CYBEREDGE GROUP

2020 Cyberthreat Defense Report

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

« Research Sponsors »

PLATINUM

(ISC)² Gigamon imperva Menlo Security

GOLD

CARBONITE an opentext company | netskope | perimeterx
COLORTOKENS | opentext | WEBROOT

SILVER

ANITIAN | Cymulate Breach & Attack Simulation | expel | ZEROFOX
CybelAngel | DivvyCloud | sysdig

Table of Contents

Introduction

CyberEdge's annual Cyberthreat Defense Report (CDR) plays a unique role in the IT security industry. Other surveys do a great job of collecting statistics on cyberattacks and data breaches and exploring the techniques of cybercriminals and other bad actors. Our mission is to provide deep insight into the minds of IT security professionals.

Now in its seventh year, the CDR has become a staple among IT security leaders and practitioners by helping them gauge their internal practices and security investments against those of their counterparts across multiple countries and industries. If you want to know what your peers in IT security are thinking and doing, this is the place to look.

This edition of the CDR is being published at the end of March 2020, as COVID-19 is affecting people and organizations across the world, but the full impact of the pandemic cannot yet be assessed. The survey associated with our report was conducted in November 2019, before the outbreak of the disease. Some of the questions are related to intentions in 2020, and obviously many of those intentions will not be realized this year. However, the survey results related to the perceptions and activities of IT security professionals through 2019 are valid, and we believe that most of the trends identified in this report will resume, and probably accelerate, when the pandemic abates and economies recover. For our views on the potential impacts of COVID-19 on our industry, see our discussion ***How Might COVID-19 Affect IT Security?*** on page 47.

CyberEdge would like to thank our Platinum, Gold, and Silver research sponsors, whose continued support is essential to the success of this report.

Top Five Insights for 2020

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. **The bad guys are more active than ever.** The percentage of organizations affected by a successful cybersecurity attack had leveled off during the previous three years, but this year it jumped from 78.0% to 80.7%. Not only that, for the first time ever, more than a third (35.7%) of organizations experienced six or more successful attacks. The number of respondents saying that a successful attack on their organization is very likely in the coming 12 months also reached a record level.

2. **Ransomware attacks and payments continue to rise.** Ransomware is trending in the wrong direction... again. 62% of organizations were victimized by ransomware last year, up from 56% in 2018 and 55% in 2017. This rise is arguably fueled by the dramatic increase in ransomware payments. 58% of ransomware victims paid a ransom last year, up from 45% in 2018 and 39% in 2017.

3. **People are the biggest problem.** The greatest barriers to establishing effective defenses are: (a) lack of skilled IT security personnel and (b) low security awareness among employees. According to the respondents, these are more serious than issues like too much data to analyze, lack of management support, and budget.

4. **But IT security is having some successes.** Respondents say the adequacy of their organization's IT security capabilities has increased in all eight of the functional areas we ask about. They rated these improvements as greatest in application development and testing, identity and access management (IAM), and attack surface reduction through patch management and penetration testing.

5. **Advanced security analytics and machine learning are becoming "must-haves."** Implementations of advanced security analytics took off over the past year and are expected to keep rising. Organizations are showing a strong preference for IT security products that feature machine learning and other forms of artificial intelligence (AI).

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**

Introduction

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, the CDR surveys the perceptions of IT security professionals, gaining insights into how they see the world.

Specifically, the CDR examines:

- The frequency of successful cyberattacks in the prior year and optimism (or pessimism) for preventing further attacks in the coming year
- The perceived impact of cyberthreats and the challenges faced in mitigating their risks
- The adequacy of organizations' security postures and their internal security practices
- The organizational factors that present the most significant barriers to establishing effective cyberthreat defenses
- Current investments in security technologies 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 around the world. IT security teams can use the data, analyses, and findings to shape answers to many important questions, such as:

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

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

The findings of the CDR are divided into four sections:

Section 1: Current Security Posture

Our journey into the world of cyberthreat defenses begins with respondents' assessments of the effectiveness of their organization's investments and strategies relative to the prevailing threat landscape. They report on the frequency of successful cyberattacks, judge their organization's security posture in specific IT domains and security functions, and provide details on the IT security skills shortage. The data will help readers begin to assess:

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

Introduction

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 obstacles to security that most concern today's organizations. The survey respondents weigh in on the most alarming cyberthreats, barriers to establishing effective defenses, and high-profile issues such as ransomware and cloud application security. These appraisals will help readers think about how their own organizations can best improve 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 changes occurring in business, technology, and threat landscapes. This section of the survey provides data on the direction of IT security budgets, and on current and planned investments in network security, endpoint security, application and data security, security management and operations, and identity and access management. Readers will be able to compare their organization's investment decisions against the broad sample and get a sense of what "hot" technologies their peers are deploying.

Section 4: Practices and Strategies

Mitigating today's cyberthreat risks takes more than investing in the right technologies. You must ensure those technologies are deployed optimally, configured correctly, and monitored adequately to give your organization a fighting chance to avoid being a front-page news story. In the final section of the survey our respondents provide information on how they are deploying and using leading-edge technologies and services such as security analytics and IT security delivered from the cloud. We also look at how IT security training and professional certification can help enterprises address the serious shortfall in skilled IT security staff.

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 other 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

- **Successful cyberattacks at record levels.** For the first time in the history of our survey, four out of five organizations experienced at least one successful cyberattack and more than one-third suffered six or more (page 7).
- **Rising pessimism.** 69% of IT security professionals believe a successful cyberattack is imminent in 2020, up from 65% last year and 62% the year before (page 9).
- **Old and new tech at risk.** Respondents worry about new technologies like containers and IoT devices and old ones like industrial control systems (page 10).
- **Gone rogue.** 'Detection of rogue insiders / insider attacks' tops the list of most-challenging IT security functions, followed by 'User security awareness' (page 11).
- **Help wanted.** The vast majority (85%) of organizations are experiencing an IT security skills shortfall, and the gap grew in all but one job category (page 12).

Perceptions and Concerns

- **Access of evil.** Malware, spear-phishing, and ransomware top the list of cyberthreat concerns, but zero-day attacks don't bother us as much as they used to (page 13).
- **Ransomware rising.** A record 62% of organizations were affected by ransomware; 58% paid the ransom; and of those 67% recovered their data (page 15).
- **People problems loom large.** The greatest barriers to defense are lack of skilled IT security personnel and employees' low security awareness (page 17).
- **Cloudy forecast.** 'Loss or theft of data and intellectual property' tops the list of cloud application security risks and challenges (page 19).

Current and Future Investments

- **Security's slice of the pie.** On average, IT security consumes 13% of the overall IT budget (page 20).
- **Budgets rising.** Six out of seven (85%) say their IT security budget is going up this year (page 22).
- **Network security's top picks.** Installations of advanced malware analysis and sandboxing jumped, and next-generation firewalls (NGFW) is the top network security technology planned for acquisition in 2020 (page 24).
- **Endpoint security's hat trick.** Containerization / micro-virtualization tops the list of endpoint security technologies respondents plan to acquire for the third consecutive year (page 26).
- **The stars of app/data security.** API gateways, database firewalls, and WAFs are atop the list of installed app/data security products (page 28).
- **Security analytics surges.** Advanced security analytics flew from the bottom of the list of installed security management and operations technologies to second place, behind only patch management (page 30).
- **Biometrics stepping up.** In the IAM category, biometrics installations burgeoned, and that technology is expected to surge this year as well (page 32).
- **We want AI.** A whopping 85% of respondents expressed a preference for security products that feature machine learning and AI (page 34).

Practices and Strategies

- **Security's Swiss Army knife.** Of nine use cases for security analytics products, 'Detecting insider threats' tops the list. Of those organizations that lack security analytics, 61% plan to acquire it in 2020 (page 36).
- **Monitor the app security stack.** A decisive 80% of respondents agreed that monitoring the entire app security stack with one platform is a best practice (page 38).
- **Decryption deficit.** Surprisingly, only 34% of SSL/TLS-encrypted web traffic is decrypted for inspection (page 40).
- **Support for zero trust.** Organizations are using a variety of technologies to support their zero-trust architectures. Of those that haven't deployed zero trust yet, 67% plan to get started in 2020 (page 41).
- **Security from the cloud.** Today, 36% of security applications and services are delivered via the cloud (page 42).
- **Everyone wants training.** Four out of five people believe IT security training has helped them better protect their organization, and 87% of those that haven't received training would welcome it (page 43).
- **Certification brings respect.** Achieving an IT security professional certification is more about knowledge and respect than money (page 45).

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=1,151)

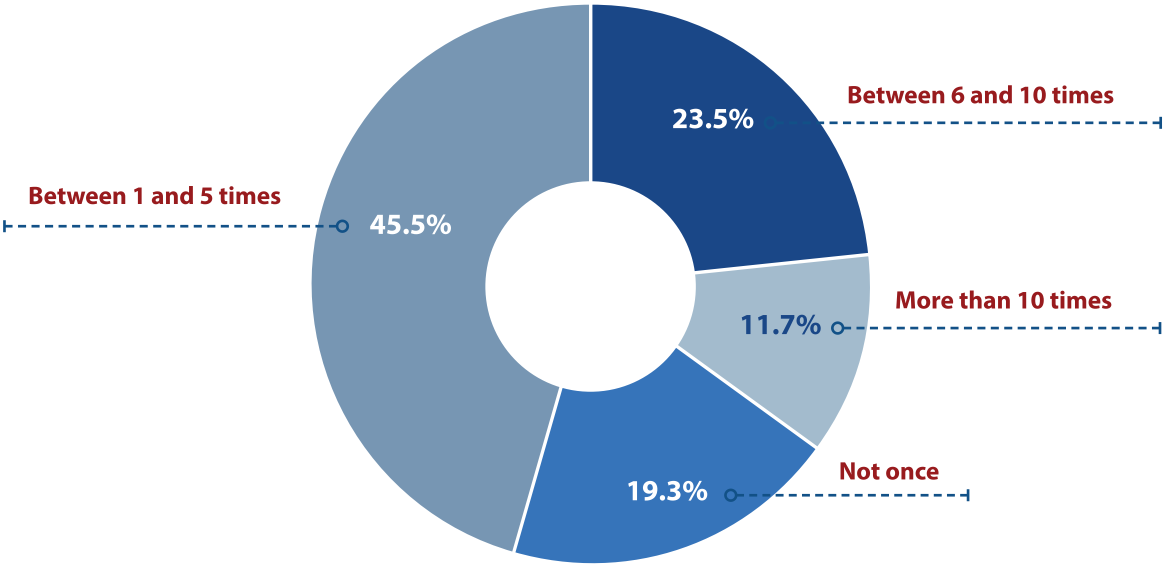

Figure 1: Frequency of successful cyberattacks in the last 12 months.

The pain is back. After plateauing in our last three reports, the portion of organizations affected by a successful cyberattack reached 80.7%, up from 78.0% last year (see Figures 1 and 2). This is the first time since we began reporting that this figure has exceeded 80%.

The percentage experiencing frequent attacks also increased. Organizations who endured 6-10 attacks over 12 months rose to 23.5% (up from 22.1% last year), and a very unfortunate 11.7% suffered through more than 10 during the year (up from 9.4%). Put them together, and we see that a record 35.2% or organizations, more than a third, joined our "frequent victim" club of six or more successful cyberattacks in one year.

Of the seven major industries surveyed for this report (see Figure 3), finance was the hardest hit, with 87.6% reporting a successful attack, followed by retail (82.7%), telecom and technology (81.9%), and education (81.5%). Next came healthcare (76.6%) and manufacturing (75.6%). The bright spot this year was government with only 60.9% experiencing a successful attack.

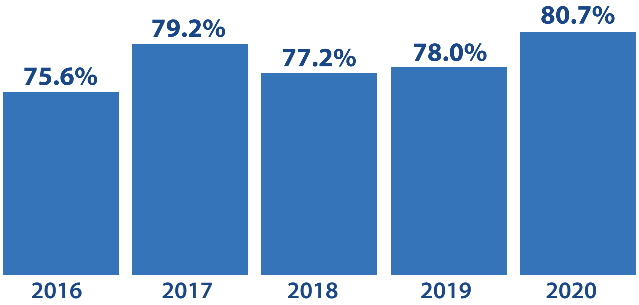

Figure 2: Percentage compromised by at least one successful attack, by year.

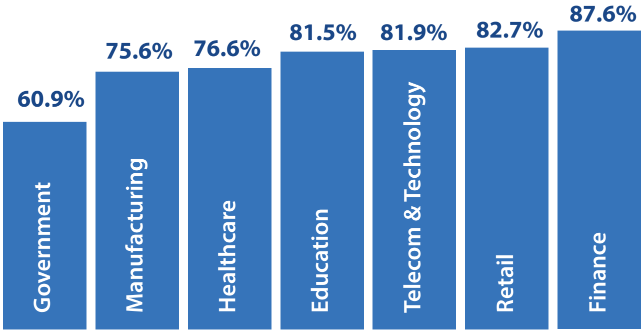

Figure 3: Percentage compromised by at least one successful attack in the past 12 months, by industry.

When we break down organizations by headcount, more than half (50.3%) of those with 10,000-24,999 employees suffered six or more attacks, and only 9.7% were never attacked successfully. Among giant enterprises with more than 25,000 employees, 46.4% experienced six or more attacks, although somewhat surprisingly, 20.9% reported no successful attacks — perhaps they have extraordinarily good defenses. Smaller organizations of 500-999 employees had the least painful experience, with only 25.1% enduring six or more successful attacks and 27.4% escaping with none.

Geographically, Mexico reclaimed the top spot for the most organizations experiencing a successful attack (93.9%). Down the list, China (83.3%), the US (82.6%), the UK (82.3%), and France (81.1%) were a bit above average. Compromised less often than most were Germany (79.2%), Canada (78.0%), Brazil (77.4%), and Japan (76.7%).

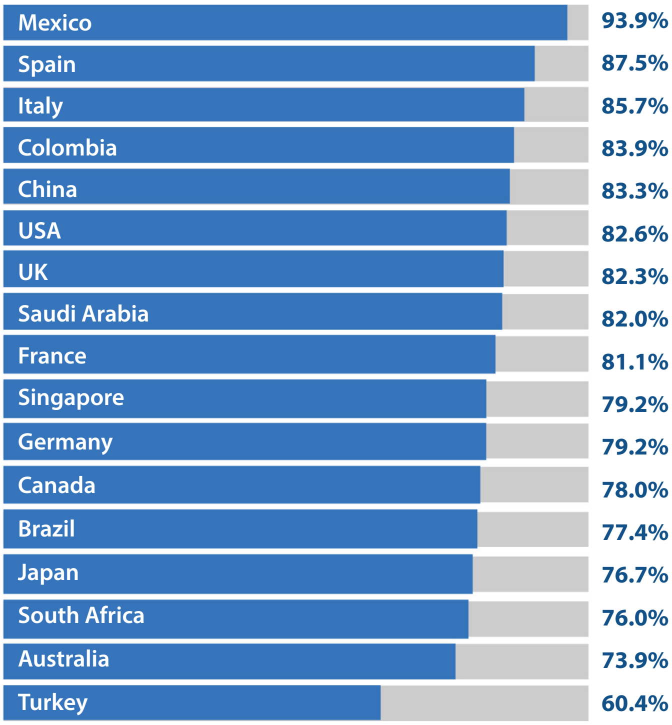

Figure 4: Percentage compromised by at least one successful attack in the past 12 months, by country.

> **“A record 35.2% of organizations, more than a third, joined our ‘frequent victim’ club with six or more successful cyberattacks in one year.”**

Future Likelihood of Successful Cyberattacks

What is the likelihood that your organization's network will be compromised by a successful cyberattack in 2020? (n=1,171)

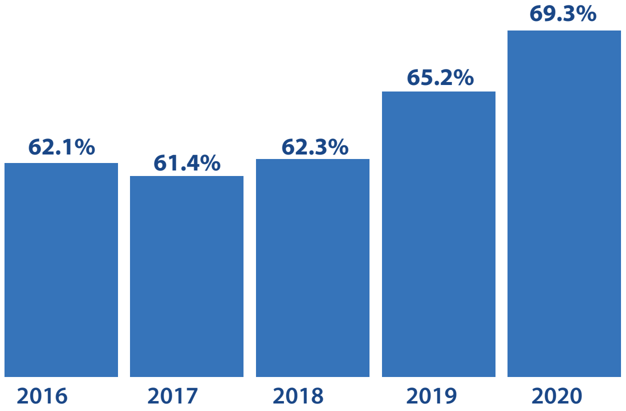

Figure 5: Percentage indicating compromise is "more likely to occur than not" in the next 12 months.

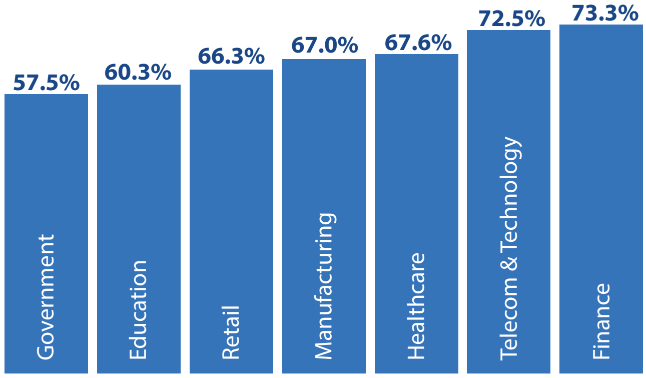

Figure 6: Percentage indicating compromise is "more likely to occur than not" in the next 12 months, by industry.

Oscar Wilde once declared that second marriages were "the triumph of hope over experience." Hope seems to triumph over experience in cybersecurity as well. We have noted every year in this report that many IT professionals who experienced a successful cyberattack in the past year think that such an attack is unlikely in the coming one. That pattern continues this year, with 80.7% of respondents reporting successful attacks last year (see Figure 2 on the previous page), but only 69.3% saying they are somewhat or very likely to experience one or more in 2020 (see Figure 5).

On an industry basis (see Figure 6), the proportion of respondents saying a compromise was more likely to occur than not was highest in finance (73.3%) and telecom and technology (72.5%), followed by healthcare (67.6%), manufacturing (67.0%), and retail (66.3%). The most confident respondents (relatively) were in education (60.3%) and government (57.5%).

Of the 17 countries we surveyed, respondents in only one, Japan, expect this year to be worse than last year. In that nation, 76.7% admitted to one or more successful attacks in 2019, and 81.7% predict at least one in 2020. Do they know something we don't?

Actually, although people are optimistic that this year will be better than last year, they are less optimistic than they were in past surveys. While there are still some souls with positive (or unrealistic?) outlooks who say that a successful attack is not likely or somewhat unlikely in the coming 12 months, their number dropped from 37.7% two years ago, to 34.8% last year, to 30.7% this year. The pessimists (or realists?) saying a successful attack on their organization is very likely jumped from 19.7%, to 21.2%, to 27.2% in those years. That last figure is a record high for our report — by far.

Does this turn toward gloom reflect a belief that cyberthreats are outpacing cyber defenses, or simply a reduction in wishful thinking? Our data is conflicting. Anxiety about many classes of cyberthreats has reached an all-time high (see page 13), as have concerns about factors inhibiting organizations from defending themselves (see page 17). On the other hand, security budgets continue to grow (see page 22), and respondents indicate greater confidence in their security posture in many areas (see page 10). On the whole, we believe that predictions of more successful attacks in 2020 probably reflect greater realism about the challenges of cybersecurity rather than a conviction that we are losing the arms race against cyberthreats.

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=1,186)

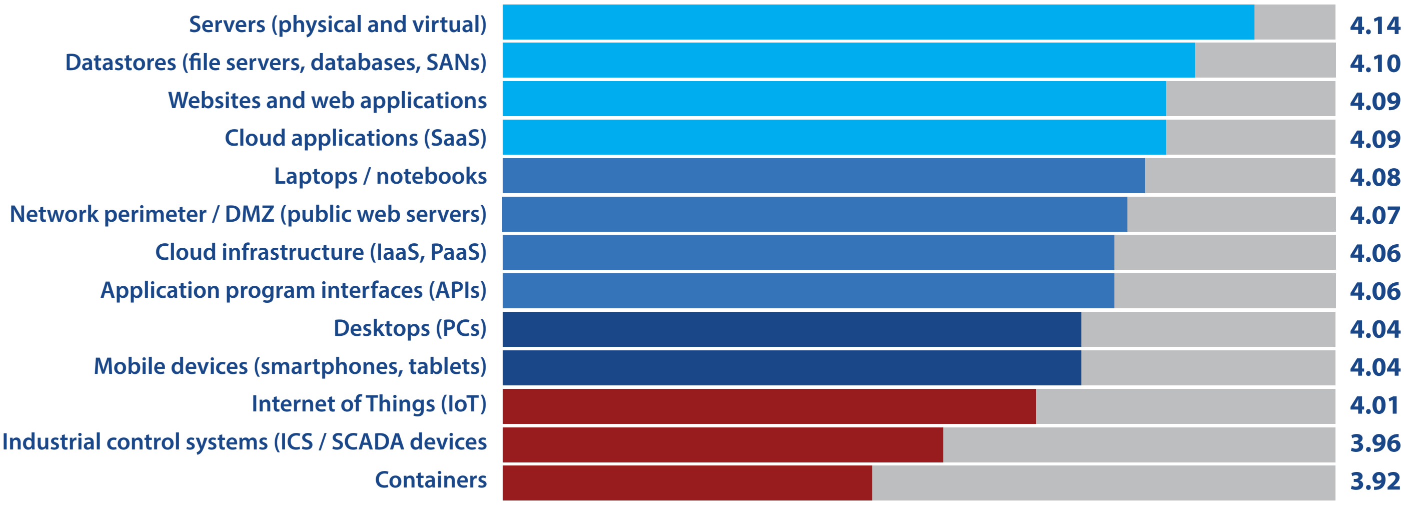

Figure 7: Perceived security posture by IT domain.

There's no doubt that cybersecurity organizations must deal with a growing, and increasingly complex, attack surface (the points from which an adversary can access systems and data). But where do they feel the most, and the least, confident? Where has their confidence changed?

The big picture has been consistent for years. When asked to rate their organization's ability to defend against cyberthreats, respondents have been most confident about assets that are under their direct control and easiest to monitor, patch, and remediate. These include physical and virtual servers, databases, and websites and web applications (see Figure 7).

Not surprisingly, our IT professionals are most concerned about IT components that are:

- Relatively new, such as containers
- Old and not designed with cybersecurity in mind, such as industrial control systems and SCADA devices
- Infrequently connected to the corporate network and harder to monitor, such as smartphones and tablets
- Combinations of the above, such as all those sensors, controllers, and devices that make up the Internet of Things (a new category we added to our survey this year)

Some of the details in the survey results are noteworthy. A few years ago there were many questions about protecting applications in the cloud. Today most respondents are confident about their security posture vis-a-vis SaaS applications and feel reasonably comfortable about using cloud infrastructure and platform services.

The trend in this data is actually positive. On a 1-5 scale, with 5 being the highest, the average score of all IT components increased from 3.82 to 4.05 (+.23) since last year. Not one component showed a decline in confidence!

How does this square with the fact that respondents are reporting more successful cyberattacks than ever before? It probably reflects the same optimism we saw in the previous question that things will be better this year than last year.

The greatest increases in "ability to defend against cyber-threats" came in three categories:

- Mobile devices (+.30)
- Laptops and notebooks (+.29)
- Application programming interfaces (+.26)

Laptops and notebooks are now seen as better defended than desktop PCs!

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=1,186)

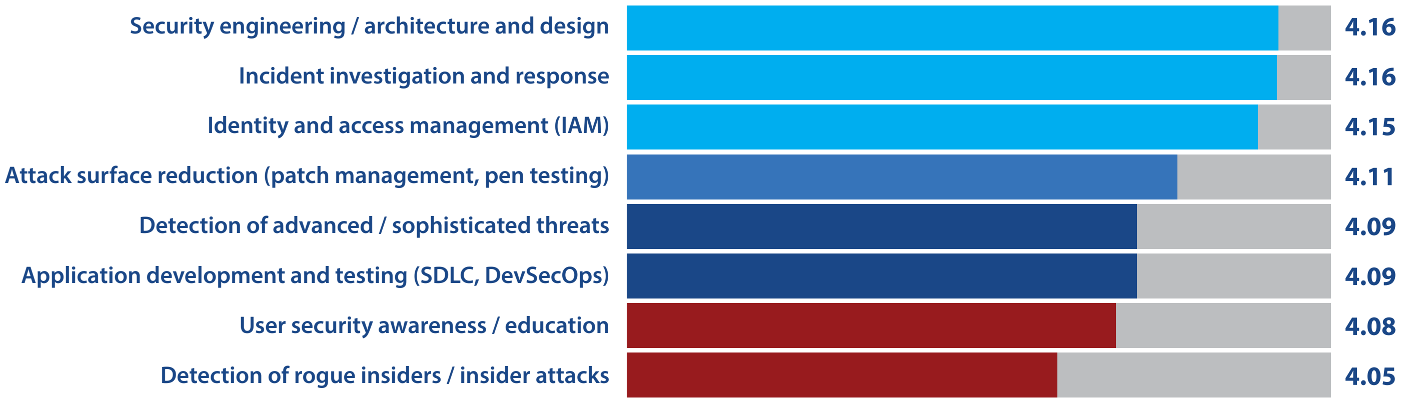

Figure 8: Perceived adequacy of functional security capabilities.

In this question we take the temperature of our research participants on their organization's capabilities in eight key cybersecurity functions. How do they rate the adequacy of their people and processes? The results are shown in Figure 8.

As we found on the last question, confidence has gone up across the board in the last year. On a 1-5 scale, with 5 being the highest, the combined score of all cybersecurity functions rose from 3.90 to 4.11 (+.21), and the scores in every category increased.

The largest increases in perceived adequacy came in:

- Application development and testing (+.30)
- Identity and access management (+.28)
- Attack surface reduction, including patch management and penetration testing (also +.28)

> **"This year, our respondents feel their organizations are least adequate in IT security capabilities related to employee behaviors."**

The improvement in application development and testing is particularly noteworthy. That category had been perceived as the weakest category for the last three years running; this year it jumped two spots on the list. We believe this is the payoff we predicted last year from the increased investment by vendors and enterprises in automating application development and testing with software development lifecycle and DevSecOps tools like those for:

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

This year, our respondents feel their organizations are least adequate in IT security capabilities related to employee behaviors. The new #1 concern: detection of rogue insiders and insider attacks. A close second: user security awareness and education. Clearly, enterprises need to devote more attention to monitoring and educating their own people.

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=1,178)

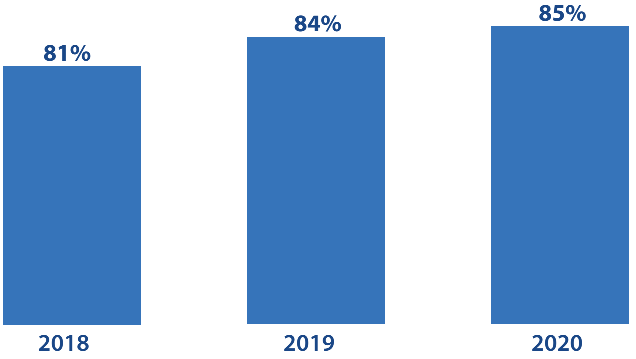

Figure 9: Percentage of organizations experiencing a shortfall of skilled IT security personnel.

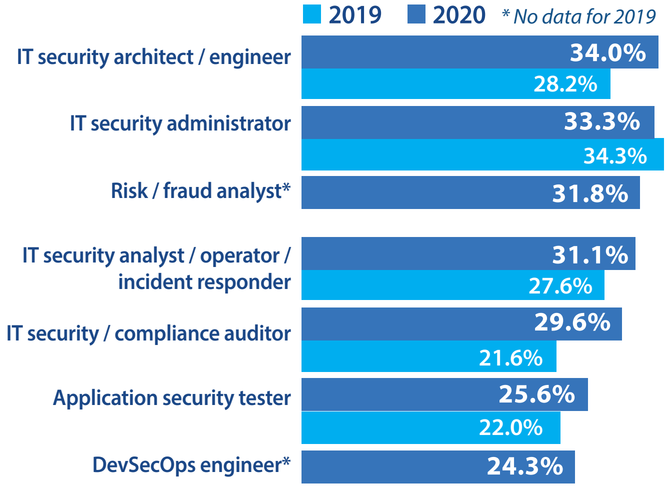

Figure 10: Cybersecurity skills shortage, by role.

If you thought the IT skills shortage couldn't get any worse (from a hiring manager's point of view), think again. Over the past three years, the percentage of organizations experiencing a shortfall of skilled IT security personnel rose from 81%, to 84%, to 85% (see Figure 9). Of course, if you happen to be a skilled IT security person, your job prospects have never been better!

If we break down the data by role (see Figure 10), we see the greatest shortfalls in IT security are architects and engineers (34.0%) and IT security administrators (33.3%), followed by risk and fraud analysts (31.8%) and IT security analysts, operators and incident responders (31.1%). Rounding out the list are IT security and compliance auditors (29.6%), application security testers (25.6%), and DevSecOps engineers (24.3%).

The gap increased in four out of the five roles that appeared in the survey both last year and this year. In some fields the rise was dramatic: from 21.6% to 29.6% (+8.0%) for IT security and compliance auditors and from 28.2% to 34.0% (+5.8%) for IT security architects and engineers. The only role that saw a (small) decrease in unfilled positions was IT security administrators.

We suspect that the relatively small shortfall for DevSecOps engineers is due to the fact that it is an emerging field and many organizations have not started to recruit people for that role.

The shortages are most acute for large organizations with between 10,000 and 24,999 employees, where a whopping 88.0% haven't met their hiring goals. The best results (again, only relatively) were reported by organizations with 500-999 employees. However, we think that a lot of those companies obtain their security expertise from systems administrators and other generalists, who are also in short supply.

Of major industries, healthcare was feeling the most pain (93.7% of organizations experienced a shortfall), followed by education (87.5%), manufacturing (87.0%), finance (85.0%), and telecom and technology (83.6%). The shortfalls were slightly less in retail (78.0%) and government (75.5%).

Around the world, we found the greatest shortages in Australia (91.7%), Mexico (90.9%), South Africa (89.8%), and China (also 89.8%).

> **"If you thought the IT skills shortage couldn't get any worse (from a hiring manager's point of view), think again."**

Section 2: Perceptions and Concerns

Concern for Cyberthreats

On a scale of 1 to 5, with 5 being highest, rate your overall concern for each of the following types of cyberthreats targeting your organization. (n=1,189)

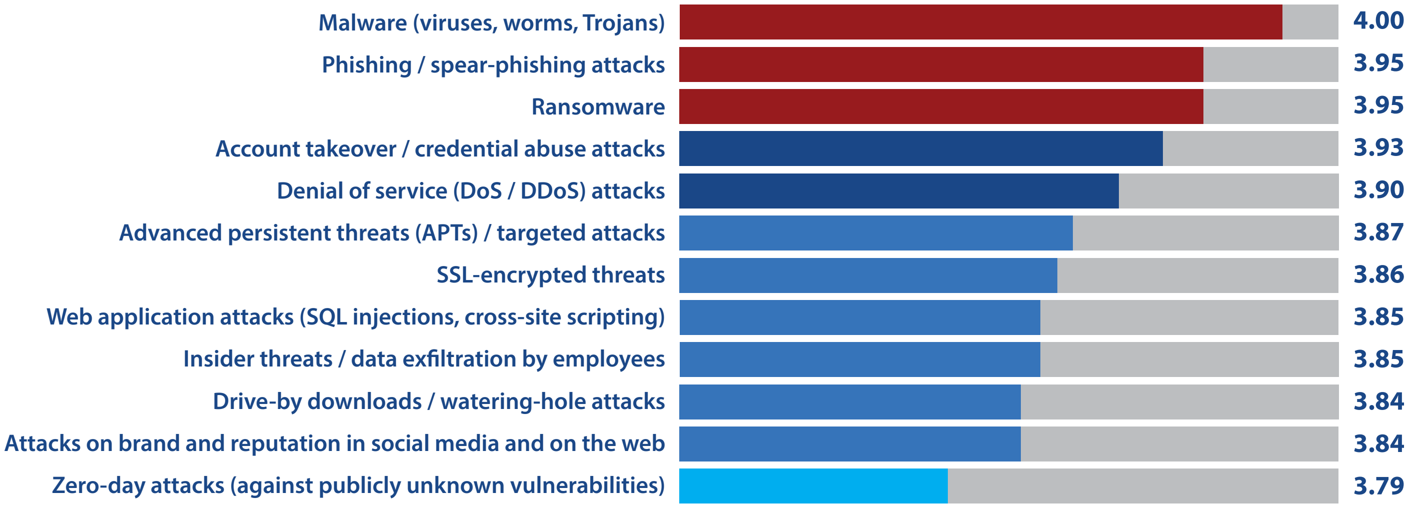

Figure 11: Relative concern for cyberthreats, by type.

If you follow the never-ending drumbeat of press articles about major data breaches, you know that malware plays a major part in most of them. This is reflected in malware's continuing position in our survey as the most-concerning type of cyberthreat (see Figure 11).

Following malware, ransomware has jumped to a tie for second place with phishing and spear-phishing. Account takeover / credential abuse attacks and denial of service (DoS) attacks round out the top tier of concerns, as they have for several years.

As a serious concern, APTs and targeted attacks have persisted (sorry). Over the past two years, they have crept up from ninth place, to eighth place, to sixth place on our list.

And we have a new loser! Or is it a new winner? Well, at any rate, we have a new Thing That Doesn't Bother Us Nearly as Much as it Used To. That's zero-day attacks, defined as attacks against publicly unknown vulnerabilities. Zero-day attacks fell from fifth place on the list two years ago, to tenth place last year, to twelfth and last this year. We think this slide reflects the industry's ability to find vulnerabilities faster and to automate patching, and enterprises' successful deployment of monitoring and analytics tools that can detect intrusions faster.

> **"Following malware, ransomware has jumped to a tie for second place with phishing and spear-phishing."**

We added a new threat type to our survey this year: attacks on brand and reputation in social media and on the web. It came in toward the bottom of our list, in a tie for tenth place. But we think this category (which includes hijacking social media accounts, using typosquatting websites for fraud, and selling counterfeit goods online) will become more of a concern in the cybersecurity community as:

- Incidents become more numerous and more serious
- Marketing and fraud groups ask IT for more help addressing them
- Digital risk protection (DRP) products and services provide technology to deal effectively with attacks on brand and reputation

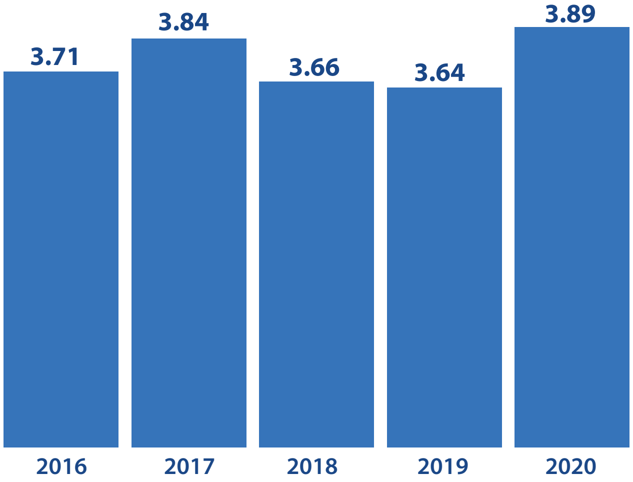

Figure 12: Threat Concern Index, depicting overall concern for cyberthreats.

Finally, what does the data tell us about broad industry trends? Unfortunately, the slight reduction in cyberthreat concern we experienced over the last two years may have ended. As you can see in Figure 12, our combined Threat Concern Index (i.e., average concern rating across all threats) declined from 3.84 in our 2017 report, to 3.66 in the 2018 edition, to 3.64 last year — and ratcheted up again to a record 3.89 in this survey. Oh well, as someone once declared: "Eternal vigilance is the price of liberty." (FYI, it turns out that there is no proof that Thomas Jefferson actually said this. Bummer.)

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=1,182)

Organizations affected by ransomware

2020	62.4% ↑
2019	56.1%
2018	55.1%

Of those affected by ransomware...

Paid ransom

2020	57.5% ↑
2019	45.1%
2018	38.7%

Didn't pay ransom

2020	42.3% ↓
2019	54.9%
2018	61.3%

Of those that paid...

Recovered data

2020	66.9% ↑
2019	61.3%
2018	49.3%

Lost data

2020	33.1% ↓
2019	38.7%
2018	50.7%

Of those that didn't pay...

Recovered data

2020	84.5% ↑
2019	80.8%
2018	87.0%

Lost data

2020	15.5% ↓
2019	19.2%
2018	13.0%

Table 1: Key ransomware statistics.

On the ransomware front there was a lot of bad news and a little bit of good news.

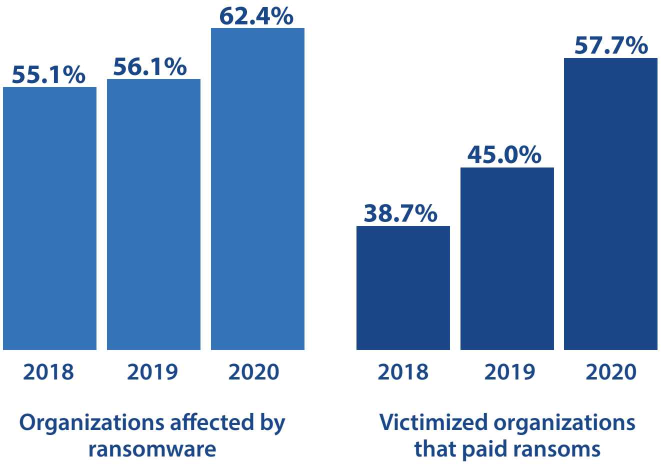

Figure 13: Percentage of organizations affected by one or more successful ransomware attacks and the percentage of victimized organizations that paid associated ransoms.

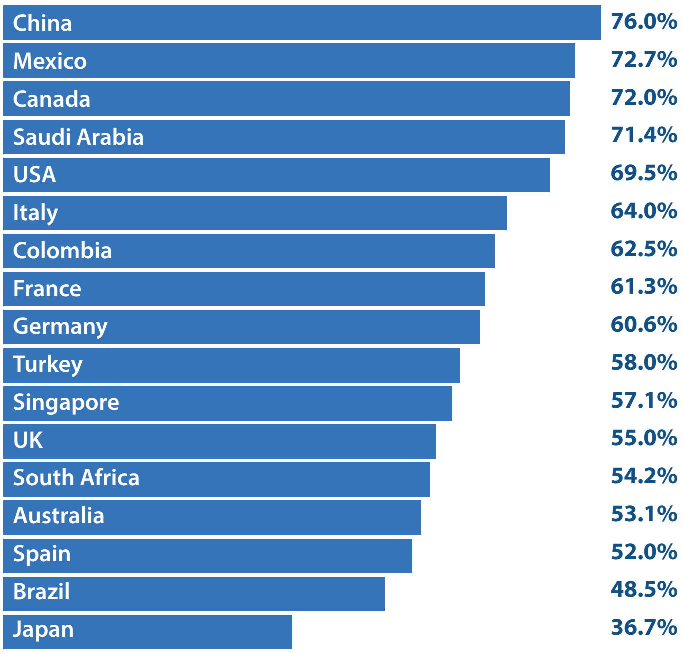

Figure 14: Percentage of organizations affected by ransomware in the last 12 months, by country.

First, the bad news. Ransomware continues to be one of the most pressing concerns of cybersecurity organizations (see Figure 11 on page 13), and no wonder! As you can see in Figure 13, the percentage of organizations affected by ransomware has risen sharply, from 55.1% in our 2018 report, to 56.1% in the 2019 report, to 62.4% now. Moreover, of the organizations affected by ransomware, those that felt compelled to pay the ransom skyrocketed, from 45.1% in last year's report to 57.5% in this one (see Table 1).

The little bit of good news? At least more enterprises got their information back. Of those that paid the ransom, 66.9% recovered their data, up from 61.3% the previous year, and up from 49.3% two years ago. Not to toot our own horn, but we feel we deserve a little credit for this trend as CyberEdge was the first to measure data recovery statistics for ransomware payers. And thanks to our friends at *The Wall Street Journal*, *Forbes*, *NPR*, and virtually every IT security trade publication that referenced our report last year, word has spread. Ransomware threat actors now realize that withholding data from victims that pay ransoms is bad for business.

So, what's been going on with ransomware lately? Cybercriminals who observed the massive success of WannaCry, NotPetya, and Bad Rabbit ramped up their ransomware attacks. Also, a vicious cycle has been in operation: more ransom payers are successfully recovering their data, which motivates more victimized organizations to pay ransoms, which encourages more ransomware attacks.

The sharp increase in victims that decided to pay up was caused by several factors. Cryptocurrencies like Bitcoin made it easier to pay. (Heck, you can buy Bitcoins in your local grocery store now!) New, sophisticated ransomware variants such as STOP/DJVA, Dharma/CrySIS, Phobos, GlobeImposter, REvil/Sodinokibi, GandCrab, and Maze intimidated some victims. Many of the newly targeted city governments, hospitals, and universities didn't have skilled staff who could recover data. And some new ransomware variants destroy backups (discussed next).

You may have noticed that some of these numbers seem rather odd. At first glance, it looks like you would have a better chance of recovering data if you refused to pay the ransom (84.5%) than if you did pay (66.9%). But as you learned in Statistics 101, correlation does not imply causation. Most of those that refused to pay probably had backed up their data and knew they could recover it without help from the cybercriminals. So, don't say CyberEdge's data implies that you should never pay ransoms!

But this leads to another question: why doesn't everyone back up their data so they don't have to worry about ransomware? We've been advising readers for years to leverage automated backup solutions, and we hope you are (for many reasons).

Unfortunately, in the relentless arms race between hackers and security experts, some new ransomware variants dwell on systems and destroy backups before encrypting data. This may be one of the reasons more organizations are electing to pay ransoms — they wake up to find systems locked and backups corrupted.

Other notable findings include:

- The countries with the highest percentage of organizations affected by ransomware were China (76.0%), Mexico (72.7%), Canada (72.0%), Saudi Arabia (71.4%), and the US (69.5%). The least affected were Spain (52.0%), Brazil (48.5%), and Japan (36.7%). (See Figure 14)
- The most severely affected major industries were finance (70.8%) and telecom and technology (70.2%). Perhaps cybercriminals saw these industries as having the deepest pockets.
- When the data is broken down by organization size, large enterprises (10,000-24,999 employees) surged to the top this year, with 77.0% being affected (up from 63.4% the previous year). Small and medium-sized organizations were the least affected: 54.7% for those with 500-999 employees and 53.8% of those with 1,000-4,999.

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=1,188)

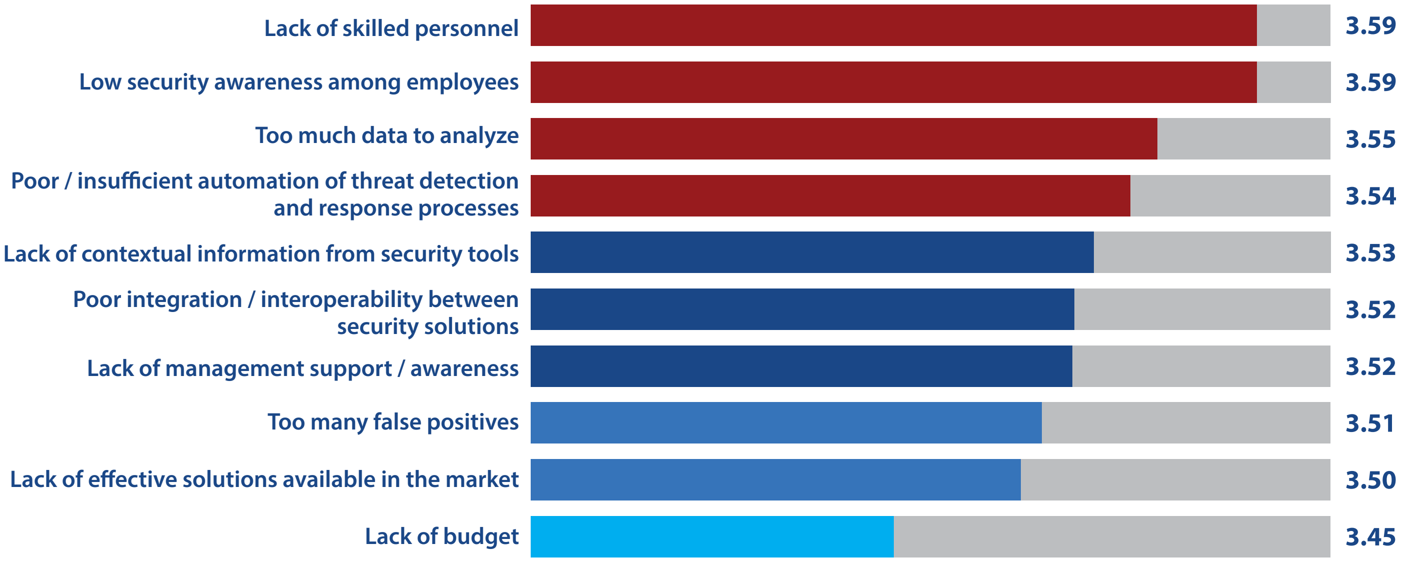

Figure 15: Inhibitors to establishing effective cyberthreat defenses.

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?

Two of our perennial leaders, lack of skilled personnel and low security awareness among employees, remain at the top of the list (see Figure 15). This finding is consistent with other information in this report, for example, the low confidence in user security awareness and education shown in Figure 8 on page 11, and our discussion on page 12 of record-level shortfalls in IT skills.

We can see a connection among the next three issues: too much data to analyze, poor automation of threat detection and response processes, and lack of contextual information from security tools. We know from our conversations with enterprises and cybersecurity vendors that IT organizations

"But after considering the relative position of these inhibitors, we must look at changes over time — and that picture is not pretty at all."

today are putting less emphasis on blocking attacks at the perimeter and more on continuous monitoring and analysis to detect threats early. That means they must get much better at collecting and analyzing vast amounts of information to detect anomalies, pulling together indicators of compromise (IoCs) and contextual information to track the course of attacks, and automating workflows to respond to them. We can see from our survey results that survey participants don't feel they are doing these well enough. Fortunately, vendors are responding to the market need for better data collection, analysis, and process automation tools, so we hope to see improvements in these areas in our coming surveys.

It's noteworthy that lack of budget has fallen from the second-biggest barrier to adequate defense in 2014 to the very bottom of the list this year. That implies that cybersecurity teams don't need to spend as much time chasing funding as in the past. On the other hand, they can't blame their problems on tight-fisted financial types any longer.

After considering the relative position of these inhibitors, we must look at changes over time — and that picture is not pretty at all. Our Security Concern Index, the average rating of all of the issues, has been trending upward for several years, and took a huge jump of .34 this year (see Figure 16). The score for every single issue increased (got worse) by between .29 and .41 (which is a lot on a scale of 1 to 5). When you look at Figure 15 and see that some inhibitors fell in relative position, remember that even their scores increased substantially year to year.

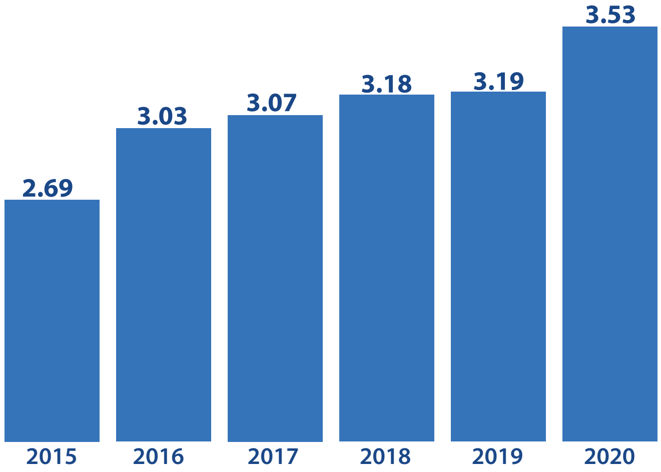

Figure 16: Security Concern Index, depicting the average rating of security inhibitors.

Are security professionals getting stressed out? Do they believe the good guys are losing the race to the bad guys? As we mentioned earlier, our data points in different directions. But at a minimum, the responses to this question indicate considerable frustration about IT staffing, user awareness, and organizations' ability to leverage data and analytics to detect and stop attacks.

Cloud Application Security Challenges

On a scale of 1 to 5, with 5 being highest, rate your overall concern for each of the following cloud application security risks and challenges. (n=1,154)

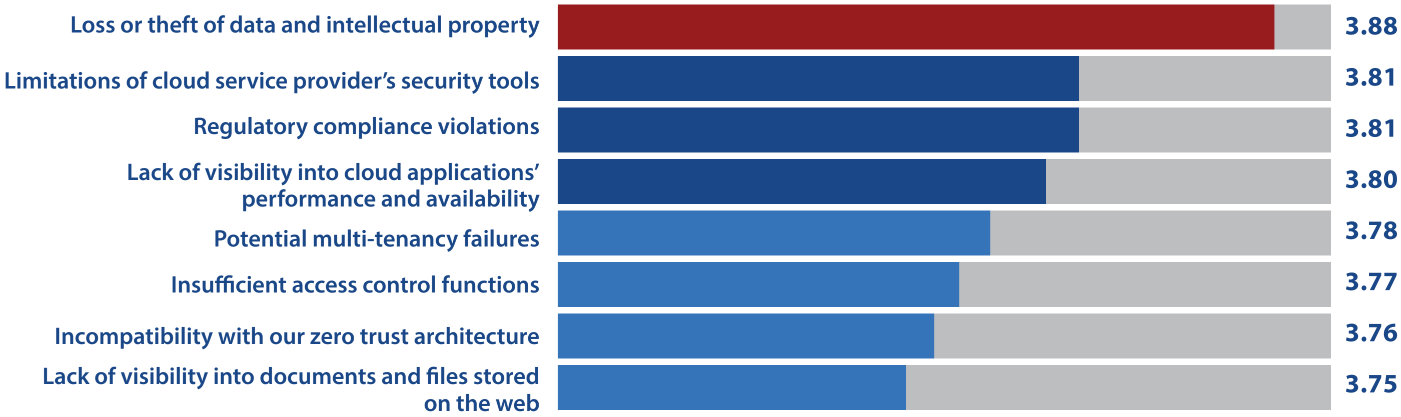

Figure 17: Concern for cloud application security risks and challenges.

Organizations are subscribing to more and more cloud-hosted software-as-a-service (SaaS) applications. They are also migrating internally developed applications to the cloud using infrastructure-as-a-service (IaaS) and platform-as-a-service (PaaS) offerings from Amazon, Google, Microsoft, and others. Most enterprises are feeling fairly comfortable about their security postures vis-à-vis both SaaS applications and cloud hosting platforms (see Figure 7 on page 10).

So we thought this would be a good time to add a new survey question that probed into what aspects of cloud application security are most and least concerning to the respondents (see Figure 17).

> **"It would be fair to say that our survey participants are somewhat apprehensive about many issues related to protecting applications and data in the cloud."**

Not surprisingly, most worrying is the risk of loss or theft of data and intellectual property. Almost one-third (31.9%) of the survey participants are extremely concerned about this issue, and roughly another third (32.7%) are very concerned.

Most respondents were also somewhat or very concerned about security or operational shortcomings in service providers' infrastructure, including their security tools, potential for multi-tenancy failures, and access control functions.

Also prompting worries are lack of visibility into cloud application performance and availability, and into documents and files stored on the web.

We should point out, however, that the scores for all of these issues are pretty tightly grouped. It would be fair to say that our survey participants are somewhat apprehensive about many issues related to protecting applications and data in the cloud, but haven't singled out any other than the general loss or theft of data.

IT Security Budget Allocation

What percentage of your employer's IT budget is allocated to information security (e.g., products, services, personnel)? (n=1,164)

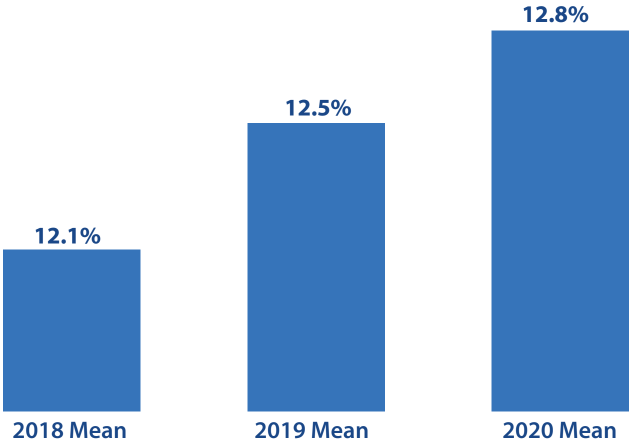

Figure 18: Percentage of IT budget allocated to information security, by year.

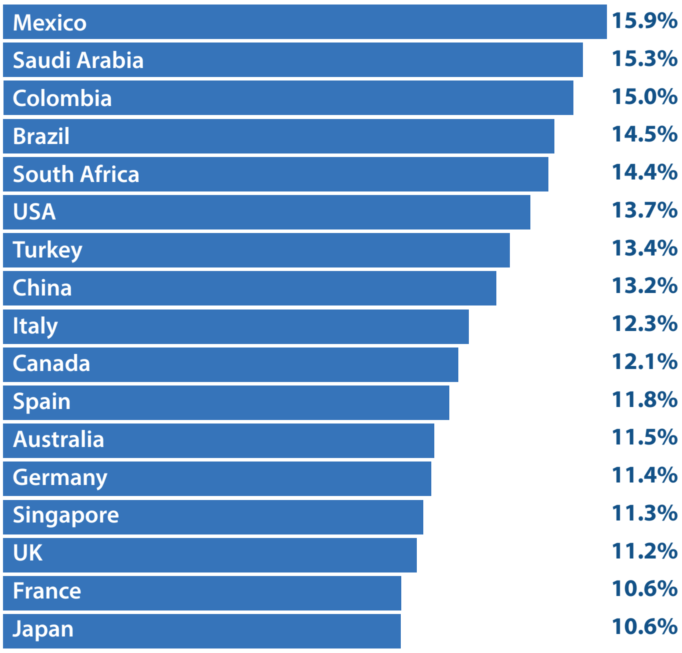

Figure 19: Percentage of IT budget allocated to security, by country.

As we do each year, we asked our respondents to specify the percentage of their employer's overall IT budget that is allocated to information security. As shown in Figure 18, the allocation continues to edge upward: the mean percentage of the IT budget currently being allocated to information security is 12.8% globally — an increase of 0.3% from a year ago, which had increased by 0.4% from the previous year.

Figure 19 depicts mean security spending by country. Relative expenditures didn't change much from the previous year. The same five countries, Mexico, Saudi Arabia, Columbia, Brazil, and South Africa, were at the top (albeit in a slightly different order). The same three countries, the UK, France, and Japan, were at the bottom (in exactly the same order).

> **"The allocation continues to edge upward: the mean percentage of the IT budget currently being allocated to information security is 12.8% globally — an increase of 0.3% from a year ago."**

Section 3: Current and Future Investments

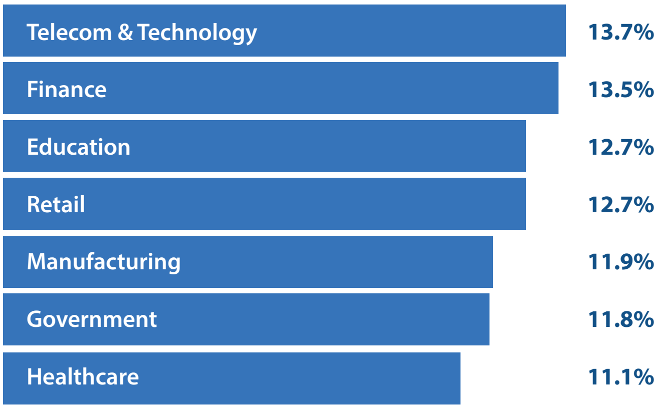

Figure 20: Percentage of IT budget allocated to security, by industry.

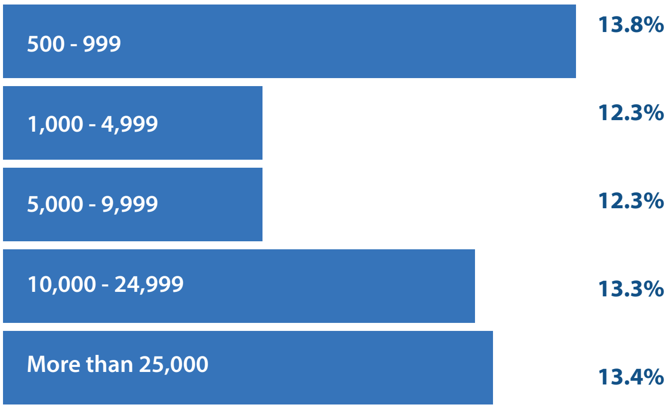

Figure 21: Percentage of IT budget allocated to security, by employee count.

Figure 20 shows spending on security by industry. Telecom and technology, finance, education, and retail, which were in the middle of the pack last year, have now moved up to the top four positions. The percentage of their budgets allocated to security rose from 12.9% to 13.7%, from 11.0% to 13.5%, from 11.8% to 12.7%, and from 11.6% to 12.7%, respectively. Government and healthcare, which were at the top last year, have fallen to the bottom. Their percentage allocations declined from 13.1% to 11.8%, and from 13.2% to 11.1%, respectively.

Figure 21 illustrates spending on security by organization size (i.e., employee count). The order and the percentages changed little from last year, except for small organizations with 500-999 employees. Those small businesses went from almost the lowest percentage last year (12.4%) to the highest this year (13.8%).

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 2020? (n=1,175)

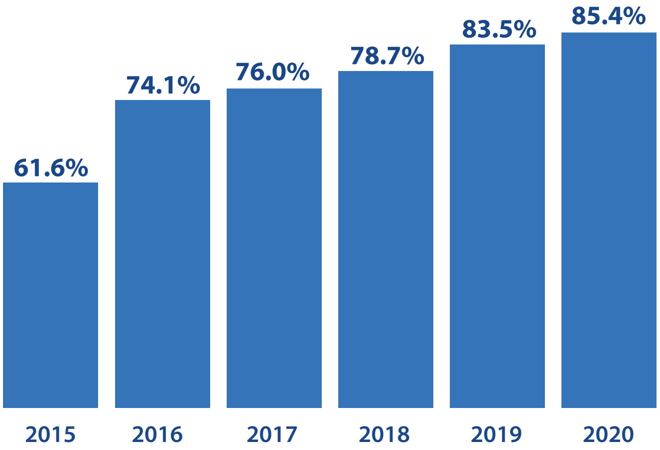

Figure 22: Percentage of organizations with rising security budgets.

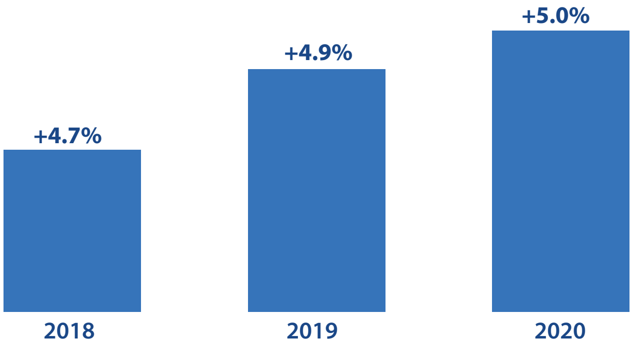

Figure 23: Mean annual increase in IT security budgets, by year.

Money is not a problem for IT security groups. Or at least it's not their biggest problem. Six out of seven of our survey participants (85.4%) said the IT security budget of their organization is going to increase in 2020. That number has been rising for years (see Figure 22).

The magnitude of the increase is substantial: budgets across the globe are expected to increase an average of 5.0% in 2020 (see Figure 23).

Looking at our seven major industries (Figure 24), retail leads the charge with an average budget increase of 5.7%. That industry is actually playing catch-up; the expected budget increase last year was 4.3%, near the bottom of the pack. Healthcare swung the other way: last year it was looking at a 5.5% increase, the highest of any industry, while this year the number is 4.8%, the lowest.

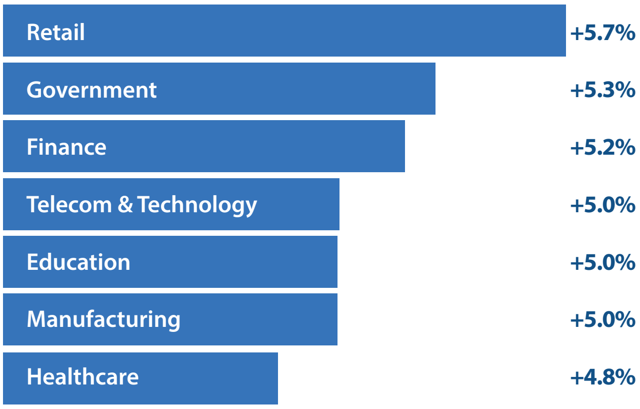

Figure 24: Mean security budget increase, by industry.

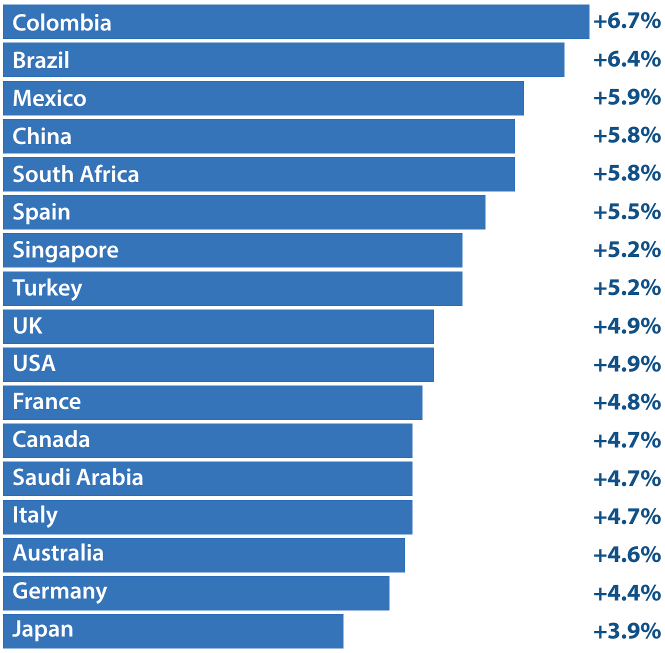

Figure 25: Mean security budget increase, by country.

As shown in Figure 25, respondents in several countries in Latin America will see funding increases of 6.0% or greater, and those in China and South Africa are not far behind at 5.8%. The UK, the US, France, and Canada are just a bit below the average, falling in the 4.7%-4.9% range. Germany and Japan bring up the rear, with 4.4% and 3.9% increases, respectively. Of course, those rates are still a lot better than decreases.

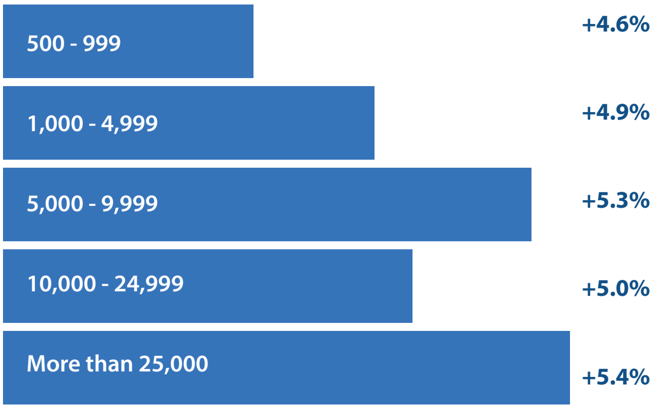

Figure 26: Mean security budget increase, by employee count.

Budget increases are substantial for organizations of all sizes, but somewhat skewed toward very large enterprises (see Figure 26).

> **"Six out of seven of our survey participants (85.4%) said the IT security budget of their organization is going to increase in 2020."**

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=1,170)

	Currently in use	Planned for acquisition	No plans
Advanced malware analysis / sandboxing	62.1%	30.1%	7.8%
Intrusion detection / prevention system (IDS/IPS)	57.5%	31.8%	10.7%
Secure web gateway (SWG)	56.7%	31.7%	11.6%
Secure email gateway (SEG)	56.6%	32.4%	11.0%
Network access control (NAC)	56.2%	33.1%	10.7%
SSL/TLS decryption appliances / platform	56.0%	33.4%	10.6%
Data loss / leak prevention (DLP)	54.9%	35.3%	9.8%
Denial of service (DoS/DDoS) prevention	54.1%	32.8%	13.1%
Next-generation firewall (NGFW)	50.6%	38.3%	11.1%
Network behavior analysis (NBA) / NetFlow analysis	49.9%	36.8%	13.3%
Deception technology / distributed honeypots	48.3%	34.0%	17.7%

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

Security technologies are the foundation of IT security programs. But it can be difficult to decide which of the many choices to prioritize. Certainly it would be helpful to know what your peers think. What cybersecurity products and services are must-haves? Which are the up-and-comers needed to fill gaps and address emerging threats? Are some technologies more hype than reality?

In this section and the four that follow we present information from more than 1,100 IT professionals about the choices their organizations have made and are making about technologies for network security, endpoint security, data-centric security, security management and operations, and identity and access management.

In each case we asked survey participants what technologies are currently in use in their organization, which are planned for acquisition in the next 12 months, and which they're not even contemplating for acquisition or deployment. To make the results easier to absorb, we put the responses in tables and color-coded the cells (see Table 2). Dark blue highlights technologies that are widely used now or are most likely to be deployed soon. Lighter shades indicate lower adoption levels and fewer planned acquisitions. The cells with the "no plans" percentages are gray.

So what do we see when we look at deployed and planned network technologies?

Advanced malware analysis / sandboxing is the most-frequently installed network security technology, used by 62.1% of the organizations. Last year that technology was deployed in only 50.4% of organizations, way down in ninth place on our list. The one-year jump of 11.7% was extraordinary. We believe the high installation rate resulted from the continuing perception that malware is the single most dangerous tool in the hacker's arsenal (see Figure 11 on page 13), combined with the maturing of malware analysis and sandboxing tools and their incorporation into cloud-based security suites.

By the way, in last year's survey, advanced malware analysis and sandboxing had the highest rating of any network security technology in the "planned for acquisition" column of the table. So our data did point it out as the "most likely to succeed" technology of the class.

The other big gainer in installations was deception technology / distributed honeypots, which went from deployment in 41.9% of enterprises to 48.3%, an increase of 6.4%. Again, this rise probably reflects a conjunction of need (adversaries are getting smarter about evading conventional monitoring) and maturing technology (products in this category are becoming more effective and easier to implement).

> **"In last year's survey, advanced malware analysis and sandboxing had the highest rating of any network security technology in the 'planned for acquisition' column of the table. So our data did point it out as the 'most likely to succeed' technology of the class"**

What are the up-and-coming network security technologies in 2020? The categories with the highest "planned for acquisition rates" are:

- Next-generation firewall (NGFW)
- Network behavior analysis (NBA) and NetFlow analysis
- Data loss / leak prevention (DLP)
- Deception technology and distributed honeypots

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=1,178)

	Currently in use	Planned for acquisition	No plans
Basic anti-virus / anti-malware (threat signatures)	71.1%	22.0%	6.9%
Advanced anti-virus / anti-malware (machine learning, behavior monitoring, sandboxing)	61.6%	30.3%	8.1%
Disk encryption	59.6%	31.2%	9.2%
Data loss / leak prevention (DLP)	58.0%	31.5%	10.5%
Application control (whitelist / blacklist)	56.6%	33.1%	10.3%
Digital forensics / incident resolution	50.8%	35.4%	13.8%
Deception technology / honeypots	46.9%	37.5%	15.6%
Containerization / micro-virtualization	46.6%	39.3%	14.1%

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

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

There are no startling changes from last year. Advanced anti-virus and disk encryption swapped the second and third places on the list, data loss / leak prevention and application control switched between fourth and fifth, and deception technology and containerization and micro-virtualization exchanged seventh and eighth positions.

Basic anti-virus and anti-malware retained its position as the biggest must-have in the endpoint security world, but market saturation and lack of major innovation in the category have caused its "planned for acquisition" rate (which includes renewals as well as new installations) to fall to a record low.

The hot categories for acquisition continue to be containerization / micro-virtualization (i.e., browser isolation), deception technology / honeypots, and digital forensics / incident resolution.

But we don't mean to imply that endpoint security vendors are resting on their laurels. The three trends we noted last year are continuing:

1. Endpoint security solutions are making greater use of machine learning and other forms of AI to identify anomalous behaviors.
2. Point tools are being integrated into endpoint protection platforms (EPPs) and endpoint detection and response (EDR) solutions, which simplifies deployment and management of endpoint security and improves analysis.
3. Endpoint security tools and suites are being integrated with other IT security technologies, such as network monitoring tools, advanced security analytics products, and security operations management platforms, to give security teams 360-degree visibility into computing environments and, in some cases, the ability to quickly block malicious activities on endpoints.

> **"The hot categories for acquisition continue to be containerization / micro-virtualization (i.e., browser isolation), deception technology / honeypots, and digital forensics / incident resolution."**

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=1,160)

	Currently in use	Planned for acquisition	No plans
API gateway / protection	63.1%	29.9%	7.0%
Database firewall	61.4%	27.6%	11.0%
Web application firewall (WAF)	59.5%	31.9%	8.6%
Database activity monitoring (DAM)	55.5%	32.2%	12.3%
Cloud access security broker (CASB)	54.9%	30.7%	14/4%
Database encryption / tokenization	54.4%	33.7%	11.9%
Application delivery controller (ADC)	53.8%	34.3%	11.9%
Static/dynamic/interactive application security testing (SAST/DAST/IAST)	52.1%	34.7%	13.2%
File integrity / activity monitoring (FIM/FAM)	51.7%	34.7%	13.6%
Runtime application self-protection (RASP)	51.4%	34.8%	13.8%
Container security tools / platform	48.1%	37.7%	14.2%
Deception technology / distributed honeypots	48.0%	34.4%	17.6%

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

Our next area for measuring security technology adoption is application and data security (see Table 4). As usual, percentages in dark blue correspond to a higher frequency of adoption or acquisition plans, while those in light blue correspond to a lower frequency.

The rising star and new must-have in the application- and data-centric security technology category is API gateway / protection. API gateways route API calls between clients and services in microservices-based applications. But while they are doing the routing, they can centralize and enforce important security functions related to authentication, encryption, message and input validation, content inspection, and DDoS protection. Over the last three surveys the percentage of organizations that have installed API gateway and protection technology has surged from 45.1% (twelfth and last on the list), to 51.2% (seventh position), to 63.1% (first place), an 18% upswing.

The other up-and-comer during the past 12 months is the application delivery controller (ADC), which routes traffic between systems and can be used to centralize and enforce security (like API gateways, but for different types of applications). The portion of organizations with installed ADCs rose from 48.1% to 53.8%, increasing by 5.7%.

The accelerating use of both API gateways and ADCs to enhance security highlights an industry trend toward the convergence of network security and application security. If you are monitoring and validating network traffic, why not also inspect and analyze application packets? If you are inspecting application traffic to find indicators of compromise, why not correlate that data with anomalous behaviors in network flows?

Database firewalls, web application firewalls, and database activity monitoring retained their positions near the top of the list of installed application- and data-centric technologies, and cloud access security brokers (CASBs) have continued to show gains in installations.

"The rising star and new 'must-have' in the application and data-centric security technology category is API gateways / protection"

The leader in the "planned for acquisition" column was container security tools and platforms. We think this is going to be a growth area for years to come. As more enterprises deploy applications using container technology, they are going to need tools that detect vulnerabilities and misconfigurations in containerized environments, enforce security policies, and monitor activities to uncover anomalous behaviors.

Other technologies showing promise for 2020 include runtime application self-protection (RASP), which automatically protects applications from within, application security testing, and file integrity and activity monitoring (FIM/FAM).

Security Management and Operations Deployment Status

Which of the following security management and operations technologies are currently in use or planned for acquisition (within 12 months) by your organization to mitigate the impact of cyberthreats? (n=1,162)

	Currently in use	Planned for acquisition	No plans
Patch management	58.1%	30.3%	11.6%
Advanced security analytics (e.g., with machine learning, AI)	57.1%	35.5%	7.4%
Security configuration management (SCM)	55.4%	32.9%	11.7%
Security information and event management (SIEM)	55.1%	33.3%	11.6%
Vulnerability assessment/management (VA/VM)	55.0%	34.9%	10.1%
Penetration testing / attack simulation software	53.3%	34.0%	12.7%
User and entity behavior analytics (UEBA)	51.8%	36.1%	12.1%
Full-packet capture and analysis	51.0%	36.8%	12.2%
Security orchestration, automation and response (SOAR)	48.6%	37.1%	14.3%
Threat intelligence platform (TIP) or service	48.2%	38.4%	13.4%

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

Last year we introduced a new question to our survey to assess the deployment status of what we've called security management and operations technologies. These technologies help organizations monitor their security posture, fix vulnerabilities and weaknesses in their defenses, detect suspicious activities on their networks, and automate security processes. They tend to be cross-domain in scope, collecting data and managing security processes across networks, locations, applications, and endpoints.

As shown in Table 5, the technologies most often in use today are primarily those designed to reduce the attack surface by uncovering and remediating vulnerabilities, misconfigurations, and problems with security controls. They include patch management (in first place, used in 58.1% of the organizations), security configuration management (third place, 55.4%), vulnerability assessment / management (fifth place, 55.0%), and penetration testing / attack simulation (sixth place, 53.3%).

> **"The dynamo of the category, however, is advanced security analytics, which leaped from use in 41.3% of organizations last year to 57.1% 12 months later"**

Section 3: Current and Future Investments

The dynamo of the category, however, is advanced security analytics, which leaped from use in 41.3% of organizations last year to 57.1% 12 months later. In seven years of surveys we have never seen a security technology show up for the first time in so many organizations (15.8%) within the span of one year. Why this surge in acceptance?

First, security analytics can help people on virtually every IT security team do their jobs faster and better. Advanced analytics are now being used to detect external and insider threats, investigate incidents, detect anomalies in network traffic, identify compromised accounts, hunt for cyberthreats, and perform many other core cybersecurity tasks (page 36).

Second, IT groups have recognized that they now collect far too much security-related data for humans to organize and analyze on their own. Advanced security analytics products that incorporate machine learning and AI features enable small staffs of analysts to find IoCs and anomalous behaviors in vast amounts of text, images, video, and files, and to react quickly. For more thoughts on the importance of security products with AI capabilities, see our discussion on page 48.

Our survey respondents also tell us that the security management and operations technologies most likely to be acquired in 2020 are:

- Threat intelligence platform (TIP) or service
- Security orchestration, automation, and response (SOAR)
- Full-packet capture and analysis
- User and entity behavior analytics (UEBA)
- Advanced security analytics

It is interesting to note that TIP and SOAR are at the bottom of our list in terms of current use, but at the top in terms of plans for acquisition. Clearly these are up-and-comers with a lot of room for growth. They also represent additional ways we might catch up to the bad guys: by getting to know more about them and their methods, and by automating security processes so we can collect data, analyze it, and react before they can cause harm.

Identity and Access Management Deployment Status

Which of the following identity and access management (IAM) technologies are currently in use or planned for acquisition (within 12 months) by your organization to securely control access to computing resources? (n=1,164)

	Currently in use	Planned for acquisition	No plans
Password management / automated reset	61.3%	27.2%	11.5%
User/account provisioning and de-provisioning	55.4%	32.7%	11.9%
Privileged account/access management (PAM)	52.9%	33.2%	13.9%
Two-/multi-factor authentication	52.6%	33.5%	13.9%
Single sign-on (SSO)	52.6%	33.7%	13.7%
Identity analytics	53.5%	33.0%	13.5%
Tokens (hardware or software)	52.3%	32.0%	15.7%
Risk-based/step-up authentication	51.4%	36.3%	12.3%
Smart cards	50.7%	32.5%	16.8%
Identity-as-a-Service (IDaaS).	49.3%	36.9%	13.8%
Biometrics	48.5%	36.9%	14.6%
Federated identity management (SAML, Oauth)	46.1%	37.1%	16.8%

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

Identity and access management (IAM) once seemed to be a rather dull field where most of the work could be palmed off on the IT operations staff. That was because we were willing to assume that anyone who connected to the network from inside a corporate facility was an employee and could be trusted, and that nobody else mattered much.

But that time has passed. Employees work from home and on the road, business partners need access to almost all the same resources as employees, and adversaries have gotten very good at stealing (or buying) valid credentials. Plus, security regulations and privacy laws require tighter access controls over data, and much better monitoring of who has accessed what. These changes have put IAM squarely in the middle of issues related to data protection, compliance, fraud reduction, customer service, and zero trust architectures.

That said, our survey shows that the deployment of IAM products hasn't changed much in the last 12 months (see Table 6). The same core technologies — password management, user and account provisioning, privileged account and access management (PAM), two- and multi-factor authentication (2FA/MFA), and single sign-on (SSO) — have stayed at the top of the list, with about the same number of installations.

But it’s worth noting that the technologies that showed the most growth in installations were the newer ones in the bottom half of the list: identity analytics (+1.7%), risk-based and step-up authentication (+2.1%), smart cards (+2.8%), Identity-as-a-Service (2.9%), biometrics (+10.9%), and federated identity management (+3.3%).

You caught that one outlier statistic, right? We knew we couldn’t sneak that by you. Yes, in the last 12 months, biometrics was implemented in almost 11% of the organizations in the survey, taking its installed base from 37.6% to 48.5%. Biometrics for authentication is not yet a must-have, but clearly it is winning over a lot of enterprises.

To confess, last year we were a bit skeptical about the level of interest in biometrics. It looks like concerns about ease of implementation were swept away by improvements in the technology and widespread acceptance of both fingerprint readers and face recognition on smartphones.

Looking ahead, the highest rates in the “planned for acquisition” column for IAM technologies are:

- Federated identity management
- Biometrics (yes, still surging ahead)
- Identity-as-a-Service
- Risk-based and step-up authentication

Preferences for Machine Learning and AI

Select the option that best describes your organization's overall preference for purchasing security products that feature machine learning (ML) or artificial intelligence (AI) technologies. (n=1,185)

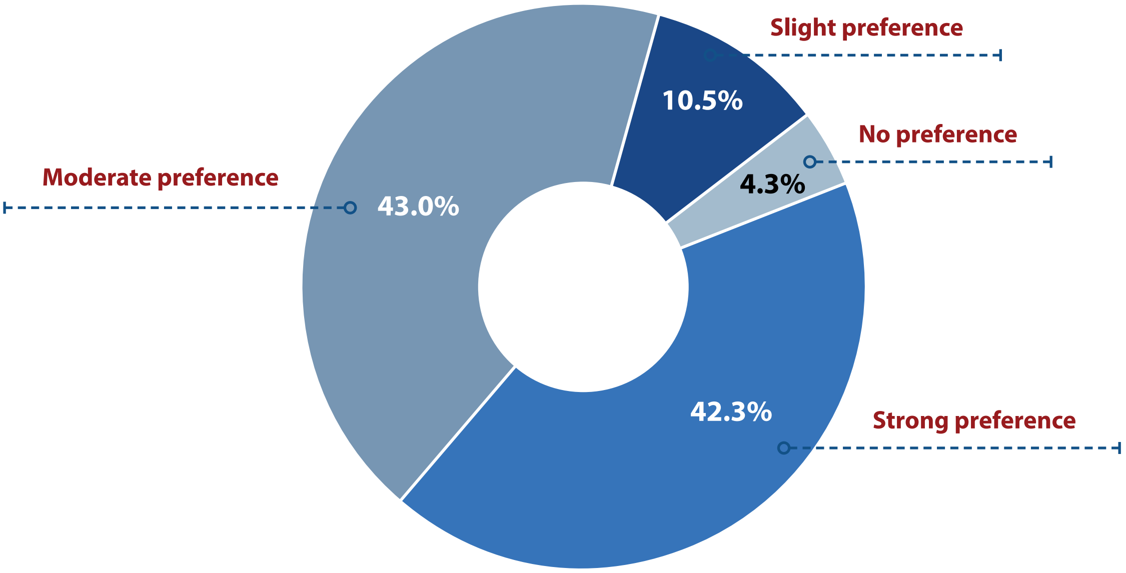

Figure 27: Preference for security products with machine learning and AI.

Why all the fuss about including machine learning (ML) and other forms of AI in IT security products?

One factor to consider: today we collect so much security-related data that, even when we know what to look for, we can't possibly analyze all of it "manually" (that is, with human brains alone). We need AI-based security tools to crunch through big data quickly and find IoCs and anomalous behaviors.

In addition, AI capabilities such as natural language processing (NLP) and image recognition act as "force multipliers," enabling us to detect threats and frauds in languages we don't understand and in images and videos we would never have time to view and interpret.

But the importance of ML and AI go even further. Consider the observation of Donald Rumsfeld, former U.S. Secretary of Defense: "There are known knowns... There are known unknowns... But there are also unknown unknowns. There are things we don't know we don't know." Threat actors are coming up with so many tricks that we can't possibly anticipate what they are going to be or how to detect them. But given enough data, ML and other AI technologies can find patterns associated with data breaches and other negative outcomes, including correlations and anomalies that no human would ever think to look for. AI can reveal to us the unknown unknowns.

> **"We might even go out on a limb and say that machine learning and other AI technologies offer our last chance to catch up with and overtake the bad guys."**

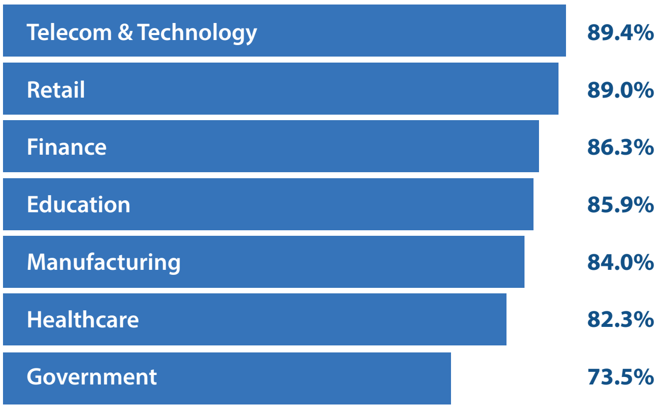

Figure 28: Strong or moderate preference for security products with machine learning and AI, by industry.

We might even go out on a limb and say that machine learning and other AI technologies offer our last chance to catch up with and overtake the bad guys.

As shown in Figure 27, the vast majority of our survey participants agree, at least to some extent. A notable 42.3% declared a strong preference for purchasing security products that feature ML and AI, and an additional 43.0% expressed a moderate preference. Only 14.8% displayed a slight preference or said they had no preference.

This strong interest cut across almost all of the major industries included in our survey (see Figure 28). Telecom and technology and retail top the list, with 89.4% and 89.0% of those respondents expressing strong or moderate preferences for products with AI. Not far behind were finance (86.3%), education (85.9%), manufacturing (84.0%), and healthcare (82.3%). The only laggard in this area was government, but even there almost three out of four respondents (73.5%) indicated a strong or moderate preference.

A breakdown by country (Figure 29) shows some intriguing results. Turkey must be a hotbed of AI enthusiasm. In that nation, 70.0% of respondents asserted a strong preference, 30.0% a moderate preference, and nobody at all admitted to any less interest. Brazil was almost as enthusiastic, with 97.0% of survey participants having strong or moderate preferences. On the other end of the spectrum, respondents in Germany, Canada, Japan, and Australia were the least impressed.

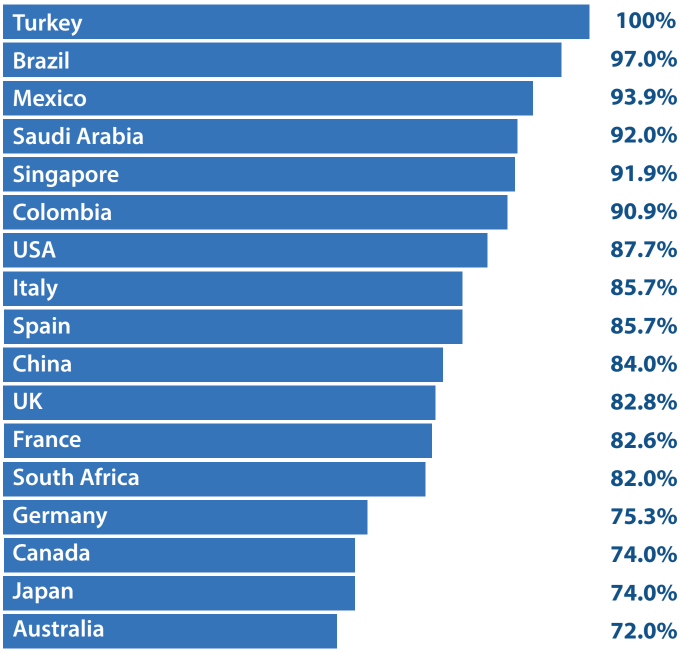

Figure 29: Strong or moderate preference for security products with machine learning and AI, by country.

Section 4: Practices and Strategies

Security Analytics Use Cases

How is your organization using security analytics products to reduce information security risks? (Select all that apply.) (n=1,179)

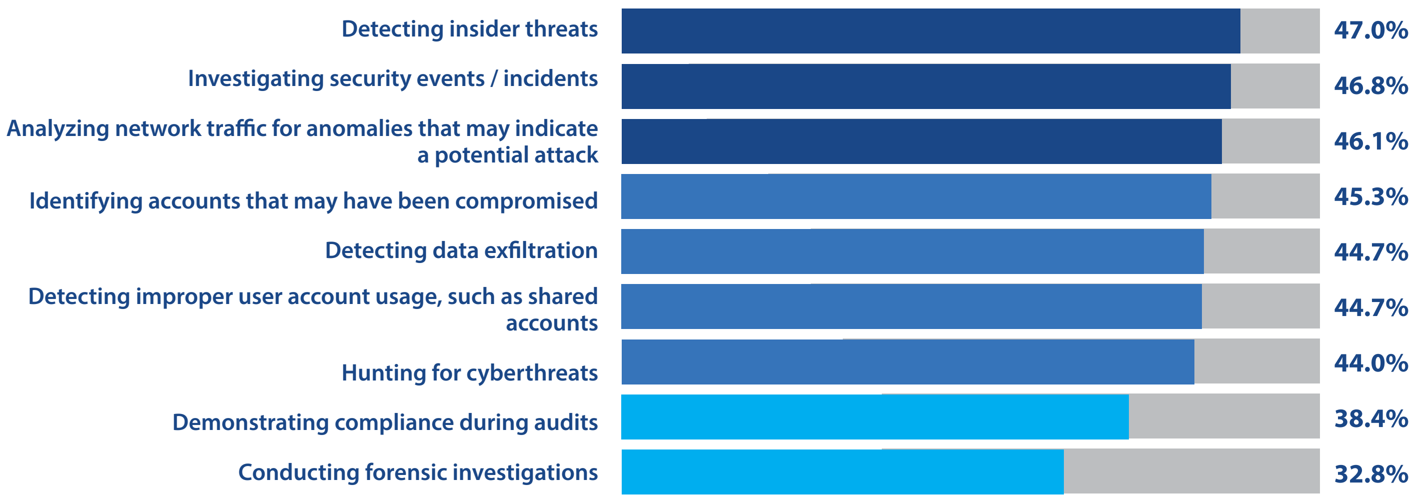

Figure 30: How security analytics products are being used.

In our discussion of security management and operations technologies, we pointed out that advanced security analytics was the dynamo of that category, with a huge surge in installations last year and the prospect of very rapid growth in 2020 as well (see pages 30 and 31). To find out more about this phenomenon, we added a question to this year's survey about exactly how organizations are using security analytics products. You can see the answers in Figure 30.

The most common use cases are detecting insider threats (47.0%), investigating security events and incidents (46.8%), and analyzing network traffic for anomalies that might indicate attacks (46.1%).

> **"The most common use cases are detecting insider threats (47.0%), investigating security events and incidents (46.8%), and analyzing network traffic for anomalies that might indicate attacks (46.1%)."**

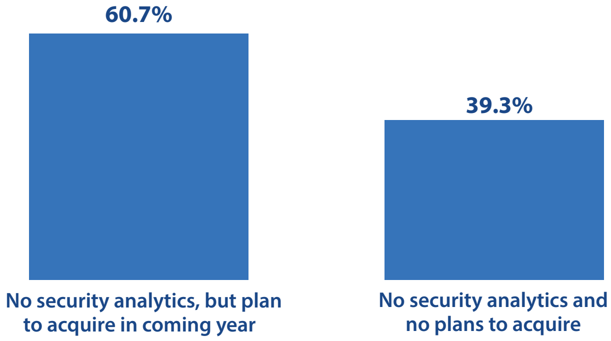

Figure 31: Plans of organizations that do not have security analytics in production.

These use cases were followed closely by identifying accounts that may have been compromised (45.3%), detecting data exfiltration (44.7%), detecting improper account usage (44.7%), and hunting for cyberthreats (44.0%). Bringing up the rear, but by no means trivial, were demonstrating compliance during audits (38.4%) and conducting forensic investigations (32.8%).

The fact that all but one of these use cases are found in at least a third of the organizations surveyed testifies to how useful security analytics are to virtually every team in the IT security group.

It is worth noting that analytics tools provide the only effective way to address certain problems in cybersecurity. For example, you can't uncover insider threats by finding IoCs like malware samples or suspicious changes to registries. You need to use analytics to find anomalous behaviors such as employees logging on to applications they don't normally use or downloading unusual volumes of data.

The data in Figure 31 provides yet more evidence of the rise of security analytics in cybersecurity. Of the respondents who said their organizations had not yet put security analytics tools into production, 60.7% said they were planning to acquire such tools in 2020.

Monitoring the Application Security Stack

Describe your agreement with the following statement: "Monitoring and managing my organization's entire application security stack (e.g., DDoS protection, WAF, RASP, API security) from one platform would likely reduce complexity and save considerable time." (n=1,194)

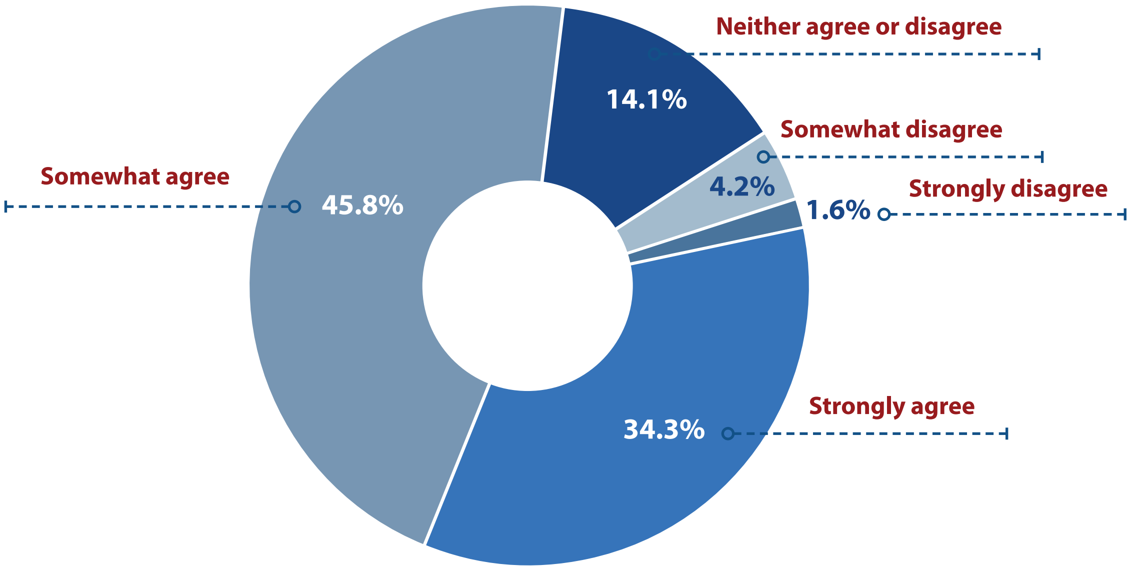

Figure 32: Agreement with statement about monitoring an application security stack from one platform.

Integration between "adjacent" tools is always an interesting topic of discussion for cybersecuity and IT operations professionals. In some technology areas, tool integration and single source solutions are a "nice to have," while in others they are deemed essential for productivity and effectiveness.

We wondered how this would play out in the field of managing application security tools such as products for DDoS protection, web application firewalls (WAFs), runtime application self-protection (RASP), and API security. To find out, we asked survey participants to rate how much they agreed with the statement: "Monitoring and managing my organization's entire application security stack (e.g., DDoS protection, WAF, RASP, API security) from one platform would likely reduce complexity and save considerable time."

As you can see from Figure 32, 34.3% strongly agreed, and another 45.8% somewhat agreed, leaving less than 20% who disagreed or had no opinion.

> **"Integration between 'adjacent' tools is always an interesting topic of discussion for cybersecuity and IT operations professionals."**

We believe that this near-unanimity comes from respondents' knowledge of the benefits of a single platform for monitoring and management, such as:

- Easier management, since they can use one console instead of many
- Better analysis and decision making, since data collected from multiple tools can be correlated and analyzed together

Section 4: Practices and Strategies

The percentage of respondents who agreed was highest in finance (87.0%), retail (also 87.0%), manufacturing (86.5%), and telecom and technology (85.0%). (See Figure 33). Agreement was a notch lower (although still high), for education (74.2%), healthcare (67.1%), and government (62.0%).

When you break the data down by organization size, you find that an integrated platform in this area is most highly prized by small organizations (500-999 employees) and medium-sized ones (1,000-4,999 employees - see Figure 34). This finding is consistent with our experience that small- and medium-sized organizations have more generalists on staff and fewer specialists who manage only one type of tool, say, WAFs. However, respondents from large and very large organizations agreed with the statement at only slightly lower rates, so clearly they too value the same types of benefits.

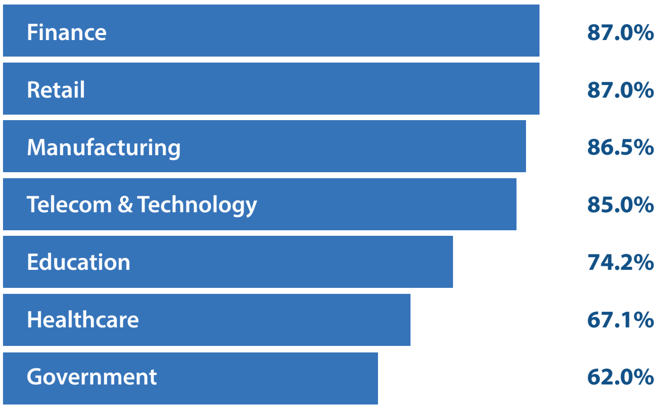

Figure 33: Agreement by industry.

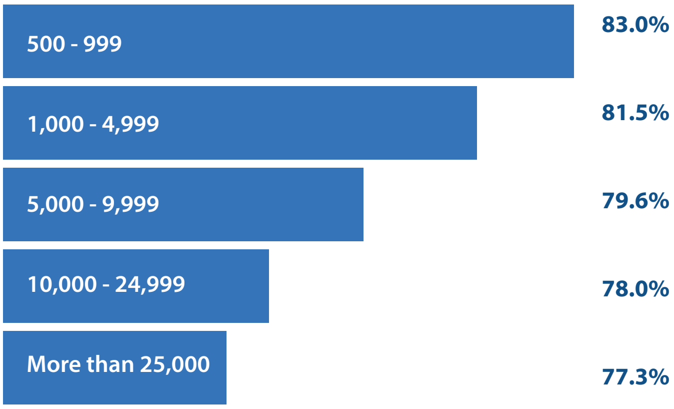

Figure 34: Agreement by employee count.

SSL/TLS Traffic Decryption

What percentage of SSL/TLS-encrypted web traffic do you estimate is being decrypted for inspection by network security tools? (n=1,150)

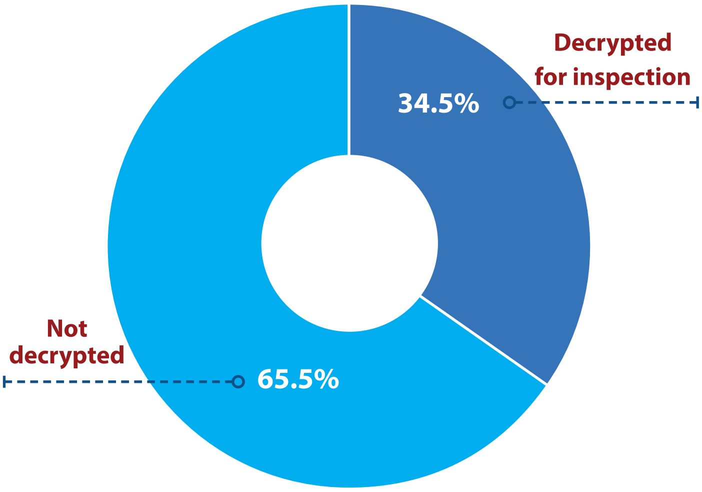

Figure 35: Percentage of SSL/TLS web traffic decrypted for inspection.

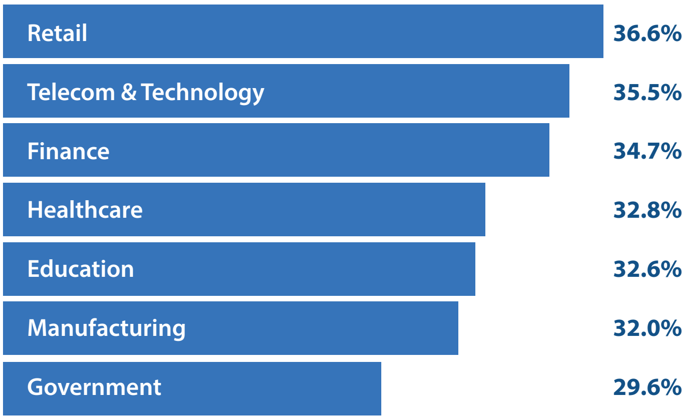

Figure 36: Percentage of SSL/TLS traffic decrypted, by industry.

Why is encrypted web traffic like the weather? Because everybody talks about it, but nobody does anything about it. Or at least they don't do enough about it.

Everyone knows that threat actors like to hide malware and command and control messages in encrypted web traffic. So we were surprised and dismayed to find that organizations decrypt only slightly over a third (34.5%) of SSL/TLS-encrypted web traffic for inspection by network security tools (see Figure 35). That leaves way too big a blind spot! We suspect the reason is that decryption uses up a lot of cycles on network and security devices, which makes it expensive.

Organizations in retail, telecom and technology, and finance do a somewhat better job than average (see Figure 36). That is probably because they have the most interactions with customers and clients over the web, and know the importance of both securing and inspecting web traffic. But we had really expected them to do even better. Government agencies are least likely to decrypt SSL/TLS traffic (29.6%). That is scary when you think about how much information about us those agencies store.

As we look around the globe, Saudi Arabia is the only country that decrypts more than half of its SSL/TLS-encrypted traffic (52.3%). China and Mexico decrypt the least (26.9% and 25.8%).

We should note that decryption isn't the only challenge enterprises face related to capturing, inspecting, and analyzing network traffic. There can be many reasons why the network traffic available to security teams may be incomplete, including SPAN (Switched Port Analyzer) connections that drop traffic when switches are overloaded, and the practice of sampling NetFlow data rather than capturing the complete traffic stream. In some cases security teams don't even realize that they don't have access to all network traffic and metadata! IT organizations need to take a holistic view of gaps in how they acquire and examine network traffic and look at network devices and services that can fill those gaps.

We hope to see these statistics improve in coming years. As someone wise once said: "Prepare and prevent, don't repair and repent."

Technologies Used for Zero Trust Architectures

Which of the following security technologies play a role in your organization's progress toward a zero trust architecture? (Select all that apply.) (n=1,170)

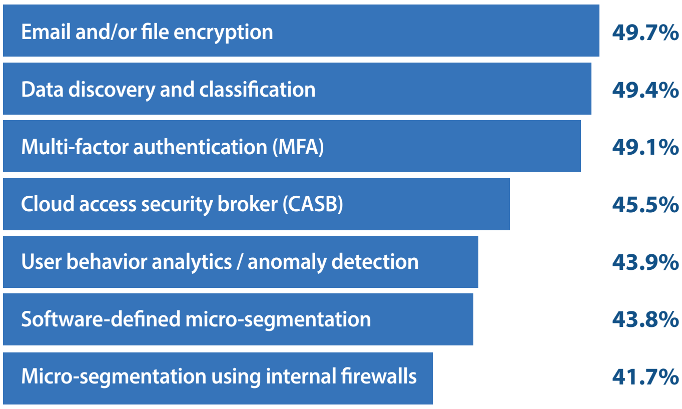

Figure 37: Security technologies playing a role in progress toward a zero trust architecture.

Zero trust architectures are a response to the de-perimeterization of today's computing environments. The central principle is that every person and process, whether physically connected to the corporate network or on the internet, starts from "zero trust" and needs to authenticate themselves and establish a level of trust before accessing any information assets. Moreover, users and processes should not be able to move laterally across systems, networks, or cloud platforms; access should be limited to what a person or process needs to do his/her/its job.

Security challenges relating to zero trust architectures include implementing effective (but not overly onerous) authentication processes, performing micro-segmentation of networks and systems so attackers with stolen credentials are restricted to small segments of the environment, and generally making it harder for unauthorized users to access data, files, and applications.

In this year's survey we added a question to find out what security technologies organizations are using to progress toward a zero trust architecture (see Figure 37).

Respondents in organizations that had started down the path most often cited email and file encryption (49.7%), data discovery and classification (49.4%), and multi-factor authentication (MFA – 49.1%). These are all well-proven and widely adopted technologies, now being pressed into service to support a new concept.

Other technologies used slightly less frequently to enable zero trust architectures are CASBs (45.5%), user behavior analytics / anomaly detection (43.9%), software-defined micro-segmentation (43.8%), and micro-segmentation using internal firewalls (41.7%).

We were a little surprised not to see software-defined micro-segmentation cited more often, since micro-segmentation is a major contributor to zero trust architectures and software-defined micro-segmentation is more flexible and dynamic than device-based types. However, software-defined micro-segmentation is a relatively new technology, and we expect to see adoption rise as enterprises become more familiar with it.

And there will be many opportunities for that. Two-thirds of organizations that have not started to implement a zero trust architecture plan to do so (see Figure 38).

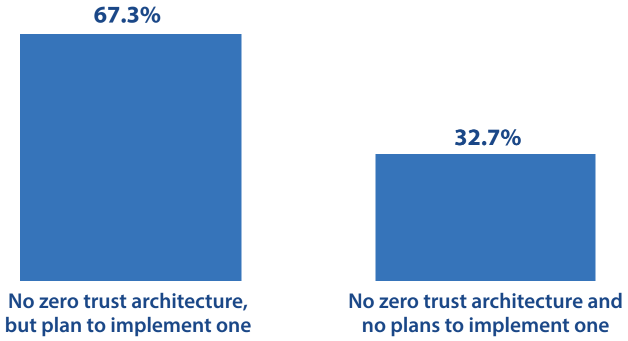

Figure 38: Plans of organizations that have not implemented a zero trust architecture.

Security Applications Delivered via the Cloud

What percentage of your information security applications and services is delivered via the cloud? (n=1,164)

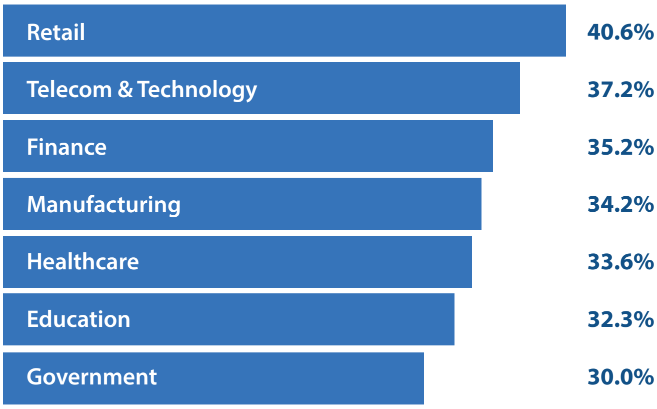

Figure 39: Percentage of security applications and services delivered from the cloud, by industry.

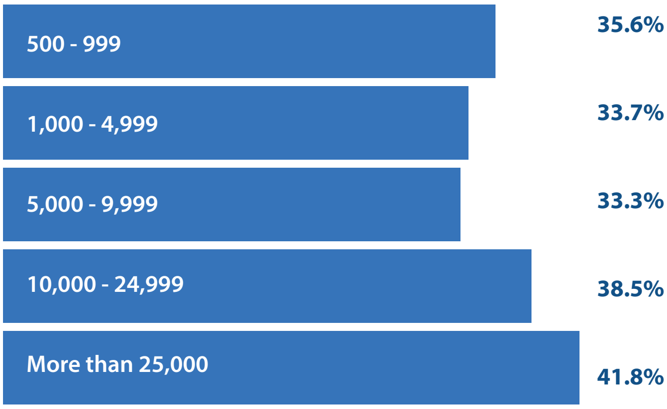

Figure 40: Percentage of security applications and services delivered from the cloud, by employee count.

We know that everybody’s applications are being moved to the cloud and/or being subscribed to in the form of X-as-a-Service (FYI, the term “X-as-a-Service” is shorthand for “Anything-as-a-Service” or “Everything-as-a-Service”).

But how much information security is being delivered from the cloud? You asked, so we found out. The answer is a little over a third, or 35.7%, to be precise.

We’re not surprised. There is hardly an IT security vendor that doesn’t provide a cloud-based version of its product. That is partly for the convenience of customers who don’t want the hassle of operating or upgrading software on premises. But there are also some strong technical reasons for hosting IT security technology in the cloud:

- The availability of massive amounts of processing power for data collection and analysis
- The superior economics of spreading infrastructure costs and security expertise across multiple customers

This was the first time we asked this question, but we expect to see the percentage rise in coming years.

We can see some variation across industries, as shown in Figure 39. Retail, telecom and technology, and finance are ahead of the pack in their adoption of cloud-based security applications and services. We surmise this is at least in part because they are early adopters of many types of technology, and because they are very distributed (cloud-based security services provide better performance for remote offices than servers and appliances in a few central data centers). Government agencies somewhat lag the other industries, probably because of laws and regulations that prohibit them from moving some types of data offsite.

Figure 40 shows results by size of organization. Clearly, very large enterprises (more than 25,000 employees) are the most comfortable obtaining their security applications and services from the cloud. However, small organizations (500-999 employees) are actually slightly more aggressive adopters than their larger counterparts. They may find the most value in offloading management tasks to the service provider.

Bolstering Security Through Formal Training

Describe your agreement with the following statement: "Classroom and/or online IT security training has helped me better protect my organization and/or my customers' critical assets." (n=1,200)

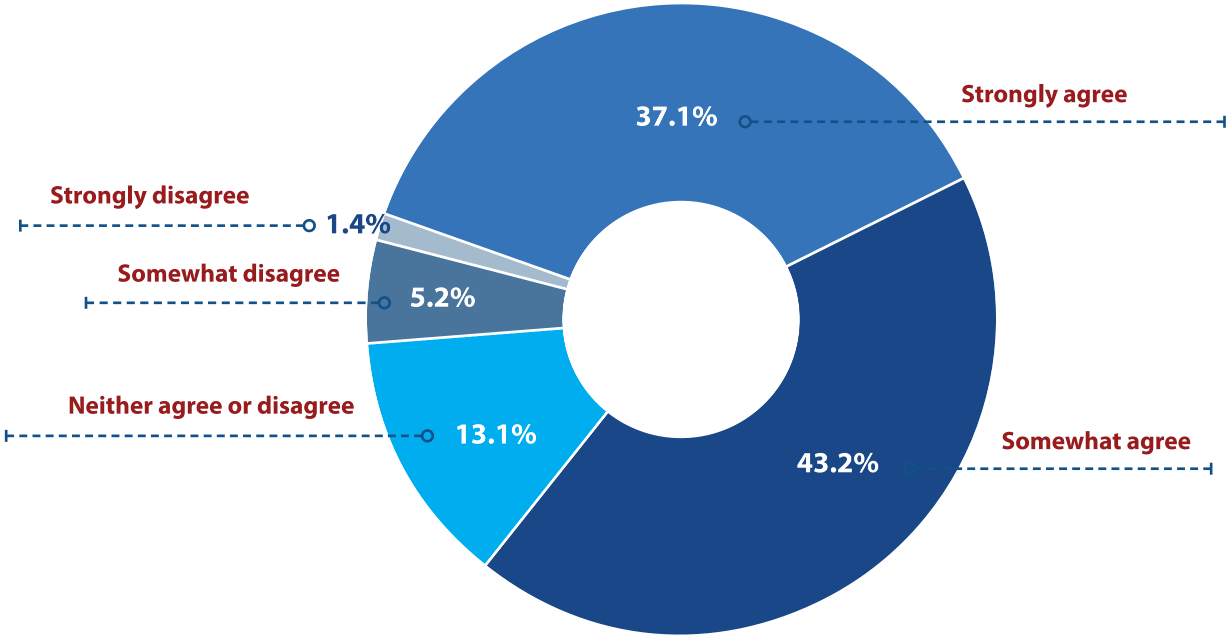

Figure 41: Agreement with statement about IT security training helping protect critical assets.

You've probably noticed one of the major themes in this report: a far-reaching shortage of skilled IT security personnel. The shortage affects every major role in IT security and is getting worse (page 12). "Lack of skilled personnel" is tied for the top spot in our list of factors that are preventing organizations from defending themselves from cyberthreats (page 17).

So what can you do about this chronic skills shortage? Here are some options:

1. Dig through that stack of resumes one more time, hoping you might have overlooked good candidates
2. Post open positions on more online job boards and dig through even more resumes
3. Hire recruiters who charge outrageous fees but don't understand the job requirements
4. Find qualified people at other companies and offer to double their compensation
5. Train existing IT team members so they can step up and fill the openings

Section 4: Practices and Strategies

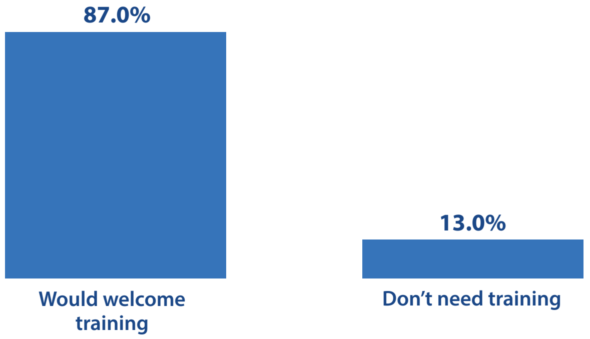

Figure 42: Attitude toward IT security training of people who have not had any.

Let's run with option #5 for a moment. You can find a number of firms offering high-quality IT security training. But do your current employees want additional training? Do they view it as a valuable opportunity to enhance their skills and career prospects, or an unpleasant obligation that takes them away from their work?

Definitely the former. We asked survey participants who have had IT security training how much they agreed with the statement: "Classroom and/or online IT security training has helped me better protect my organization and/or my customers' critical assets." Four out of five, a total of 80.3%, agreed or strongly agreed (see Figure 41). Only 6.6% disagreed, and the rest had no opinion.

We also asked respondents who hadn't received IT security training if they were interested. A whopping 87% said they would welcome training, and only 13% thought they didn't need any (see Figure 42).

Memo to IT managers: Offer IT security training to your current staff. They value it, and it will help them do a better job for your organization.

**"Memo to IT managers:
Offer IT security training to your current staff. They value it, and it will help them do a better job for your organization."**

Benefits of Achieving Professional Certification

Which of the following benefits have you experienced as a result of achieving one or more IT security professional certifications? (Select all that apply.) (n=1,200)

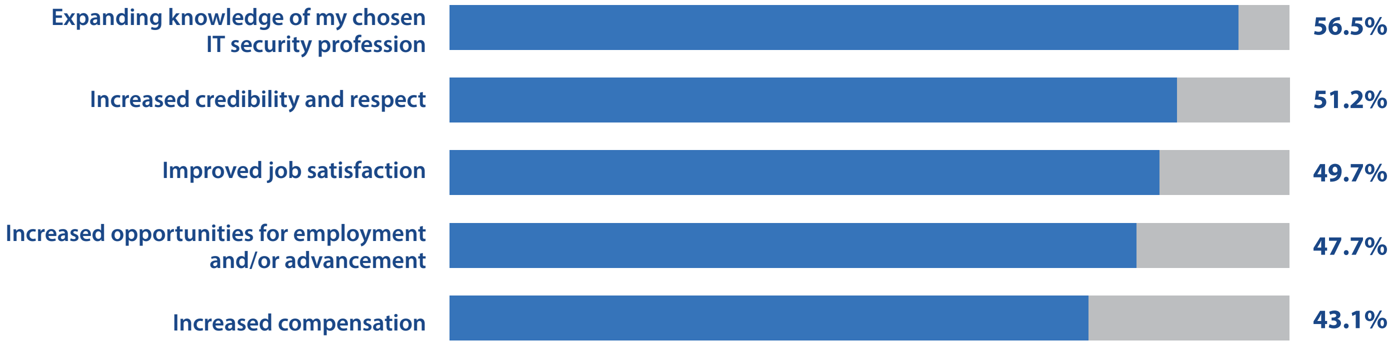

Figure 43: Benefits from achieving IT security professional certification.

While we're on the topic of training to fill the gaps in advanced IT security skills, let's consider professional certification. There are many reasons to attend training courses that lead to IT security certification. But what benefits from these credentials do people experience in practice?

We asked our survey participants who have earned one or more certifications to select the benefits they received related to knowledge, recognition, and career advancement.

Spoiler alert: We expected increased compensation to be the #1 benefit in most situations, but it wasn't first in any country, industry, or organization size in our survey.

As you can see in Figure 43, the benefit cited most often was expanded knowledge, followed by increased credibility and respect and improved job satisfaction. Increased opportunities for employment or advancement and higher compensation were not far behind, but they were in the last two positions.

Expanded knowledge of my chosen IT security profession		Increased credibility and respect	Improved job satisfaction
Canada China France Germany Japan	Singapore South Africa Spain Turkey USA	Brazil Colombia Italy Mexico Saudi Arabia	Australia UK

Table 7: Professional certification benefit cited most often, by country.

> **"The benefit cited most often was expanded knowledge, followed by increased credibility and respect and improved job satisfaction."**

There were some interesting differences among countries regarding the benefit cited most often (see Table 7). Expanded knowledge was the most common benefit in 10 of the countries in our survey, while increased credibility and respect was the most important in five, and improved job satisfaction in the remaining two. If you can see a pattern in this variation (language? culture? employment practices?) let us know.

We also asked respondents who haven't yet received any IT security certifications if they planned to work toward one. By a two-to-one ratio they plan to do so (see Figure 44).

The bottom line: almost all the IT professionals we surveyed not only like training, they see benefits in certifications in terms of job satisfaction and career advancement.

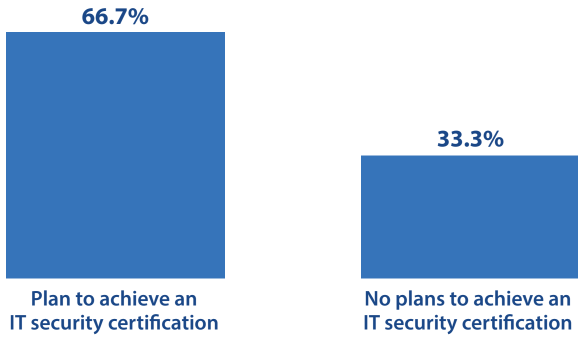

Figure 44: Plans of respondents who do not have IT security certification.

How Might COVID-19 Affect IT Security?

As this report is being published in March 2020, the road ahead has taken a sharp turn, and no one really knows where it's heading. COVID-19 has upended lives and economies across the world. Some of the trends captured in this survey may be altered or even reversed for a time. However, while any predictions made today are highly speculative, there is value in exploring how COVID-19 might affect our industry.

Changes to business are altering the threat landscape

Threat actors are already taking advantage of the pandemic. Websites are selling non-existent masks and disinfectants. Phishing campaigns feature malware attachments disguised as safety recommendations and pandemic maps.

However, the bigger issue is that COVID-19 is changing the way we do business, and cybercriminals and state-sponsored hackers are monitoring those changes so they can pounce on new targets. IT security teams must try to anticipate the changes wrought by COVID-19 and how threat actors will attempt to exploit them. For example:

- **Much more business is being conducted online,** for small- and medium-sized businesses as well as large ecommerce companies. Cybercriminals will be highly motivated to attack these new targets.
- **Vastly more employees are working from home,** dramatically expanding the attack surface of many organizations. Undoubtably threat actors will develop new ways to penetrate corporate networks by compromising weakly defended family PCs and home wireless networks.
- **Adoption is soaring for online meeting and team collaboration tools.** We wouldn't be surprised if adversaries are working furiously creating techniques to steal credentials, gain a foothold on collaborative platforms, and access confidential data shared by users.

These changes are also forcing enterprises to rethink network and security architectures. For instance, if most employees are working from home, instead of backhauling all network traffic to the corporate data center for inspection, VPN split tunneling can be used to send much of the traffic directly to the cloud where it can be inspected by a cloud web proxy with isolation, a cloud firewall, or another cloud-based security service.

IT security teams: crisis management now, accelerating adaptation later?

Today, most IT security teams will be locked into crisis management, supporting overstressed employees and systems while coping with their own personal and family challenges. Also, the dire economic outlook will likely lead to cuts in IT security budgets for the first time since this survey began. Most projects to upgrade security technologies and practices will be slowed or temporarily halted.

But we think these dark clouds will have a silver lining, eventually. When the pandemic recedes and economic activity recovers, enterprises will need to accelerate the adoption of key security technologies such as:

- Network security and application and data security technologies to safeguard higher levels of ecommerce
- Endpoint security and wireless security products to protect workers at home
- Advanced authentication and and zero trust solutions to provide remote employees with secure access to applications
- Cloud security investments to defend online meeting and team collaboration tools and other cloud-based apps

During this crisis, and perhaps beyond, more employees and IT security teams will work from home, which will increase the demand for:

- Advanced tools to better monitor, manage, and update remote systems
- IT security solutions that offer centralized management across hybrid environments, delegated administration, and other features for administering highly distributed environments

In conclusion

No one can predict where the COVID-19 pandemic will take us. However, we suggest that you devote some time to anticipating how threat actors are going to exploit the current disruption, and how you can block them. We are also optimistic enough to think that the trends we discuss on the next three pages of this report will resume when we've gotten a little farther down the road ahead.

Long-term Trends in IT Security

Our previous reports concluded with a summary of four or five key technologies that were likely to influence the agenda of IT security professionals in coming years. This time we're taking a slightly different approach to peering down the road ahead. We're outlining a handful of common strategies that multiple vendors and service providers are following to respond to the challenges facing IT security organizations today.

To start, let's summarize some of the issues facing IT security groups that have been highlighted in our survey:

- An ever-expanding array of platforms and device types to defend, each with its own set of vulnerabilities: SaaS applications, PaaS, and IaaS platforms that host applications in the cloud, mobile devices, industrial control systems, and internet of things devices and sensors
- The rapid evolution of virtualization and container technologies for deploying and managing applications
- DevOps orchestration and automation techniques and tools for developing and testing software
- Low levels of user security awareness
- Rogue insiders
- Cybercriminal gangs and state-sponsored hacker organizations that continually grow bigger, more organized, and more professional
- A persistent shortage of skilled IT security professionals

Each of these issues brings its own set of challenges for enterprises and for the IT security vendors and service providers that support them. Some of these challenges relate to a loss of visibility and control, the need to deploy security tools and manage policies in extremely diverse and dynamic environments, the inability to trust insiders and account credentials, and a constant stream of innovative new attack techniques.

So how can this litany of woe help us understand the road ahead? By enabling us to see that the multitude of enhancements and additions to IT security products and services represents a small set of logical responses to these issues. Each of these responses is an answer to the question: "What strategies will allow us to cope with the growing complexity and diversity of our computing environment and the increasing sophistication of our adversaries?"

Let's look at those strategies and see how they are being applied.

Extend the reach of today's IT security tools across the entire attack surface.

Security vendors and service providers are busy adapting their solutions to cloud platforms, mobile devices, ICS and IoT networks and devices, virtual environments, and containers.

This extension of existing solutions into new realms goes far, far beyond simply porting functionality to a new platform or integrating with a new set of APIs. It requires, among other changes and enhancements:

- Leveraging network packet brokers (NPBs) to aggregate traffic from multiple (or even several) network segments to be inspected by existing network security tools
- Utilizing utilities and management tools in the new environments to provide visibility into activities and events there, and where possible, control over those activities
- Providing extra features to detect and remediate vulnerabilities unique to those environments
- Unifying dashboards, reporting, and management so organizations can view and administer as much as possible of their infrastructure from one console

One increasingly common use case for expanding IT security solutions' reach is multi-cloud environments, where organizations find themselves with some applications hosted on Amazon Web Services, others on Microsoft Azure, and still others on Google Cloud or other public cloud platforms.

This type of work is not as glamorous as inventing brand-new technologies, but it allows IT security organizations to make better decisions, increase the productivity of existing staffs, and take advantage of new platforms and devices with confidence.

There is a human side to this issue, as well. Extending the reach of security tools to new environments requires IT team members who understand security issues in those environments. Because there is intense competition for the limited supply of security professionals with this knowledge, we believe that more enterprises will fill the gap with existing personnel by providing them with additional IT security training.

Incorporate automation and orchestration.

Software development and IT operations processes have become much more complex and dynamic over the past few years. IT security vendors and service providers fell behind in many areas, but recently they've been making rapid strides to catch up by adding automation and orchestration capabilities to their products and services. The greatest progress is being made in three areas:

1. DevSecOps, which is the integration of security into automated processes for creating, testing, and deploying new software functionality. For example, code testing tools can be invoked automatically every time developers promote code from one stage of the development process to the next. Policies for access control, malware scanning, and other security controls can be assigned to software modules early in development and moved with them through integration, test, staging, and production phases of the development lifecycle.
2. Cloud environments, where code instances are continuously spun up, moved, and removed based on fluctuating demand. To ensure that security features and policies will "follow" these instances, security vendors are adding orchestration features to their products or integrating with DevOps products like Ansible, Chef, and Puppet and cloud platform tools from Amazon, Microsoft, and Google.
3. Workflows for analyzing data and remediating vulnerabilities and misconfigurations. Security vendors are integrating their products with other technologies and adding workflow modules that perform tasks like collecting data from many sources, correlating the data and adding context, analyzing the data to detect patterns, sending alerts to security operations centers and analysts with information and recommendations for action, patching systems, and fixing misconfigurations.

Automation allows these tasks to be performed at scale, without human intervention, so IT security teams can protect dynamic environments against fast-moving threats.

Strengthen analysis and pattern recognition with artificial intelligence.

The volume of security-related data has been growing rapidly and is likely to explode when more IoT applications come online. Security tools are also getting better at collecting and correlating data from more sources: network and security devices, servers, virtual machines and containers, cloud platforms, mobile devices, and many types of endpoints. These tools also collect data in more formats: security events, network packets, conventional emails and documents, images, video files and streams, software code files, text messages, and social media posts. And all of this data can be informed by threat intelligence that includes both signatures and IoCs and information about the techniques of threat actors.

The potential for detecting patterns associated with cyberattacks and insider threats is vastly expanded by the availability of more data, of more types, from more sources, as well as more threat intelligence. But that potential can be realized only if security tools build in the capabilities to handle huge quantities of data and find correlations that might never be obvious to the unaided human mind. That's why security vendors and service providers are racing to add big data and AI features to their products, especially in the areas of machine learning and pattern recognition.

The Road Ahead

Getting ahead of the bad guys with threat hunting and deception.

Most security solutions are either preventative or reactive, in that they either find and remediate vulnerabilities before they are exploited by attackers, or monitor network traffic and security events and take action when they detect an IoC or a pattern of actions associated with threats. But there are a few areas in cybersecurity that are essentially proactive.

Threat hunting starts with understanding the techniques of likely attackers, then actively searching for artifacts and activities indicating those techniques are being used. Deception technology has evolved beyond setting up honeypots to creating complete decoy environments to lure attackers and study their methods. Both approaches give IT security groups rare opportunities to stop reacting to attacks and get ahead of the bad guys. In the coming years we expect to see a lot of innovation in proactive approaches to security.

Pioneer innovative new technologies like those for API protection, container security, RASP, zero trust architectures, brand protection, and breach and attack simulation.

By focusing most of our discussion on general strategies to improve IT security solutions, we don't mean to downplay the impact of security vendors and service providers that develop brilliant, original new technologies for inspecting and parsing network traffic, controlling activities on endpoints, protecting applications and data, managing security processes, and controlling identity and access.

Here are some of the innovative fields we are keeping an eye on:

- API gateways and application delivery controllers that build security into products that optimize application traffic on networks
- Container security platforms designed to protect the components of containerized environments, such as images, containers, hosts, and registries
- RASP to protect applications from compromise while they are executing
- Technology products for zero trust architectures, particularly adaptive authentication technologies that create risk scores at login time and micro-segmentation products that sharply limit the chance that attackers and rogue insiders can reach sensitive information
- Brand protection and digital risk protection solutions that help enterprises scan social media and the dark web for frauds, counterfeit goods, disparagement, and threats to physical as well as digital security
- Breach and attack simulation, which facilitates continuous testing of security controls, employee security, and lateral movement by adversaries

Will the strategies and technologies we highlight here play a big role in 2020? Be sure to check the eighth annual Cyberthreat Defense Report, scheduled for release in the first quarter of 2021.

Appendix 1: Survey Demographics

This year's report is based on survey results obtained from 1,200 qualified participants hailing from 17 countries (see Figure 45) across six major regions (North America, Europe, Asia Pacific, Latin America, the Middle East, and Africa). Each participant had to have an IT security role (see Figure 46). This year, 42% of our respondents held CIO, CISO, or other IT security executive positions.

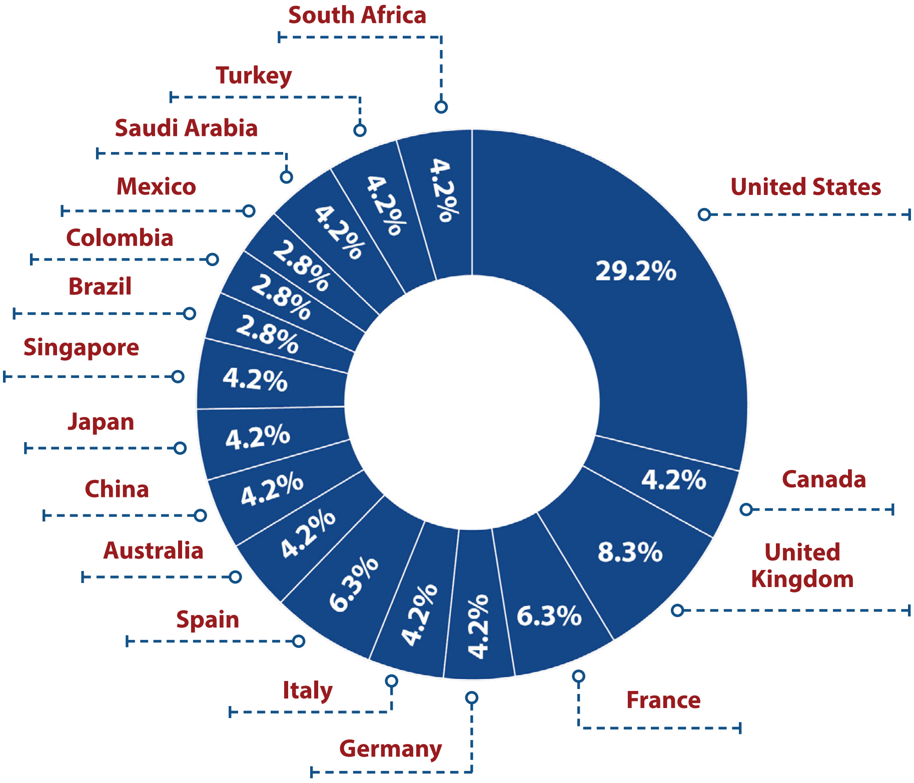

Figure 45: Survey participation by country.

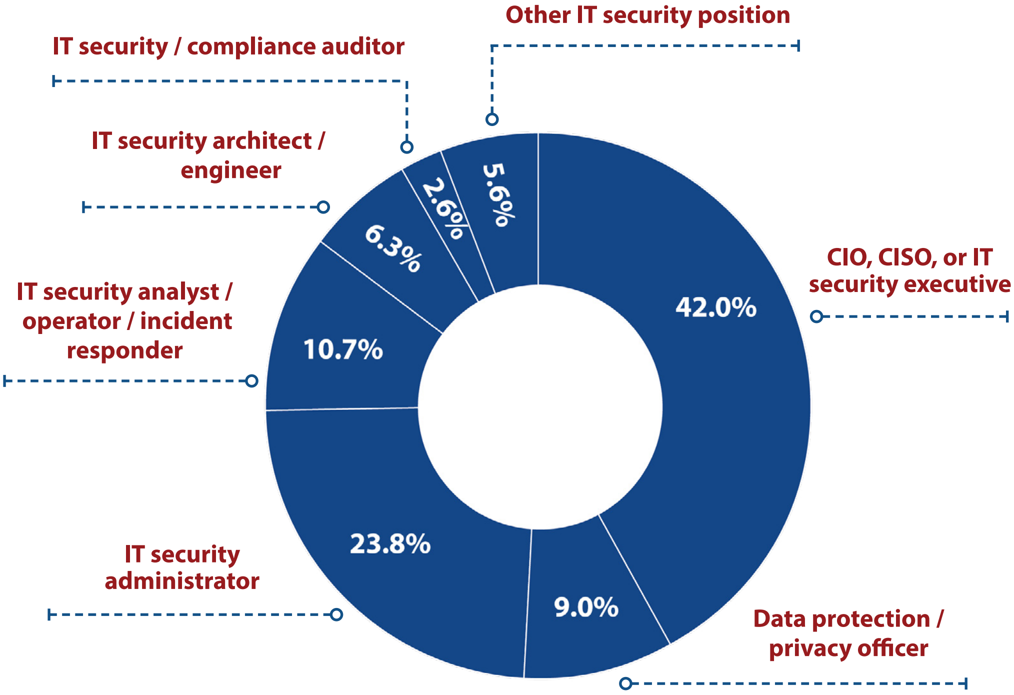

Figure 46: Survey participation by IT security role.

Appendix 1: Survey Demographics

This study addresses perceptions and insights from research participants employed with commercial and government organizations with 500 to 25,000+ employees (see Figure 47). A total of 19 industries (plus "Other") are represented in this year's study (see Figure 48). The Big 7 industries — education, finance, government, healthcare, manufacturing, retail, and telecom & technology — accounted for nearly two-thirds of all respondents. No single industry accounted for more than 15% of participants.

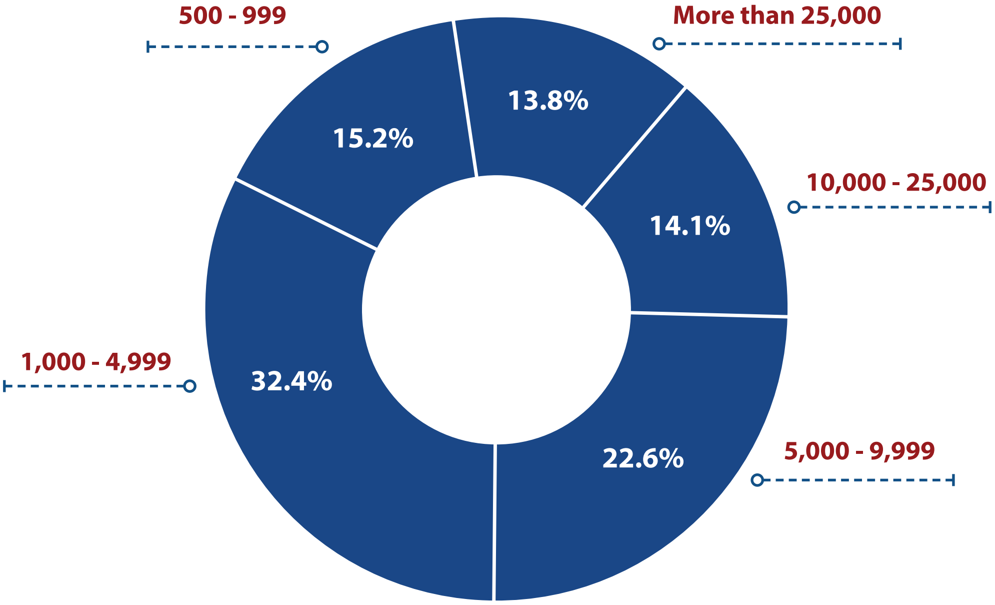

Figure 47: Survey participation by organization employee count.

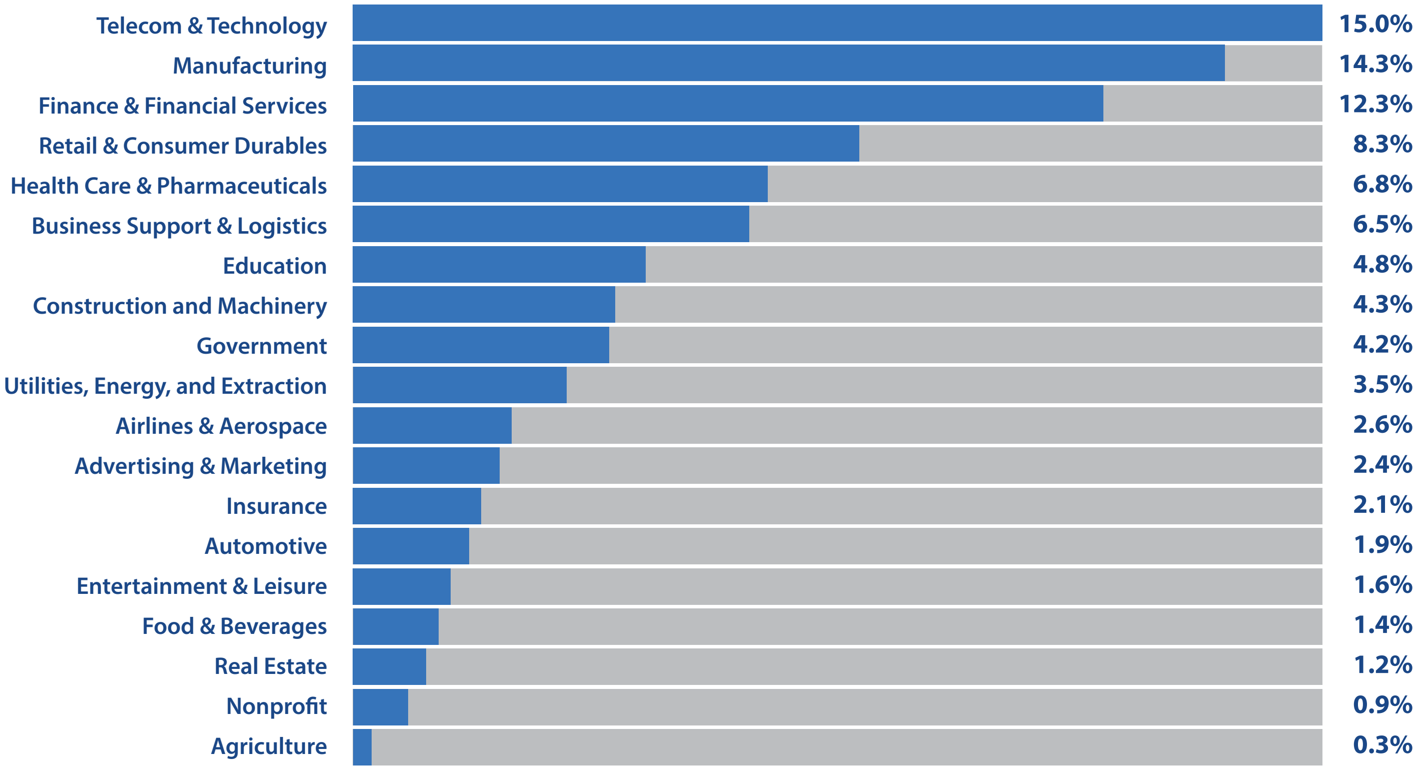

Figure 48: Survey participation by industry.

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 2019.

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

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

Appendix 3: Research Sponsors

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

Platinum Sponsors

(ISC)^2 | www.isc2.org

(ISC)^2 is an international nonprofit membership association focused on inspiring a safe and secure cyber world. Best known for the acclaimed Certified Information Systems Security Professional (CISSP®) certification, (ISC)^2 offers a portfolio of credentials that are part of a holistic, pragmatic approach to security. Our membership, more than 150,000 strong, is made up of certified cyber, information, software and infrastructure security professionals who are making a difference and helping to advance the industry. Our vision is supported by our commitment to educate and reach the general public through our charitable foundation — The Center for Cyber Safety and Education™.

Gigamon | www.gigamon.com

Gigamon is the first company to deliver unified network visibility and analytics on all data-in-transit, from raw packets to apps, across physical, virtual and cloud infrastructure. We aggregate, transform and analyze network traffic to solve for critical performance and security needs, including rapid threat detection and response, freeing your organization to drive digital innovation. In short, we enable you to run fast, stay secure and innovate.

Imperva | www.imperva.com

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

Menlo Security | www.menlosecurity.com

Menlo Security provides a complete, global cloud security platform that secures cloud transformations with zero compromise on risk, user experience, and visibility and control. Its solutions — built on the world's first and only Isolation Core™ — solve for email security, web security, data protection, and threat prevention. Headquartered in Palo Alto, CA, Menlo is trusted by hundreds of companies including many Global 2000 enterprises and financial services institutions worldwide as they seek to achieve the fullest benefits of SaaS.

Appendix 3: Research Sponsors

Gold Sponsors

Carbonite | www.carbonite.com

Carbonite and Webroot, OpenText companies, have combined forces to offer businesses and MSPs comprehensive cyber solutions. Cyber Resilience means being able to continuously deliver on your business commitments, even in the face of massive security breaches, cyberattacks, and data loss. With Carbonite and Webroot, you get complete endpoint protection, DNS protection, security awareness training, and data backup and disaster recovery, so even if the unthinkable happens, you can recover without missing a beat.

ColorTokens | www.colortokens.com

ColorTokens, a leader in proactive security, provides a new generation of security that empowers global enterprises to secure cloud workloads, dynamic applications, endpoints, and users. Through its award-winning cloud-delivered solution, ColorTokens enables security and compliance professionals to leverage real-time visibility, workload protection, endpoint protection, application security, and zero-trust network access — all while seamlessly integrating with existing security tools.

Netskope | www.netskope.com

The network perimeter is dissolving. A new perimeter is needed that can protect data and users everywhere, without introducing friction to the business. The Netskope security cloud provides unrivaled visibility and real-time data and threat protection when accessing cloud services, websites, and private apps from anywhere, on any device. Only Netskope understands the cloud and delivers data-centric security from one of the world's largest and fastest security networks, empowering the largest organizations in the world with the right balance of protection and speed they need to enable business velocity and secure their digital transformation journey. Reimagine your perimeter with Netskope.

OpenText | www.opentext.com

OpenText, The Information Company™, enables organizations to gain insight through market leading information management solutions, on-premises or in the cloud. OpenText™ Security Suite, powered by OpenText™ EnCase™, provides 360-degree visibility across laptops, desktops and servers for proactive discovery of sensitive data, identification and remediation of threats and discreet, forensically-sound data collection and investigation. With agents deployed on more than 40 million endpoints, clients that include 78 of the Fortune 100 and more than 6,600 EnCE™ certified users, Security Suite delivers the industry gold standard for incident response and digital investigations.

PerimeterX | www.perimeterx.com

PerimeterX is the leading provider of application security solutions that keep your business safe in the digital world. Delivered as a service, the company's Bot Defender, Code Defender and Page Defender solutions detect risks to your web applications and proactively manage them, freeing you to focus on growth and innovation. The world's largest and most reputable websites and mobile applications count on PerimeterX to safeguard their consumers' digital experience.

Webroot | www.webroot.com

Carbonite and Webroot, OpenText companies, have combined forces to offer businesses and MSPs comprehensive cyber solutions. Cyber Resilience means being able to continuously deliver on your business commitments, even in the face of massive security breaches, cyberattacks, and data loss. With Carbonite and Webroot, you get complete endpoint protection, DNS protection, security awareness training, and data backup and disaster recovery, so even if the unthinkable happens, you can recover without missing a beat.

Appendix 3: Research Sponsors

Silver Sponsors

Anitian | www.anitian.com

The Anitian Cloud Security Platform offers the fastest path to security and compliance for existing and new cloud applications — enabling high-growth SaaS companies and enterprises to dramatically accelerate time-to-market. Featuring a complete, automated and pre-engineered cloud security and compliance environment, the Anitian platform wraps more than 15 critical security technologies around a cloud application in hours — and includes configurations, documents, licenses, and onboarding — to make your cloud application secure and compliant with FedRAMP or PCI DSS up to 80% faster and at 50% of the cost.

CybelAngel | www.cybelangel.com

CybelAngel is a leading digital risk management platform that provides enterprises with actionable threat intelligence from data leaks both inside and outside the firewall. CybelAngel enables effective remediation and improved cybersecurity posture. By leveraging artificial intelligence and proven machine learning capabilities, it monitors, detects and manages digital risk from third parties and across all layers of the Internet. Global organizations rely on CybelAngel to protect their intellectual property, brand, and reputation.

Cymulate | www.cymulate.com

Cymulate, changing the paradigm of security testing. Digital transformation is driving constant change in the IT environment, creating a dynamic attack surface, exposed to an evolving threat landscape. This demands a continuous security testing program. Cymulate, a SaaS-based breach and attack simulation (BAS) platform enables businesses to continuously assess their preparedness to handle cyberthreats effectively, on their production environment, anytime, from anywhere. Automated and simple to use, Cymulate identifies security gaps and weaknesses, by initiating thousands of attack simulations that challenge security controls and IT infrastructure resiliency. It provides security professionals actionable insights to constantly maintain an optimal security posture.

DivvyCloud | www.divvycloud.com

DivvyCloud protects your cloud and container environments from misconfigurations, policy violations, threats, and IAM challenges. We provide full lifecycle protection through preventative security during the CI/CD pipeline and automated, real-time detection and remediation at runtime. Our customers, including 3M, Spotify, Fannie Mae, and Kroger, achieve continuous security and compliance and can fully realize the benefits of Amazon Web Services, Microsoft Azure, Google Cloud Platform, Alibaba Cloud, and Kubernetes technology without the loss of control. Freedom is good. Chaos is bad.

Expel | www.expel.io

Expel is flipping today's managed security model on its head (Ouch!) by taking a technology-driven approach that lets analysts focus on what humans do best: exercise judgement and manage relationships. The company offers 24x7 monitoring through its security operations center-as-a-service, using the security tools customers already have in place. Expel then helps customers make better, faster decisions about security issues by giving them real answers and specific recommendations instead of repackaging customers' alerts and tossing them back in their laps. Expel also offers practical advice on how to prevent issues from happening over and over again.

Appendix 3: Research Sponsors

Sysdig | www.sysdig.com

Sysdig enables companies to confidently run cloud-native workloads in production. With the Sysdig Secure DevOps Platform, cloud teams embed security, maximize availability, and validate compliance. The Sysdig platform is open by design, with the scale, performance, and usability enterprises demand. The largest companies rely on Sysdig for cloud-native security and visibility.

ZeroFOX | www.zerofox.com

ZeroFOX, the global category leader in public attack surface protection, safeguards modern organizations from dynamic security risks across social, mobile, surface, deep and dark web, email and collaboration platforms. Using diverse data sources and artificial intelligence-based analysis, the ZeroFOX Platform identifies and remediates targeted phishing attacks, credential compromise, data exfiltration, brand hijacking, executive and location threats and more. The patented ZeroFOX SaaS technology processes and protects millions of posts, messages and accounts daily across the social and digital landscape, spanning LinkedIn, Facebook, Slack, Twitter, Instagram, Pastebin, YouTube, mobile app stores, the deep & dark web, domains, email and more.

Appendix 4: About CyberEdge Group

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

- Advanced Threat Protection (ATP)
- Application Security
- Cloud Security
- Container Security
- Data Security
- Deception Technology
- DevSecOps
- DoS/DDoS Protection
- Endpoint Security
- ICS/OT Security
- Identity and Access Management (IAM)
- Intrusion Prevention System (IPS)
- Managed Security Services Providers (MSSPs)
- Mobile Device Management (MDM)
- Network Behavior Analysis (NBA)
- Network Detection & Response (NDR)
- Network Forensics
- Next-generation Firewall (NGFW)
- Patch Management
- Penetration Testing
- Privileged Account Management (PAM)
- Risk Management/Quantification
- Secure Email Gateway (SEG)
- Secure Web Gateway (SWG)
- Security Analytics
- Security Configuration Management (SCM)
- Security Information & Event Management (SIEM)
- Security Orchestration, Automation, and Response
- Threat Intelligence Services
- User and Entity Behavior Analytics (UEBA)
- Unified Threat Management (UTM)
- 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 citation: "Source: 2020 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 are available for download at no charge on the CyberEdge website **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**.