CYBEREDGE GROUP

2018 Cyberthreat Defense Report

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

« Research Sponsors »

PLATINUM

CODE42 Gigamon GREAT BAY IMPERVA paloalto NETWORKS

GOLD

Fidelis Cybersecurity MICRO FOCUS WEBROOT

SILVER

CloudPassage iovation illusive Logsign

Table of Contents

Introduction

Many, if not most, IT security vendors publish reports on their respective views of the cyberthreat landscape – often slanted toward their particular areas of expertise. Although these reports yield helpful insights, until the launch of our inaugural Cyberthreat Defense Report (CDR) in 2014, no research organization had ever taken a vendor-agnostic look at how enterprises actually perceive cyberthreats and how they leverage third-party products and services to overcome them. CyberEdge is proud to have filled that void.

Now in its fifth year, the CDR has become a staple among IT security leaders and practitioners by helping them gauge their internal practices and security investments against their peers – now across 17 countries and 19 industries. Simply put, there is no other report of its kind. And we are proud to have received a 2017 MarCom Platinum Award for our efforts!

The cyberthreat landscape has changed considerably over the past half-decade. And so have our defenses. Table 1 highlights key results from our 2014 CDR as compared to this year's findings.

In some ways, we're facing the same challenges that we did five years ago:

- Malware and spear phishing still cause the most headaches.
- Securing mobile devices remains a top challenge.
- Organizations continue seeking technologies to catch threats missed by traditional signature-based defenses.
- Our industry continues to underinvest in employee security awareness training, despite knowing that this problem persists.

However, increased investment in the cloud, adoption of application containers, increased reliance on mobile devices, and the damaging effects of ransomware are all examples of recent trends that keep IT security professionals on their toes.

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**

	2014	2018
Organizations victimized by one or more successful cyberattacks	62%	77%
Optimism for dodging a successful cyberattack in the coming year	62%	38%
IT security's weakest links	Mobile devices Laptops / notebooks Social media	Containers Mobile devices Cloud infrastructure
IT security's greatest inhibitors	Low security awareness among employees	Lack of skilled IT security personnel
Greatest cyberthreat concerns	Malware Spear phishing	Malware Spear phishing
Hottest network security technology planned for acquisition	Next-generation fire-wall (NGFW)	Advanced malware analysis
Hottest endpoint security technology planned for acquisition	Advanced malware analysis	Containerization / micro-virtualization
Change in next year's IT security budget	No change	Increase 5-9%

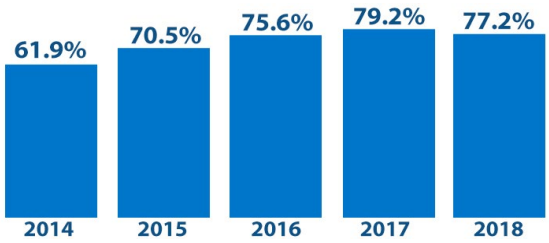
Table 1: Key comparisons from the 2014 and 2018 Cyberthreat Defense Reports

Introduction

Top Five Insights for 2018

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. **Has the bleeding stopped?** For the first time in five years, the percentage of respondents' organizations affected by a successful cyberattack has decreased—from 79.2% to 77.2%. The frequency of repeated successful attacks has also fallen.



2. **Flipping the ransomware coin**. Flip a coin once to determine whether your organization will be affected by ransomware. And if it will be, flip it again to determine whether paying the ransom will actually get your data back.

3. **Container security headaches.** Application containers (think Docker) have tied mobile devices as the most difficult IT components to secure. DevSecOps remains the most challenging IT security function for the second straight year.

4. **Security stuck in the cloud.** More than nine in 10 security professionals acknowledge cloud security challenges. Maintaining data privacy, controlling access, and monitoring for threats are at the top of the list.

5. **Rising shortage of IT security personnel.** In each of the past five years, we asked IT security professionals to identify their greatest inhibitors. "Lack of skilled personnel" has risen from fifth place (2014), to fourth place (2015), to third place (2016), to second place (2017), and now to first place (2018) over that span.

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 actual 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

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?

Introduction

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; and
- 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.

Section 4: Practices and Strategies

Mitigating today's cyberthreat risks takes more than investing in the right technologies. You must ensure those technologies are both 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 determine which security technologies are more apt to be deployed in the cloud versus on premises. We explore how organizations are decrypting SSL traffic for inspection. We uncover how organizations are embracing third-party threat intelligence, UEBA technology, and CASBs. And lastly, we learn how organizations are leveraging MSSPs to help keep the security trains running on time.

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

- **Has the bleeding stopped?** For the first time in five years, the percentage of respondents' organizations affected by a successful cyberattack decreased (page 7).
- **Pessimism or realism?** Six in 10 respondents feel a successful cyberattack in the coming year is more likely than not (page 8).
- **Containers—the new weakest link.** Application containers edge mobile devices as IT security's new weakest link (page 9).
- **Application development headaches.** Secure application development and testing is the security process organizations struggle with the most (page 10).
- **Cyberthreat hunting a bit off target.** Less than a third of respondents are confident their organization's investment in cyberthreat hunting solutions is sufficient (page 11).
- **Cybersecurity skills shortage eases slightly.** Eight in 10 organizations are suffering from the global shortfall of skilled IT security personnel (page 12).

Perceptions and Concerns

- **Cyberthreat migraines.** Malware, ransomware, and spear phishing give IT security the strongest headaches (page 13).
- **Flipping the ransomware coin.** Flip a coin once to see if your organization will be victimized by ransomware. Flip it again to see if paying the ransom gets your data back (page 15).
- **Inhibitors to success.** For the first time in five years, lack of skilled personnel trumps low security awareness among employees as IT security's greatest inhibitor to success (page 17).
- **Cloud security woes.** Nine in 10 organizations are experiencing cloud security challenges (page 19).
- **Explaining our patching failures.** More than four in five organizations experience vulnerability patching challenges (page 20).

Current and Future Investments

- **Security's slice of the IT budget pie.** On average, IT security consumes 12% of the overall IT budget (page 21).
- **Security budgets set new record.** The average security budget is going up by 4.7% in 2018 (page 23).
- **Network security's greatest hits.** Advanced malware analysis/sandboxing is the hottest network security technology planned for acquisition in 2018 (page 25).
- **Containerization is hot to trot.** Containerization/micro-virtualization tops the rankings for both endpoint security and mobile security technologies that respondents plan to acquire in the coming year… again (pages 27 and 29).
- **API gateways are in demand.** Application programming interface (API) gateway tops the most wanted list of application and data security technologies for 2018 (page30).
- **Ending the prevention vs. detection debate.** Investing in both cyberthreat prevention and detection is part of a balanced defense-in-depth strategy (page 31).

Practices and Strategies

- **Cloud vs. on-premises deployments.** IT security organizations demand the flexibility of deploying security technologies in the cloud, on premises, or both (page 32).
- **Keys to decrypting SSL.** Leveraging built-in decryption features in combination with standalone appliances is the key to mitigating the risks of encrypted threats (page 33).
- **Smart reasons for integrating threat intelligence.** Enterprises source threat intelligence to improve their abilities to block, detect, and investigate threats (page 34).
- **UEBA—IT security's Swiss Army knife.** Smart security teams are turning to user and entity behavior analytics (UEBA) technology to prevent account hijacking, detect privilege access abuse, and more (page 35).
- **Shining a light on CASBs.** Organizations of all sizes turn to cloud access security brokers (CASBs) to prevent unwanted data disclosures, detect advanced threats, mitigate Shadow IT, and more (page 36).
- **MSSPs to the rescue.** Nearly nine out of 10 organizations are leveraging managed security service providers (MSSPs) to offload one or more IT security functions (page 37).

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=1,136)

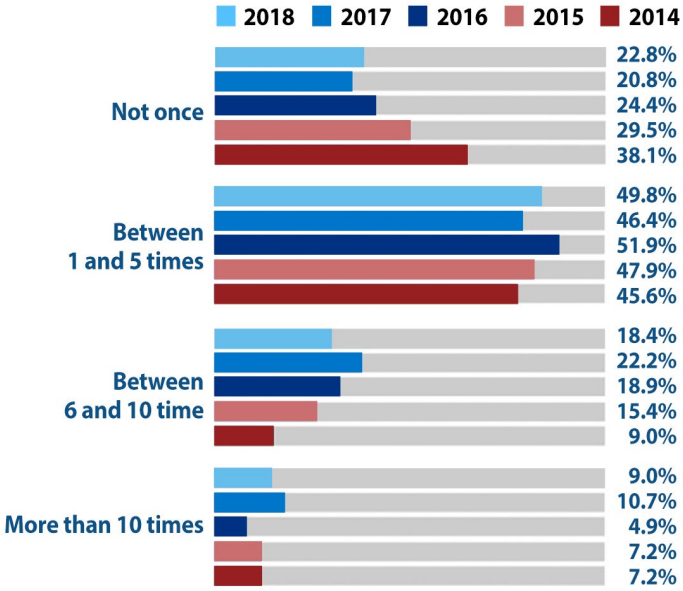


Figure 1: Frequency of successful attacks in the past 12 months.

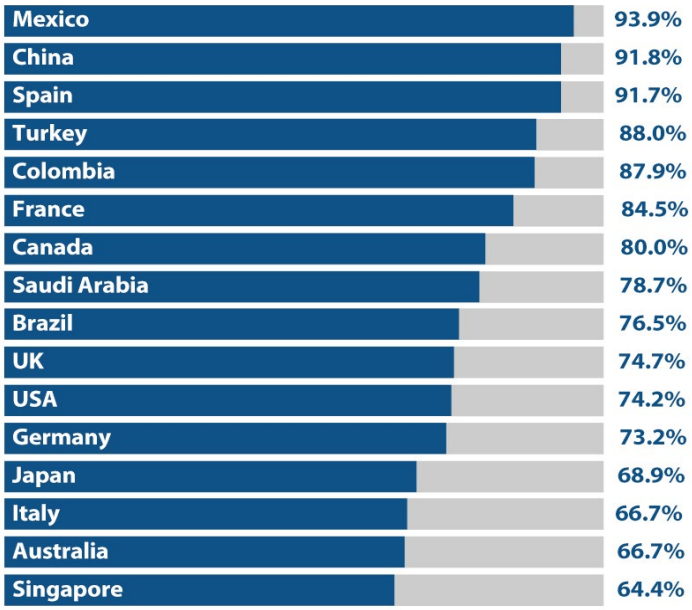


Figure 2: Percentage compromised by at least one successful attack in the past 12 months.

"For the first time in our five-year CDR history, there was a year-over-year decrease in organizations being hit by at least one successful attack."

The percentage of organizations affected by successful cyberattacks rose steadily over the past three years. Now, at the risk of jinxing the entire IT security industry, we have reason to believe the bleeding has finally stopped! (Yes, we have knocked on wood. Multiple times, to be safe.)

For the first time in our five-year CDR history, there was a year-over-year decrease in organizations being hit by at least one successful attack: down from 79.2% to 77.2% (see Figure 1). Perhaps even more significant is the nearly 17% decline for those being hit six or more times in the past year. To complete the picture, at least as far as the aggregate results are concerned, there was also a drop in those that were victimized "more than 10 times" (from 10.7% to 9.0%).

Digging even deeper into the data, we can also report that Singaporean organizations are faring the best in two areas: they were most likely to avoid falling victim to a cyberattack even once (35.6%) and least likely (0%) to be hit more than 10 times. On a related note, the data shows Mexico (93.9%) taking over the lead from China (91.8%) as the country with the greatest percentage of respondents' organizations being hit by at least one successful cyberattack in 2017 (see Figure 2).

Once again, larger organizations (> 10,000 employees) were hit "6 times or more" at more than twice the rate of their smaller counterparts. This finding is not particularly surprising when you consider that larger organizations are likely to have a substantially greater attack surface to defend – not to mention the widely accepted perception of being "juicier" targets.

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 2018? (n=1,175)

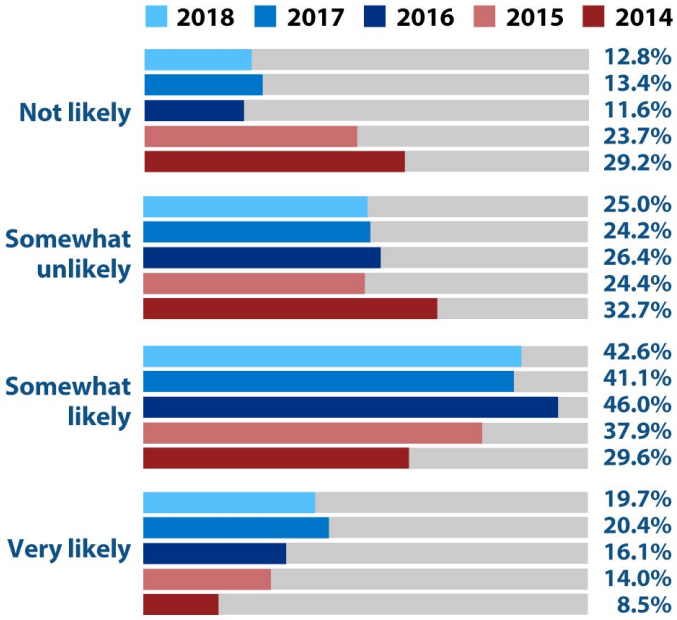


Figure 3: Likelihood of being successfully attacked in the next 12 months.

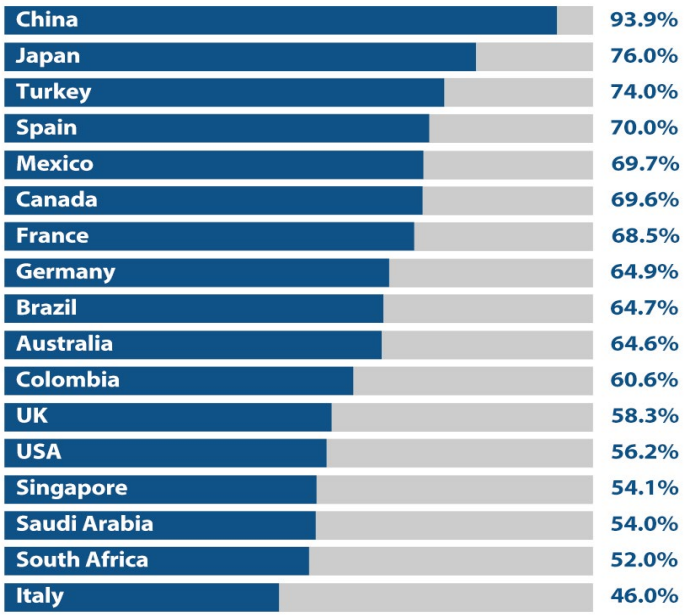


Figure 4: Percentage indicating compromise is "more likely to occur than not" in the next 12 months.

"Pessimism is the new reality among IT security professionals."

Each year, we ask respondents to estimate the likelihood of their organization being victimized by a successful cyberattack in the coming year. In 2014, 62% were optimistic, believing that an attack was unlikely. This year, the opposite holds true, with 62% being pessimistic, believing that an attack is more likely than not (see Figure 3). This figure has held steady for the last three years, which leads us to believe that pessimism is the new reality among IT security professionals.

However, buried deep inside this mountain of pessimism is a pocket full of optimism. In the last section, we learned that 77.2% of respondents indicated their organization had been successfully breached last year (see Figure 1 on page 7). So, shouldn't those same individuals be gun shy in the coming year? The answer, oddly enough, is "no!" As just mentioned, only 62% (okay, 62.3%) believe an attack is more likely than not in 2018. So, at least some of 2017's victims are optimistic for the future.

Other notable findings:

- 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 13.4% in 2017 to 12.8% for 2018.
- Geographically, China (92.0%), Japan (76.0%), and Turkey (74.0%) were the flag bearers for what we refer to as the "realist camp" (see Figure 4).
- Telecom & technology (66.8%), retail (65.9%), and manufacturing (65.4%) employ the most pessimistic (realistic) IT security professionals.

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=1,196)

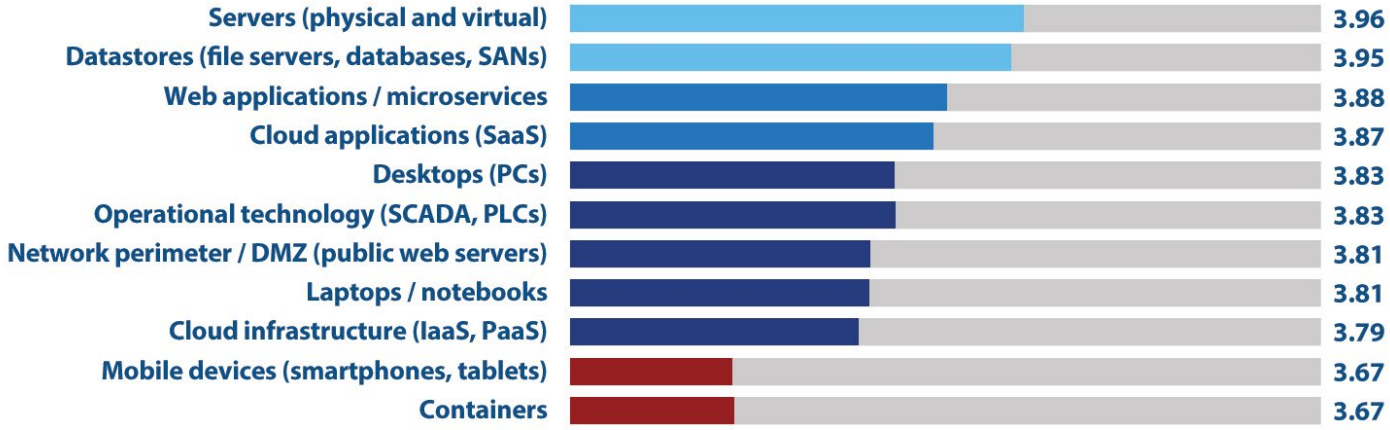


Figure 5: Perceived security posture by IT domain.

Data on the perceived ability to defend against cyberthreats in different IT domains (see Figure 5) helps inform priorities for future spending on security technology and services.

Once again, respondents expressed relatively high confidence in their defenses for both physical and virtual servers, while indicating that application containers and mobile devices comprise the greatest security challenges to today's organizations. And, once again, we can get behind this finding; after all, IT can be expected to be better at securing resources over which it has greater control (e.g., servers) than less control (e.g., mobile devices). It also makes sense to us to see containers and cloud infrastructure services (IaaS, PaaS) toward the bottom of the standings, as enterprise experience with these items remains immature (relatively speaking).

At the same time, however, there are a few findings that caught us a bit by surprise and for which the explanations are less clear. For example:

- Is a relative lack of attention and investment the reason why "network perimeter / DMZ" dropped from third position on the list of IT domains in 2017 to seventh in 2018?

"Application containers and mobile devices comprise the greatest security challenges to today's organizations."

- Does the ascension of "desktops" from eighth to fifth position over the past year signal that organizations are finally getting a handle on the shortcomings of traditional AV (and other legacy endpoint security technologies)?
- Is the appearance of "web applications" near the top of the chart merely a reflection of that vector's (temporarily) falling out of favor with attackers? There's certainly no data to show that such assets are any less vulnerable than they have been in the past.

In addition, it would be remiss of us not to mention that a significant trend has now reversed: while the weighted scores received for all domains increased for two years in a row, this time around the scores declined across the board, by an average of more than 0.12. One possible (optimistic) explanation for this reversal is growing recognition of the need to catch up with the sophistication of cyberattacks today.

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=1,196)

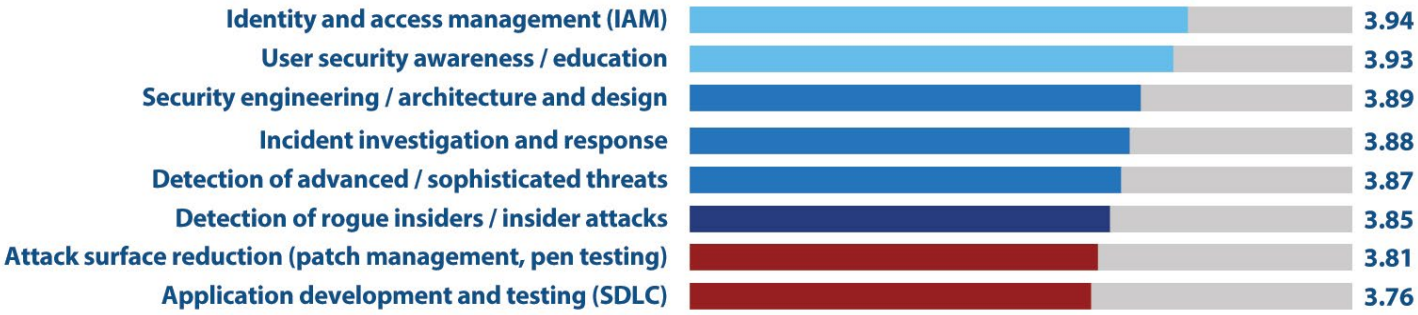


Figure 6: Perceived adequacy of functional security capabilities.

We know you get it: people and processes are at least as important as technological countermeasures when it comes to establishing effective cyberthreat defenses. That's why, for the second year in a row, we endeavored to gain some insight into how organizations are faring with some of the softer, non-technical aspects of the security equation.

Weighted scores of respondents' perceived adequacy of their organization's capabilities for several of the most significant functional areas of IT security (i.e., high-level processes) are shown in Figure 6. We're compelled to share one observation right out of the gate: a notable decline in scores across the board. This drop, averaging 0.14, is very similar to what has occurred with the technology domains from the previous question. Again, the explanation that makes the most sense to us is that enterprise security teams are beginning to realize that what they've done in the past is losing ground to advancements by today's threat actors. In other words, renewed effort and investment are needed for your organization's security processes – not just its technologies.

"Secure application development and attack surface reduction remain at the bottom of the rankings, cementing their position as the Achilles' heels of the typical IT security department."

Other notable findings:

- Secure application development and attack surface reduction remain at the bottom of the rankings, cementing their position as the Achilles' heels of the typical IT security department.
- The two new entries to the list – detection of advanced threats and detection of insider attacks – are not far behind, reinforcing our point that sophisticated and elusive threats seem to be a significant challenge for most organizations.
- Considering the finding of low security awareness among employees as the second-greatest inhibitor to establishing effective cyberthreat defenses (see Figure 14 on page 17), mindful security teams would be well served by reconsidering the adequacy of their efforts in user security awareness and education.

Section 1: Current Security Posture

Cyberthreat Hunting Capabilities

Describe your agreement with the following statement: "My organization has invested adequately in cyberthreat hunting solutions to detect threats missed by automated security defenses." (n=1,199)

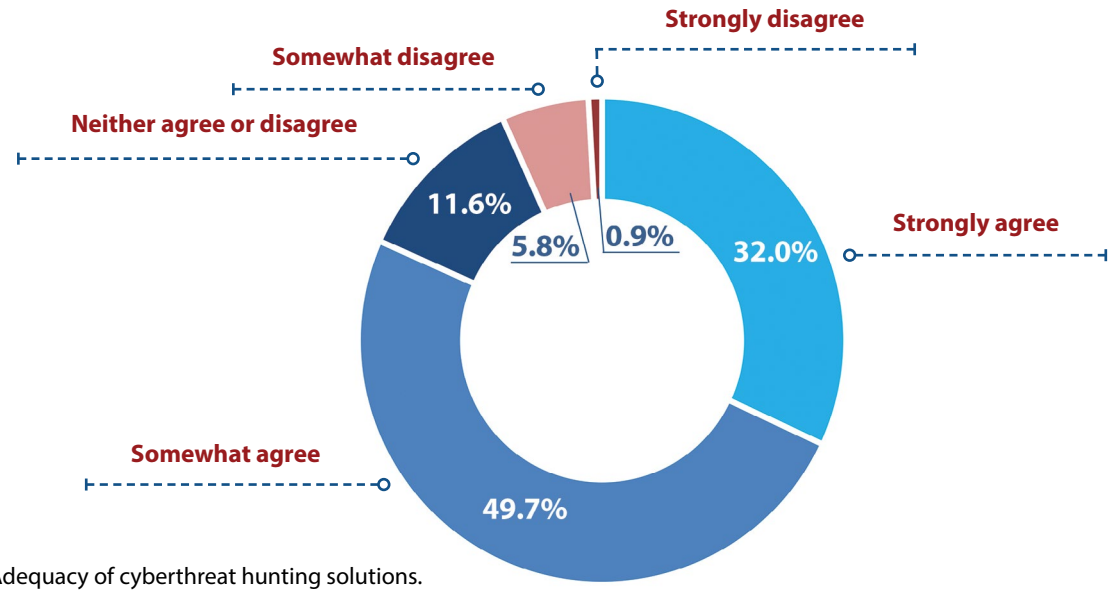


Figure 7: Adequacy of cyberthreat hunting solutions.

In the 2016 CDR (page 33), we highlighted establishing a formal cyberthreat hunting program as a way for forward-leaning organizations to more thoroughly leverage available threat intelligence sources and significantly enhance their security defenses. Now, for this 2018 edition, we asked participants to indicate whether they believe their organization has invested adequately in cyberthreat hunting solutions, specifically to uncover threats missed by other technological countermeasures (see Figure 7).

As for the results, we find ourselves forced – counter to our optimistic tendencies – to take a "glass half empty" stance when interpreting them. Instead of pointing out that nearly 82% generally agree with the adequacy of their organizations' investments in this area, we think a more appropriate/accurate interpretation is that:

a. Only one third (32.0%) are confident about the adequacy of their cyberthreat hunting investments, and

b. Nearly half (49.7%), despite acknowledging the efforts already made by their organizations, believe there is still room for improvement in this area.

Why? Because the alternative – that there's little interest in or perceived need to do more in terms of proactively uncovering missed threats – just doesn't add up. For that to be the case, we'd have to believe that everyone is happy with dwell times on the order of 200+ days (i.e., where threats that get through go undetected for that long). But we can't buy that.

Instead, it makes far greater sense, at least to us, that some investments have been made, probably on related software/technologies, but the returns have not yet been fully realized. The methods and processes to take full advantage of those investments remain undeveloped. In other words, more investment is probably needed, not so much in the "what" (i.e., tools), but in the "how" (i.e., maturing related processes and techniques and/or hiring more personnel with deep threat hunting experience/skillsets).

Two closing observations on this topic: looking at the combined results for "strongly agree" and "somewhat agree," (1) respondents for smaller organizations (<5,000 employees) trail their counterparts at larger ones by 11%, and (2) respondents within the education and government verticals trail those from the other "big 7" industries (finance, healthcare, manufacturing, retail, and telecom & technology) by an average of 12%.

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)

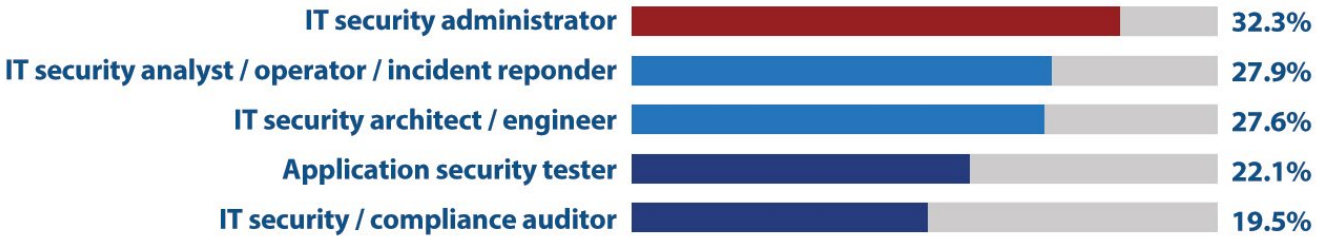


Figure 8: Cybersecurity skills shortage by role.

"Our results this time around show a modest improvement in this area."

Last year's stunning finding that nearly nine out of 10 organizations were experiencing a shortage of IT security talent validated recurring headlines that claim there's a global shortage of one to two million cybersecurity professionals. The good news – if it can be called that – is that our results this time around show a modest improvement in this area, with only eight out of 10 (i.e., four in five) now indicating that their organizations are impacted by the security talent shortfall.

As for how that shortfall breaks down, the aggregate data from this year shows the staffing challenge to be most acute for security administrators, with just shy of one-third (32.3%) of respondents selecting that role as a problem area for their organization (see Figure 8). Trailing only slightly behind and in a virtual tie are the roles of security analyst (27.9%) and security architect (27.6%). Even for the least selected role, security/compliance auditor, it is still the case that nearly one in five organizations are struggling to meet their needs.

Other findings of interest:

- Australia (64.6%), Germany (68.1%), and Brazil (76.5%) are the countries least impacted by the cybersecurity skills shortage, while Japan (98.0%), Spain (92.0%), and Mexico (90.9%) are being impacted the most.

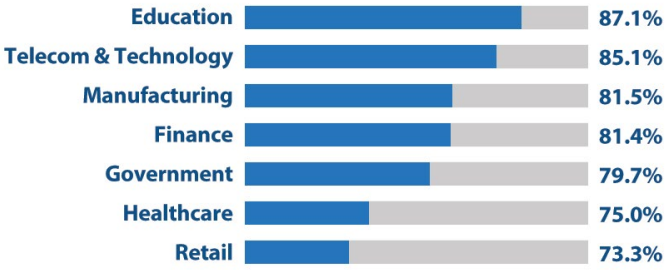


Figure 9: Percentage affected by the cybersecurity skills shortage.

- Education (87.1%) is the most impacted of the listed industries when it comes to this challenge, while retail (73.3%), healthcare (75.0%), and government (79.7%) organizations appear to be the least affected (see Figure 9).
- The IT security skills shortage varies little by organization size, both in terms of the overall level of impact and the impact by role.
- Respondents from organizations based in the Asian countries of Japan (53.1%), China (46.0%), and Singapore (41.7%) selected "IT security architect/engineer" as the role their organization is struggling hardest to fill.

Section 2: Perceptions and Concerns

Types of 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=1,196)

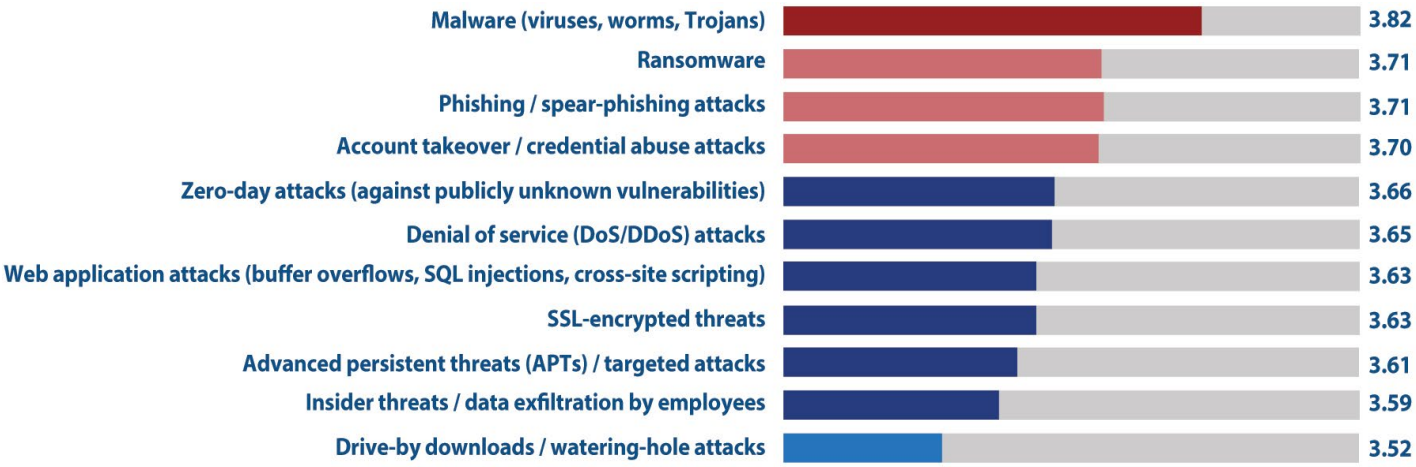


Figure 10: Relative concern for cyberthreats by type.

Since the inception of the CDR, malware (e.g., viruses, worms, Trojans) has consistently been a top-two concern for security professionals among various types of cyberthreats – along with phishing/spear phishing. Last year, malware stood atop the list and this year is no different. However, for the first time, there is a virtual three-way tie for second place among phishing/spear phishing, ransomware, and account takeover/credential abuse attacks (see Figure 10). The last of the three is a new addition in this year's report – and rightly so, given its high position on the list.

"One glimmer of hope from this year's results is the first-ever decline in overall concern for cyberthreats."

The most significant changes to this year's rankings are the rise of ransomware (from fifth to tied for second) and the fall of insider threats (from third to tenth). The former is easy to explain, given how much attention ransomware has received by both the trade press and mainstream media. The latter change is less clear, perhaps explained by infrequent publicly disclosed data breaches stemming from insider threats over the past 12 months.

One glimmer of hope from this year's results is the first-ever 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 of 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.

Over the past four years, the Threat Concern Index has risen from 3.10, to 3.26, to 3.71, to 3.84. But for the first time, that number has dropped – to 3.66 – the lowest in three years. We believe this decline correlates directly with the first-ever drop in successful cyberattacks, as reported by our respondents (see Figure 1 on page 7). Perhaps this is more evidence that IT security has finally stopped the bleeding of rising cyberattacks.

Section 2: Perceptions and Concerns

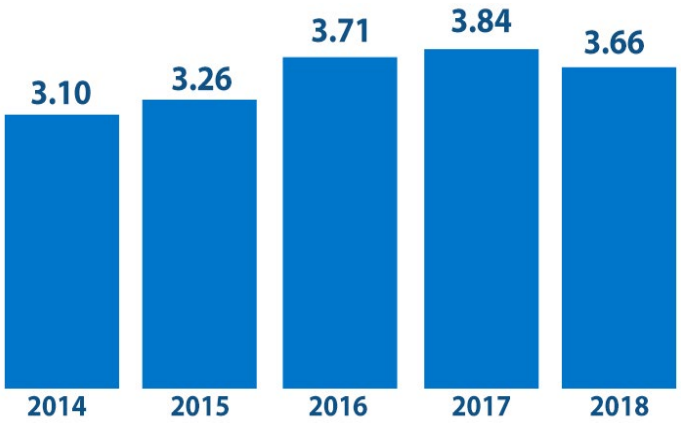


Figure 11: Threat Concern Index depicting overall concern for cyberthreats.

Two additional observations:

- None of the 11 types of cyberthreats depicted in the survey rated higher this year than last year's results.
- The total span of the weighted scores was its lowest yet (0.30), reinforcing last year's supposition that to many respondents, a "threat is a threat" – all types warrant concern and, presumably, attention.

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=1,176)

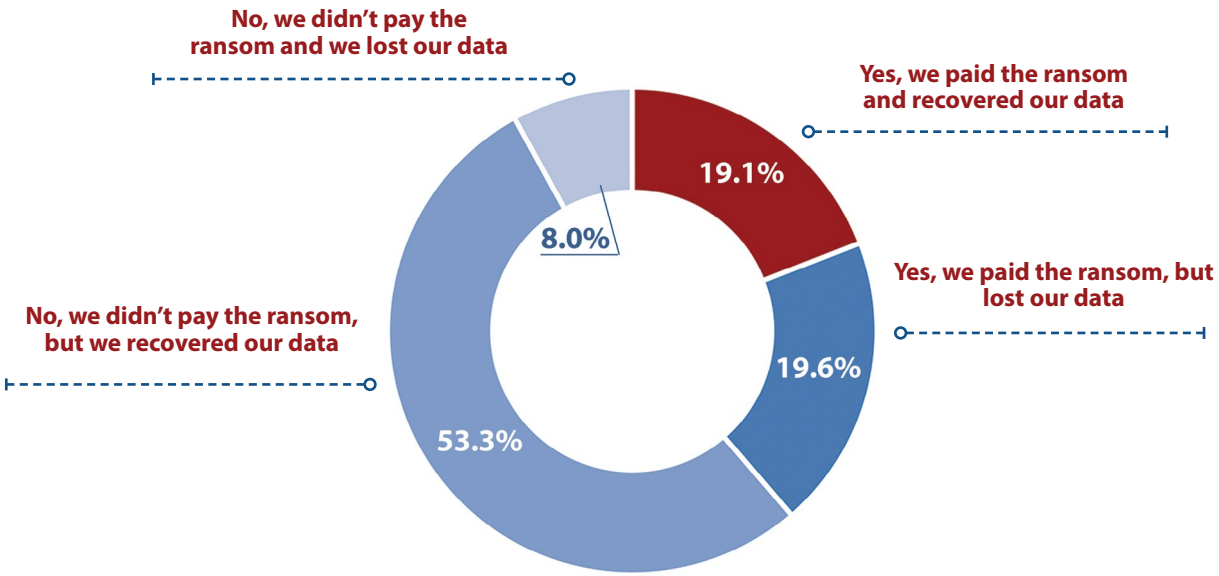


Figure 12: How victims responded to ransomware.

"It's like flipping a coin twice consecutively – once to determine if your organization will be victimized by ransomware, and then, if you decide to pay the ransom, flip it again to determine if you'll get your data back."

Ransomware continued to garner media attention in 2017 – and rightfully so. WannaCry, alone, dominated both IT security trade press and mainstream media when it hit the scene in May 2017, infecting more than 300,000 computers across 150 countries in a matter of days. Estimates for total damage caused by WannaCry range from hundreds of millions to billions of dollars.

In this year's report, we asked respondents if their organizations were affected by ransomware in 2017 and, if so, what action they took. Did victimized organizations actually pay the ransom? And, if so, did they get their data back? Figure 12 provides a breakdown of responses.

Collectively, 55% of organizations were victimized by ransomware in 2017. But if we isolate the responses for organizations that paid the ransom versus those that didn't, we gain useful insights (see Table 2). It turns out that 86.9% of victims refused to pay the ransom, but got their data back anyway – presumably through offline backups. That's the good news. The bad (horrifying) news is that of organizations that felt compelled to pay the ransom, only half (49.4%) got their data back!

It's like flipping a coin twice consecutively – once to determine if your organization will be victimized by ransomware (55% chance), and then, if you decide to pay the ransom, flip it again to determine if you'll get your data back (49.4%). The clear lesson here is the critical importance of maintaining up-to-date offline backups. Fortunately, there are robust, enterprise-class, cloud-based backup solutions on the market to aid in this endeavor.

Section 2: Perceptions and Concerns

Other notable findings:

- Once again, China (74.0%) and Mexico (71.9%) are atop the list of countries affected by ransomware (see Figure 13), with newly added Spain (80%) in first position. Germany (39.2%), Japan (42.9%), and Australia (46.0%) round out the fortunate bottom three.
- Key industries affected by ransomware, in decreasing order of frequency, include: education (60.3%), telecom & technology (59.9%), manufacturing (59.7%), retail (50.6%), finance (50.4%), government (50.0%), and healthcare (44.0%).
- Mid-size enterprises with 5,000 to 9,999 employees (63.4%) are affected by ransomware the most, while smaller organizations with 500 to 999 employees (49.3%) are affected the least.

	Paid Ransom	Refused Ransom
Recovered data	49.4%	86.9%
Lost data	50.6%	13.1%

Table 2: Data recovery by ransomware victims.

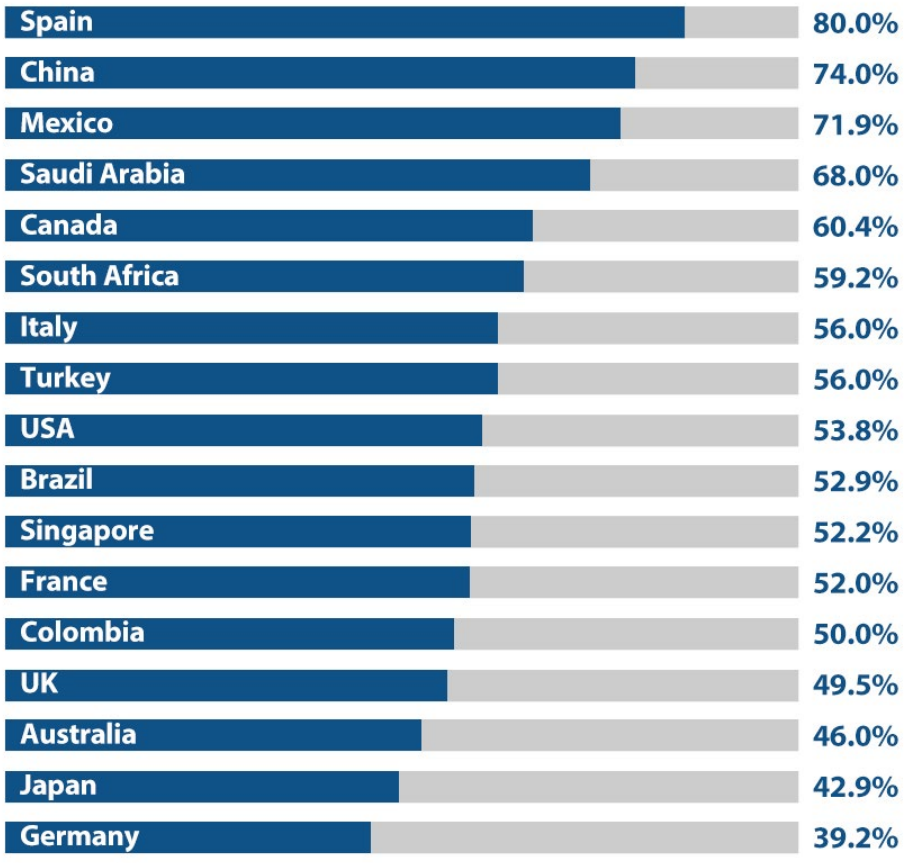


Figure 13: Percentage affected by ransomware in the past 12 months.

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=1,194)

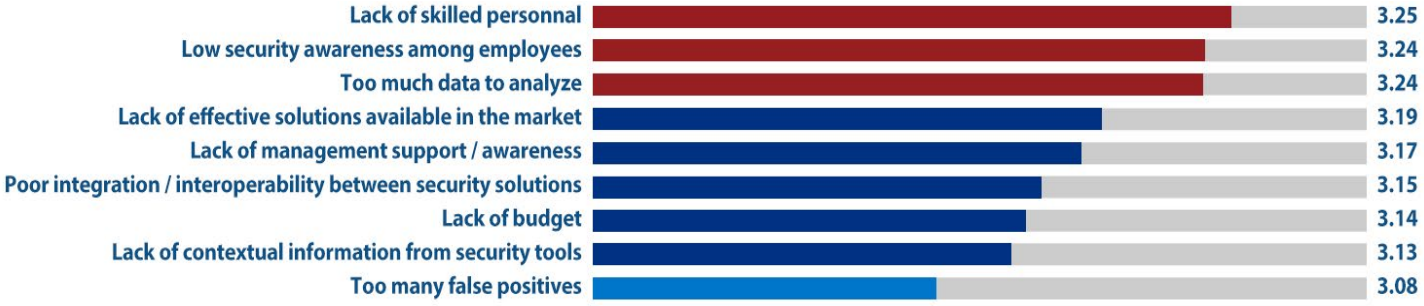


Figure 14: Inhibitors to establishing effective cyberthreat defenses.

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?

When we first asked the question in 2013 (for our 2014 CDR), we thought for sure that "lack of budget" would come out on top. We were shocked when it only came in at second place, right after "low security awareness among employees." But what's even more surprising is that "low security awareness among employees" remained the top concern among security professionals for the next three years – until this year (see Figure 14).

In 2018, there is a new king of security inhibitors – "lack of skilled personnel." But if you've been paying close attention to inhibitor rankings over the last four years, this shouldn't come as a surprise: 2014: fifth place; 2015: fourth place; 2016: third place; 2017: second place; 2018: first place.

This doesn't mean that "low security awareness among employees" is no longer of concern. Far from it. In fact, it was only nudged out of first position by one-hundredth of a point. Furthermore, you could say that there was a virtual three-way tie for first place, with "too much data to analyze" also one-hundredth of a point behind.

Stepping onto our proverbial soap box for a moment, we want to reiterate our shock and disappointment about IT security organizations' not doing enough to train company personnel about how to minimize cybersecurity risks through safe computing. (Hello? Is anyone listening? Bueller? Bueller?) Suffering from a shortage of high-quality security talent is completely understandable. But failing – year after year – to invest in your company's "human firewall" is both inexplicable and inexcusable. Okay, we've put away our soap box until next year.

"In 2018, there is a new king of security inhibitors – 'lack of skilled personnel.'"

Other notable findings:

- "Too many false positives" (ninth place) and "lack of contextual information from security tools" (eighth place) round out the inhibitors of least concern.
- While "lack of skilled personnel" has been rising as a security inhibitor, "lack of budget" has fallen – from second in 2014 to seventh in 2018. Clearly, having enough budget is no longer a leading concern.

As for the biggest upward mover year over year, "lack of effective solutions available in the market" holds that dubious honor, jumping five spots (and more than a tenth of rating point) into fourth position on the list.

Section 2: Perceptions and Concerns

This year, we created a new chart called the "Security Concern Index" (see Figure 15). We averaged together all of 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 things standing in the way of doing their jobs.

Although we've presented multiple pieces of evidence to suggest that IT security has finally stemmed the tide of successful cyberattacks, this doesn't mean that life is peachy keen. Far from it. In fact, overall concern for security inhibitors has risen steadily from 2.58 in 2014 to 3.18 in 2018 (on a five-point scale).

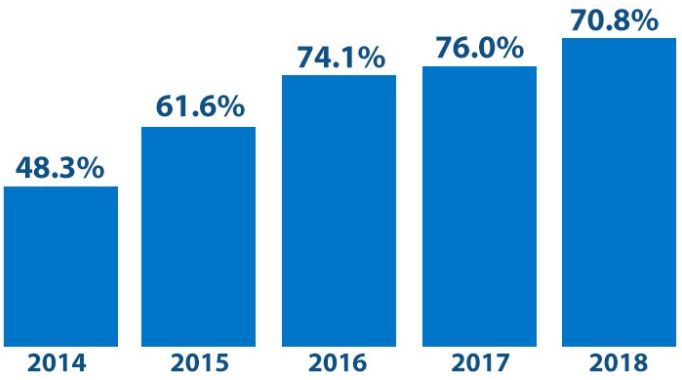


Figure 15: Security Concern Index, depicting average ratings among security inhibitors.

Section 2: Perceptions and Concerns

Cloud Security Challenges

Which of the following are your organization's most significant cloud security challenges? (Select all that apply.) (n=1,176)

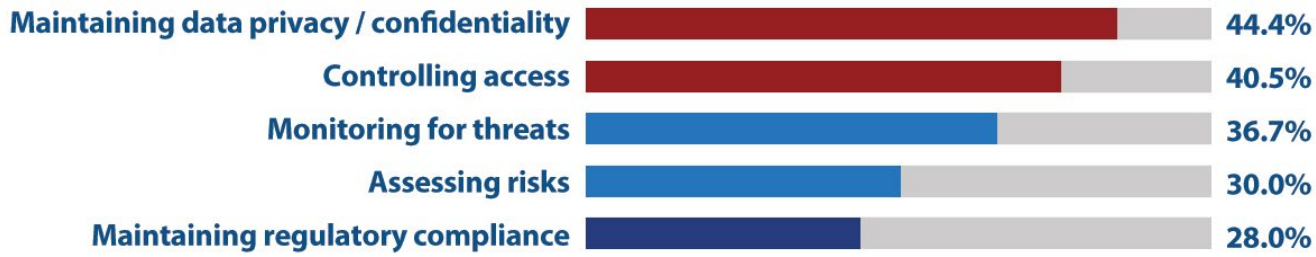


Figure 16: Cloud security challenges.

For the first time, this year we asked respondents to identify their cloud security challenges – if any. Anecdotally, we frequently hear security professionals express security concerns about their company's applications and data being migrated to the cloud. So, what are their concerns, specifically?

First, we learned that 91% of respondents acknowledged one or more cloud security concerns. So, security risks in the cloud are definitely a clear and present danger.

Second, we learned the hierarchy of their cloud security concerns (see Figure 16), with maintaining the privacy and confidentiality of data (44.4%) placed at the top of that list. Controlling access (40.5%) and monitoring for threats (36.7%) are next in line, followed by assessing risks (30.0%) and maintaining regulatory compliance (28.0%).

These findings present a double-edged sword. On one hand, they're headaches for enterprises. But on the other hand, they present compelling opportunities for security vendors – especially purveyors of CASBs, which are poised to address many of these concerns (see page 36).

"91% of respondents acknowledged one or more cloud security concerns."

Other notable findings:

- Results varied only slightly from a geographical perspective. Respondents from Colombia (100%) and Mexico (100%) express the most cloud security concerns, while respondents from Turkey (85.4%), Germany (86.1%), and Australia (87.2%) express the fewest.
- Results also varied slightly by industry. Respondents from the finance (94.8%) and telecom & technology (92.7%) verticals express the most cloud security concerns, while government (80.9%) express the fewest. Is that, perhaps, because federal, state, and local governments are apprehensive to embrace the cloud in the first place?
- Results varied insignificantly by organization size (i.e., employee count).

Section 2: Perceptions and Concerns

Vulnerability Patching Challenges

What is preventing your organization from patching systems more rapidly? (Select all that apply.) (n=1,162)

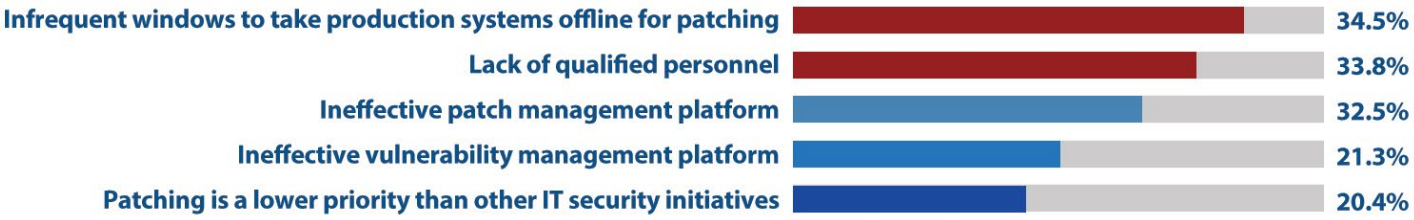


Figure 17: Vulnerability patching challenges.

"83.4% of organizations are experiencing patching challenges."

In 2015, Verizon's well-known (and highly respected) Data Breach Investigations Report (DBIR) indicated that "99.9% of the exploited vulnerabilities were compromised more than a year after the CVE was published." (See page 15 of the report if you'd like to check it out.) That statistic is both shocking and, frankly, embarrassing. It's something that has stuck out in our minds for the past three years.

IT analyst firms have reaffirmed in recent years the importance of regularly scanning for vulnerabilities and patching them. So, assuming enterprises have been listening (which, granted, could be a leap of faith), why does it take an entire year to deploy a stinkin' patch? Are IT security teams simply falling asleep at the wheel?

Well, we attempted to shed light on this mystery in this year's CDR. We essentially asked security professionals what, if anything, is standing in the way of patching systems more rapidly. The results are enlightening.

First, we learned that 83.4% of organizations are experiencing patching challenges. So, if your organization falls into this camp, don't feel badly.

Second, we learned that there is no single obstacle that is clearly to blame. It's actually a combination of five different factors (see Figure 17). Atop the list of patching inhibitors is having infrequent windows to take production systems offline for patching (34.5%). Offline systems, even when thoughtfully scheduled, can negatively impact revenue and/or employee productivity. Next is "lack of qualified personnel" (33.8%). We don't think we need to explain that further, as it's one of the recurring themes of this year's CDR.

"Ineffective patch management platform" (32.5%) and "ineffective vulnerability management platform" (21.3%) indicate room for product growth in the patching and vulnerability management industries, respectively. These stats should be a wake-up call for vendors in these segments, as their customers are screaming for innovation.

Other notable findings:

- Respondents from Australia (68.9%), Germany (71.8%), and Brazil (73.5%) note the fewest vulnerability patching challenges, while their counterparts in France (95.8%), China (94.0%), and Japan (93.6%) indicate the most.
- Respondents from the retail (77.5%) and education (78.3%) industries have a better handle on vulnerability patching than their telecom & technology (87.9%) and finance (85.8%) counterparts.
- There is little variance with regard to vulnerability patching challenges by organization size (i.e., employee count).

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=1,134)

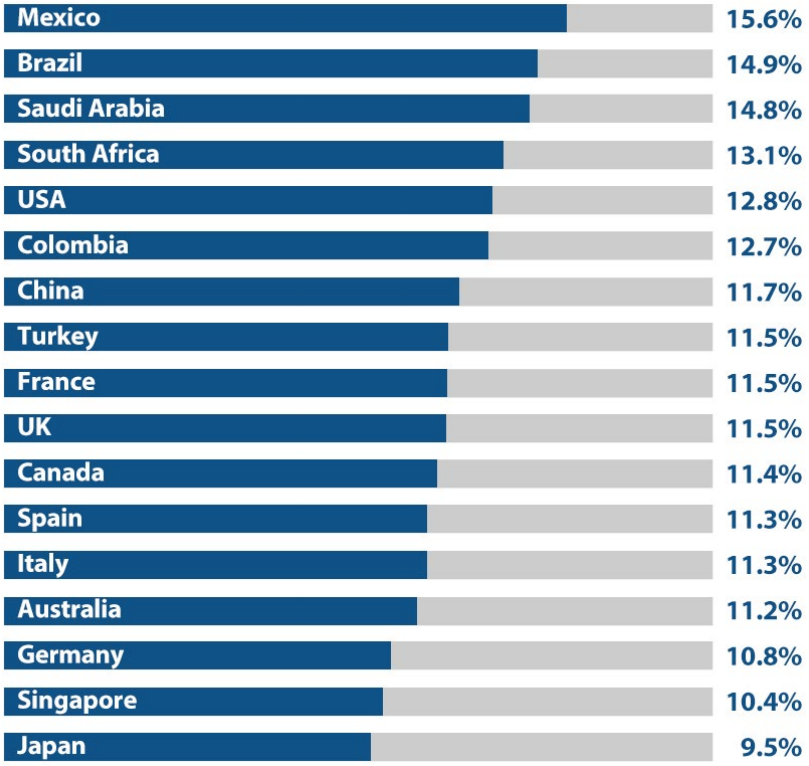


Figure 18: Percentage of IT budget allocated to security, by country.

As we've done for the past three years, we asked our IT security respondents to specify the percentage of their employers' overall IT budgets that is allocated to information security (e.g., products, services, personnel). But this year, rather than providing only ranges of responses to choose from (e.g., 6%-10%, 11%-15%, 16%-20%), we asked respondents to designate specific percentages, if known.

This approach enables us to calculate a mean percentage of IT security budget allocation – globally, by country, by industry, and by organization size – a practice we'll repeat moving forward. And it still allows us to group responses together into ranges so we can compare this year's results to those in previous years.

"The mean percentage of the IT budget that is allocated to information security is 12.1% globally."

Figure 19: Percentage of IT budget allocated to security, by industry

Section 3: Current and Future Investments

For the first time, we can state that the mean percentage of the IT budget that is allocated to information security is 12.1% globally. Figure 18 depicts mean security spending by country, Figure 19 by industry, and Figure 20 by organization size (i.e., employee count).

Figure 21 compares the percentage of organizations (globally) designating 11% or more of their overall IT budgets to information security for the past four years. As you can see, this figure has dropped for the first time in three years – from 58.4% in 2016, to 58.7% in 2017, falling to 51.3% in 2018 – perhaps an outcome of fewer successful cyberattacks felt last year (see Figure 1 on page 7).

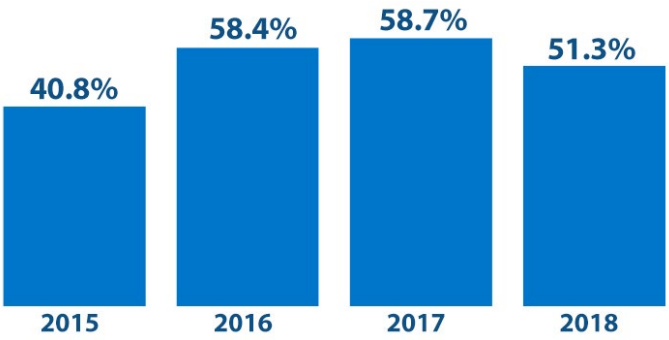


Figure 21: Percentage spending 11% or more on security.

Other notable findings:

- Respondents from the United States, on average, designate 13.1% of their IT budgets to information security, one full point above the global mean of 12.1%. Mexico (15.6%), Brazil (14.9%), and Saudi Arabia (14.8%) appear to allocate the most IT budget to security, while Japan (9.5%), Singapore (10.4%), and Germany (10.8%) allocate the least.
- Of the big 7 industries, telecom & technology (13.0%) and healthcare (12.4%) allocate the most IT budget to information security, while manufacturing (11.6%) and government (11.8%) allocate the least.
- It's clear that the larger the organization (i.e., the more employees), the bigger the security slice of the IT budget pie. Organizations with 500 to 999 employees allocate 11.1% of the IT budget to security (falling below the mean), while organizations with more than 25,000 employees allocate the most (13.4%).

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

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=1,160)

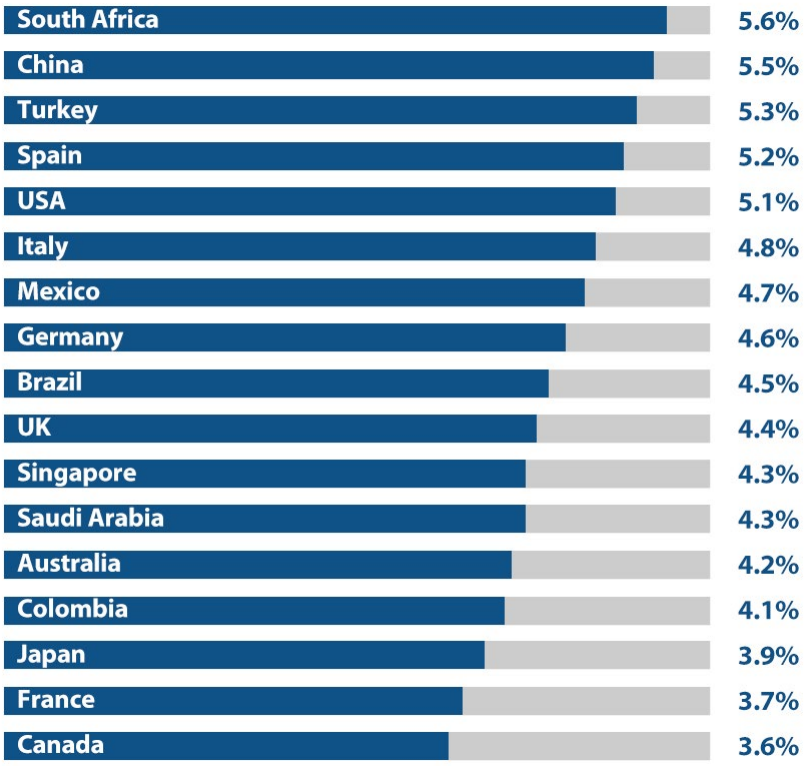


Figure 22: Mean security budget increase, by country.

This year, we took an approach similar to the one described in the last section. Rather than asking respondents to select a range of potential IT security budget changes (e.g., increase by 5-9%, decrease by less than 5%), we asked them to select the specific (positive or negative) budget change percentage for 2018, if known.

This approach enables us to calculate a mean IT security budget change percentage – globally, by country, by industry, and by organization size (i.e., employee count). But, of course, we can still group responses (e.g., all with budget increases) for comparison with results from prior years.

"The mean IT security budget change for 2018 is +4.7% globally."

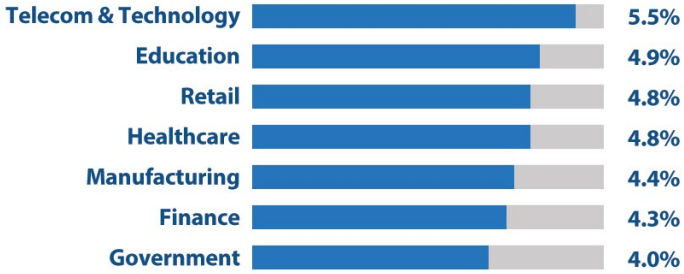


Figure 23: Mean security budget increase, by industry.

Section 3: Current and Future Investments

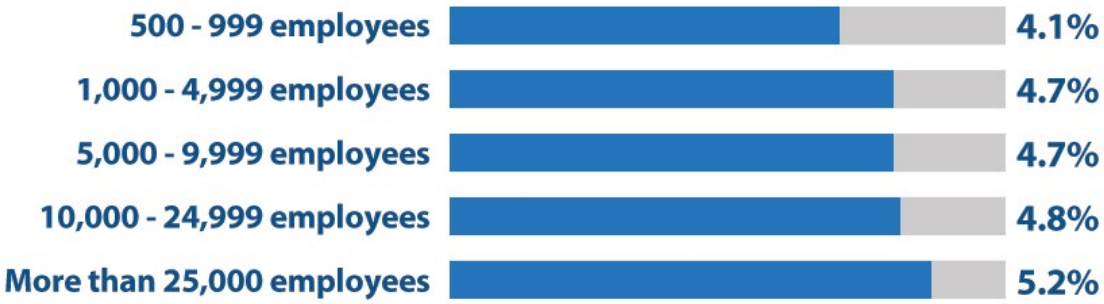


Figure 24: Mean security budget increase, by organization size.

For the first time, we can state that the mean IT security budget change for 2018 is +4.7% globally. Figure 22 depicts mean security budget increases by country, Figure 23 by industry, and Figure 24 by organization size (i.e., employee count). It's clear that IT security budgets for 2018 are going up across the board.

In the last section, enterprises saw a glimmer of hope – that the percentage of organizations allocating 11% or more of their overall IT budgets to security has fallen for the first time in three years (see Figure 21 on page 22). However, that does not mean that IT security budgets are on the decline. In fact, Figure 25 indicates that IT security budgets are healthier than ever, with a record 78.7% of organizations investing more in security in 2018.

The apparent conflict between these two findings (lower percentages of IT budget spent on security versus record IT security budget increases) can be explained by offsetting increases in overall IT spending. In other words, although the size of the security slice of the IT budget pie is declining, the pie is getting larger, resulting in a net increase in IT security spending for 2018.

Other notable findings:

- IT security budgets in the United States, on average, are rising by 5.1%, which is 0.4 percentage points higher than the 4.7% mean. The fastest-growing IT security budgets are from South Africa (5.6%), China (5.5%), and Turkey (5.3%), while the slowest-growing IT security budgets are from Canada (3.6%), France (3.7%), and Japan (3.9%).

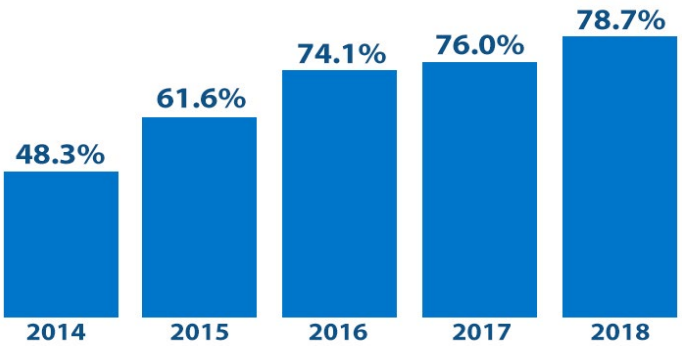


Figure 25: Percentage of organizations with rising security budgets.

- Of the big 7 industries, the fastest-growing IT security budgets are found in telecom & technology (5.5%) and education (4.9%), as opposed to slow-growing IT security budgets in government (4.0%) and finance (4.3%).
- Once again, it's clear that the larger the organization (i.e., the more employees), the greater the spending on security. IT security budgets from organizations with 500 to 999 employees are increasing by 4.1% in 2018, on average, while those from organizations with more than 25,000 employees are increasing by 5.2%.

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=1,167)

	Currently in use	Planned for acquisition	No plans
Network-based anti-virus (AV)	68.3%	22.7%	9.0%
Web application firewall (WAF)	66.3%	24.0%	9.7%
Intrusion detection / prevention system (IDS/IPS)	60.6%	29.0%	10.4%
Secure web gateway (SWG)	59.9%	27.0%	13.1%
Secure email gateway (SEG)	59.7%	29.0%	11.3%
Security information and event management (SIEM)	55.8%	28.2%	16.0%
Privileged account / access management (PAM)	55.4%	29.4%	15.2%
Denial of service (DoS/DDoS) prevention	55.3%	30.5%	14.2%
SSL/TLS decryption appliances / platform	55.0%	30.9%	14.1%
Security analytics / full-packet capture and analysis	54.3%	30.8%	14.9%
Data loss / leak prevention (DLP)	52.6%	33.4%	14.0%
Next-generation firewall (NGFW)	52.5%	35.9%	11.6%
Threat intelligence service	49.8%	34.2%	16.0%
Network behavior analysis (NBA) / NetFlow analysis	49.3%	35.0%	15.7%
Advanced malware analysis / sandboxing	46.7%	40.8%	12.5%
User and entity behavior analytics (UEBA)	45.8%	34.7%	19.5%
Deception technology / distributed honeypots	39.9%	35.9%	24.2%

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

The next four sections are structured similarly. In each section, we asked respondents to indicate whether each security technology is currently in use, whether it is planned for acquisition, or whether they have no plans for deploying that specific technology. (We always allow for, and subsequently weed out, "don't know" responses as we never want respondents to guess. That's why our sample sizes vary by question.)

In this section, we presented respondents with a list of popular network security technologies. ("SSL/TLS decryption appliances/platform" is new to this year's list.) Table 3 depicts this year's deployment status results. 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."

Of the 17 choices presented, network-based antivirus (68.3%), web application firewall (66.3%), and intrusion detection/prevention system (60.6%) round out the top three most widely deployed network security technologies. This makes complete sense as these technologies, and the handful that

Section 3: Current and Future Investments

follow them in Table 3, have been around for years and are viewed as staples of a sensible network security strategy.

Perhaps what's more interesting to note are those network security technologies with the highest planned acquisition rates for 2018. They include: advanced malware analysis / sandboxing (40.8%), NGFW (35.9%), deception technology / distributed honeypots (35.9%), and network behavior analysis (NBA) / NetFlow analysis (35.0%).

"The biggest winners in 2018 are web application firewall (WAF), deception technology/distributed honeypots, and threat intelligence services."

On the whole, this year's results are remarkably similar to those from 2017 – which is always comforting to a researcher. All "currently in use," "planned for acquisition," and "no plans" results are within a few percentage points of last year's results – with one exception. The "currently in use" percentage for advanced malware analysis / sandboxing dropped from 66.9% in 2017 to 46.7% in 2018. The "planned for acquisition" percentage for that same technology increased from 24.4% in 2017 to 40.8% in 2018. But why?

Our only explanation is that the consensus prediction among security research analysts has come to fruition – network-based sandboxing is no longer a standalone product, but rather a feature in other network security products. Companies that invested in hardware-based sandboxing appliances nearing end-of-life are now in the midst of replacing them with cloud-based sandboxing alternatives. Assuming this is the case, we expect cloud-based sandboxing adoption to increase in 2018 – which is good news for NGFW, SEG, and SWG vendors, in particular.

Other notable findings:

- The biggest winners in 2018 (i.e., technologies with the largest increases in adoption) are web application firewall (WAF), deception technology/distributed honeypots, and threat intelligence services. Adoption in all three of these technologies (coincidentally) increased 4.3% last year.
- The biggest losers in 2018 (i.e., technologies with the largest decreases in adoption), excluding the 20-point drop in dedicated sandboxing solutions, are data loss/leak prevention (DLP), secure email gateway, and secure web gateway vendors, whose adoption rates fell 4.6%, 3.3%, and 2.3%, respectively.
- The highest "no plans" results correspond to deception technology/distributed honeypots (24.2%) and UEBA technologies. We expect these percentages to fall in next year's report as associated vendors succeed in getting the word out regarding the value propositions of these promising network security technologies.

Every single network security technology on this list plays an important role in a sensible defense-in-depth strategy. With an average adoption rate of 54.5%, there is clearly plenty of opportunity for network security vendors to expand in their respective markets.

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=1,179)

	Currently in use	Planned for acquisition	No plans
Basic anti-virus / anti-malware (threat signatures)	67.9%	27.0%	5.1%
Disk encryption	62.8%	25.6%	11.6%
Advanced anti-virus / anti-malware (machine learning, behavior monitoring, sandboxing)	60.2%	28.5%	11.3%
Data loss / leak prevention (DLP)	57.4%	32.4%	10.2%
Application control (whitelist / blacklist)	56.6%	30.6%	12.8%
Self-remediation for infected endpoints	53.3%	33.7%	13.0%
Digital forensics / incident resolution	49.7%	32.7%	17.6%
Containerization / micro-virtualization	49.3%	34.6%	16.1%
Deception technology / honeypot	47.3%	32.2%	20.5%

Table 4: 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 4). Once again, percentages in dark blue correspond to a higher frequency of adoption and/or acquisition plans, while percentages in light blue correspond to a lower frequency.

Of the nine options presented (same list as last year), signature -based basic antivirus/anti-malware (67.9%) is the most commonly deployed endpoint security technology, which has been the case since 2014. No surprise there, since AV has been around since the Stone Age – or so it seems. The next most widely used endpoint technologies are disk encryption (62.8%) and advanced antivirus/anti-malware (60.2%). Also no surprise, as they joined basic antivirus/anti-malware in the top three in each of the last two years.

"The hottest endpoint security technology planned for acquisition for the second consecutive year is containerization/micro-virtualization."

The hottest endpoint security technology planned for acquisition for the second consecutive year is containerization/micro-virtualization (34.6%), with adoption already ticking up from 40.5% last year to 49.3% this year. For those unfamiliar, this technology enables users to open content accessed via the Internet within the safety of a lightweight container/virtual machine (VM). Once the user closes the content, the container/VM vanishes, leaving the host operating system

Section 3: Current and Future Investments

completely unaffected. Next in line for acquisition are self-remediation for infected endpoints (33.7%) and digital forensics/incident resolution (32.7%).

This year's "head-scratching award" goes to basic anti-virus/anti-malware, already recognized as the most widely deployed endpoint security technology year after year. What's perplexing is that while adoption fell from 79.8% to 67.9%, its "planned for acquisition" rate increased from 14.3% to 27.0% over that same period. In other words, why would adoption fall 11.9% while acquisition plans simultaneously increase by 12.7%?

Perhaps there is confusion in the market, spawned by the impending convergence of existing endpoint protection platform (EPP) offerings with leading-edge endpoint detection and response (EDR) solutions. Although EPP offerings incorporate a full suite of endpoint protection capabilities, they rely heavily on antivirus (AV) signatures to block known threats while EDR solutions incorporate machine learning and/or artificial intelligence to detect emerging, unknown threats.

At this point, virtually all organizations have reached the foregone conclusion that leveraging AV signatures alone to detect cyberthreats is an exercise in futility – and a costly mistake. As EPP and EDR technologies continue to converge, organizations will realize the best of both worlds – using AV signatures to block basic, known threats while preserving computing resources for AI / machine learning algorithms to detect sophisticated, unknown threats.

Anyway, that's our story and we're sticking to it.

Section 3: Current and Future Investments

Mobile Security Deployment Status

Which of the following mobile security technologies are currently in use or planned for acquisition (within 12 months) by your organization to guard mobile devices (smartphones and tablets), and corporate data accessed by mobile devices, against cyberthreats? (n=1,160)

	Currently in use	Planned for acquisition	No plans
Mobile device anti-virus / anti-malware	59.9%	27.0%	13.1%
VPN to on-premises security gateway	59.0%	27.5%	13.5%
Mobile device file / data encryption	57.5%	29.0%	13.5%
VPN to cloud-based security gateway	55.8%	30.9%	13.3%
Mobile device / application management (MDM/MAM)	53.8%	30.9%	15.3%
Network access control (NAC)	53.1%	31.3%	15.6%
Virtual desktop infrastructure (VDI)	53.0%	30.3%	16.7%
Containerization / micro-virtualization	41.5%	38.1%	20.4%

Table 5: Mobile security technologies in use and planned for acquisition.

Next up is mobile security (see Table 5). Once again, percentages in dark blue correspond to a higher frequency of adoption and/or acquisition plans, while percentages in light blue correspond to a lower frequency.

Of the eight options presented (same as last year), mobile device anti-virus/anti-malware (59.9%) is the most commonly deployed mobile security technology, as it was in both 2016 and 2017. No real surprise, as this was one of the first mobile security technologies deployed to protect data accessed on smartphones and tablets. The next two most widely deployed mobile technologies are VPN to on-premises security gateway (59.0%) and mobile device file/data encryption (57.5%).

Overall, the results are pretty similar to last year's. The only change worth noting is the decrease in mobile device/application management (MDM/MAM) adoption, which dropped by 6.9% over the past year – from 60.7% to 53.8%. Perhaps this can be explained by the increased adoption by larger organizations of enterprise mobility management (EMM) platforms, which (perhaps too transparently) incorporate MDM and MAM as underlying core technologies.

"Containerization/micro-virtualization is, once again, at the top of this year's shopping list."

The hottest mobile security technology planned for acquisition in 2018 has not changed from last year. Containerization/micro-virtualization (38.1%) is, once again, at the top of this year's shopping list. Next in line are network access control (31.3%) and both MDM/MAM and "VPN to cloud-based security gateway" (tied at 30.9%).

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=1,045)

	Currently in use	Planned for acquisition	No plans
Web application firewall (WAF)	66.1%	23.3%	10.6%
Database firewall	64.6%	24.7%	10.7%
Database encryption / tokenization	56.9%	28.6%	14.5%
Database activity monitoring (DAM)	54.8%	30.9%	14.3%
File integrity / activity monitoring (FIM/FAM)	53.6%	30.8%	15.6%
Runtime application self-protection (RASP)	53.6%	30.2%	16.2%
Static/dynamic/interactive application security testing (SAST/DAST/IAST)	50.9%	31.1%	18.0%
Container security tools / platform	49.6%	34.8%	15.6%
Deception technology / distributed honeypots	49.2%	30.9%	19.9%
Cloud access security broker (CASB)	48.8%	33.7%	17.5%
Application delivery controller (ADC)	48.3%	32.5%	19.2%
API gateway	45.1%	40.7%	14.2%

Table 6: Application and data security technologies in use and planned for acquisition.

Our fourth and final area for measuring security technology adoption is application and data security. Here we evaluate adoption of 12 security technologies (see Table 6), including two new entrants this year – container security tools/platform and API gateway. As usual, percentages in dark blue correspond to a higher frequency of adoption and/or acquisition plans, while percentages in light blue correspond to a lower frequency.

Enterprises continue to invest heavily in technologies to guard the confidentiality, integrity, and availability of sensitive data and the applications used to access it. At the top of the list is web application firewall (WAF) technology (66.1%), which nudged out last year's leader, database firewall technology (64.6%). Next in line is database encryption/tokenization (56.9%) followed by database activity monitoring (54.8%).

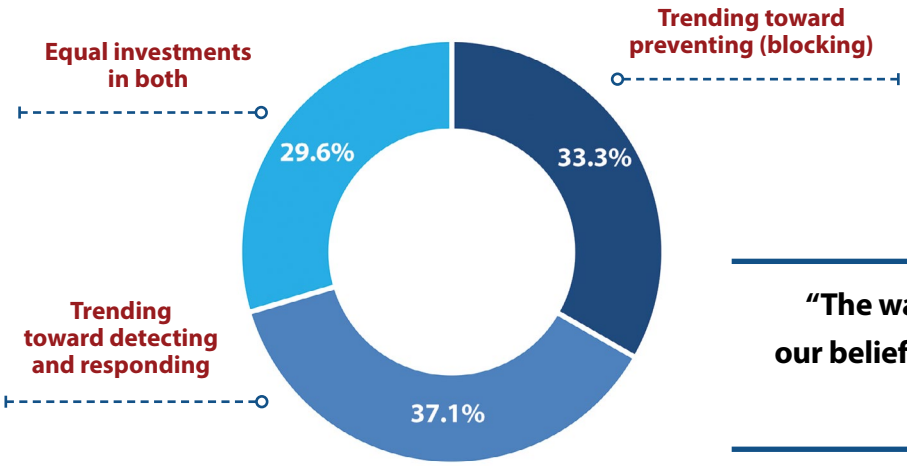
The hottest application and data security technology planned for acquisition in 2018 is a new entrant to the list – API gateway (40.7%) – which achieved the highest "planned for acquisition" percentage of any security technology referenced in this year's CDR. The next-highest technologies on the planned for acquisition list are container security tools/platform (also new this year) and CASB at 34.8% and 33.7%, respectively

The biggest year-over-year increase in adoption goes to deception technology/distributed honeypots, which increased 3.5%, from 45.7% in 2017 to 49.2% in 2018. The biggest one-year drop in adoption goes to application delivery controller (ADC) technology, which fell 10.4%, from 58.7% in 2017 to 48.3% in 2018. This sizable decrease may be the result of cloud-native applications reducing the need for traditional ADC offerings.

Section 3: Current and Future Investments

Cyberthreat Detection vs. Prevention Investments

Are your organization's recent IT security investments trending in favor of preventing (blocking) or detecting and responding to cyberthreats? (n=1,163)



"The way we see it, the results support our belief that the prevention vs. detection debate is a bit silly."

Figure 26: Cyberthreat detection versus prevention spending trends.

The question of whether new investments should focus more on the prevention of cyberthreats or on detecting and responding to them has been a significant source of debate for the past handful of years – especially among the vendor community. The arguments go something like this:

For prevention: Because they actually block cyberthreats, prevention solutions have the advantage of avoiding not only the intended malicious outcomes, but also all the resource-intensive efforts associated with investigation, remediation, and recovery.

For detection and response: The ever-increasing sophistication of cyberthreats, rise of targeted attacks, and dissolution of a well-defined perimeter all but guarantees some number of threats will gain access to the enterprise network. As a result, it is essential that enterprise defenses include a robust set of capabilities to monitor for, identify, correlate, investigate, and respond to suspicious activities that may in fact be real threats.

Please, hold off on the hate mail. We're the first to admit that this treatment grossly over-simplifies things. However, we also believe it captures the essence of the topic, without having to drag everyone through a lot of muddy details. Besides, what really matters here is what our respondents had to say on the subject. To that end, we asked them to let us know whether their employers' recent IT security investments were trending in favor of "preventing (blocking) or detecting and responding to cyberthreats."

Turning to Figure 26 for the results, we see a roughly even, three-way split among those favoring prevention (33.3%), detection and response (37.1%), and both (29.6%). One observation: the slight edge garnered by detection and response could be the result of organizations having under-invested in this area in the past, at least on relative basis.

On the surface, this outcome might seem anticlimactic. The way we see it, however, is that the results support our belief that the prevention vs. detection debate is a bit silly. It is important that organizations invest in both prevention and detection as part of a sensible defense-in-depth strategy.

Section 4: Practices and Strategies

Cloud Deployment Practices for Security

Are the following security technologies deployed on-premises (i.e., on site), in the cloud, or both? (n=1,114)

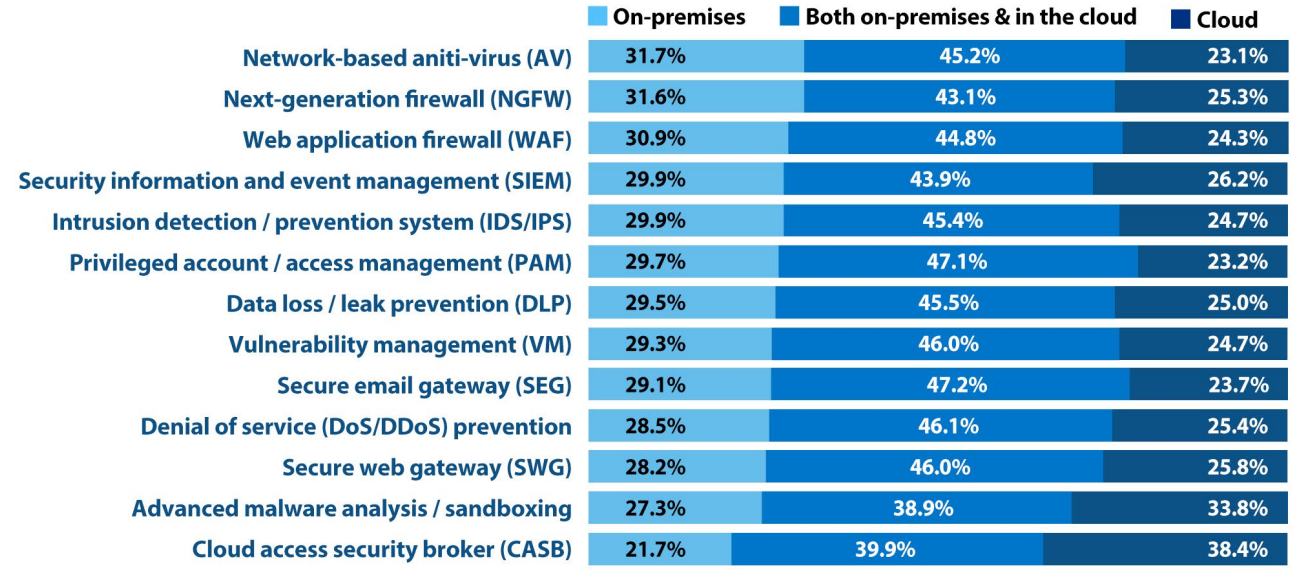


Figure 27: Common security technology deployment practices.

The time-to-market, scalability, and overall agility advantages of cloud computing/services are widely accepted, as evidenced by the steadily growing adoption of SaaS and IaaS offerings. To understand the extent this trend applies to cyber-threat defenses, this year we asked participants to indicate where/how their organizations have deployed various security technologies: on premises, in the cloud, or both.

A first peek at the data suggests that on premises is still the dominant deployment option, at least on average (see Figure 27). However, a more accurate statement of the findings is that "both" leads the way, across the board. What's not clear about this result is whether it is driven by organizations employing a different option for different sites or different use cases, or if it's because the corresponding offerings involve a hybrid approach (i.e., one that combines on-premises components with in-the-cloud components and/or management and operational support). For what it's worth, our gut says it's more of the latter than the former, but we'll need to dig a bit deeper next year to back that up.

What's clear, in any case, is that cloud deployment and delivery have made significant in-roads in cybersecurity – despite the inherent sensitivity that surrounds this particular domain/

"Cloud deployment and delivery have made significant in-roads in cybersecurity."

discipline of IT and the accompanying predisposition to "keep it in house." There's no doubt, at least in our minds, that the prevailing shortage of skilled IT security personnel is a major factor in this development (see page 12).

Other notable findings:

- Core perimeter defenses, including network AV and NGFWs, are the most likely to be deployed on premises/ kept in house.
- CASBs and advanced malware analysis/sandbox technologies are the least likely to be deployed on premises only, and as a result, are leading the way for cloud-based delivery.
- Following not far behind with relatively high rate of cloud-only deployment is security information and event management (SIEM), a result that mirrors the growing popularity of managed detection and response (MDR) and SOC-as-a-service offerings.

Section 4: Practices and Strategies

SSL/TLS Decryption Practices

Which statement best describes your organization's approach to decrypting SSL/TLS traffic so that it can be inspected for cyberthreats? (n=1,140)

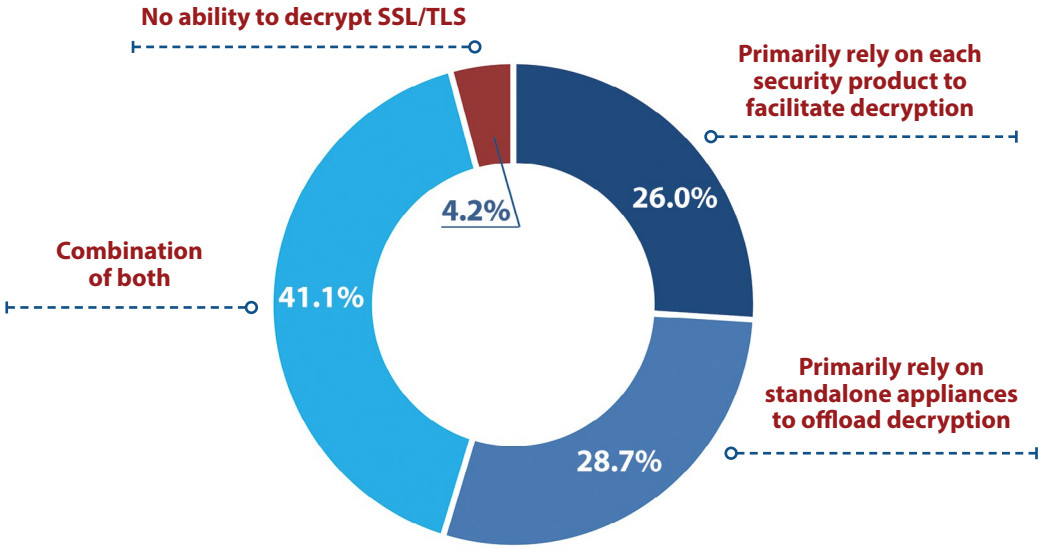


Figure 28: Approaches for decrypting and inspecting SSL/TLS-encrypted network traffic.

A key finding from the 2016 CDR (page 12) was that over half of respondents (52%) only somewhat agreed their organizations had the necessary tools to inspect SSL-encrypted traffic. Fast forward two years, and the data suggests there has been marked improvement on this front, with only 4.2% now indicating their organization lacks the ability to decrypt SSL/TLS-encrypted traffic so that it can be inspected for cyberthreats (see Figure 28).

"Fast forward two years, and the data suggests there has been marked improvement, with only 4.2% now indicating their organization lacks the ability to decrypt SSL/TLS-encrypted traffic."

As for how decryption is being accomplished, just over a quarter (26.0%) of respondents' organizations are relying exclusively on the native capabilities incorporated in the tools that are doing the inspection. More interesting, though, is that nearly seven out of 10 are using standalone decryption appliances, at least to some extent. This result suggests a strong understanding in the market of the benefits of standalone appliances and their more sophisticated cousins, the so-called decryption/visibility platforms – not the least of which are improved performance, reduced cost and complexity, and better adaptability of the inspection and enforcement infrastructure from which decryption responsibilities are being offloaded.

Digging into the demographic breakdowns, the data also shows:

- Although small organizations (500 to 999 employees) have the highest response rate for lacking the ability to decrypt SSL/TLS network traffic (6.1%), on an absolute basis they are only incrementally below the average (4.2%) in this area.
- Education and government organizations are the most likely to lack the ability to decrypt SSL/TLS, each with a response rate of approximately 10%.
- The telecom & technology vertical exhibited the greatest reliance on native decryption capabilities, with 36% of associated respondents indicating exclusive use of that approach.

Section 4: Practices and Strategies

Threat Intelligence Practices

Select the following reasons your organization has integrated commercial and/or open source threat intelligence into your existing security infrastructure. (Select all that apply.) (n=1,162)

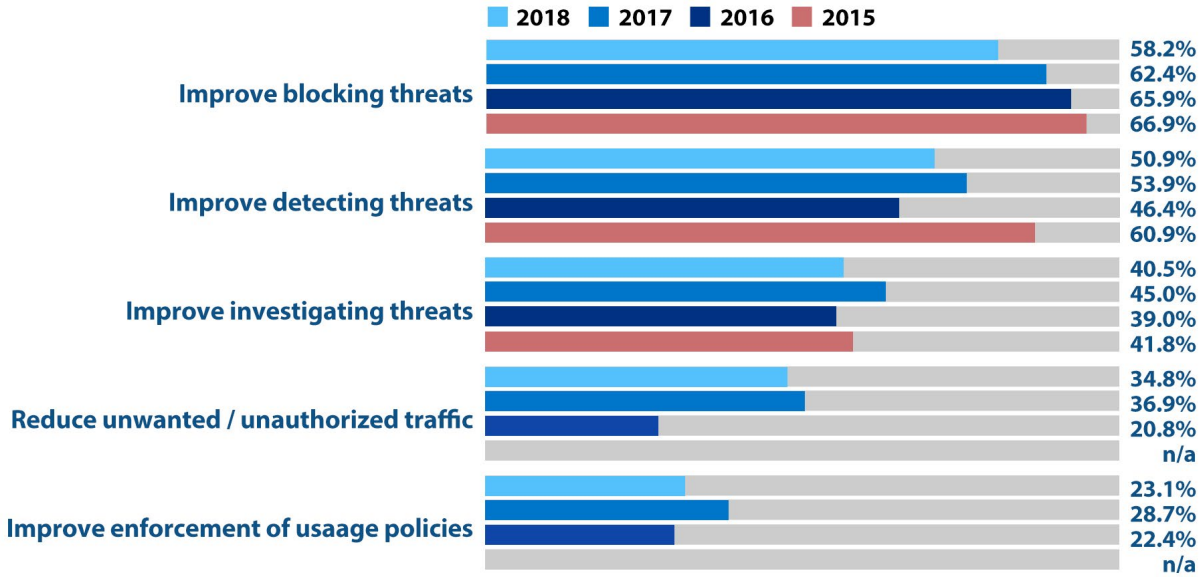


Figure 29: How threat intelligence is being leveraged.

Year after year, when we ask respondents the reasons why their organizations are taking advantage of supplemental (i.e., third-party) threat intelligence sources/services in their environments, the top-line result is the same (see Figure 29): to improve their ability to block threats (58.2%). And year after year, we continue to wonder when everyone's going to realize the benefits of a mature threat intelligence program, where this invaluable resource is used more thoroughly, including for proactive threat hunting and strategic purposes like informing long-term security strategy and technology investment decisions.

For the most part – with half or fewer using threat intelligence to improve threat detection capabilities (50.9%), improve threat investigation capabilities (40.5%), or help keep unwanted traffic off the network (34.8%) – we continue to wonder this same thing. But maybe we shouldn't. Let's face it, using threat intelligence to deliver better threat blocking is not only the "quick win" use case, it's also, arguably, the use case with the greatest bang for the buck. After all, stopping threats outright eliminates the need for a whole bucket of downstream activities, including detection, investigation, and remediation. So, better blocking belongs at the top of the list, period.

"Let's face it, using threat intelligence to deliver better threat blocking is the use case with the greatest bang for the buck."

What continues to vex us, though, is that the response rates for the other use cases are remaining stagnant (or even retreating). But that finding is true of all the use cases, including blocking. This leads us to the possible explanation that interest in supplemental sources of threat intelligence is waning, at least relative to what organizations already get from their security product vendors – another hypothesis we'll need to test out in the future.

In the meanwhile, one final observation from the data for this question: improving threat detection capabilities was selected as the top use case by both US-based respondents (58.5%) and those from large enterprises (i.e., more than 25,000 employees).

Section 4: Practices and Strategies

User and Entity Behavior Analytics Practices

Select the following reasons your organization operates user and entity behavior analytics (UEBA) technology. (Select all that apply.) (n=1,150)

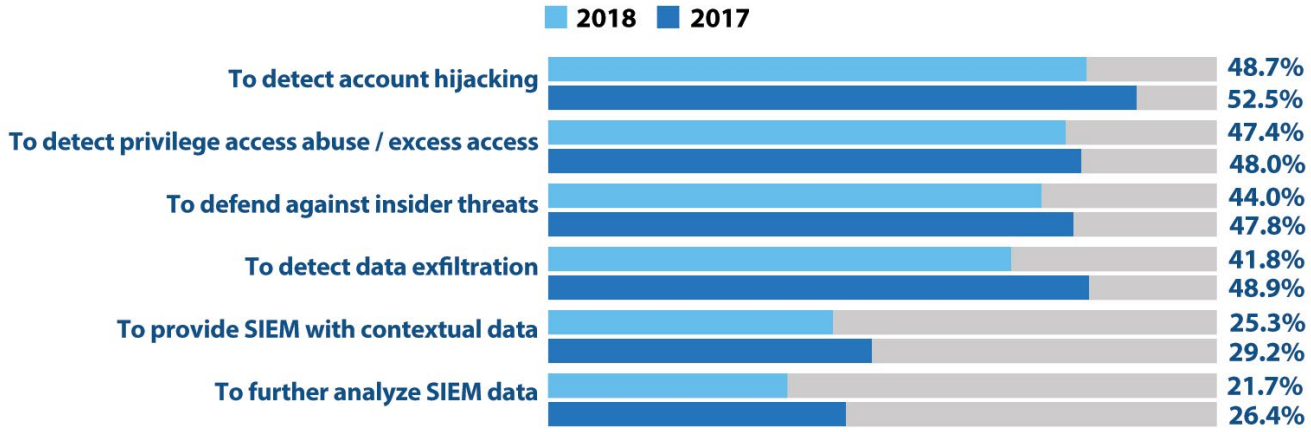


Figure 30: How UEBA is being leveraged.

User and entity behavior analytics continues to be a hot-ticket item on the planned acquisitions list for organizations in the coming year (see Table 3 on page 25). Thus, we once again sought to better understand which use cases are most responsible for the steadily growing interest in this no-longer-emerging-but-now-nearly-mainstream technology.

"UEBA leaders are working to more fully deliver on the long-promised value propositions of SIEMs."

For the second consecutive year, our results show a tight cluster (see Figure 30), with the use of UEBA for detecting account hijacking (48.7%) slightly edging out detecting privilege access abuse (47.4%) and defending against insider threats (44.0%). Falling in order of importance from its second-place position last year to fourth place, is the use case of detecting data exfiltration (41.8%). Overall, this re-ordering makes sense to us. Organizations, in general, are best served by thwarting threats sooner rather than later in their lifecycle – in other words, before reaching the data exfiltration phase.

As for the battle between SIEMs and UEBA to determine which becomes the favored, top-level security operations tool and which operates more as another data source to the other, the jury is apparently still out. Once again, the data shows only modest uptake of both related use cases, suggesting that most organizations are continuing to operate their SIEM and UEBA solutions independently. Another, more probable explanation, however, is that these technologies are converging. Ongoing market activities certainly back this position, as we're regularly seeing established SIEM players add UEBA capabilities to their solutions, while UEBA leaders are working to more fully deliver on the long-promised value propositions of SIEMs.

Returning to the data:

- For respondents from China (70.0%) and South Africa (62.0%), addressing the insider threat problem is by far the most significant driver for UEBA investments, while for Japanese respondents (54.3%), detecting data exfiltration tops the charts.
- Our healthcare respondents (50.6%) share the concern for insider threats, while for those in the manufacturing sector (54.2%) it's more about tackling data exfiltration challenges.
- It appears that medium-size organizations (5,000 to 9,999 employees), in particular, are struggling with the insider threat problem, as 47.3% of respondents from that demographic cited detecting insider threats as the top use case for UEBA.

Section 4: Practices and Strategies

Cloud Access Security Broker Practices

Select the reasons your organization operates cloud access security broker (CASB) technology. (Select all that apply.) (n=1,146)

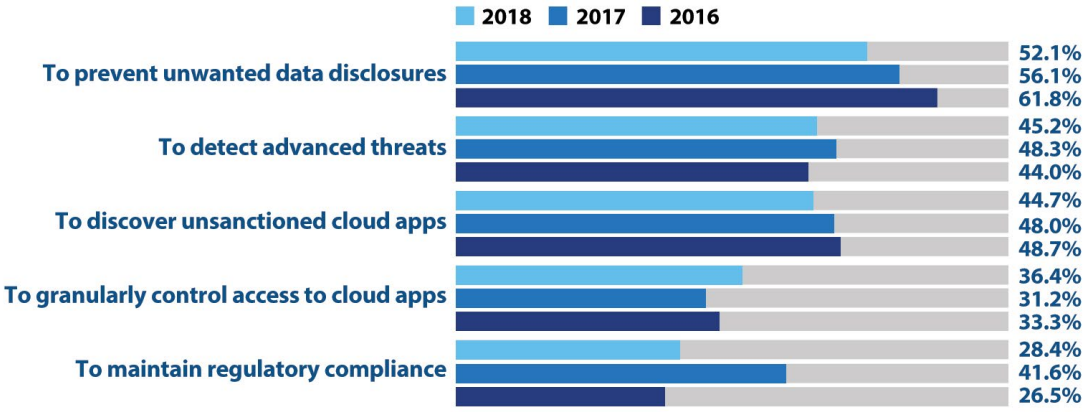


Figure 31: How cloud access security brokers are being leveraged.

With everything they've got going for them, there's good reason to expect CASBs will, one day, rival network firewalls and endpoint anti-malware software as the most widely deployed security technologies. The accelerating adoption of cloud services, continued inconsistency in the breadth and depth of native security capabilities offered by associated providers, and the rich feature sets and flexibility of leading CASBs are all points in their favor and, undoubtedly, major contributors to the excellent traction they continue to exhibit in the market (see Table 6 on page 30).

As the Swiss Army knives of cloud application and data protection, leading CASB solutions are capable of providing everything from visibility into shadow IT (employee use of unsanctioned applications) and cloud application usage patterns to comprehensive access control, data protection, threat prevention, and even compliance support. Of course, the availability of a bunch of capabilities doesn't mean they're all going to be used, or valued, to the same degree.

For the third year in a row, preventing unwanted data disclosures was the most common reason selected by respondents (52.1%) for their organization's investment in CASB technology (see Figure 31). Cited progressively less often and, therefore, presumably less important, were the need to detect advanced threats plaguing cloud services (45.2%), discover use of unsanctioned applications (44.7%), and granularly control access to cloud services (36.4%).

"For the third year in a row, preventing unwanted data disclosures was the most common reason selected by respondents."

Related observations:

- For respondents from Mexico (56.3%) and the United Kingdom (52.6%), discovering unsanctioned cloud apps is the most significant driver for CASB investments, while those from a handful of countries (Brazil, Colombia, Saudi Arabia, and Turkey) consider detection of advanced threats to be the top objective.
- Our retail respondents (57.3%) share the concern for discovering unsanctioned cloud apps, while those from the rest of the big 7 industries follow the order shown in the figure.
- There was very little variation in the results by size of organization, with the lone exception being respondents from very small organizations (500 to 999 employees), who trail the rest of the field when it comes to regulatory compliance as a reason for investing in a CASB solution (23.1% vs. 30%).

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=1,151)

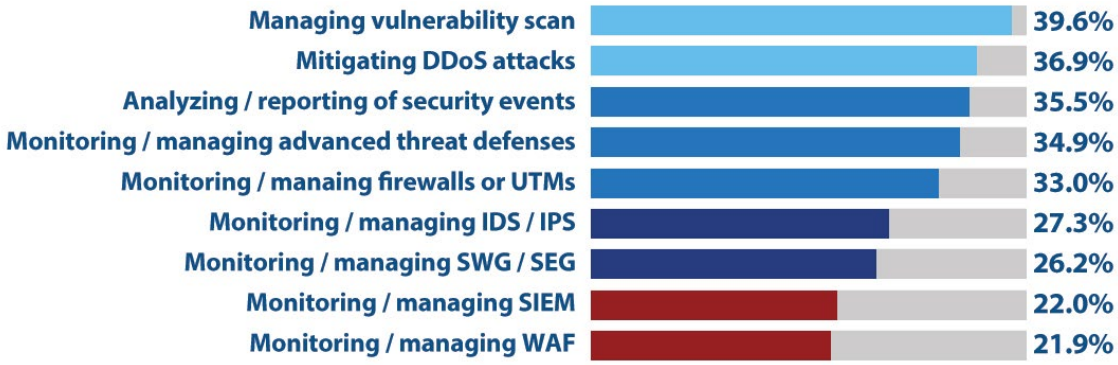


Figure 32: How managed security service providers are being leveraged.

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 – nearly nine in 10 according to our data – turning to MSSPs to pick up part of the load."

With so much on their plates, it's not surprising to see so many organizations – nearly 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 unload, our data shows vulnerability scanning (39.6%), DDoS mitigation (36.9%) and event analysis/reporting (35.5%) are leading the way (see Figure 32). At the other end of the spectrum, monitoring and managing web application firewalls (21.9%) 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 (35.5%), the similar-sounding entry of monitoring/managing one's SIEM didn't fare as well (22.0%). Our takeaway here is that what matters most to buyers is less the specific technology being employed, and more the functions/capabilities being delivered.

Other notable findings:

- "Monitoring / managing advanced threat defense technologies" is the top function for which respondents from China (56.0%) and Italy (40.4%) indicate their organizations utilize MSSPs.
- "Mitigating DDoS attacks" was the top function for using MSSPs selected by respondents from both the largest (> 25,000 employees) and smallest organizations (500 to 999 employees), with response rates of 43.8% and 39.9% respectively.
- With an overall usage rate of 93.8%, medium-size organizations (5,000 to 9,999 employees) are the sweet spot for MSSPs, while the smallest organizations (500 to 999 employees), somewhat surprisingly, trail the field at 82.8%.

The Road Ahead

This year's survey results indicate a "balancing of the scales" – at least to some extent. Sure, enterprise security teams still have plenty of gaps to shore up in their defenses. For example:

- Mobile devices (smartphones and tablets), perennially designated as the weakest link in most organizations' defenses, have now been joined by containers (see Figure 5 on page 9).
- Building security into applications in the first place and reducing their attack surface are not exactly strong suits for today's organizations (see Figure 6 on page 10).
- Less than a third of respondents are confident their organization's investment in cyberthreat hunting solutions is sufficient to enable effective detection of threats missed by other countermeasures (see Figure 7 on page 11).

But there are also a handful of signs that the patient is on the road to recovery – or, at least, in stable condition:

- For the first time in four years, there was a drop in the percentage of respondents' organizations that were hit by at least one successful cyberattack in the preceding year. In addition, there was a year-over-year decline in those being victimized six or more times (see Figure 1 on page 7).
- For the first time in four years, there was a drop in the Threat Concern Index, which measures the weighted concern across 10 classes of cyberthreats plaguing today's enterprises (see Figure 11 on page 14).
- For the first time in three years (i.e., all the years for which we have data), there was a drop in the percentage of respondents' organizations that are spending 11% or more of their IT budget on information security (see Figure 21 on page 22).

Looking beyond the scope of this year's survey, here are some key areas where we believe additional/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.

Micro-segmentation. For many of today's computing environments – be they physical, virtual, or hybrid – the unfortunate reality is that once a threat gets past perimeter defenses, there are few controls to limit lateral traversal within the network. Sure, internal firewalling has always been an option. But its success has been limited as cost, complexity, and rigidity quickly become gating factors. Micro-segmentation promises much-needed relief on this front by enabling organizations to logically divide their environments into highly granular segments – down to the level of individual workloads – each with its own set of enforced security policies.

Of course, the devil is in the details. The first stop for enterprises turning to micro-segmentation to limit the impact of initially successful breaches is selecting the solution model that best aligns with the architecture and management/operation of their computing environment. Core choices include native (i.e., part of your primary virtualization/cloud platform of choice), traditional (i.e., a combination of physical and virtual firewalls), and overlay (i.e., agents and existing enforcement points coordinated via a sophisticated policy engine) – each with its own set of pros and cons (of course).

A few more key criteria to consider:

- **Scope of coverage** – does it work (ideally seamlessly) for all of your virtual, cloud, and physical infrastructure?
- **Manageability** – how easy/hard is it to visualize your infrastructure/environment and then create, test, and maintain a highly granular set of security policies?
- **Automation** – to what extent are policies and their enforcement automatically pushed out, and do they automatically "follow" workloads when they move?
- **Intelligent adaptability** – to what extent are policies automatically adjusted in response to changes in the computing environment?

Next-generation SIEMs. Traditional SIEMs have always been relatively good at collecting disparate logs and other bits and pieces of security data. But then what? A bunch of pretty reports, glacially slow search capabilities, and a handful of static correlation rules only get you so far. And let's face it, that "distance" (i.e., value derived) keeps shrinking as data volumes grow, threats become increasingly sophisticated,

The Road Ahead

infrastructure and systems get more diverse and distributed, and skilled analysts capable of mining/interpreting all of the collected events become harder to find and retain.

Enter security analytics. This new(ish) discipline and the closely associated technologies of machine learning, statistical analysis, and behavioral modeling are changing the SIEM game by delivering a far greater capacity for actually detecting threats missed by an organization's other countermeasures. Because of the added contextual detail and session reconstruction capabilities provided, the impact is even greater for solutions that incorporate UEBA.

But true next-generation SIEMs don't stop there. Instead, they also include functionality to enable SOC personnel to efficiently and effectively respond to detected threats and incidents. The key here is finding solutions that offer more than basic ticketing and case management features. Other capabilities to look for include an extensive library of pre-built API calls for connecting to and coordinating your security and network infrastructure, plus the ability to develop and implement playbooks that not only codify best-practice response activities, but also fully automate them.

DevSecOps tools. Forgive us for the gross oversimplification, but DevOps is all about harmonizing and de-serializing the efforts of (software) development, QA, and operations personnel to speed the delivery (and ideally improve the quality) of new apps, features, and fixes. DevSecOps, then, brings security into the fold, too. The net result: applications that are faster (to market), better, cheaper, and more secure than ever before. Sounds great – I'll take two servings please!

Of course, getting started on a DevOps/DevSecOps path is no small endeavor. The organizational (re-alignment) issues alone can be a substantial hurdle. Enterprises that manage the initial transition/transformation then face the question of how best to begin bringing security into the mix. Our suggestion is to go after some low-hanging fruit. Ever the fans of doing more to reduce one's attack surface, we mean starting out with investments in application security testing (ideally, a combination of both the static and dynamic varieties) and open source vulnerability management tools.

While the former is instrumental to removing security defects from custom-developed code, the latter does much the same for the plethora of open source components that pervade today's code bases. One further suggestion: do everything you can to automate the use of these tools, as well as the response activities that (should) follow whenever a defect is found; otherwise, you won't truly be doing DevSecOps.

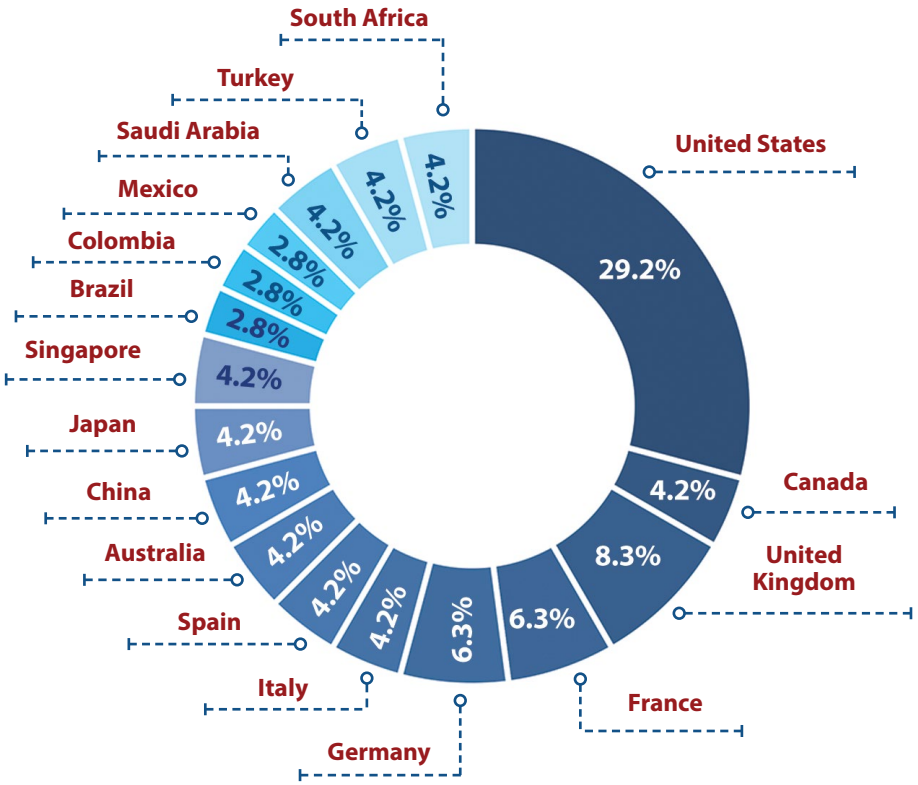
API gateways. Two additional trends from the application development landscape are: (a) the replacement of traditional application architectures with microservices (to enable greater re-use of components, speed of development, and agility); and (b) the increasing externalization not only of individual services, but also, in some cases, entire applications (to enable third-party integration and unlock unforeseen potential). Throw IoT, mobile devices, cloud services, and software-defined computing into the mix, and the outcome is an exponential growth in APIs and their usage.

For externalization scenarios in particular, there is a resulting need to not only mediate API access, but also ensure reliable fulfillment of associated requests. Answering the call in this case is a relatively new infrastructure component known as the API gateway. Essential security features of these products include: multi-layer authentication, authorization, and auditing (i.e., of the requesting device, service/application, and user); threat protection; data leakage protection; and data encryption.

Beyond the realm of security, important capabilities involve language transformation (i.e., XML/JSON, SOAP/REST), request/response validation, session persistence, caching, load balancing, and usage rate monitoring and control. Maybe we're off base here, but the net result sounds a lot like an ADC to us, which is why we expect to see some crossover and/or consolidation between these product segments before too long.

For further insights on these and other emerging areas pertinent to IT security, be sure to tune in for the sixth annual CDR, currently scheduled for release in the first quarter of 2019.

Appendix 1: Survey Demographics



This year's CDR is based on survey results obtained from 1,200 qualified participants hailing from six major regions (North America, Europe, Asia Pacific, Latin America, the Middle East, and Africa) and 17 countries spanning the globe. First-time additions included respondents from Italy and Spain.

Figure 33: Survey participation by country.

As for the roles of our survey participants, nearly a third held senior positions (CIO, CISO, or IT security executive) with IT security responsibilities. Just over one quarter identified as IT security administrators, followed by approximately one in 10 from the ranks of (a) analysts, operators, and incident responders, (b) data protection/ privacy officers, (c) security architects/engineers, and (d) those identifying their position within IT security as "other."

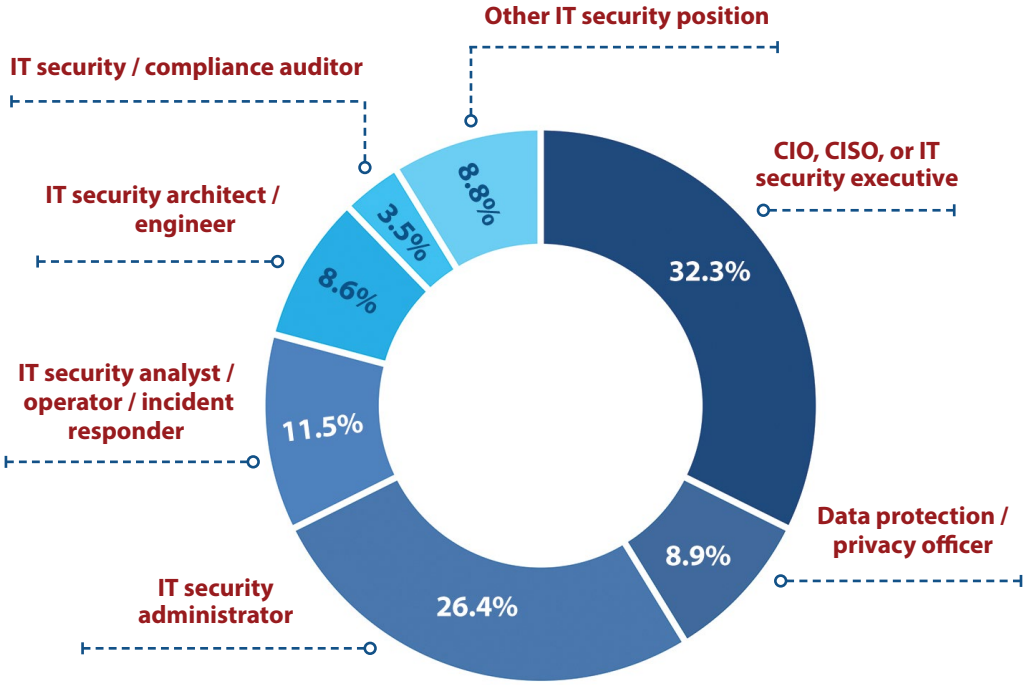
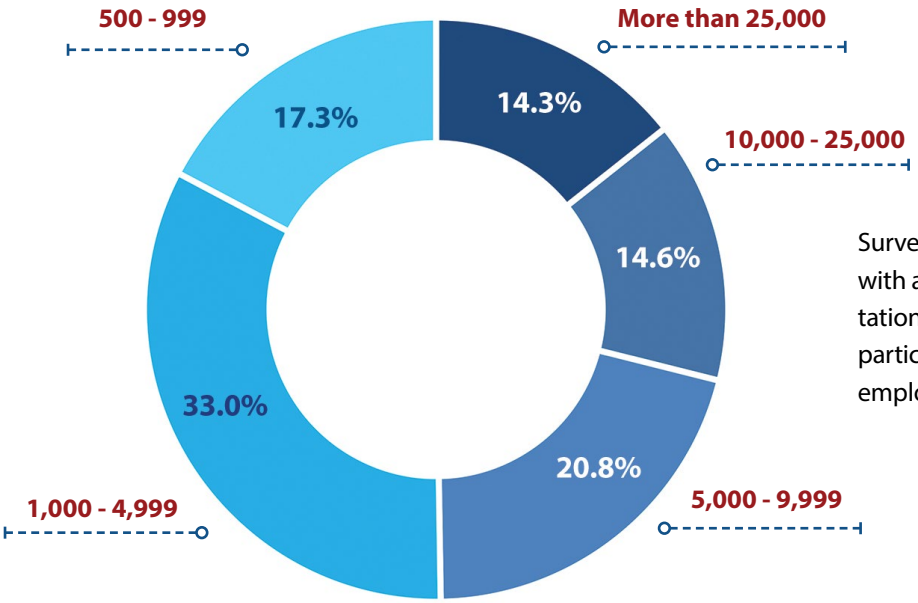


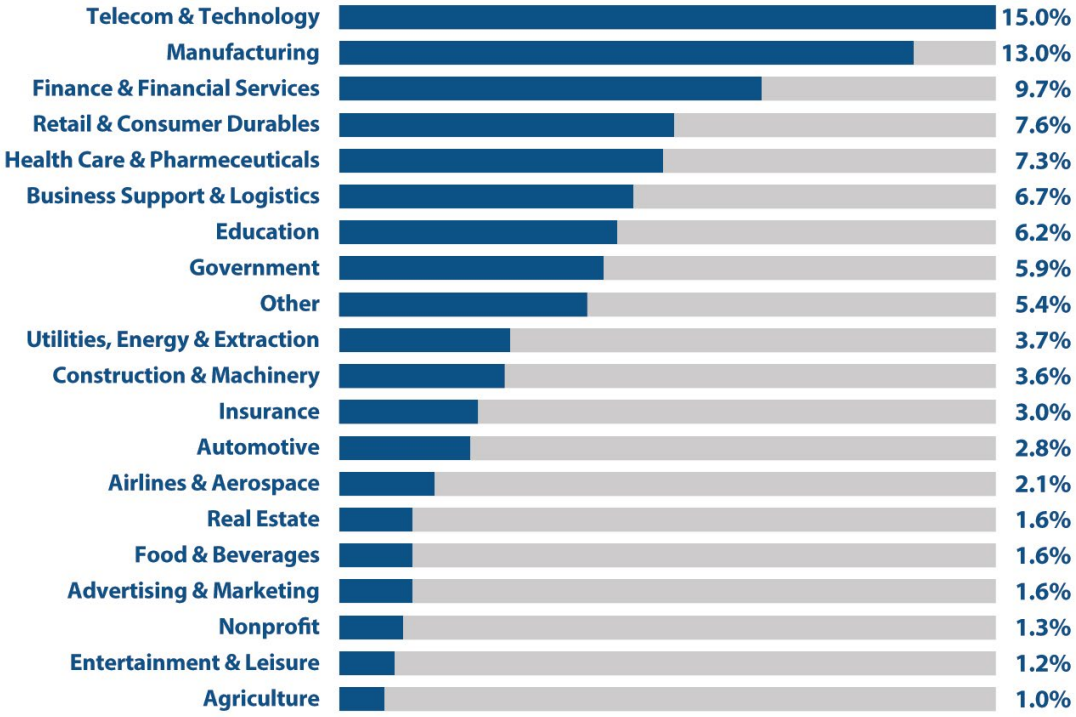
Figure 34: Survey participation by IT security role.

Appendix 1: Survey Demographics



Survey respondents were from organizations with at least 500 employees. Strong representation was obtained from all size groupings, with participants from enterprises with 1,000 to 4,999 employees leading the way (33.0%).

Figure 35: Survey participation by organization employee count.



Distribution of survey participants by vertical industry was fairly broad, with representation across 19 industry segments, and a twentieth category designated as "other." The big 7 industries – education, finance, government, healthcare, manufacturing, retail, and telecom & technology – accounted for just shy of two-thirds of all respondents. No single industry accounted for more than 15% of participants.

Figure 36: Survey participation by industry.

Appendix 2: Research Methodology

CyberEdge Group developed a 27-question (10- to 15-minute) web-based survey instrument 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 2017.

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: 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
- 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)
- Operational Technology
- Patch Management
- Penetration Testing
- Privileged Account Management (PAM)
- Secure Email Gateway (SEG)
- Secure Web Gateway (SWG)
- Security Analytics
- Security Configuration Management (SCM)
- Security Information & Event Management (SIEM)
- 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 textual and graphical elements of 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 referencing textual and/or graphical elements of 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 textual and/or graphical element from this report, you must incorporate the following statement into a corresponding footnote or other citation: "Source: 2017 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**.