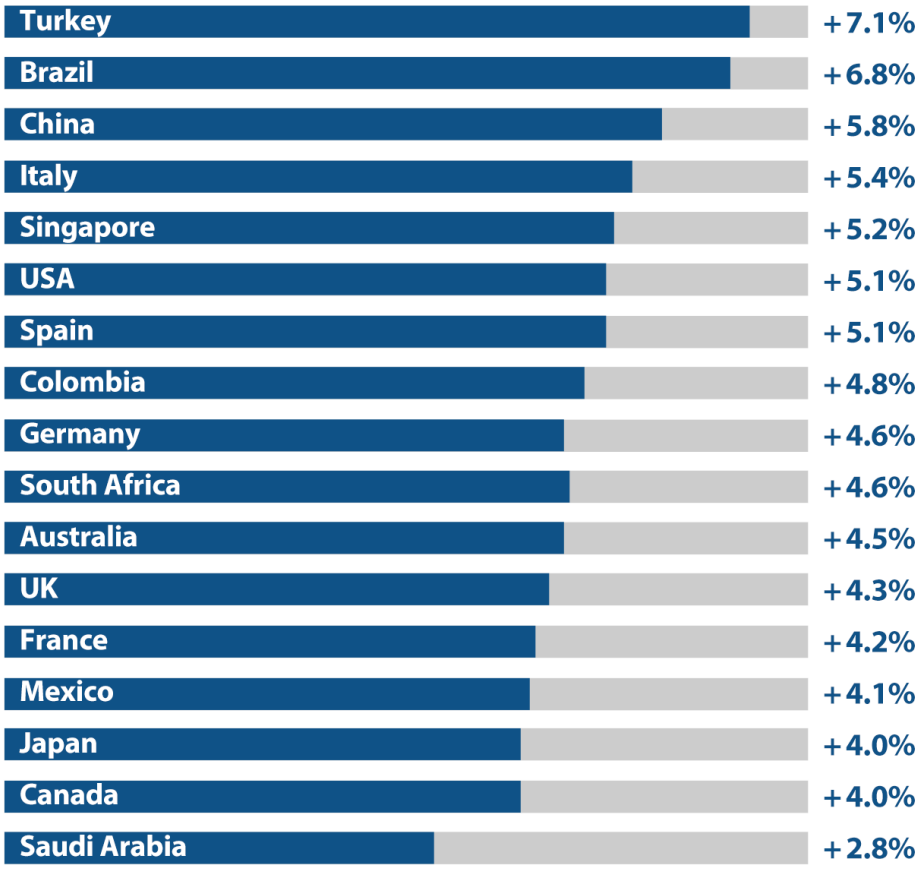

Figure 22: Mean security budget increase, by country.

Again this year, we asked respondents to select the specific percentage by which they expected their organization's IT security budget to increase or decrease in 2019.

The headline here is that the mean expected IT security budget change for 2019 is +4.9% globally – up from +4.7% a year ago. Figure 22 depicts mean security budget increases by country, Figure 23 by industry, and Figure 24 by organization size. What's clear from these figures is that IT security budgets for 2019 are going up across the board.

"The mean expected IT security budget change for 2019 is +4.9% globally – up from +4.7% a year ago."

In fact, Figure 25 shows that IT security budgets are healthier than ever, with a record 83.5% of organizations planning to invest more in security in 2019. Across our global audience, only 5.4% of respondents indicated they expect the IT security budget for their organization to contract.

Section 3: Current and Future Investments

Figure 23: Mean security budget increase, by industry.

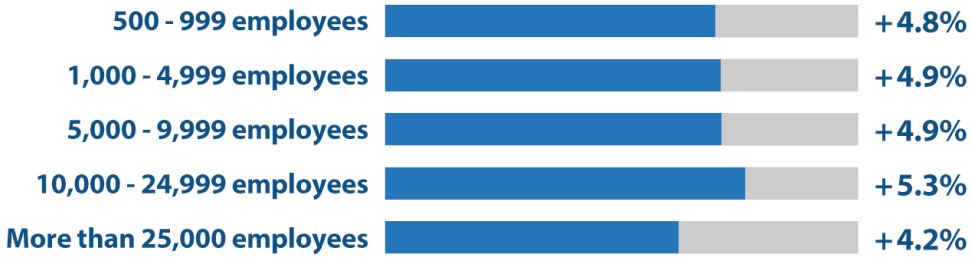

Figure 24: Mean security budget increase, by organization size.

Overall, we admit to being somewhat surprised by these results. As discussed previously, with little that is new or significant going on regarding high-profile threats, breaches, and/or regulations, we would have expected smaller increases, if not actual contraction, in IT security budgets. We guess, however, that the machinery at work here is much like a freight train: slow to gain momentum, but also slow to shed it once things get rolling.

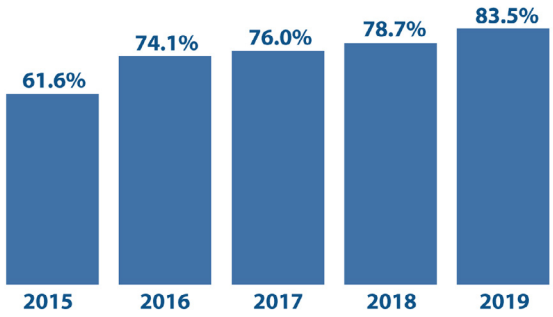

Figure 25: Percentage of rising security budgets.

Other notable findings:

- IT security budgets in the United States, on average, are rising by 5.1%, which is 0.2 percentage points higher than the global mean. The fastest-growing IT security budgets are from Turkey (7.1%), Brazil (6.8%), and China (5.8%), while the slowest-growing IT security budgets are from Saudi Arabia (2.8%), Canada (4.0%), and Japan (4.0%).
- Among the big 7 industries, we'd expect to see some fluctuations from year to year, and that's precisely what we got – with education and retail moving from near the top of the list last year (+4.9% and +4.8% respectively) to the bottom of the list this time around (+4.2% and +4.3%).
- The same sort of reversal also took place for the largest organizations (>25,000 employees), as they went from the top spot a year ago (+5.2%) to the smallest amount of budget increase in 2019 (+4.2%).

We'd also like to point out a bit of positive news for the SMB (small-medium business) community, as this year's results show that segment now keeping pace with the gains of larger organizations (instead of trailing behind, as it has in past years).

Section 3: Current and Future Investments

Network Security Deployment Status

Which of the following network security technologies are currently in use or planned for acquisition (within 12 months) by your organization to guard all network assets against cyberthreats? (n=1,158)

	Currently in use	Planned for acquisition	No plans
Network-based anti-virus (AV)	63.9%	25.7%	10.4%
Network access control (NAC)	59.8%	29.2%	11.0%
SSL/TLS decryption appliances / platform	59.4%	29.8%	10.8%
Intrusion detection / prevention system (IDS/IPS)	59.1%	29.5%	11.4%
Secure web gateway (SWG)	58.5%	30.3%	11.2%
Secure email gateway (SEG)	58.4%	30.1%	11.5%
Denial of service (DoS/DDoS) prevention	55.4%	31.5%	13.1%
Data loss / leak prevention (DLP)	53.1%	33.1%	13.8%
Advanced malware analysis / sandboxing	50.4%	40.0%	9.6%
Next-generation firewall (NGFW)	50.4%	36.8%	12.8%
Network behavior analysis (NBA) / NetFlow analysis	49.7%	35.8%	14.5%
Deception technology / distributed honeypots	41.9%	36.1%	22.0%

Table 2: Network security technologies in use and planned for acquisition.

The next five sections are structured the same. For each one, we asked respondents to indicate whether the listed security technologies are currently in use at their organization, are planned for acquisition by their organization within the next 12 months, or are not planned for acquisition/deployment by their organization. (The sample sizes vary by question because we allowed for, and subsequently weeded out, "don't know" responses. We never want respondents to guess.)

Table 2 depicts this year's deployment status results for popular network security technologies. Cells in dark blue correspond to a higher frequency of adoption and acquisition plans, cells in light blue to lower frequencies, and cells in gray to "no plans." Changes to the list include the departure of several technologies that were moved to new questions on security operations (e.g., security analytics and threat intelligence) and identity management (e.g., privileged account management), along with the addition of network access control (which was previously covered as part of our investigation into attack surface reduction solutions).

Our first observation, once again, is that this year's results track closely to those from the year before. This finding isn't particularly surprising to us, and here's why.

Section 3: Current and Future Investments

On one hand, doing security "in the network" is getting harder. Driven by increased user mobility and adoption of cloud services, the so-called dissolving perimeter is logically causing a shift away from network-based security toward endpoint-, server-, and datacenter-based security. To be clear, this doesn't mean different technologies per se, only different locations. Think fewer hardware appliances and more portable (and dynamically deployable) software modules involving essentially the same core set of capabilities.

On the other hand, we have a pair of factors that are working to balance out the equation: (1) for many organizations, no longer having one well-defined perimeter means having to instead account for multiple internal ones; and (2) network-based security still has the advantage of minimizing the impact to mission-critical computing devices – not to mention avoiding the control issues that invariably arise among different operational teams.

Other notable observations:

- Despite its declining rate of use, network anti-virus (AV), remains atop the heap as the most frequently deployed network security technology in our list.

"The biggest winners in 2019 are SSL/TLS decryption platforms, advanced malware analysis / sandboxing, and deception technology / distributed honeypots."

- The biggest winners in 2019 (i.e., technologies with the largest increases in adoption) are SSL/TLS decryption platforms (+4.4%), advanced malware analysis / sandboxing (+3.7%), and deception technology / distributed honeypots (+2.0%).
- For the second consecutive year, advanced malware analysis / sandboxing (40.0%) and NGFW (36.8%) have the highest planned acquisition rates for the coming 12 months.

Our final thought for this topic is that with an average "no plans" rate of only 12.6%, it seems reasonable to expect most organizations will eventually count most (if not all) of the network security technologies listed here as an active part of their cyberthreat defenses.

Section 3: Current and Future Investments

Endpoint Security Deployment Status

Which of the following endpoint security technologies are currently in use or planned for acquisition (within 12 months) by your organization to guard desktops, laptops, and servers against cyberthreats? (n=1,184)

	Currently in use	Planned for acquisition	No plans
Basic anti-virus / anti-malware (threat signatures)	65.9%	28.5%	5.6%
Disk encryption	61.9%	27.8%	10.3%
Advanced anti-virus / anti-malware (machine learning, behavior monitoring, sandboxing)	61.4%	28.1%	10.5%
Application control (whitelist / blacklist)	57.2%	28.8%	14.0%
Data loss / leak prevention (DLP)	56.7%	31.2%	12.1%
Digital forensics / incident resolution	49.6%	36.0%	14.4%
Containerization / micro-virtualization	45.6%	37.8%	16.6%
Deception technology / honeypot	44.9%	37.3%	17.8%

Table 3: Endpoint security technologies in use and planned for acquisition.

We repeated the same approach used to assess adoption of network security technologies to gain insight into deployment status and acquisition plans for endpoint security technologies (see Table 3). Once again, percentages in dark blue correspond to a higher frequency of adoption and acquisition plans, while those in light blue correspond to a lower frequency.

Overall, the results are in line with what we would expect. Despite dropping nearly 14 percentage points over the past three years, signature-based (or basic) anti-virus / anti-malware (65.9%) remains the most commonly deployed of the listed endpoint security technologies. Let's face it: basic AV is (probably) never going away. After all, in addition to being programmatically "required" by numerous compliance regimens, it's fundamentally a highly accurate and relatively efficient way to weed out an immense chunk of known threats.

Other repeat performances from last year:

- Disk encryption (61.9%) and advanced anti-virus / anti-malware (61.4%) continue to be the next most widely used endpoint security technologies.
- Application control and data loss / leak prevention (DLP) continue to fall in the middle of the pack in terms of both current and planned usage.
- Containerization / micro virtualization (37.8%) continues to be the hottest endpoint security technology planned for acquisition.

Our take on these findings is that the endpoint security market appears to have settled into a period of relative stability. For the most part, developing new innovations is taking a backseat (at least temporarily) to enhancing what's already available – for example, tweaking ML and

Section 3: Current and Future Investments

AI algorithms, adding new analytics on the management side to fine-tune the processing and correlation of endpoint telemetry, and continuing to consolidate a full suite of both endpoint protection (EPP) and endpoint detection and response (EDR) capabilities into a single, cohesive offering.

Another competing ambition/initiative for leading security solution providers and enterprises alike is better integration and collaboration between endpoint security and other major components of the cyberthreat defense puzzle (e.g., net/app/data sec tools and overarching vulnerability/threat/event/incident management systems). So, instead of maintaining a heavy focus on the evolution of endpoint security and implementation of the latest/greatest technologies, the primary goal on the table right now is to enable cross-component sharing of security findings and coordination of responses to further boost overall security effectiveness.

"Containerization / micro virtualization continues to be the hottest endpoint security technology planned for acquisition."

Section 3: Current and Future Investments

Application and Data Security Deployment Status

Which of the following application and data-centric security technologies are currently in use or planned for acquisition (within 12 months) by your organization to guard enterprise applications and associated data repositories against cyberthreats? (n=1,153)

	Currently in use	Planned for acquisition	No plans
Web application firewall (WAF)	63.0%	27.5%	9.5%
Database firewall	62.1%	27.2%	10.7%
Database activity monitoring (DAM)	56.1%	31.8%	12.1%
Database encryption / tokenization	55.6%	32.8%	11.6%
Cloud access security broker (CASB)	52.7%	32.1%	15.2%
File integrity / activity monitoring (FIM/FAM)	52.6%	34.0%	13.4%
API gateway / protection	51.2%	38.8%	10.0%
Container security tools / platform	50.5%	35.0%	14.5%
Runtime application self-protection (RASP)	49.9%	33.9%	16.2%
Static/dynamic/interactive application security testing (SAST/DAST/IAST)	49.3%	35.2%	15.5%
Application delivery controller (ADC)	48.1%	36.0%	15.9%
Deception technology / distributed honeypots	45.0%	36.8%	18.2%

Table 4: Application and data security technologies in use and planned for acquisition.

Our next area for measuring security technology adoption is application and data security. Here we evaluate 12 security technologies (see Table 4), all of which were covered last year as well. As usual, percentages in dark blue correspond to a higher frequency of adoption or acquisition plans, while those in light blue correspond to a lower frequency.

The showcase technology for this category is the API gateway, as it notched not only the greatest year-over-year gain in current deployment status (+6.1%), but also came in as the most sought-after app/data security technology for the year ahead (cited as "planned for acquisition" by 38.8% of respondents). The burgeoning popularity of this relatively new class of technology follows logically from the continuing shift away from traditional, monolithic applications in favor of microservices-based application architectures, as well as from the increasing externalization of application services – both of which are highly dependent on APIs.

The result is the need not only to securely mediate access to APIs, but also to ensure reliable fulfillment of the associated application/service requests. Leading API gateway solutions are filling these needs, and more, as they rapidly morph into a next-generation version of the venerated application delivery controller (ADC).

Section 3: Current and Future Investments

Other notable findings:

- For the second consecutive year, WAF (63.0%) nudged out database firewall (62.1%) as the most widely deployed app/data security technology.
- While cloud access security brokers (CASBs) and database activity monitoring (DAM) posted year-over-year increases in adoption of 3.9% and 1.3%, respectively, deception technology backtracked the most, with adoption declining by 4.2%.
- With the second-highest "planned for acquisition" percentage in this list, deception technology (36.8%) appears poised for a strong year (despite having faltered a bit in 2018).

"The showcase technology for this category is the API gateway."

Our closing thought for this topic is that API gateways had better enjoy their day in the sun. Application containers are a major enabler of microservices-based applications. As such, we expect that container security tools/platforms – positioned in the middle of the pack this time around, per Table 4 – will soon be displacing API gateways as the app/data security technology with the greatest adoption gain. For more information on this rapidly maturing class of technology, see our featured blurb in the Road Ahead section of this report.

Section 3: Current and Future Investments

Security Management and Operations Deployment Status

Which of the following security management and operations technologies are currently in use or planned for acquisition (within 12 months) by your organization to mitigate the impact of cyberthreats? (n=1,155)

	Currently in use	Planned for acquisition	No plans
Patch management	59.9%	26.7%	13.4%
Security configuration management (SCM)	57.1%	29.9%	13.0%
Vulnerability assessment/management (VA/VM)	56.0%	31.9%	12.1%
Security information and event management (SIEM)	55.0%	31.5%	13.5%
Penetration testing / attack simulation software	51.6%	34.1%	14.3%
Threat intelligence service(s)	49.9%	35.0%	15.1%
Full-packet capture and analysis	49.2%	35.0%	15.8%
User and entity behavior analytics (UEBA)	46.5%	36.5%	17.0%
Advanced security analytics (e.g., with machine learning, AI)	41.3%	46.9%	11.8%

Table 5: Security management and operations technologies in use and planned for acquisition.

One of the more significant changes to this year's report is the addition of a question delving into the deployment status of what we're calling security management and operations technologies. These technologies are all about ongoing monitoring and management of an organization's security posture and processes – as opposed to providing real-time policy enforcement (like a firewall or CASB) and/or on-the-spot threat detection/prevention (like anti-malware software). They also tend to be cross-domain in scope versus focusing on an individual area (as is the case with network, endpoint, and app/data security technologies).

The result is the nine technologies shown in Table 5, many of which were covered in other areas/ways in previous editions of the Cyberthreat Defense Report. Once again, percentages in dark blue correspond to a higher frequency of adoption or acquisition plans, while those in light blue correspond to a lower frequency.

"These results paint a clear picture of organizations still struggling to get a handle on the detection of advanced/unknown cyberthreats."

Section 3: Current and Future Investments

From the inaugural run of this question, we have two high-level observations to get things started. First is the scorching "planned for acquisition" rate of 46.9% for advanced security analytics (the highest for any technology in this year's study), along with the rates for its nearest contenders: user and entity behavior analytics (36.5%), full-packet capture and analysis (35.0%), and threat intelligence services (35.0%). In aggregate, these results paint a clear picture of organizations still struggling to get a handle on the detection of advanced/unknown cyberthreats.

Our second top-level observation is that with none of the listed technologies having an adoption rate over 60%, there is clearly plenty of room for improvement in these areas by enterprise security teams – not to mention plenty of opportunity for associated solution providers.

Other notable findings:

- Technologies typically associated with attack surface reduction are well represented, with patch management (59.9%), security configuration management (57.1%), and vulnerability assessment/management (56.0%) gaining top honors as the most widely deployed security management technologies.
- The middle-of-the-pack adoption rate for security information and event management (SIEM) is somewhat surprising … but is probably reflective of similarly positioned cloud / managed detection and response (MDR) services' displacing traditional SIEM offerings.
- Given the relatively high "no plans" rate for user and entity behavior analytics (17.0%) – which we consider an invaluable technology for uncovering unknown and insider threats – we can't help but wonder whether respondents are expecting this technology to be absorbed into other security solutions as a feature set (versus remaining independent/standalone).

Maybe we're just InfoSec junkies, but we can't wait for the 2020 Cyberthreat Defense Report so we can start looking for trends in this crucial area!

Section 3: Current and Future Investments

Identity and Access Management Deployment Status

Which of the following identity and access management (IAM) technologies are currently in use or planned for acquisition (within 12 months) by your organization to securely control access to computing resources? (n=1,163)

	Currently in use	Planned for acquisition	No plans
Password management / automated reset	64.4%	25.5%	10.1%
User/account provisioning and de-provisioning	58.3%	28.8%	12.9%
Privileged account/access management (PAM)	56.8%	28.9%	14.3%
Two-/multi-factor authentication	53.9%	32.3%	13.8%
Single sign-on (SSO)	53.4%	30.8%	15.8%
Identity analytics	51.8%	30.1%	18.1%
Tokens (hardware or software)	51.2%	29.9%	18.9%
Risk-based/step-up authentication	49.3%	33.1%	17.6%
Smart cards	47.9%	32.1%	20.0%
Identity-as-a-Service (IDaaS)	46.4%	35.3%	18.3%
Federated identity management (SAML, Oauth)	42.8%	35.4%	21.8%
Biometrics	37.6%	41.3%	21.1%

Table 6: Identity and access management technologies in use and planned for acquisition.

Rather than resorting to a politically incorrect analogy involving step-children with bright-colored hair, let's just say that identity and access management (IAM) is often viewed as one of the least glamorous pieces of the cyberthreat defense puzzle. That negative assessment, however, is not reflective of its critical impact, which is why we've added a question to expose details (and eventually trends) in this important corner of the information security landscape.

Table 6 provides our inaugural set of data on adoption and acquisition plans for IAM technologies. For the fifth and final time <grin>, percentages in dark blue correspond to a higher frequency of adoption or acquisition plans, while those in light blue correspond to a lower frequency.

In our opinion, the three technologies identified as most commonly "in use" are precisely where they belong. Instrumental for controlling who can gain access to which IT services and for layering in additional safeguards for high-value / risk assets, respectively, user/account provisioning and de-provisioning (58.3%) and privileged account/access management (56.8%), are cornerstones of a good security architecture. And the fact that they are surpassed by the third technology -- password management / automated reset (64.4%) – speaks to its business-driven nature. Password management / automated reset is widely used both to help avoid unduly restricting access to apps/services and to automate a high-frequency task.

Section 3: Current and Future Investments

In comparison, we're positively shocked to see such aggressive plans for biometric technology, which garnered a planned-for-acquisition rate of 41.3%. Don't get us wrong. High levels of interest in strong authentication make total sense. It's just that biometrics has always suffered from somehow being both the least intrusive (nothing else to carry or remember) and the most intrusive (involving body parts) option for achieving this much-needed capability. At this point, we can only guess that the interest lies in more-transparent methods of biometric authentication, such as unique typing and speech patterns/cadence. Of course, another factor could be the spill-over effect of rising familiarity with and convenience of biometrics in consumer devices (think Apple) sparking demand for similar capabilities in the enterprise.

We'll have to wait until next year for trend data on these technologies, of course. But we're eager to see the results for identity analytics, in particular, which we consider a powerful and promising technology for efficiently uncovering instances of unnecessary, unused, and outlier access/accounts (that needlessly expand an organization's attack surface).

Section 3: Current and Future Investments

Machine Learning and Artificial Intelligence Investments

Describe your agreement with the following statement: "Investments we've made in security products that feature machine learning and/or artificial intelligence (AI) technologies have improved our ability to detect advanced threats." (n=1,181)

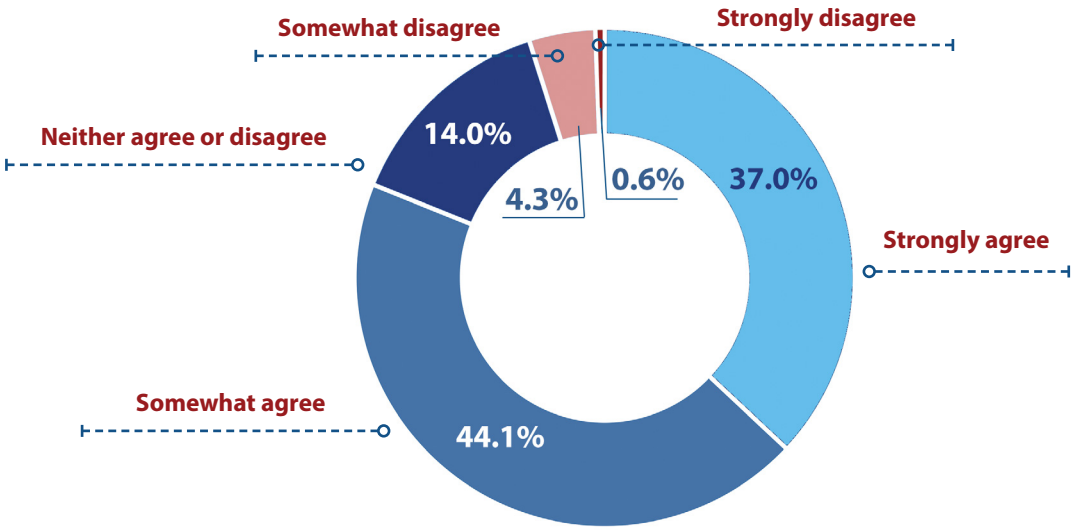

Figure 26: Impact of machine learning / artificial intelligence on threat detection.

Given the success of ML and AI in other areas of business, not to mention IT, few would argue against the potential for these closely coupled technologies to make a meaningful contribution in the realm of IT security. The million-dollar question, then, is "Are we there yet?"

Judging solely by the results of our inquiry into the extent to which respondents believe ML and AI have improved their organization's ability to detect advanced threats, we'd have to say that the answer is an emphatic "yes." As depicted in Figure 26, a whopping 81.1% of respondents generally agree that machine learning and artificial intelligence technologies are helping to defeat advanced cyberthreats. The breakdown, too, is impressive, with nearly half (45.6%) of this group indicating they "strongly agree" with the premise.

"A whopping 81.1% of respondents generally agree that machine learning and artificial intelligence technologies are helping to defeat advanced cyberthreats."

Other notable findings:

- An astounding 94.4% of respondents indicated their organizations have acquired products that feature ML and/or AI technology.
- Only 4.9% of respondents indicated they believe investments in security products featuring ML/AI technology have NOT helped improve their organization's ability to detect advanced threats.

Section 3: Current and Future Investments

- Compared to those from the other big 7 industries, organizations in the education segment are incrementally slower to adopt products with ML/AI technology (with 10.1% not yet having done so) and somewhat less convinced of their benefit (with only 77.5% generally agreeing there's been a resulting improvement in threat detection capability).

While these results certainly paint ML/AI technologies in a positive light, we feel compelled to offer a few words of caution. Specifically, our limited exploration of the topic does not include these questions:

- How much "true AI" (i.e., cognition) is available in today's products (as opposed to implementations focusing mostly on ML)?
- How much do today's implementations rely on human intervention and/or accurate "training" datasets?
- How effective are today's solutions in handling scenarios beyond the most promising use cases of outlier detection and high-volume event processing?

Our bottom line on this one is that although the early returns from the field are undoubtedly promising, enterprise security teams still need to proceed with their eyes wide open when making investments in security products claiming to feature a heavy dose of ML and/or AI technologies.

Section 4: Practices and Strategies

SSL/TLS Inspection Practices

Describe your agreement with the following statement: "Efficiently exposing SSL/TLS traffic for inspection by our security tools remains a challenge." (n=1,169)

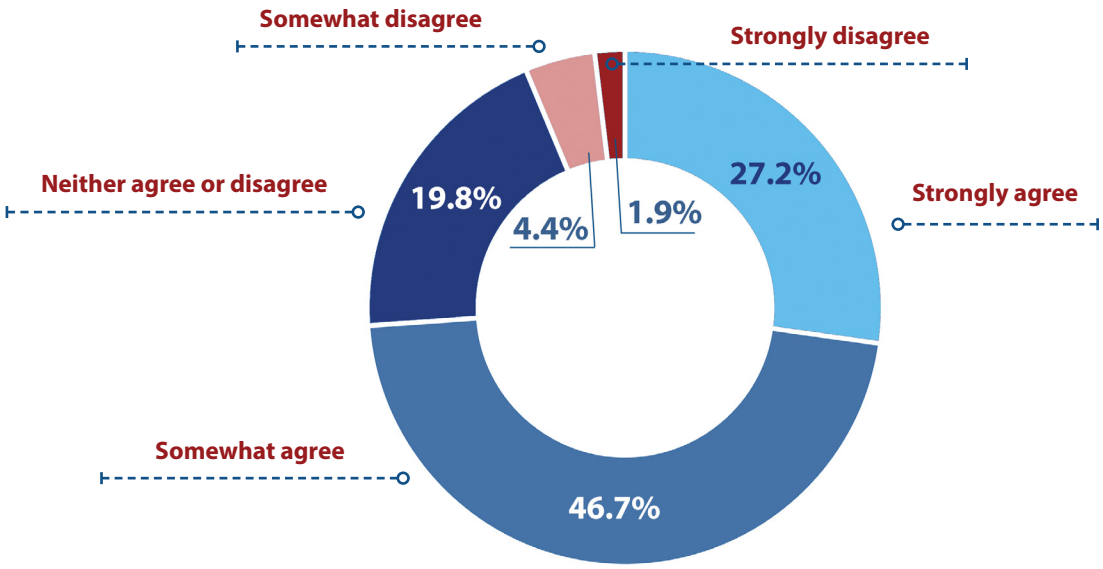

Figure 27: Adequacy of SSL/TLS decryption capabilities.

A key finding from the 2018 CDR (page 33) was that only 4.2% of respondents' organizations lacked the ability to decrypt SSL/TLS-encrypted traffic so it could be inspected for cyber-threats. Additional findings revealed the leading approaches for accomplishing decryption to be: relying primarily on individual security products to do it their own (26.0%); relying primarily on standalone, decryption-offload appliances (28.7%); and using a combination of both techniques (41.1%). What wasn't examined, however, was the perceived level of effectiveness of these efforts to maintain visibility – for security as well as other purposes – in a world where the percentage of network traffic that is encrypted continues to steadily climb.

To shed some light on this missing aspect of the topic, this year we asked participants to indicate whether they believe efficiently exposing SSL/TLS traffic for inspection remains a challenge for their organizations. The results, depicted in Figure 27, are interesting – particularly considering the findings from last year. Specifically, although most organizations have the means/tools to decrypt SSL/TLS traffic (2018 CDR), the perceived adequacy of those means /tools is fairly low. This is evidenced by 73.9% of our respondents' concurring (i.e., "somewhat" plus "strongly" agreeing) that efficiently decrypting network traffic remains a challenge. What's more, only 6.3% responded that it isn't a challenge.

Digging into the demographic breakdowns, the data also shows: (a) organizations in the manufacturing and education sectors are struggling more with this issue than those from the other big 7 industries; and (b) there is very little variation in the distribution of responses based on size of organization.

Our closing thought for this topic is that the need for SSL/TLS decryption efficiency and centralization is only going to grow as both the percentage and net volume of encrypted traffic continue to increase across physical, virtual, and cloud environments. As a result, alongside the ability to provide comprehensive coverage, capacity, scalability and overall performance are now and forever will be critical criteria for evaluating candidate solutions in this area.

Section 4: Practices and Strategies

Threat Intelligence Platform Practices

Select the following reasons your organization has integrated a threat intelligence platform (TIP) into your existing security infrastructure. (Select all that apply.) (n=1,156)

Figure 28: How threat intelligence platforms are being leveraged.

In simple terms, a threat intelligence platform (TIP) is a threat intelligence management system. It represents and supports the logical progression from availability/use of a single, supplemental threat intelligence feed – the typical scenario a few years back – to an environment that enables and accounts for numerous intelligence sources. Functionally, this entails capabilities such as the aggregation, normalization, enrichment, and analysis of threat intelligence data in advance of sharing the pre-processed results with any number of commonly deployed countermeasures (e.g., NGFWs, endpoint protection software, and SIEM systems).

Think of it this way: a TIP not only provides the enterprise security team with a richer body of intelligence on which to draw (e.g., for threat detection, blocking, and investigation purposes), but also a bunch of automation capabilities for processing that intelligence and actually putting it to use. That's how we see it, at least.

To gain some insight into how security teams are deriving value from TIPs today, we asked respondents to select the reasons why their organizations integrated such a solution into the existing security infrastructure. Figure 28 shows the results. While "improving the ability to detect cyberthreats" (53.7%) predictably garnered the top spot on our list, it only slightly edged out the second-place response of "improving the ability to validate security alerts" (52.9%). Trailing by a modest margin was "improving the ability to prioritize responses to security alerts" (43.3%) – another valuable use case, for sure.

"A TIP not only provides the enterprise security team with a richer body of intelligence on which to draw, but also a bunch of automation capabilities for processing that intelligence and actually putting it to use."

A few other TIP use cases that extend beyond the security operations center include proactive threat hunting, threat predictions based on in-depth correlation and analysis, and executive-level reporting and data sharing for both incident management and security planning purposes.

As a side note, we're also seeing enterprises invest in threat intelligence gateways (TIGs). This closely related component/technology focuses on the immediate application of threat intelligence. By automatically blocking traffic from millions of known-bad IP addresses and domains, TIGs inherently weed out countless threats while greatly reducing the load on downstream networking and security devices alike.

Both TIPs and TIGs are valuable security tools. We look forward to gauging adoption of these technologies for years to come.

Section 4: Practices and Strategies

Security Analytics Practices

Which approach best describes how your organization is adding (or planning to add) security analytics capabilities/technology to its cyberthreat defenses? (n=1,109)

Figure 29: How security analytics is being added.

For every one of the six years we've published the CDR, respondents have rated having "too much data to analyze" as a top-three obstacle to adequately defending their organizations from cyberthreats. It's not surprising, therefore, to see a solid level of interest in security analytics. Indeed, Table 5 on page 30 shows very respectable "currently in use" rates for several flavors of related solutions, including SIEM (55.0%), UEBA (46.5%), and advanced analytics incorporating ML and/or AI (41.3%). Note: additional findings and commentary on the evolving role of ML and AI technologies in InfoSec can be found on page 34.

Security analytics solutions deliver on the central promise of helping enterprise security teams "cut through the noise" by applying a growing variety of algorithms and analysis techniques to the mountains of security data available in their environments. The result, at a minimum, is a prioritized view into what matters most from a threat/risk perspective, with highly facilitated means for SecOps personnel to investigate matters further and reach their own conclusions. And, in the best cases, the outcome is the explicit identification of a previously unknown cyberthreat that was lurking in the weeds. Either way, it's a major win for today's security teams.

"Security analytics solutions deliver on the central promise of helping enterprise security teams cut through the noise."

Returning to our survey, this year we sought to uncover details on how organizations are going about adding security analytics capabilities to their cyberthreat defense portfolio. As shown in Figure 29, complementing an existing SIEM with a separate security analytics product (29.4%) only slightly edged out the second-place approach of relying on the organization's existing SIEM vendor to add security analytics capabilities into their product (28.3%). Somewhat less favored were the options of replacing the organization's existing SIEM with a new product that combines SIEM and analytics (24.1%) and engaging an MSSP to deliver security analytics capabilities as an integral (or add-on) component of its managed service offering (18.2%).

Digging into the demographic breakdowns, the only significant differences were the relatively high affinity for the MSSP approach among respondents from Australia (32.4%) and Singapore (25.6%), as well as those in the government sector (31.5%).

Section 4: Practices and Strategies

Security Orchestration, Automation, and Response Practices

How is your organization currently using security orchestration, automation, and response (SOAR) technology? (Select all that apply.) (n=1,132)

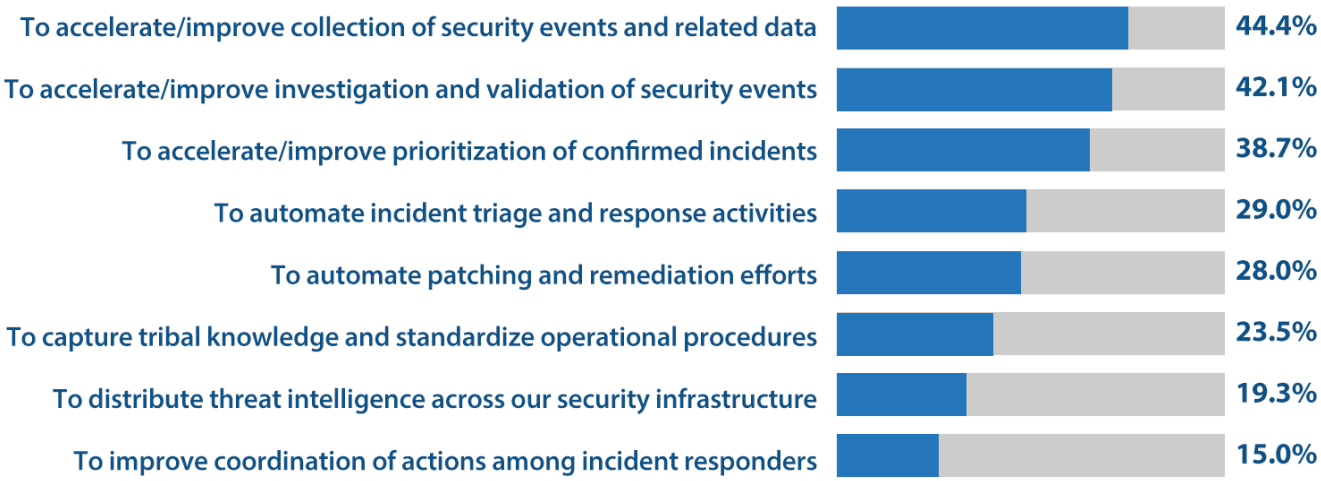

Figure 30: How security orchestration, automation, and response technology is being leveraged.

Another major inhibitor keeping security teams from adequately defending their organizations from cyberthreats is the lack of skilled personnel (see Figure 14 on page 16). This situation – which has been going on for several years and is expected to persist into the foreseeable future – emphasizes the need for organizations to find other (i.e., non-human) ways to boost the efficiency and productivity of their security operations.

Enter security orchestration, automation, and response (SOAR). Emerging SOAR offerings promise to do everything from stitching together (read: integrating) all of an organization's disparate policy enforcement infrastructure (read: firewall, gateways, and other types of "controllers") and existing event management systems to handling playbook coding and execution. In general, the idea is to bring a whole new level of automation, speed, and accuracy to every corner of the security operations landscape – from vulnerability and patch management to incident response.

Given the broad scope of potential SOAR use cases, we decided to figure out precisely how organizations are using the technology now – in other words, which value propositions are resonating the most and, therefore, garnering attention first. As revealed by Figure 30, the results are heavily skewed in favor of accelerating/improving various aspects of the threat management lifecycle – from event/data collection (44.4%) and validation (42.1%) to prioritization of (38.7%) and response to (29.0%) confirmed incidents.

Lower priorities, at least for the time being, include using SOAR to help with patching, to capture/codify standard practices, and to enable coordination of and collaboration among incident responders across shifts and/or geographies.

For more information on this potentially game-changing technology – including some high-level evaluation criteria and keys to success – be sure to check out the Road Ahead section of this report.

Section 4: Practices and Strategies

Use of Managed Security Services Providers

Which of the following IT security functions does your organization outsource to a managed security service provider (MSSP)? (Select all that apply.) (n=1,200)

Figure 31: How managed security service providers are being leveraged.

For enterprise security teams, the challenges – and workload – are ever growing. The volume, diversity, and sophistication of threats are constantly on the rise, along with the need to account for an ever-expanding technology footprint, or attack surface. New applications, development methodologies (e.g., DevSecOps), architectures/deployment models (e.g., containers and microservices for apps, and hybrid cloud for datacenters), infrastructure (e.g., OT and IOT), and technology (e.g., software-defined networking, micro-segmentation) are always popping up. And don't get us started on the tangle of security- and privacy-related compliance regimes today's enterprises need to address.

With so much on their plates, it's not surprising to see so many organizations – nine in 10 according to our data – turning to MSSPs to pick up part of the load. As for the specific parts they are choosing to shed, our data shows vulnerability scanning (38.3%), event analysis/reporting (37.6%) and DDoS mitigation (37.5%) are leading the way (see Figure 31). At the other end of the spectrum, monitoring and managing WAFs (13.1%) is the least likely security chore to be out-tasked – a result that is not particularly surprising given the tight relationship between WAF effectiveness and in-depth knowledge of the web applications that are the object of its defensive capabilities.

Interestingly, while security event analysis/reporting placed relatively favorably (37.6%), the similar-sounding entry of monitoring/managing one's SIEM didn't fare as well (17.8%). Our takeaway here is that what matters most to buyers is less the specific technology being employed, and more the functions/capabilities being delivered.

"With so much on their plates, it's not surprising to see so many organizations – nine in 10 according to our data – turning to MSSPs to pick up part of the load."

Other notable findings:

- "Monitoring/managing advanced threat defense/hunting technologies" was the top function for which respondents from China (46.9%) and Italy (43.8%) indicate their organizations utilize MSSPs.
- "Mitigating DDoS attacks" was the top purpose for using MSSPs selected by respondents from the finance industry (37.5%).
- With the highest overall usage rate (96.0%), medium-size organizations (5,000 to 9,999 employees) appear to be the sweet spot for MSSPs.

The Road Ahead

You'll get no argument from us that information security is an extremely challenging field in which to work. Because the bad guys need to get it right only once to bring the pain, InfoSec professionals and practitioners need to be on their game every single day, in every single way. And with the breakneck pace at which today's businesses are adopting new technology, there's never a shortage of gaps in defenses for the enterprise security team to work on. Good examples from this year's survey include:

- Application containers and mobile devices (smartphones and tablets) are, once again, revealed as the weakest links in most organizations' defenses (see Figure 5 on page 9).
- Building security into applications in the first place remains a challenge for today's organizations, along with adequately detecting insider attacks (see Figure 6 on page 10).
- With year-over-year increases to the percentage of organizations not only victimized by it but also electing to pay associated threat actors, ransomware is a significant (even growing) challenge for most organizations (see Table 1 on page 14).

But let's not forget that being challenging has an upside, too. It's precisely what makes InfoSec so interesting, invigorating, and rewarding … not to mention providing all of us with a certain degree of job security. If that's not enough to keep you running strong (it is for us!), then hopefully some of the good news findings from this year's survey can help make up the difference:

- Nearly four in five respondents believe their organization has made improvements in its vulnerability and patch management capabilities over the past year … a positive step toward reducing their respective attack surfaces (see Figure 17 on page 19).
- With a global average year-of-year growth rate of 4.9%, IT security budgets are in solid shape … and not a significant obstacle to achieving effective cyberthreat defenses (see page 22 and Figure 14 on page 16).
- ML and AI technologies are having a positive impact on the ability of organizations to combat advanced threats (see Figure 26 on page 34).

Finally, it's time once again to go beyond the scope of this year's survey and provide suggestions for some of the top areas where we believe proactive attention and investments have the potential to keep things heading in the right direction by significantly enhancing an organization's ability to defend against current and future generations of cyberthreats.

Container Security Platforms. As the initial wave(s) of containerized applications transition from the Dev/Test environment into production, enterprises – if they haven't already done so – will need to take a more strategic approach to container security. Continuing to rely on tactical, piecemeal efforts featuring too-great emphasis on vulnerability scanning will only erode many of the gains containers are meant to deliver (easier/quicker app revs, more-efficient resource utilization, and superior scalability).

For organizations in such a position, container security platforms (CSPs) are a promising option that warrants close consideration. The goal of this rapidly maturing class of offerings is to provide the full set of security functionality that collaborating DevOps and security teams will need. This functionality accounts not only for all the key components of a containerized environment (images, containers, hosts, registries, and orchestrator) wherever they reside (on-prem or in the cloud), but also for each phase of the container lifecycle (i.e., build, deploy/ship, run).

As such, table stakes for a CSP include:

- Multi-phase vulnerability scanning and security configuration management
- Secrets management
- Automatic network segmentation / least-privilege access control (aka: container firewalling)
- Runtime monitoring for anomalous behavior (with configurable response actions)
- Policy and compliance auditing/reporting
- Out-of-the-box integration with all common CI/CD tooling

The Road Ahead

Evaluators intent on getting the most for their money should also look for these next-level capabilities:

- Context-based prioritization of all vulnerability and configuration findings
- Threat/anomaly detection that automatically accounts for changing application behavior
- Continuous posture improvement through automated, cross-phase sharing of security information

Security Orchestration and Automation. The orchestration and automation of security solutions is both necessary and inevitable. It is necessary because it represents perhaps the only navigable path out of the perfect storm today's security teams are stuck in: an increasingly hostile threat landscape and an ever-growing attack surface, compounded by a shortfall of skilled personnel and other resources. It is inevitable because infrastructure-as-code is the future of IT, and security has no choice but to evolve along the same trajectory.

For forward-leaning organizations intent on making significant progress in the next decade (that) it will take this endgame to come about, emerging SOAR offerings promise to deliver everything from faster incident response times and enhanced operational accuracy/consistency to reduced manpower requirements. We also expect adjacent SIEM solutions to add related capabilities in relatively short order.

The key ingredients for a successful deployment are the same with either option, and include:

- Deep, bi-directional integration with substantially all the security tools in your environment
- A predictable and palatable pricing model (e.g., one that doesn't artificially constrain security data rates/volumes, API calls, or users)
- A significant number of security processes and tasks that are already granularly defined – to ensure both a handful of quick wins and sustained demonstration of value

For organizations not yet ready to SOAR, we recommend at least starting to soften the beachhead. Good precursor activities include defining/documenting key SecOps processes and scripting some of your own automations – not only for the efficacy and efficiency gains they deliver but also to help socialize the value of automated response (which has traditionally been viewed as a risky undertaking).

Risk Quantification. One of the greatest and most enduring challenges in information security has little to do (at least directly) with preventing, detecting, or responding to cyberthreats. Establishing a clear, business-based picture of an organization's cyber risk is an elusive holy grail that, if done right, promises to deliver:

- An economic understanding of exposure to cyber risk
- A lingua franca for use by all stakeholders (from the board of directors to the people in the SecOps trenches)
- A decision-making framework for prioritizing and optimizing InfoSec activities, investments, and insurance

Doing it right, however, is the rub. Traditional methods – for example, involving internal assessments, third-party audits, and pen tests – fall far short of the mark. They suffer not only from being resource intensive, static, and subjective, but also from "speaking" in technical terms and metrics. Emerging trust-rating solutions, with their origins in the vendor/third-party risk management arena, take a significant step forward. By spitting out an actual number – in this case, a figure analogous to a credit score – such tools open the door to a base level of impact analysis, as well as external benchmarking and monitoring of third-party risk. The result, though, is not only based on closed/proprietary algorithms and often limited to an assessment of externally available signals, but also remains relative and non-financial (precluding comparison with other forms of business risk).

More fully achieving the benefits of risk quantification will depend on finding an advanced solution that:

- Uses an open (if not standard) method and algorithms for calculating cyber risk
- Measures cyber risk as a probability (i.e., range) of potential financial losses within a given timeframe

The Road Ahead

Without the objective understanding and quantification of cyber risk such a solution can provide, no cyber risk management program can be truly effective.

ICS/OT Security. There is little debate that industrial control systems (ICSs) and other forms of operational technology (OT) are rapidly gaining intelligent networking capabilities. They are also increasingly being interconnected and linked to the broader IT environment, and therefore, presenting potential targets for an expanding collection of threat actors.

The good news is that the same general principles and techniques used to secure regular 'ole IT remain applicable when it comes to defending ICS/OT environments. This high-level consistency, however, does not preclude the need to invest in new ICS/OT-centric security tools and products. Extending visibility and control to these domains is simply impossible without an in-depth understanding of the relevant communication protocols, technologies, and operational distinctions (e.g., zero tolerance for downtime).

Enterprises with the luxury of time will be served best by taking a holistic approach to planning these investments – for example, by evaluating their needs at each layer of the ICS/OT environment (sensor/device, controller, local/distributed management systems, and cloud) and considering how well individual products will work together before making any purchases. For others that are under the gun to get something done immediately, here are three areas to focus on first, based on both their potential impact and traction in the market:

- Continuous ICS/OT security management – including both vulnerability and anomaly-based threat detection
- An IT/OT gateway – for border control and threat filtering (much like an NGFW)
- Secure/privileged remote access – to granularly control and audit access to ICS/OT infrastructure

For further insights on these and other emerging areas pertinent to IT security, be sure to tune in for the seventh annual CDR, currently scheduled for release in the first quarter of 2020.

Appendix 1: Survey Demographics

- Accounts not only for externally measured signals (i.e., data), but also internal conditions and "softer" elements, such as culture and processes

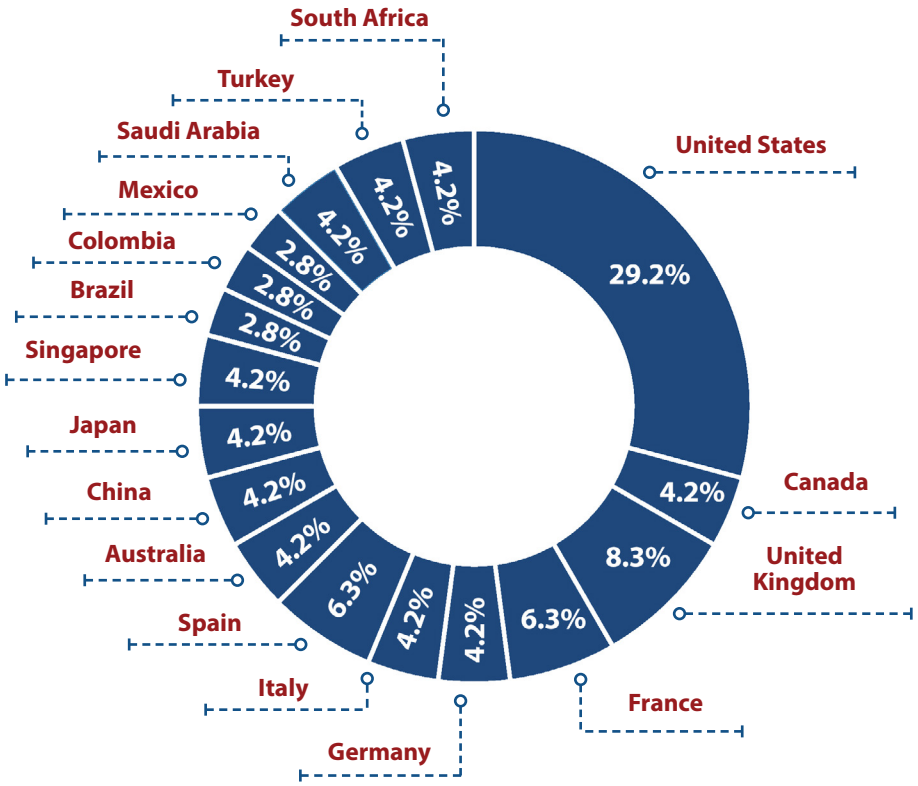

Figure 32: Survey participation by country.

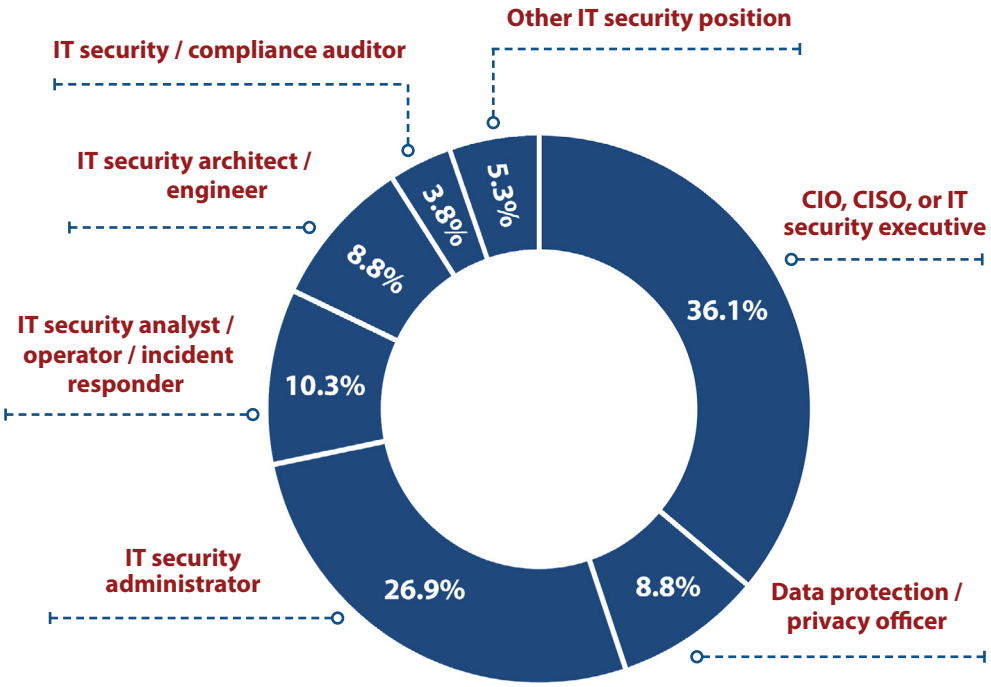

Figure 33: Survey participation by IT security role.

Appendix 1: Survey Demographics

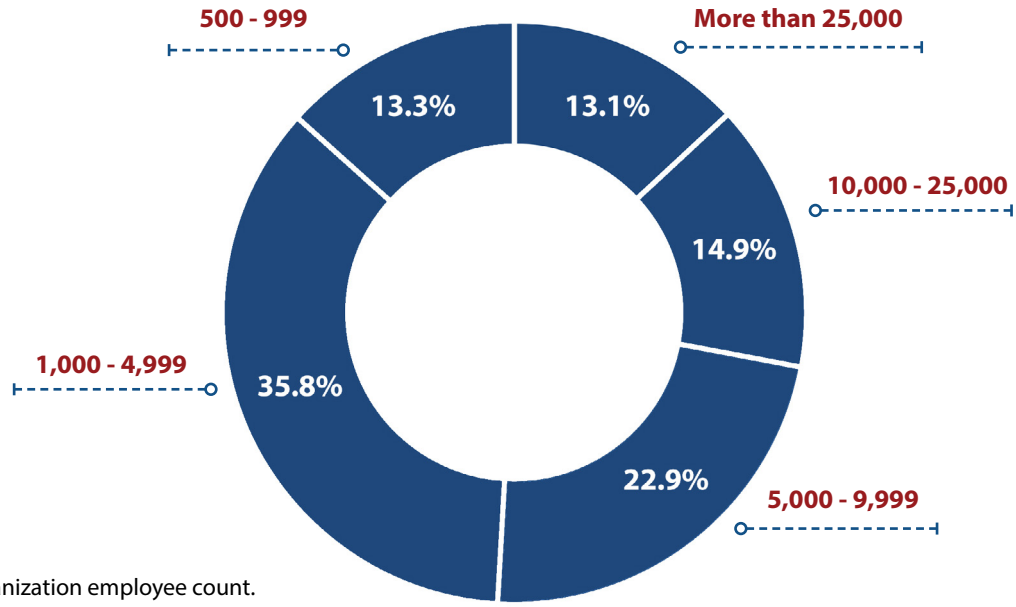

Figure 34: Survey participation by organization employee count.

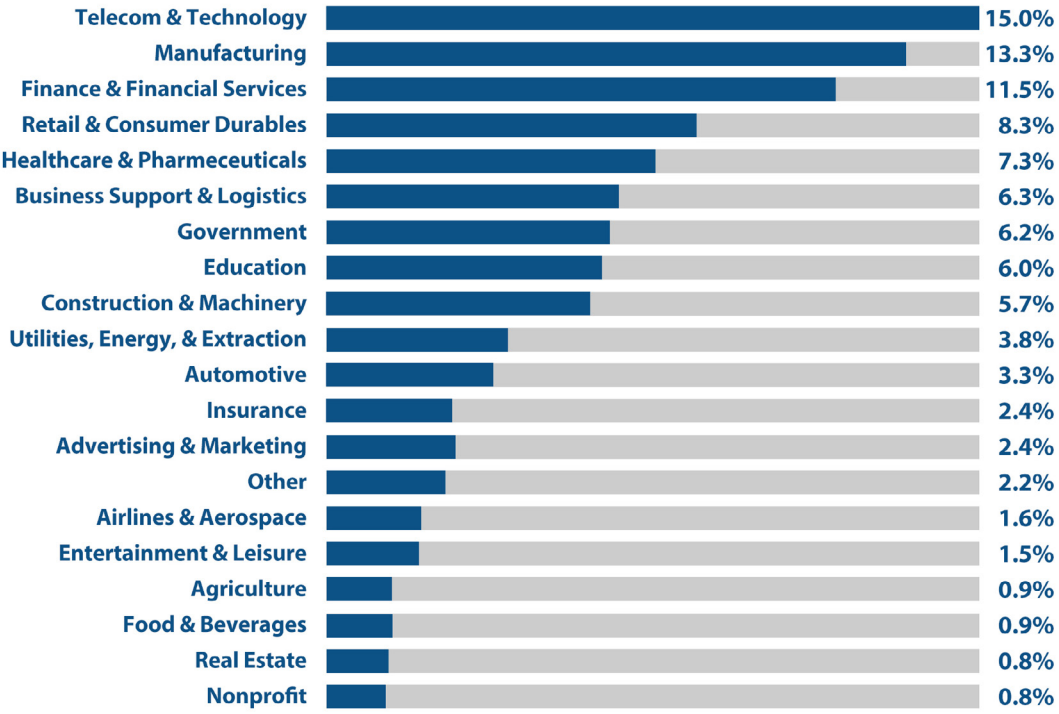

Figure 35: Survey participation by industry.

Appendix 2: Research Methodology

CyberEdge Group developed a 27-question (10- to 15-minute) web-based survey in partnership with its sponsoring vendors. (No vendor names were referenced in the survey.) The survey was promoted to information security professionals across North America, Europe, Asia Pacific, the Middle East, Latin America, and Africa in November 2018.

Non-qualified survey responses from non-IT security professionals and from participants employed by organizations with fewer than 500 global employees were discarded. Most survey questions (aside from demographic questions) included a "don't know" choice to minimize the potential for respondents to answer questions outside of their respective domains of expertise, which altered the sample size ("n") for each set of survey question responses.

All qualified survey responses were inspected for potential survey "cheaters," meaning survey takers who responded to questions in a consistent pattern (e.g., all A responses, A-B-C-A-B-C responses) in an attempt to complete the survey quickly in hopes of receiving the incentive. Suspected cheater survey responses were deleted from the pool of responses.

Appendix 3: Research Sponsors

CyberEdge is grateful for its Platinum, Gold, and Silver sponsors, for without whom this report would not be possible.

Platinum Sponsors

Code42 | www.code42.com

Code42 is the leader in next-gen data loss protection. Native to the cloud, the Code42 Next-Gen Data Loss Protection solution rapidly detects insider threats, helps satisfy regulatory compliance requirements and speeds incident response — all without lengthy deployments, complex policy management or blocking user productivity. Because the solution collects and indexes every version of every file, it offers total visibility and recovery of data — wherever it lives and moves. Security, IT and compliance professionals can protect endpoint and cloud data from loss, leak and theft while maintaining an open and collaborative culture for employees. Backed by security best practices and control requirements, Code42 Next-Gen Data Loss Protection preserves files for compliance and can be configured for GDPR, HIPAA, PCI and other regulatory frameworks. More than 50,000 organizations worldwide, including the most recognized brands in business and education, rely on Code42 to safeguard their ideas.

DXC Technology | www.dxc.technology

As the world's leading independent, end-to-end IT services company, DXC Technology (NYSE: DXC) leads digital transformations for clients by modernizing and integrating their mainstream IT, and by deploying digital solutions at scale to produce better business outcomes. The company's technology independence, global talent, and extensive partner network enable 6,000 private and public-sector clients in 70 countries to thrive on change. DXC is a recognized leader in corporate responsibility.

Gigamon | www.gigamon.com

Gigamon® is the recognized leader in network visibility solutions, delivering the powerful insights needed to see, secure and empower enterprise networks. Our solutions accelerate threat detection and incident response times while empowering customers to maximize their infrastructure performance across physical, virtual and cloud networks. Since 2004 we have cultivated a global customer base which includes leading Service Providers, Government Agencies as well as Enterprise NetOps and SecOps teams from more than 80 percent of the Fortune 100.

Appendix 3: Research Sponsors

Imperva | www.imperva.com

Recognized by industry analysts as a cybersecurity leader, Imperva champions the fight to secure data and applications wherever they reside. In today's fast-moving cybersecurity landscape, your assets require continuous protection, but analyzing every emerging threat taxes your time and resources. For security to work, it has to work for you. By accurately detecting and effectively blocking incoming threats, we empower you to manage critical risks, so you never have to choose between innovating for your customers and protecting what matters most. At Imperva, we tirelessly defend your business as it grows, giving you clarity for today and confidence for tomorrow. Imperva—Protect the pulse of your business.

Gold Sponsors

Aqua Security | www.aquasec.com

Aqua Security enables enterprises to secure their container and cloud-native applications from development to production, accelerating application deployment and bridging the gap between DevOps and IT security. Aqua's Cloud native Security Platform provides full visibility into container activity, allowing organizations to detect and prevent suspicious activity and attacks in real time. Integrated with container lifecycle and orchestration tools, the Aqua platform provides transparent, automated security while helping to enforce policy and simplify regulatory compliance.

LookingGlass | www.lookingglasscyber.com

LookingGlass Cyber Solutions delivers unified threat protection against sophisticated cyber attacks to global enterprises and government agencies by operationalizing threat intelligence across its end-to-end portfolio. Scalable threat intelligence platforms and network-based threat response products consume our machine-readable data feeds to provide comprehensive threat-driven security. Augmenting the solutions portfolio is a worldwide team of security analysts who continuously enrich our data feeds and provide customers unprecedented understanding and response capability into cyber, physical and 3rd party risks. Prioritized, relevant and timely insights enable customers to take action on threat intelligence across the different stages of the attack life cycle.

Recorded Future | www.recordedfuture.com

Recorded Future delivers the only complete threat intelligence solution powered by patented machine learning to lower risk. We empower organizations to reveal unknown threats before they impact business and enable teams to respond to alerts 10 times faster. To supercharge the efforts of security teams, our technology automatically collects and analyzes intelligence from technical, open web, and dark web sources and aggregates customer-proprietary data. Recorded Future delivers more context than threat feeds, updates in real time so intelligence stays relevant, and centralizes information ready for human analysis, collaboration, and integration with security technologies. 91 percent of the Fortune 100 use Recorded Future.

StackRox | www.stackrox.com

StackRox helps enterprises secure their containerized and Kubernetes environments at scale. The StackRox Kubernetes Security Platform enables security and DevOps teams to enforce their compliance and security policies across the entire container life cycle, from build to deploy to run. The StackRox platform provides visibility across all Kubernetes environments; provides dedicated compliance checks for CIS, NIST, PCI, and HIPAA; prevents misconfigurations in Kubernetes and containers to reduce the attack surface; and detects and stops attacks at runtime. StackRox integrates with existing DevOps and security tools, enabling teams to quickly operationalize container and Kubernetes security.

Appendix 3: Research Sponsors

Silver Sponsors

Arctic Wolf Networks | www.arcticwolf.com

Arctic Wolf Networks delivers the industry-leading security operations center (SOC)-as-a-service that redefines the economics of cybersecurity. The AWN CyberSOC™ service is anchored by Concierge Security™ teams who provide custom threat hunting, alerting, and reporting. Arctic Wolf's purpose-built, cloud-based service offers 24x7 monitoring, vulnerability assessment, threat detection, and response.

Bandura | www.banduracyber.com

Bandura pioneered the Threat Intelligence Gateway (TIG) in part with the U.S. Department of Defense. Organizations worldwide use the Bandura TIG for the automation and control needed to operationalize millions of threat indicators—blocking known threats before they even reach the network firewall. Underlying Bandura's robust technology are multiple issued and pending patents. Connect to our website to learn more about how the Bandura TIG reduces an organization's attack surface, operationalizes threat intelligence, and helps to get more out of existing security investments.

CTERA | www.ctera.com

Trusted by Fortune 100, government organizations and leading service providers, CTERA provides the only cyber-hardened and completely unified multi-cloud data management platform that allows enterprises to address the full continuum of global file services from the edge to the cloud infrastructure of their choice. CTERA is leading the digital transformation of enterprises to cloud-enabled file services, with millions of corporate users and tens of thousands of enterprise locations worldwide.

DisruptOps | www.disruptops.com

DisruptOps implements Guardrails around an organization's cloud environment to enforce security, operational and cost management best practices. Delivered as a SaaS service, DisruptOps' automation platform elevates cloud security operations by both finding AND fixing issues, enabling customers to achieve their objectives of agility and innovation while maintaining operational control. DisruptOps is headquartered in Kansas City, MO and is backed by Rally Ventures and other security industry luminaries.

Edgeworx Solutions | www.edge-worx.com

Our mission is to assist our customers in maximizing the return on investment in network infrastructure investments, identify and eliminate potential IT security risks, avoid the need for costly bandwidth upgrades, optimize end-user performance, and improve the access and response time of enterprise and cloud-based business applications. Our network of business partners and technology alliances helps our customers to maximize the value of their IT investments and ensure business continuity. We use what we sell and we sell what we use. When on assignment our consultants and engineers need to rely on the best-of-breed technology available to do their job right.

Illusive Networks | www.illusivenetworks.com

Illusive helps organizations prevent business damage from cyberattackers operating within the network perimeter—both insiders and outsiders—by destroying their ability to move laterally toward critical assets. To preemptively harden the attack surface, Illusive identifies and removes high-risk credentials and connections between systems. By planting lightweight deceptions on endpoints across the environment, Illusive enables early detection, regardless of the attacker's starting point. Combining real-time source forensics and threat intelligence gathered from interactive decoys, Illusive provides risk-aware insights that enable responders at all skill levels to rapidly triage and remediate incidents. Using agentless machine learning, Illusive provides scalable, elastic security that is easy and non-intrusive to deploy and operate as the business environment changes.

Appendix 4: About CyberEdge Group

CyberEdge Group is an award-winning research, marketing, and publishing firm serving the needs of information security vendors and service providers. Our highly experienced consultants have in-depth technical expertise in dozens of IT security technologies, including:

- Advanced Threat Protection (ATP)
- Application Security
- Cloud Security
- Container Security
- Data Security
- Deception Technology
- DoS/DDoS Protection
- Endpoint Security
- ICS/OT Security
- Identity and Access Management (IAM)
- Intrusion Prevention System (IPS)
- Managed Security Services Providers (MSSPs)
- Mobile Device Management (MDM)
- Network Behavior Analysis (NBA)
- Network Forensics
- Next-generation Firewall (NGFW)
- Patch Management
- Penetration Testing
- Privileged Account Management (PAM)
- Risk Management/Quantification
- Secure Email Gateway (SEG)
- Secure Web Gateway (SWG)
- Security Analytics
- Security Configuration Management (SCM)
- Security Information & Event Management (SIEM)
- Security Orchestration, Automation, and Response
- Threat Intelligence Platforms / Gateways
- Threat Intelligence Services
- User and Entity Behavior Analytics (UEBA)
- Virtualization Security
- Vulnerability Management (VM)
- Web Application Firewall (WAF)

For more information on CyberEdge Group and our services, call us at 800-327-8711, email us at info@cyber-edge.com, or connect to our website at www.cyber-edge.com.

CyberEdge Acceptable Use Policy

CyberEdge Group, LLC ("CyberEdge") encourages third-party organizations to incorporate text and graphics from this report into presentations, reports, website content, product collateral, and other marketing communications without seeking explicit written permission from CyberEdge, provided such organizations adhere to this acceptable use policy.

The following rules apply to referencingor reusing text and/or graphics from this report:

1. **Report distribution.** Only CyberEdge and its authorized research sponsors are permitted to distribute this report for commercial purposes. However, organizations are permitted to leverage the report for internal uses, including training.
2. **Source citations.** When citing a text or graphics from this report, you must incorporate the following statement into a corresponding footnote or other citation: "Source: 2019 Cyberthreat Defense Report, CyberEdge Group, LLC."
3. **Quotes and excerpts.** Quotes and excerpts extracted from this report must not be modified in any way. Rephrasing is not permitted.
4. **Figures and tables.** Figures and tables extracted from this report must not be modified in any way. Artwork for figures and tables for the most recent Cyberthreat Defense Report may be available for download at no charge on the CyberEdge website at **www.cyber-edge.com/cdr.**
5. **No implied endorsements.** CyberEdge does not endorse technology vendors. Cited CyberEdge content should never be used to imply favor from CyberEdge.

If you have questions about this policy or would like to incorporate content from this report in a manner not addressed by this policy, submit an email to research@cyber-edge.com.

Copyright © 2019, CyberEdge Group, LLC. All rights reserved. The CyberEdge Group name and logo are the property of CyberEdge Group, LLC. All other company names, trademarks, and service marks are the property of their respective owners. Version 1.1