CYBEREDGE GROUP

2021 Cyberthreat Defense Report

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

« Research Sponsors »

PLATINUM

(ISC)² Gigamon imperva MENLO SECURITY perimeterx

GOLD

ConnectWise HERJAVEC GROUP KnowBe4 MICRO FOCUS thycotic

SILVER

APPGUARD The Malware Disruptor BINARY DEFENSE britive Cymulate Breach & Attack Simulation EclecticIQ interos

Introduction **3**
Research Highlights **6**
Section 1: Current Security Posture **7**
Past Frequency of Successful Cyberattacks 7
Future Likelihood of Successful Cyberattacks 9
Security Posture by IT Domain 11
Assessing IT Security Functions 13
The IT Security Skills Shortage 15
Section 2: Perceptions and Concerns **17**
Concern for Cyberthreats 17
Concern for Web and Mobile Attacks 19
Responding to Ransomware 21
Barriers to Establishing Effective Defenses 24
Benefits of Unified App and Data Security Defenses 26
Boosting Careers with Cybersecurity Certifications 27
Section 3: Current and Future Investments **29**
IT Security Budget Allocation 29
IT Security Budget Change 31
COVID-19 Effects on IT Security Purchase Priorities 33
Network Security Deployment Status 35
Endpoint Security Deployment Status 37
Application and Data Security Deployment Status 39
Security Management and Operations Deployment Status 41
Identity and Access Management Deployment Status 43
Preferences for Machine Learning and AI 45
Section 4: Practices and Strategies **47**
Security Applications Delivered via the Cloud 47
Benefits of Embracing DevSecOps Practices 49
SSL/TLS Traffic Decryption Challenges 51
Emerging IT Security Technologies 53
The Impact of COVID-19 on the IT Security Industry **55**
The Road Ahead **56**
Appendix 1: Survey Demographics **59**
Appendix 2: Research Methodology **61**
Appendix 3: Research Sponsors **62**
Appendix 4: About CyberEdge Group **65**

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 eighth 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.

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

Top Five Insights for 2021

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

1. Successful cyberattacks make the biggest jump in six years. When CyberEdge launched the first CDR in 2014, 62% of organizations were compromised by successful cyberattacks. That number has risen to 86%. The percentage of organizations experiencing a successful attack rose 5.5% this year, the largest increase in six years. We believe this surge is due in large part to the dramatic rise in BYOD policy adoptions and a massive increase in third-party risks.

2. Rewarding ransom payers is good for business (if you are a cybercriminal). For the first time, more than two-thirds of organizations (69%) were victimized by ransomware. The percentage of ransom-paying organizations that recover their compromised data has increased steadily in recent years, from 49% in 2018 to 72% in 2021. Cybercriminals have learned that withholding data following payment receipt is bad for business. Unfortunately, this trend has enticed most victims to pay ransoms (57% in 2021), which in turn has funded more ransomware attacks, resulting in more organizations being compromised by ransomware than ever before.

3. Adoption of cloud security solutions is rising. The COVID-19 pandemic has sparked more interest in cloud-based IT security solutions than ever before. A year ago, 36% of security applications and services were delivered via the cloud. This year, that number has risen to 41%.

4. IT security spending increases are slowing. For the first time since we began tracking this statistic four years ago, the percentage of a typical IT budget spent on security has remained flat (at 13%) rather than rising. And for the first time in our eight-year CDR history, the percentage of organizations with rising security budgets has fallen (from 85% to 78%) and the average security budget increase has also declined (from +5% to +4%). So, overall IT security spending is still rising, but at a slower pace than usual.

5. Pessimism is the new normal. Eight years ago, 38% of CDR respondents felt that it was more likely than not that their company would be compromised by a successful cyberattack in the coming year. Sadly, eight years later, that number has doubled to 76%. IT security professionals are no longer just measured on their abilities to prevent cyberattacks from happening, but also their abilities to detect, terminate, and remediate from in-progress attacks.

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

By revealing these details, we 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 our approach and progress in addressing 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?
- Do other IT security practitioners think 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. Our data can lead to better market traction and success for solution providers, 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 countermeasures they should add 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 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? 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

- **Most successful attacks in six years.** The percentage of organizations compromised by successful attacks rose by 5.5% – the largest annual increase in six years (page 7)!
- **Deepening pessimism.** For the first time, three-quarters (76%) of security professionals believe a successful attack is imminent – up from 38% seven years ago (page 9).
- **The weakest link: mobile devices.** Following a rise in WFH and BYOD policy adoptions, mobile devices are rated as most challenging to secure (page 11).
- **Shedding light on third-party risks.** A new entrant in this year's CDR, third-party risk management (TPRM), is deemed the most challenging IT security function (page 13).
- **Feeling overwhelmed.** The vast majority (87%) of organizations are experiencing an IT security skills shortfall, and it has worsened during the pandemic (page 15).

Perceptions and Concerns

- **Cyberthreat migraines.** Malware, ransomware, and spear phishing continue to cause the most headaches; zero-day attacks not as much (page 17).
- **Web and mobile attacks.** Nine out of 10 organizations (91%) have been affected by cyberattacks targeting web and mobile applications (page 19).
- **Fueling ransomware.** More than two-thirds of organizations (69%) were victimized by ransomware and most (57%) paid the ransom (page 21).
- **Security awareness gap.** For the second consecutive year, the number one barrier to IT security's success is "low security awareness among employees" (page 24).
- **Unified app and data security.** "Simplified security monitoring" is the top benefit achieved by integrating application and data security to the same platform (page 26).
- **Cybersecurity career boosts.** Nearly all (99%) respondents agree that achieving a specialized cybersecurity certification would benefit their career (page 27).

Current and Future Investments

- **Security spending plateau?** The percentage of a typical IT budget spent on security remained flat (12.7%) for the first time in three years (page 29).
- **Slowing security spending.** For the first time in CDR history, the percentage of organizations with rising security budgets has declined (from 85% to 78%) and the average security budget increase has declined (from +5% to +4%) (page 31).
- **Pandemic-fueled spending reprioritization.** The COVID-19 pandemic forced around seven out of eight (86%) organizations to reprioritize IT security spending (page 33).
- **Network security's top picks.** NGFWs, DoS/DDoS prevention, and deception are the top network security technologies planned for acquisition in 2021 (page 35).
- **Endpoint security shopping list.** Deception and browser isolation are the endpoint security technologies most sought after this year (page 37).
- **The stars of app/data security.** API gateways and WAFs remain supreme, while bot management and FIM/FAM are on many shopping lists for 2021 (page 39).
- **TIPs tipping the scale again.** Threat intelligence platforms (TIPs) are atop the list of security management and operations technologies planned for acquisition (page 41).
- **Biometrics still red hot.** Biometrics tops the list of identity and access management (IAM) technologies planned for acquisition this year (page 43).
- **Demand for ML/AI holds strong.** Once again, 85% of respondents prefer security products that feature machine learning (ML) and artificial intelligence (AI) (page 45).

Practices and Strategies

- **Security is going cloud.** 41% of security applications are delivered via the cloud, up from 36% last year (page 47).
- **Reaping the benefits of DevSecOps.** More than nine out of 10 organizations (93%) are realizing the benefits of DevSecOps (page 49).
- **Decryption challenges.** Nearly nine in 10 organizations (88%) are facing challenges with decrypting SSL/TLS traffic for cyberthreat inspection (page 51).
- **Embracing emerging technologies.** Most organizations have embraced emerging security technologies: SD-WAN (82%), zero trust (75%), and SASE (74%) (page 53).

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?

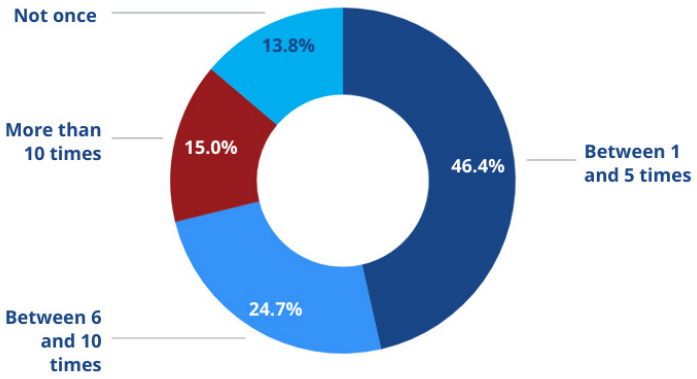


Figure 1: Frequency of successful cyberattacks in the last 12 months.

The last year has been enormously challenging, both personally and professionally, on so many levels. When the world was turned upside down by the COVID-19 pandemic, cybercriminals exploited the situation in many ways. Phishing campaigns, deceptive domains, and malicious apps are just a few of the tactics these crooks employed to convert pain into profit.

In last year's CDR, we saw a small uptick in successful cyber-attacks as we crossed the 80% threshold for the first time in our report's history. This year, we saw the largest annual increase in successful attacks within the last six years. Just over 86% of our responding organizations experienced at least one successful cyberattack within the preceding 12 months, with about four in 10 organizations experiencing six incidents or more (see Figures 1 and 2).

Of the seven major industries surveyed for this report, education was the hardest hit with 92.3% of organizations reporting a successful attack, followed by manufacturing (90.3%), telecom and technology (87.4%), and finance (85.5%). Next came healthcare (84.6%) and retail (81.7%). The bright spot this year was government, with only 72.5% of respondents experiencing a successful attack (see Figure 3).

Geographically, Colombia claimed the top spot this year for the most organizations experiencing a successful attack (93.9%). Down the list, China (91.5%), Germany (91.5%), Mexico (90.6%), Spain (89.8%), and the United States (89.7%) were a bit above average. Countries that fared the best included the United Kingdom (71.1%), Japan (80.9%), Australia (81.6%), and Turkey (82.0%) (see Figure 4).

"This year, we saw the largest annual increase in successful attacks within the last six years."

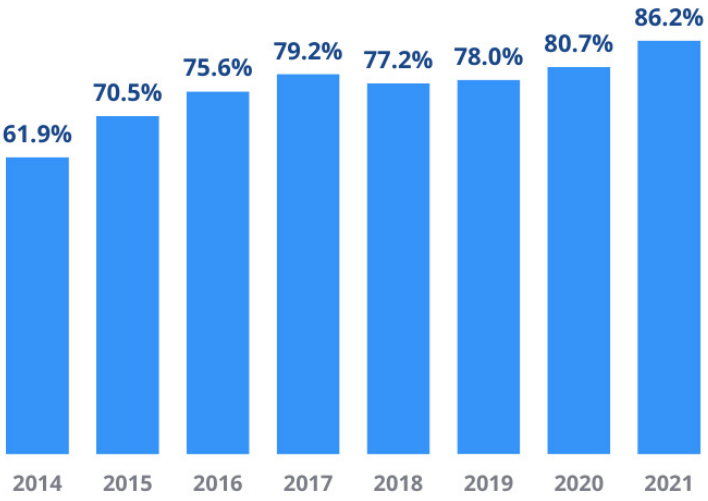


Figure 2: Percentage of organizations compromised by at least one successful attack.

Section 1: Current Security Posture

Aside from COVID-19-specific threats, what other trends caused such a big jump in successful cyberattacks? We're glad you asked. Last year, CyberEdge conducted a multi-sponsor research study titled, "The Impact of COVID-19 on Enterprise IT Security Teams" (see page 55 for more information).

We surveyed 600 enterprise IT security professionals from seven major countries. Key revelations included:

- 114% increase in remote workers
- 59% increase in BYOD adoptions
- 73% observed increased third-party risks

With the majority of IT security organizations already under-staffed before any of us knew what a coronavirus was, having to support so many additional remote workers, many of whom were (and perhaps still are) using unmanaged devices, caused organizations' collective attack surfaces to increase exponentially almost overnight. Frankly, we're fortunate that we didn't see more than a 5.5% increase in victimized organizations.

Our hats are off to all of you who worked so tirelessly to defend your company's digital assets during such trying times! We dedicate this year's CDR to you.

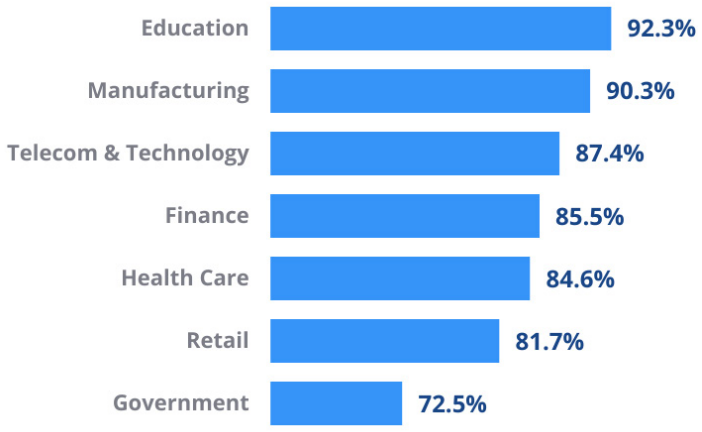


Figure 3: Percentage compromised by at least one successful attack in the past 12 months, by industry.

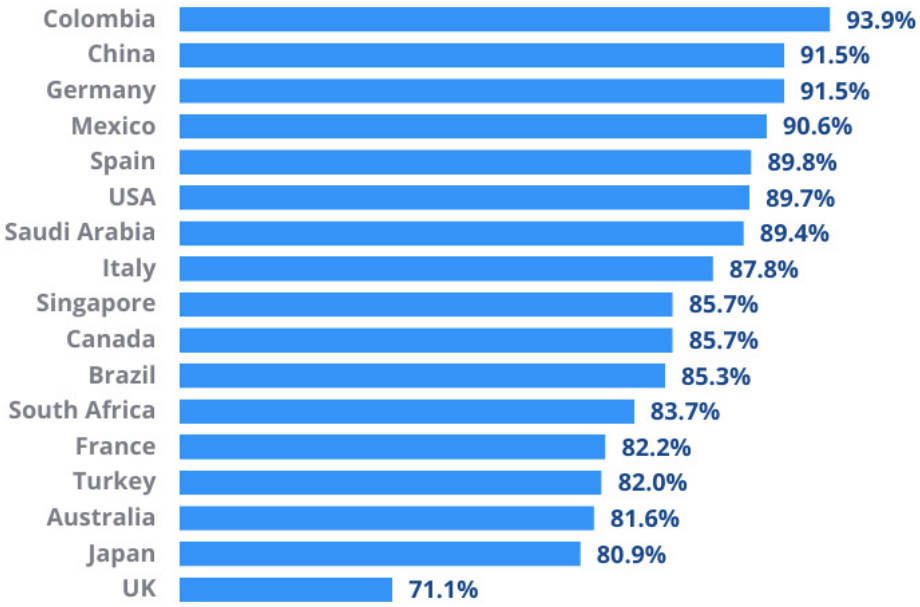


Figure 4: Percentage compromised by at least one successful attack in the past 12 months, by country.

Section 1: Current Security Posture

Future Likelihood of Successful Cyberattacks

What is the likelihood that your organization's network will be compromised by a successful cyberattack in 2021?

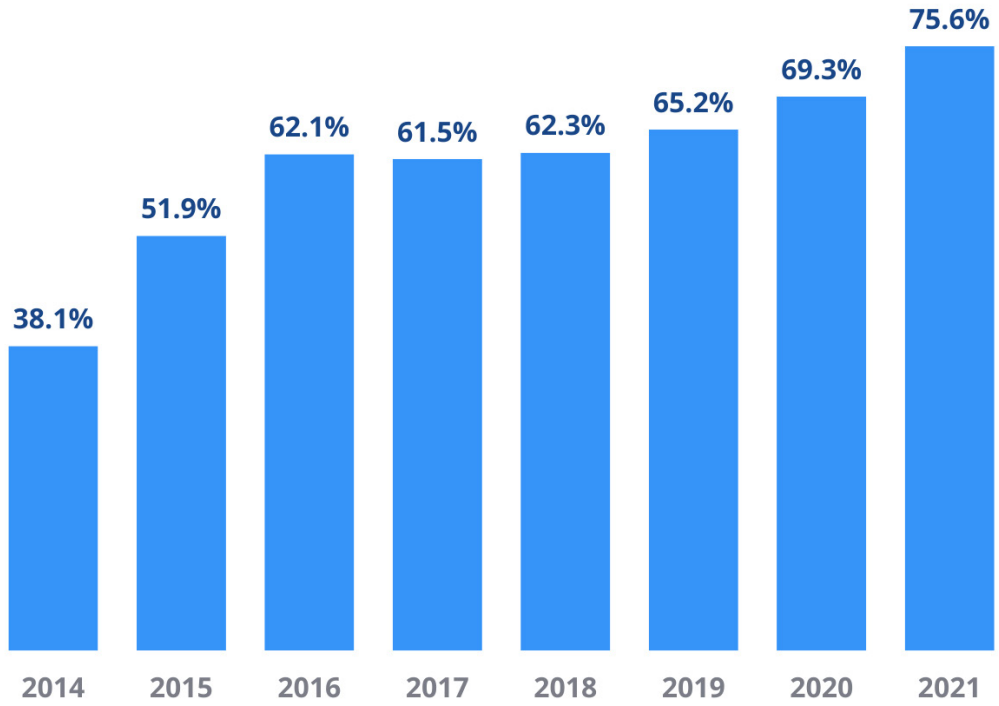


Figure 5: Percentage indicating compromise is "more likely to occur than not" in the next 12 months.

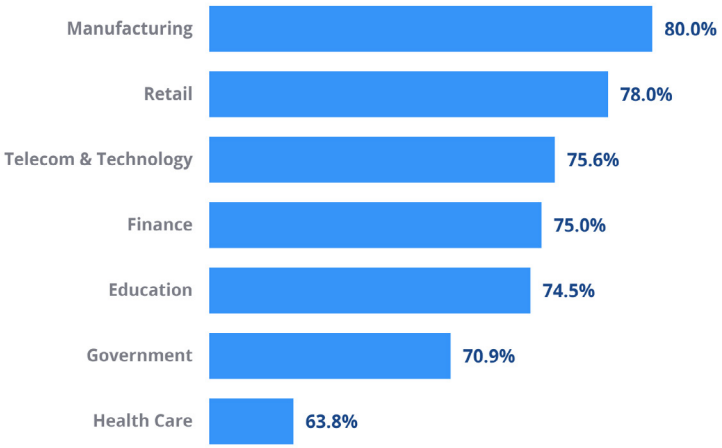


Figure 6: Percentage indicating compromise is "more likely to occur than not" in the next 12 months, by industry.

In a 2019 study published by the National Academy of Sciences of the United States, Boston-area scientists found that the most optimistic people live an average of 11-15% longer than their more pessimistic peers. While most view optimism to be a healthy trait, we're not so sure that mentality bodes well for cybersecurity professionals. And our CDR respondents certainly agree.

When we first asked the question at the top of this page for our 2014 CDR, only 38.1% felt like a successful cyberattack in the coming year was more likely than not. Fast forward to last November when our survey was live, and that number nearly doubled to 75.6% (see Figure 5). Now, considering that 86.2% of organizations were victimized by successful attacks last year, 75.6% actually reflects a degree of optimism that the coming 12

Section 1: Current Security Posture

"Over time, cybersecurity professionals have come to realize that it's more of a question of when their organizations will be victimized by a data breach than if."

months will see an improvement. But over time, cybersecurity professionals have come to realize that it's more of a question of when their organization will be victimized by a data breach than if.

On an industry basis, the proportion of respondents saying a compromise was more likely to occur than not was highest in manufacturing (80.0%), retail (78.0%), and telecom and technology (75.6%). The most confident respondents (relatively) were in healthcare (63.8%) and government (70.9%) (see Figure 6).

Of the 17 countries we surveyed, the majority of respondents in each one felt that a successful cyberattack on their employer was more likely than not. Respondents in China were the most pessimistic, and in fact the percentage there expecting a successful attack soared from 63.3% last year to 90.0% this year. Respondents in Australia and the United States also turned much more pessimistic, with those expecting successful attacks rising from 70.0% to 86.0% and from 71.6% to 82.1%, respectively. Respondents in Brazil (52.9%), South Africa (54.2%), and Italy (56.0%) were the least pessimistic.

So, how can IT security organizations channel all of this pessimism toward a positive outcome? Well, you can start by planning for the worst while still hoping for the best. Specifically, smart IT security teams should:

- Invest in modern malware detection and cyberthreat hunting technologies that leverage machine learning (ML) and artificial intelligence (AI)
- Select security analytics solutions that can quickly help you determine whether any data was compromised/leaked
- Adopt security orchestration, automation, and response (SOAR) technology that enables security teams to work more cohesively and accomplish more with fewer resources
- Pre-determine policies and procedures to accelerate recovery from ransomware and other attacks
- Invest in training and certification as tactics for both recruitment and retention to help close that IT security skills gap

Long gone are the days of evaluating cybersecurity professionals solely on their abilities to prevent data breaches from occurring. These days, IT security teams are evaluated on their abilities to rapidly detect, validate, investigate, terminate, and recover from cyberattacks.

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) for each of the following IT components:

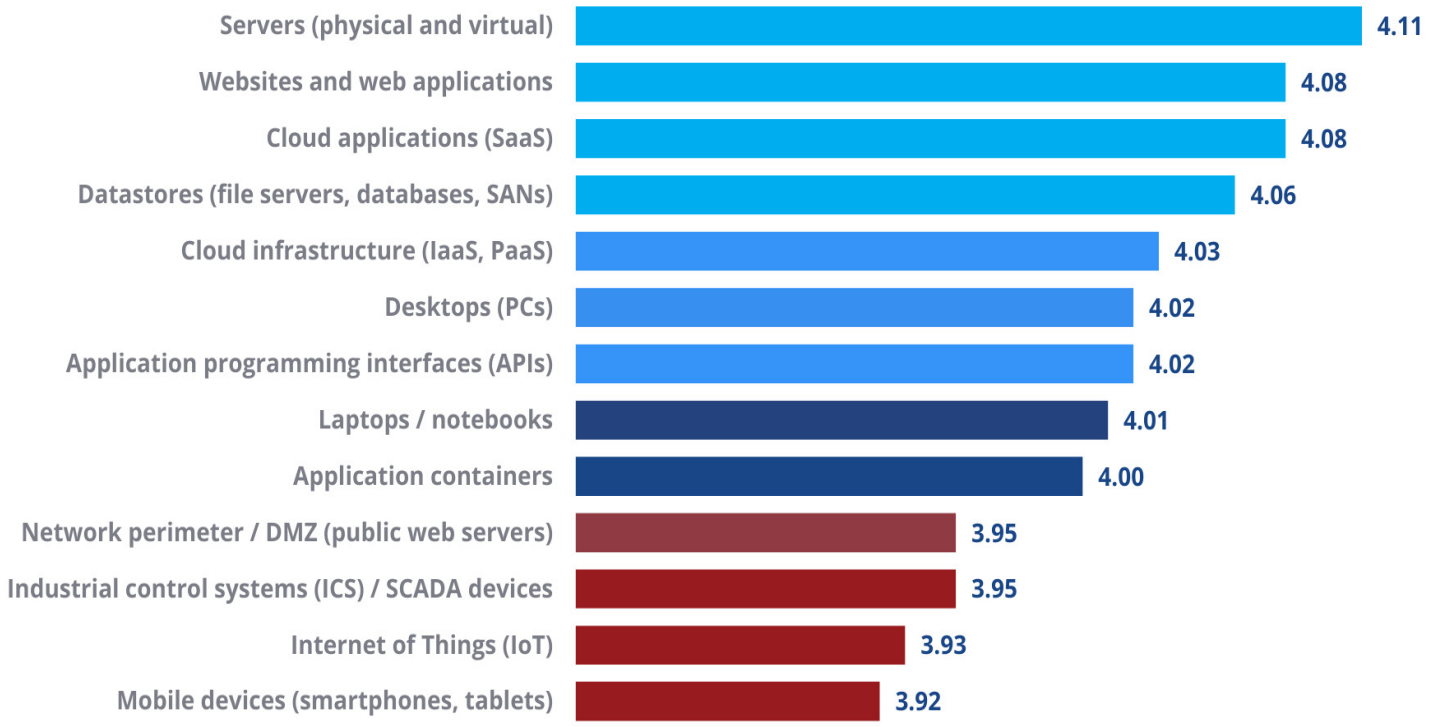


Figure 7: Perceived security posture by IT domain.

The IT security component rated most challenging to secure this year is mobile devices (see Figure 7). That's up from fourth last year. The reason for the jump? Two words: COVID and BYOD.

Last year, CyberEdge published a multi-sponsor survey report titled, "The Impact of COVID-19 on Enterprise IT Security Teams" (see page 55). Upon surveying 600 IT security professionals regarding how the pandemic has affected their practices and security investments, we learned that the number of organizations with bring-your-own-device (BYOD) policies jumped nearly 60% due to the massive, almost-overnight increase in remote workers. These mobile devices were largely, if not almost entirely, unmanaged with few or no security protections.

Next in line are Internet of Things (IoT) devices, which in the context of business equate to copiers, VoIP phones, building automation systems, closed-circuit TV (CCTV) systems, climate control systems, alarm systems, and more. Each of these IP-enabled components has an operating system, an application, and the potential for exploitable vulnerabilities.

The third type of IT component that causes the most security concerns includes industrial control systems (ICS) and SCADA devices. These devices are commonly used by manufacturers, electric power generators, nuclear power plants, chemical manufacturers, oil refineries, and water and wastewater

Section 1: Current Security Posture

treatment facilities. Just like IoT devices, each has an operating system and an application with potentially exploitable vulnerabilities.

On a positive note, servers, websites and web applications, and datastores are of lesser concern, most likely because these are static assets that can be more easily monitored. Cloud applications used to be a significant headache for IT security teams. But with modern-day cloud access security broker (CASB) capabilities often baked into next-generation firewall (NGFW) and secure web gateway (SWG) solutions, the "shadow IT" phenomenon has declined significantly as an issue.

So, in the grand scheme of things, how do this year's overall security posture assessments compare to last year's? Well, of the 13 IT components depicted in this survey question, confidence has declined in 12.

"The IT security component rated most challenging to secure this year is mobile devices. That's up from fourth last year. The reason for the jump? Two words: COVID and BYOD."

The only IT component that respondents are more bullish about defending this year is application containers, which rose to #9 on the list from #13 last year. Kudos to those innovative security vendors who've launched new solutions to safeguard Docker, Kubernetes, and other application container platforms. Our proverbial hats are off to you!

In case you're wondering, IT components that reflect the greatest drop in safeguarding confidence are:

- Network perimeter / DMZ (public web servers) (-0.12)
- Mobile devices (smartphones, tablets) (-0.11)
- Internet of Things (IoT) (-0.08)

Section 1: Current Security Posture

Assessing IT Security Functions

On a scale of 1 to 5, with 5 being highest, rate the adequacy of your organization's capabilities in each of the following functional areas of IT security:

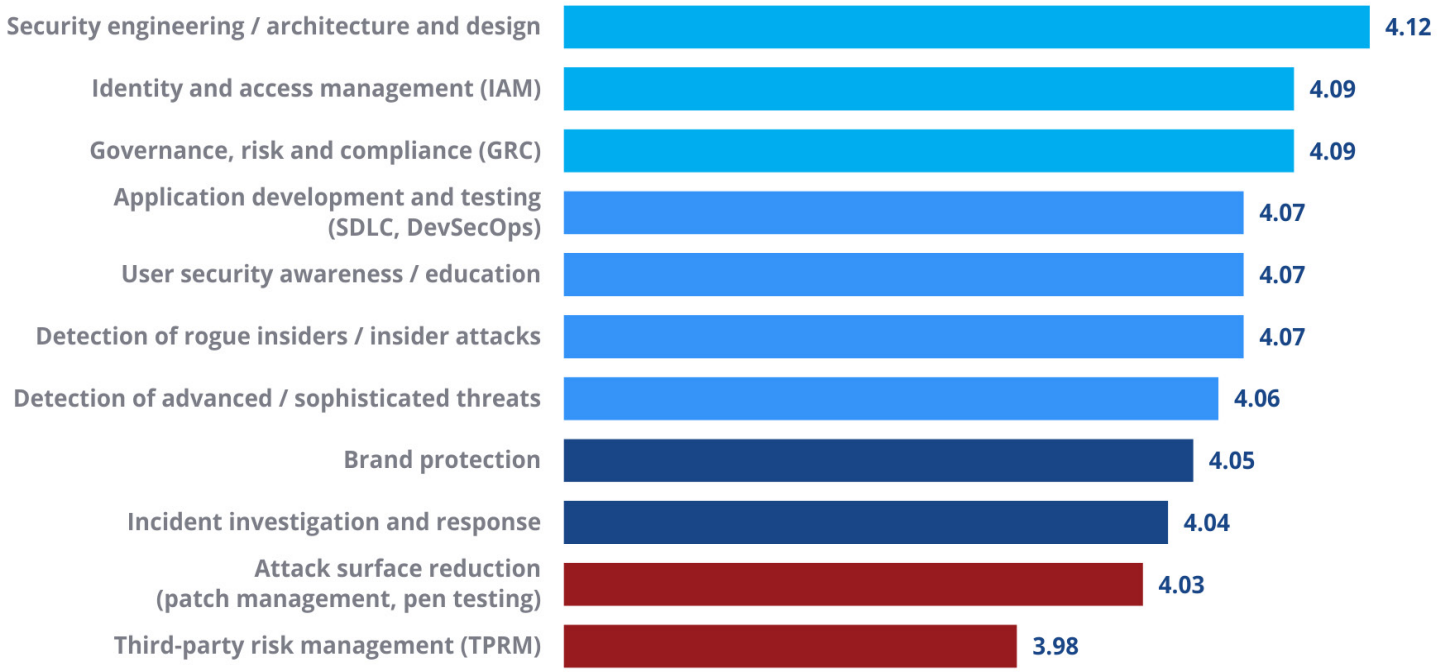


Figure 8: Perceived adequacy of functional security capabilities.

In this question, we presented a list of 11 IT security functions and asked respondents to rate the adequacy of their capabilities (see Figure 8). We added three new IT security functions to the list this year:

- Third-party risk management (TPRM)
- Brand protection
- Governance, risk and compliance (GRC)

We'd sure like to thank our sponsors that play in the TPRM space for encouraging us to add it to the list because, as it turns out, TPRM is the IT security function rated most challenging this year! And it makes sense, given several high-profile data breaches that have stemmed from victims' partners, suppliers, and contractors. Companies that suffered breaches included Target (2013), Home Depot (2014), Capital One (2019), Quest Diagnostics (2019), Facebook (2019), Marriott (2020), and General Electric (2020). And let's not forget about FireEye, Microsoft, VMware, and dozens of other companies affected by last year's SolarWinds zero-day vulnerability.

Attack surface reduction – which includes vulnerability management, patch management, security configuration management, and penetration testing – was rated as the second-biggest challenge this year. In our humble opinions, too many organizations underinvest in this critically important area. If security teams were more efficient at finding and mitigating security risks, we wouldn't need to rely as much on "next-gen"

Section 1: Current Security Posture

threat detection technologies because so many cyberthreats would be rendered harmless if the vulnerabilities they were designed to exploit were already patched.

The functional area with the greatest decline in confidence over the past year was incident investigation and response, which fell three places on our list. There are two reasons why we believe this is a direct result of the massive, almost-overnight increases in remote workers and BYOD policy adoptions (see page 55) stemming from the COVID-19 pandemic. First, we already know that the sheer volume of cyberthreats increased last year, resulting in a record number of successful attacks. This equates to an increased volume of incidents to investigate and remediate. Second, it's far more challenging to investigate employee-owned, unmanaged devices than company-owned laptops and smartphones.

Brand protection is a new entrant to our list this year and is also the newest IT security function to get on CISOs' radar. In the context of cybersecurity, it relates to protecting intellectual property (IP) of companies and their associated brands against counterfeiting, copyright piracy, trademark squatting, patent theft, rogue websites, and social media impersonation. As this security capability is still emerging, it naturally ranks high on the list of most-challenging IT security functions. Thankfully, several security vendors have rolled out brand protection solutions that help track down and shut down fraudulent activities on the web.

"We'd sure like to thank our sponsors for encouraging us to add TPRM to the list, because it is the IT security function rated most challenging this year!"

From there, the next set of IT security functions are rated pretty close together. The security function that IT security organizations are most bullish about – despite being among the hardest to do well – is security engineering/architecture and design. Kudos to all of the security architects out there who are helping to make smart investments to keep their organizations safe (or as safe as they can be).

Section 1: Current Security Posture

The IT Security Skills Shortage

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

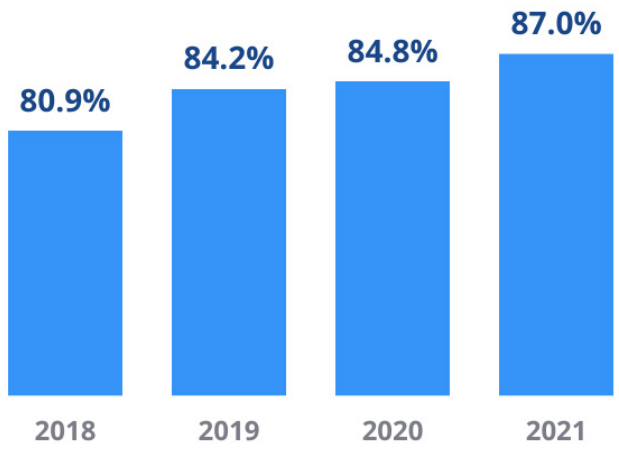


Figure 9: Percent of organizations experiencing a shortfall of skilled IT security personnel.

"Unfortunately, nearly nine in 10 organizations (87%) experienced a shortfall in IT security personnel last year, which is a new CDR record."

If there was ever a year when we needed plenty of skilled IT security personnel, it was 2020 – when the tidal wave of remote workers and new BYOD policy adoptions occurred. IT security teams had to immediately figure out how to more than double remote access capacity and secure unmanaged devices practically overnight.

Unfortunately, nearly nine in 10 organizations (87%) experienced a shortfall in IT security personnel last year (see Figure 9), which is a new CDR record and a 2.2% increase from the previous year. Two percentage points don't seem like a lot, but overworked security professionals definitely felt the impact of being thrown into the fire to contend with the ripple effect of the pandemic (i.e., more unmanaged devices, larger attack surface, increased cyberthreats, and more incidents to investigate).

To add insult to injury, many organizations (especially in the travel, leisure, and hospitality industries) were forced to reduce workforce spending, including IT security staffing. As a result, many IT security teams had to contend with furloughs, reductions in hours, and layoffs.

If we break down the data by role, we see the greatest shortfalls in IT security are IT security administrators (40.4%), who are responsible for installing, configuring, monitoring, and maintaining IT security infrastructure components. Next are IT security analysts, operators, and incident responders (35.0%). These workers are on the front line of monitoring the organization for potential data breaches and other attacks. IT security architects and engineers were at the top of last year's list of job shortages; however, this group has fallen to third position this year at 32.6% (see Figure 10).

Surprisingly, DevSecOps engineers (25.7%) are least in demand. It's not because IT security organizations haven't embraced DevSecOps, as this year's CDR shows an impressive 93% of

Section 1: Current Security Posture

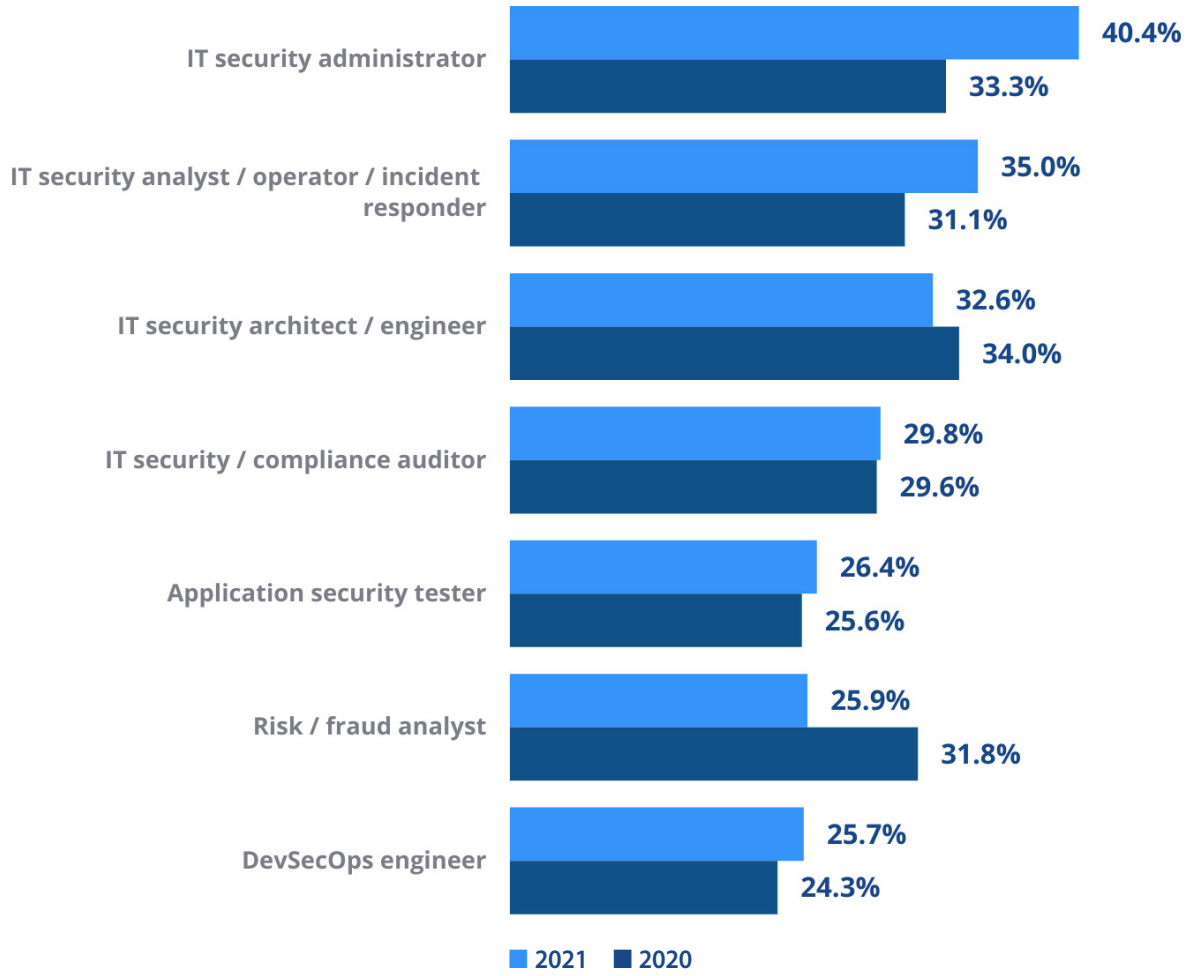


Figure 10: Cybersecurity skills shortage, by role.

organizations have implemented, or are starting to implement, DevSecOps practices (see page 49). The most likely reason for this seeming contradiction is that many enterprises are training application developers and testers to integrate security into their jobs, rather than hiring people with DevSecOps titles.

Just like last year, IT security skill shortages are felt the hardest by organizations with 10,000 to 24,999 employees (91%). Organizations with only 1,000 to 4,999 employees (85.1%) are not as impacted but still are definitely feeling the pain like everyone else.

With regard to major industries, telecom and technology (89.6%), retail (87.4%), and healthcare (87.3%) are the most affected by the shortage. Education (83.6%) and government (83.7%) are the least affected.

Around the world, we found the greatest shortages in Japan (whoa… 98.0%), Singapore (93.9%), and Canada (89.8%). IT security teams in Brazil (76.5%), China (80.0%), and the United Kingdom (81.4%) are faring a little better than the 87.0% global average.

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.

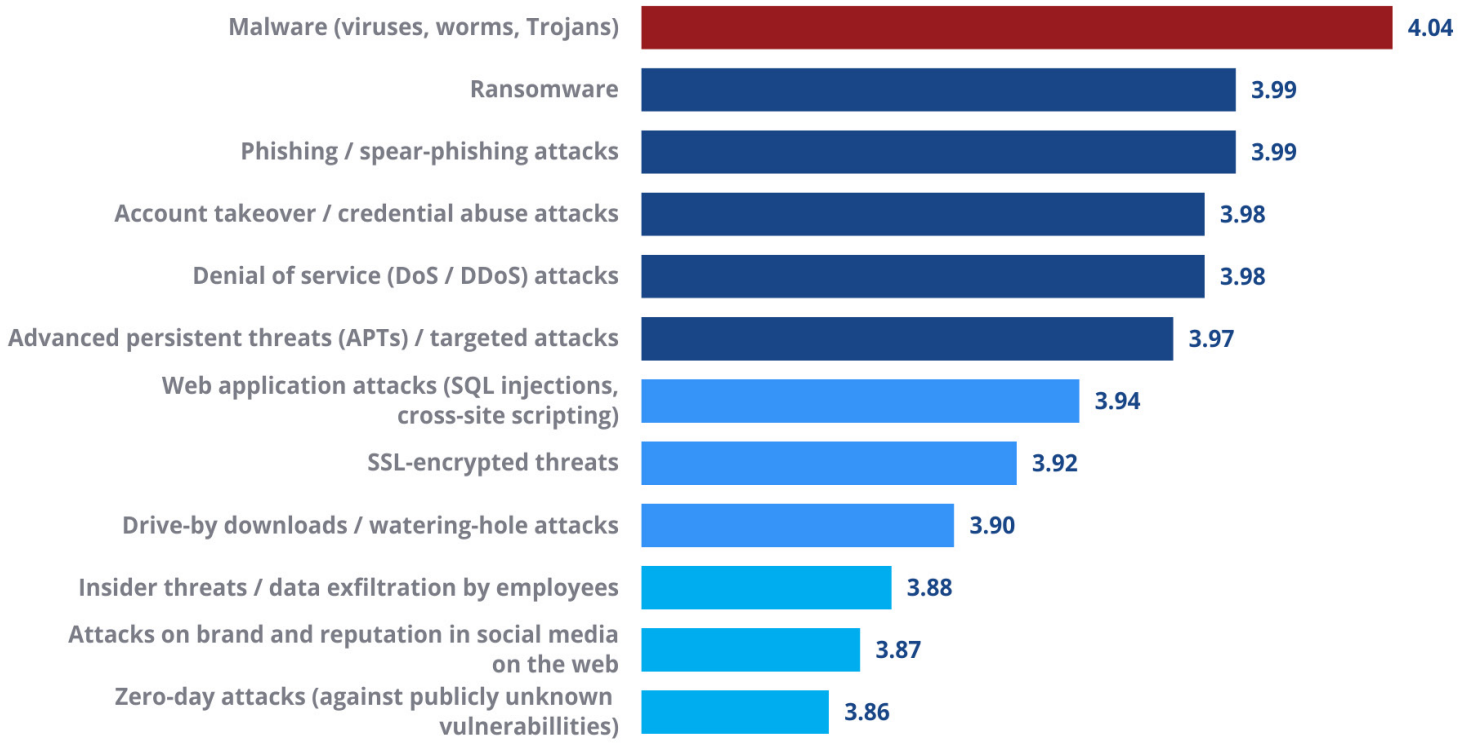


Figure 11: Relative concern for cyberthreats by type.

Of the 12 classes of cyberthreats we track each year, concern for malware has been atop the list for six straight years (see Figure 11). According to the 2020 Verizon Data Breach Investigations Report (DBIR), 17% of the data breaches researched for that report involved malware. So, it makes sense that malware, once again, achieved the highest 1-to-5 rating with a score of 4.04.

The next two classes of cyberthreats – ransomware (3.99) and phishing/spear-phishing attacks (3.99) – have appeared in the top three for the last four years. This year, they tied for second place, closely followed by account takeover/credential abuse attacks (3.98) and denial of service (DoS/DDoS) attacks (3.98), which tied for fourth place.

"IT security professionals are more concerned about cyberthreats than ever before."

The biggest gainer in this year's CDR is advanced persistent threats (APTs)/targeted attacks (3.97), up 0.10 from last year. The next biggest gainer is web application attacks (3.94), up 0.09 from last year.

Section 2: Perceptions and Concerns

At the bottom of the list for the second straight year is zero-day attacks (3.86), as it should be, since less than 1% of registered vulnerabilities in MITRE's CVE database originate as zero-day vulnerabilities in any given year. Plus, security vendors have made incredible strides over the years at detecting never-before-seen cyberthreats without the use of threat signatures. First, it was sandboxing and now it's ML and AI algorithms to the rescue.

As a reminder, respondents completed our survey in November 2020, about a month before the world learned of the infamous SolarWinds zero-day attacks that wreaked havoc on hundreds of commercial and government agencies around the globe. Next year's CDR survey will be conducted in November 2021. It will be interesting to see whether concern for zero-day attacks lingers 11 months after the SolarWinds catastrophe.

One class of cyberthreat that we want to keep our eyes on in the years ahead is brand reputation attacks (3.87). We added this to the list last year and it remains in second-to-last position. But we believe that this low level of concern may be an "ignorance is bliss" phenomenon, as monitoring social media and the web for hijacked and/or impersonated social media accounts, counterfeit goods websites, and fraudulent websites will become more of a concern in the cybersecurity community as:

- Incidents become more frequent and serious
- Marketing discovers these concerns and asks IT for help
- Digital risk protection (DRP) and brand protection solutions become more prevalent

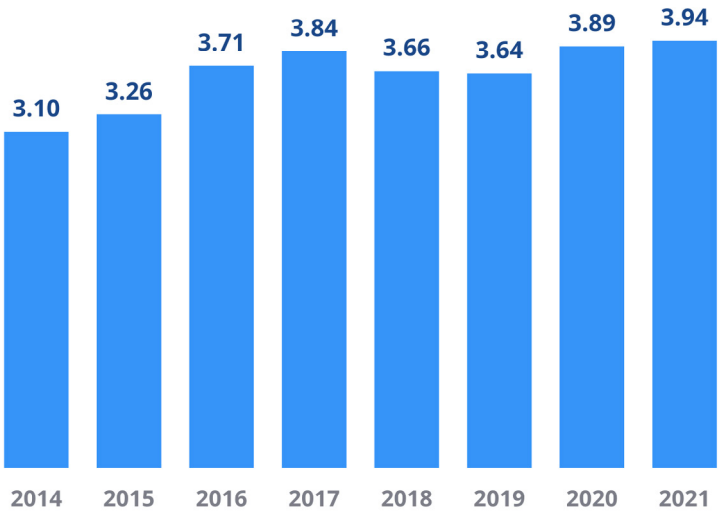


Figure 12: Threat Concern Index, depicting overall concern for cyberthreats.

Finally, with all of the chaos that IT security professionals experienced last year stemming from the COVID-19 pandemic (see page 55), how has overall concern for all classes of cyberthreats changed from a year ago? CyberEdge's "Threat Concern Index" averages the 1-to-5 ratings across all 12 cyberthreat classes to produce a single composite rating (see Figure 12). In our 2020 CDR, the Threat Concern Index rating was 3.89, a new record at the time. This year, that record has been broken with a rating of 3.94. Put another way, IT security professionals are more concerned about cyberthreats than ever before.

Section 2: Perceptions and Concerns

Concern for Web and Mobile Attacks

Which of the following attacks on your web and mobile applications are most concerning? (Select up to three.)

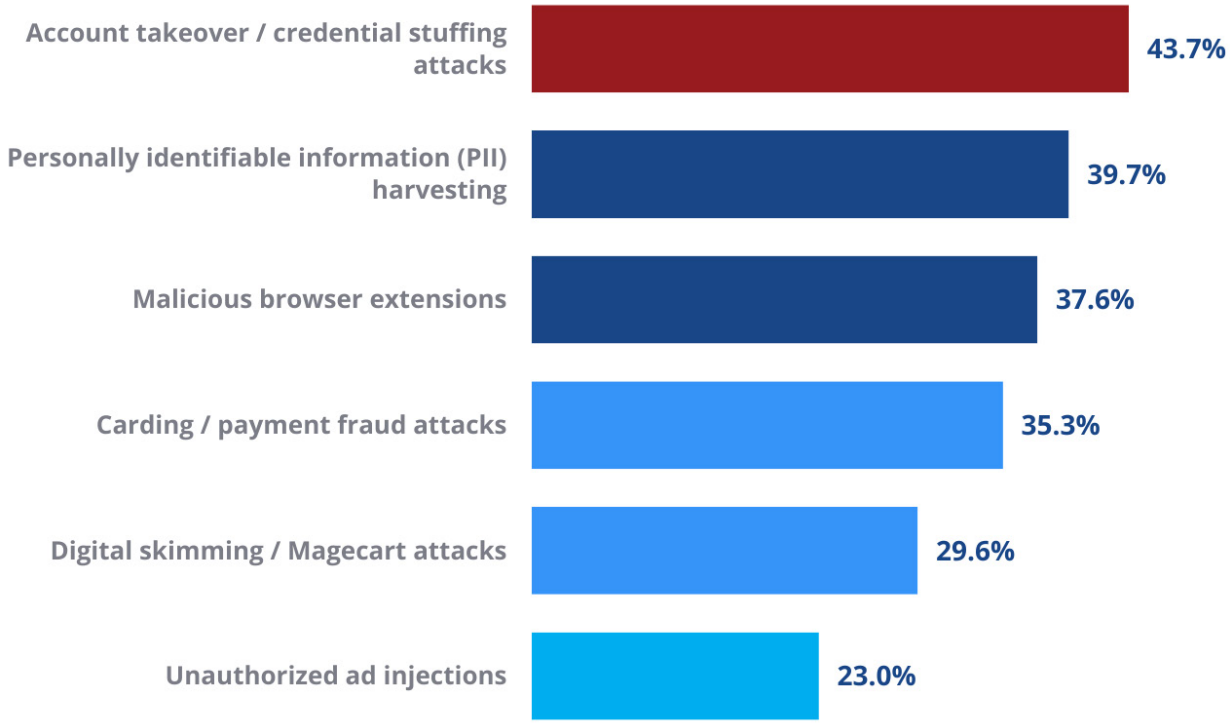


Figure 13: Most-concerning web and mobile application attacks.

Because attacks on web and mobile applications continue to rise, we added a new question to this year's CDR survey. From the five most common types of web and mobile application attacks, we asked respondents to select up to three that concern them the most. The results are insightful (see Figure 13).

Atop the list, as no surprise to many, is account takeover attacks (43.7%), which commonly use a technique called "credential stuffing." This is an automated attack that uses breached username/password pairs to fraudulently gain access to consumer or business user accounts.

"Our data also confirmed that web an mobile attacks are pervasive. More than nine out of 10 organizations surveyed reported being affected by cyberattacks targeting web and mobile applications."

Section 2: Perceptions and Concerns

Here's how it works:

1. The attacker acquires usernames and passwords from the dark web following a website data breach.
2. The attacker uses automated bots to test the stolen credentials against retail e-commerce, financial services, and social media websites, or alternately against the websites of targeted enterprises.
3. Successful logins (usually around 0.1% to 0.2% of total login attempts) allow the attacker to take over the account matching the stolen credentials.
4. The attacker exfiltrates credit card numbers and other personally identifiable information (PII) from a consumer's account, or leverages a business user's credentials to obtain privileged access, move laterally through the enterprise's data center and cloud applications, and steal intellectual property, personal information, financial account numbers, and other goodies.

Next on the list is PII harvesting (39.7%), which involves exploiting security vulnerabilities in JavaScript or other third-party code components. Security flaws in client-side code provide attackers the means of injecting malicious code designed to gain access to the user data at the point of entry, including PII such as Social Security numbers, dates of birth, credit card numbers, and more.

In third place is malicious browser extensions (37.6%). These are malicious programs posing as third-party web browser extensions linked to popular social media and online shopping sites such as Facebook, Rakuten, and Honey. These extensions, commonly written in JavaScript, are designed to exfiltrate information about the user or to download and execute malicious code.

Rounding out the list are the bottom three:

- Carding/payment fraud attacks (35.3%), where attackers use bots to test lists of recently stolen credit/debit card details on merchant websites
- Digital skimming/Magecart attacks (29.6%), where attackers inject malicious code into third-party JavaScript to steal credit card data
- Unauthorized ad injections (23.0%), where attackers (often through malicious browser extensions) inject banner ads that replace or overlay original, legitimate ads and redirect users to malicious websites

Our data also confirmed that web and mobile attacks are pervasive. More than nine out of 10 organizations surveyed (91%) reported being affected by cyberattacks targeting web and mobile applications.

Section 2: Perceptions and Concerns

Responding to Ransomware

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

Ransomware is unrelenting! The past 12 months saw a record-setting number of successful ransomware attacks. According to this year's CDR research, 68.5% of organizations were affected by one or more successful ransom attacks (see Figure 14). That's an all-time high, up from 62.4% last year.

Why the continuing surge in attacks? Here at CyberEdge, we think it may be the result of a three interacting trends, illustrated in Figure 15.

The first trend is that the percentage of organizations that successfully recovered their data following a ransom payment is at an all-time high of 71.6%, up from 66.8% a year ago. But this is a double-edged sword. The more confident organizations are that they will recover their data upon paying ransoms, the more

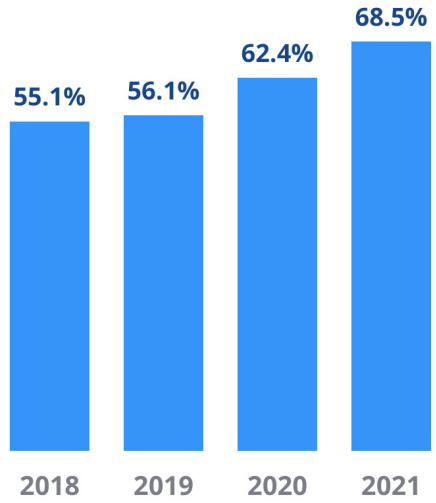


Figure 14: Percentage of organizations affected by ransomware.

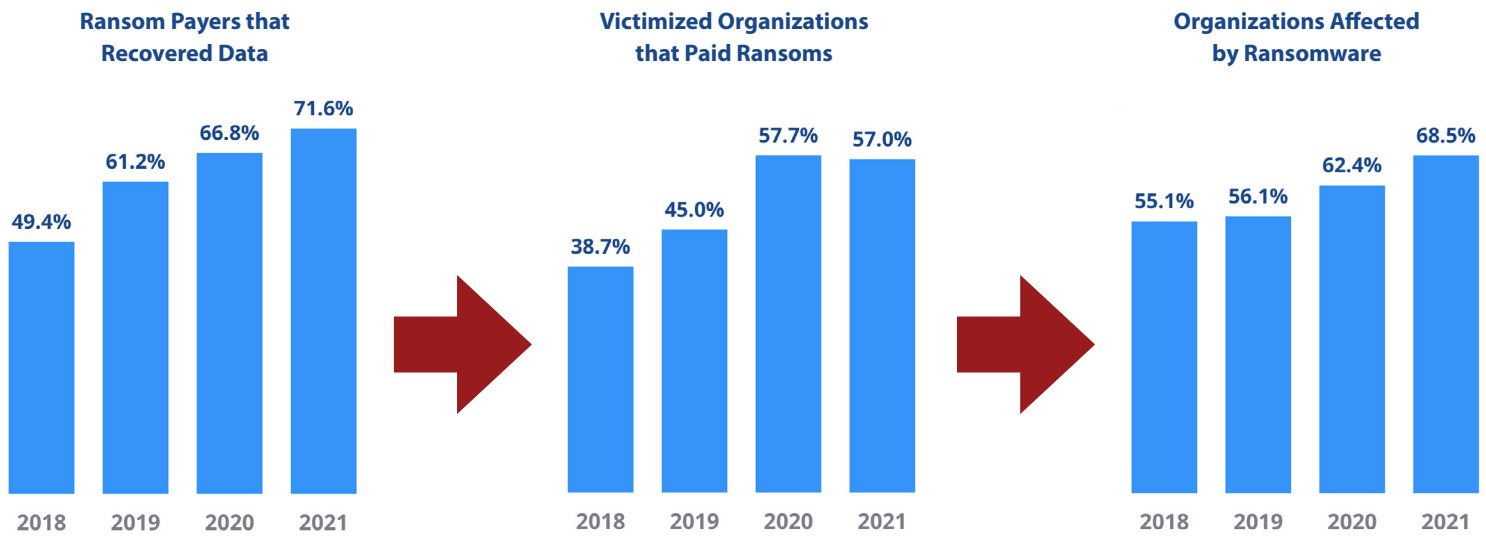


Figure 15: The ransomware vicious cycle: increased odds of recovering data … entice more victims to pay ransoms … which motivates more ransomware attacks.

Section 2: Perceptions and Concerns

likely they'll be to actually pay the ransoms. That percentage has risen over the past two years to the 57% range. Finally, the trend of more organizations paying ransoms motivates cybercriminals to increase their volume of ransomware attacks, which means another surge in the number of ransomware victims. This is a vicious cycle that, unfortunately, doesn't seem likely to be broken anytime soon.

Another trend – toward exponentially higher ransom payments – is elevating ransomware to the status of a bona fide catastrophe for many victims. According to research by Coveware, a ransomware incident response vendor, average ransomware payments increased 1,732% between the first quarter of 2019 and the third quarter of 2020, from $12,762 to $233,817 (see Figure 16). The average fell unexpectedly in the fourth quarter of 2020, to $154,108. Perhaps organizations are saying "no more," or perhaps they are negotiating more effectively with the cyber-criminals. Regardless, while a $12,000 payment two years ago was a nuisance, a $154,000 ransom today can be a serious blow to small businesses, hospitals, school districts, local government agencies, and other small and medium-sized organizations that have recently become the target of choice for ransomware.

Other notable findings from this year's CDR regarding successful ransomware attacks include:

- Australia (79.6%), the United States (78.5%), and Saudi Arabia (77.6%) were the countries most affected, while Japan (56.0%), Singapore (57.1%), and the United Kingdom (57.9%) were least affected (see Figure 17).
- The most severely affected major industries were telecom and technology (75.4%) and education (72.7%), while the least affected were government (50.0%) and healthcare (59.4%) (see Figure 18).
- When the data is broken down by organization size, those with more than 25,000 employees fared the best (56.9%). Organizations with employee numbers ranging from 500 to 9,999 were about equally affected (range of 68.6% to 70.6%).

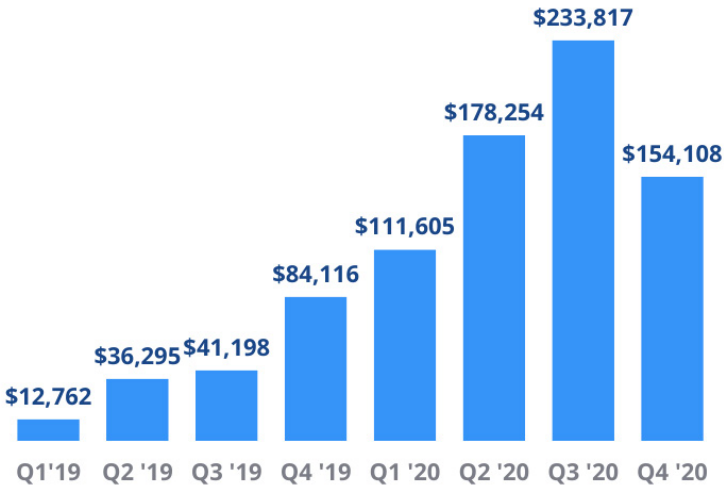


Figure 16: Average ransom payments, by quarter (data source: Coveware Quarterly Ransomware Reports).

In September of last year, for a brief period, we thought we had seen the world's first death by cyberattack. A woman in Düsseldorf, Germany, with a life-threatening condition had to be transported to a hospital in Wuppertal 30 kilometers (19 miles) away because the local hospital in Düsseldorf was victimized by a ransomware attack. The attack compromised 30 of the hospital's servers, which prevented it from processing new patients. Unfortunately, that woman died.

At first, the media touted the occurrence as the first fatality caused by a cyberattack. But two months later, German authorities concluded that the delay in transport was not a contributing factor in the patient's death.

Given steady increases in successful attacks in the multi-billion-dollar ransomware industry, many of which affect hospitals, will 2021 be the first year we witness death by cyberattack?

Section 2: Perceptions and Concerns

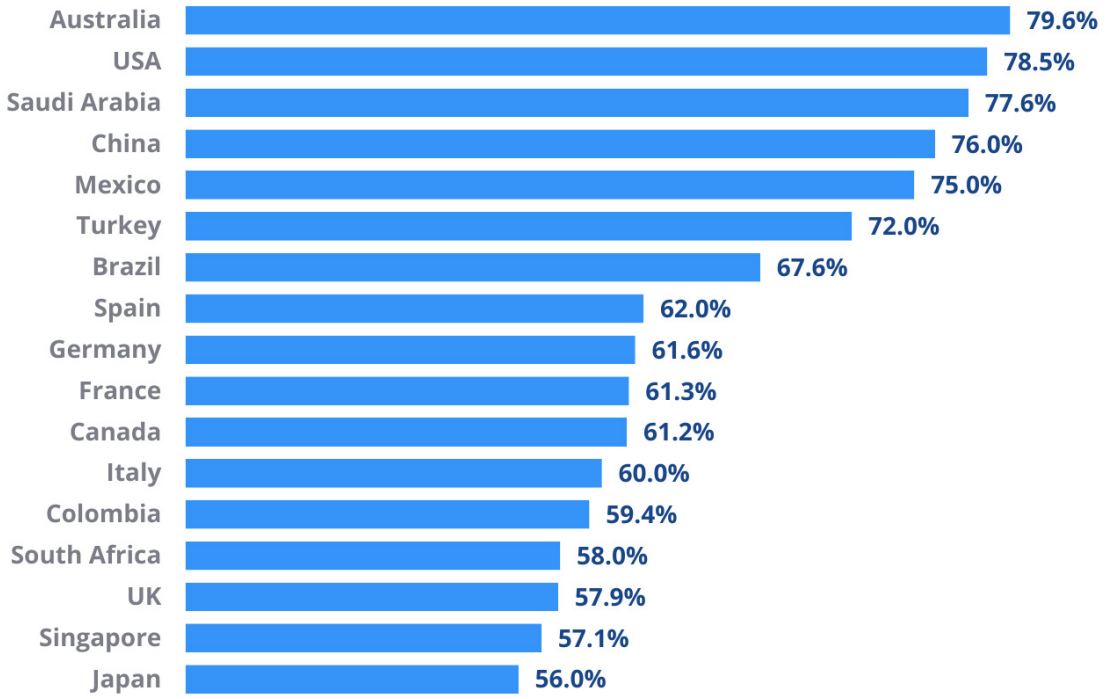


Figure 17: Percentage of organizations affected by ransomware in the last 12 months, by country.

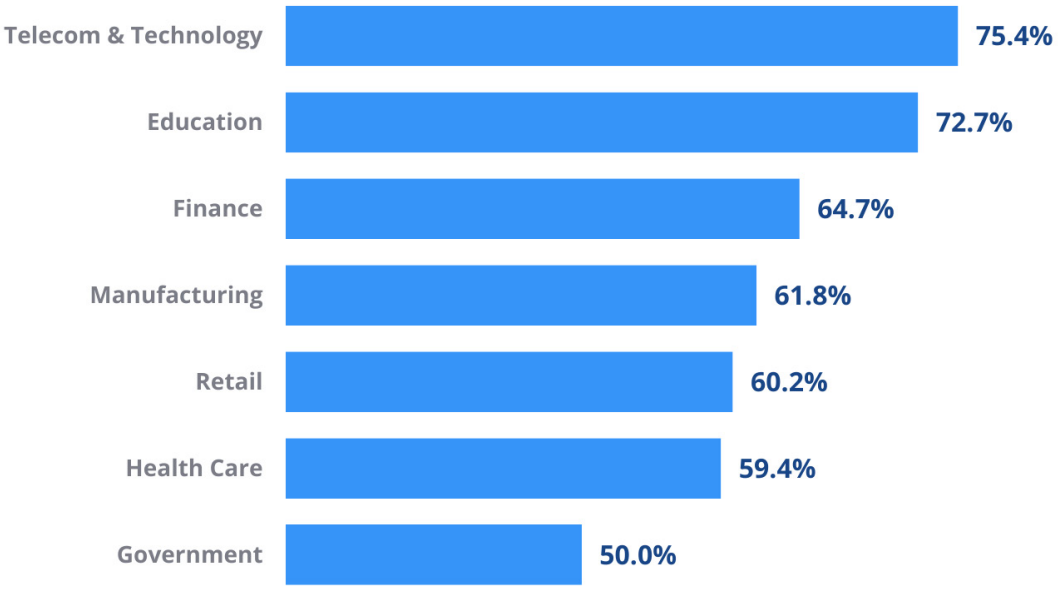


Figure 18: Percentage of organizations affected by ransomware in the last 12 months, by industry.

Section 2: Perceptions and Concerns

Barriers to Establishing Effective Defenses

On a scale of 1 to 5, with 5 being most serious, rate how each of the following inhibit your organization from adequately defending itself against cyberthreats.

Figure 19: Inhibitors to establishing effective cyberthreat defenses.

Each year, we ask respondents to tell us what's inhibiting them from adequately defending their organizations against cyberthreats. What's standing in the way of their success? Is it lack of budget? Inadequate security defenses?

Our two perennial leaders, low security awareness among employees and lack of skilled personnel, remain atop the list this year (see Figure 19). They highlight two longstanding problems that have plagued security teams for years.

First, too many organizations only train employees once – when they join the company or government agency -- on how to avoid falling victim to cyberattacks. Smart security teams do things differently. They provide all employees with ongoing security

"Smart security teams are investing in IT security training and certification as both a recruiting and a retention tool."

Section 2: Perceptions and Concerns

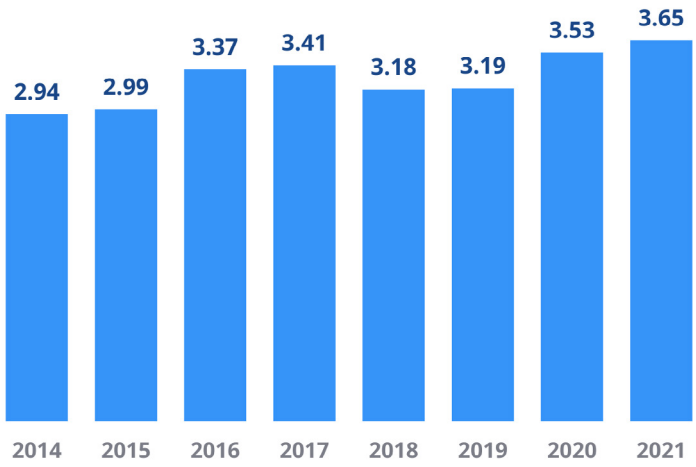


Figure 20: Security Concern Index, depicting the average rating of security inhibitors.

awareness training. Also, they employ simulated phishing platforms. These send harmless phishing emails to employees every month to expose carelessness and educate potential victims on the importance of constant vigilance. Both initiatives dramatically increase security awareness and reduce risks of ransomware and successful data breaches

Second, we previously learned that 87% of organizations experienced an IT security skills shortfall last year (see page 15). Smart security teams are investing in IT security training and certification as both a recruiting and a retention tool. Also, we know that 81% of IT security professionals would like to work from home part or all of the time. By relaxing requirements to report to the office every day, a sensible work-from-home policy can improve job satisfaction and make it a little easier to recruit the security personnel you're looking for.

Third on this year's list of inhibitors is poor integration/interoperability between security solutions, up from the number six position last year. This factor is also responsible for this year's highest rating change (0.17 increase). Nobody wants security solutions that work in isolation. The best security solutions share intelligence and perform functions with other security solutions, even if they are provided by different vendors.

On the opposite end of the spectrum is lack of budget. It is once again at the bottom of the list despite the fact that, as we'll later learn, security is now consuming a slightly smaller percentage of the overall IT budget (see page 29) and IT security budgets this year are not rising as much as in previous years (see page 31).

If you average out all of the 1-to-5 ratings from research participants for all 10 of the inhibitors represented in our survey, you get a single number. That number is represented in our Security Concern Index (see Figure 20). This is a way for us to gauge how stressed IT security professionals are from one year to the next. Are things getting worse or are they getting better?

Well, this year's Security Concern Index is 3.65, which is an all-time high, up from 3.53 a year ago. And for the second consecutive year, all 10 inhibitor ratings increased year-over-year. Of course, given all of the personal and professional challenges stemming from the COVID-19 pandemic over the last year, it's no wonder stress levels are through the roof. Many security team members have been asked to do more with fewer resources – while at home with screaming kids in the background. Once again, our proverbial hats are off to IT security professionals everywhere.

Section 2: Perceptions and Concerns

Benefits of Unified App and Data Security Defenses

Which of the following have been the biggest benefits of leveraging a unified platform for application and data security defenses (e.g., WAF, DDoS protection, RASP, API security, data risk analytics, database security)? (Select up to three.)

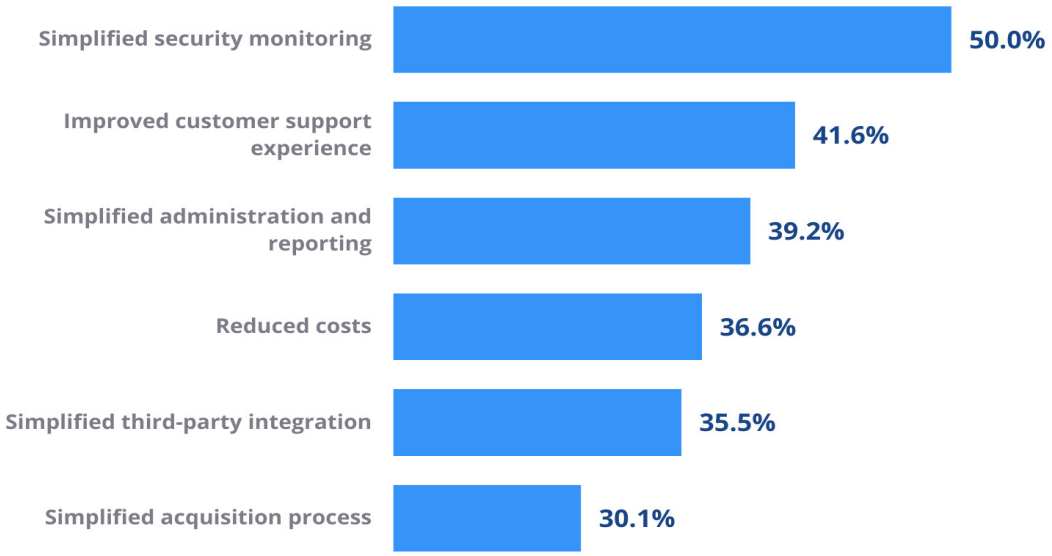


Figure 21: Benefits achieved by unifying application and data security defenses.

If you ran an ice cream parlor, it would be unrealistic (and colossally stupid) to source your chocolate ice cream from one supplier, your vanilla ice cream from another, and your strawberry ice cream from a third. There are enormous efficiencies to be gained from sourcing all your ice cream flavors from one supplier.

We believe this same concept holds true for application and data security defenses. Sure, there are pure play API security vendors, and pure play risk analytics vendors, and pure play database security vendors. But wouldn't it be great if you could source all of your application and data security defenses from a single vendor? Our respondents think so.

We asked our respondents to select up to three benefits of unifying their application and data security defenses within a single platform. The results are insightful (see Figure 21).

At the top of the list is simplified security monitoring (50.0%). Security analysts have one pane of glass to stare at instead of many. Next is an improved customer support experience (41.6%), which makes perfect sense as security administrators have one number to call when they need technical assistance. Third is simplified administration and reporting (39.2%). A unified platform means one management interface and one set of reports for all application and data security concerns.

The three remaining benefits are reduced cost (36.6%), simplified third-party integration with key security tools like SIEMs (35.5%), and a simpler acquisition process (30.1%). It's interesting to note that no single benefit achieved less than 30%. Our data reinforces the notion that smart security teams are selecting one reputable vendor that can satisfy all of their application and data security needs rather than sourcing solutions from two, three, or more niche vendors. The economies of scale are just too compelling.

Section 2: Perceptions and Concerns

Boosting Careers with Cybersecurity Certifications

Based on your organization's current climate, which of the following types of cybersecurity certifications do you believe would be most beneficial to your career path? (Select up to three.)

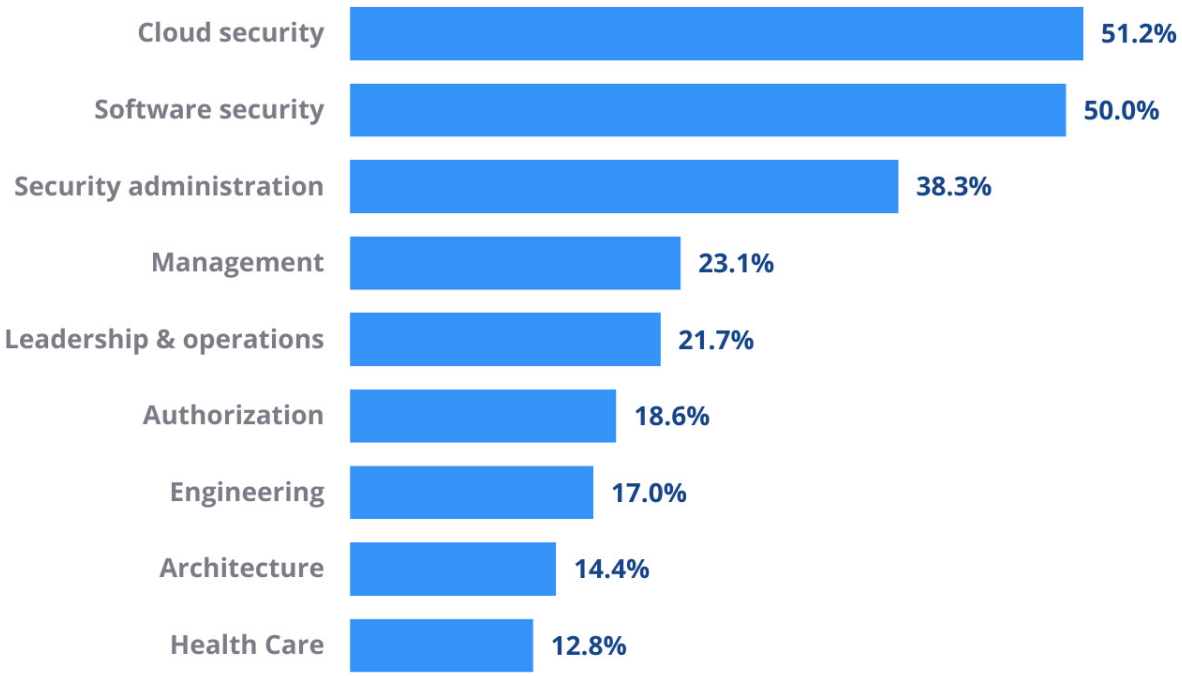


Figure 22: Types of specialty cybersecurity professional certifications deemed most beneficial to IT security career paths.

CyberEdge has always been a huge proponent of IT security training and certification. Our founder and CEO, Steve Piper, has maintained his CISSP certification from (ISC)² for more than a decade. And many of CyberEdge's research and marketing consultants have earned cybersecurity certifications from (ISC)² and other prominent providers. Last year, CyberEdge surveyed 600 IT security professionals to assess how the pandemic has affected their respective security teams (see page 55). One of the valuable lessons we learned is that 78% of those respondents

"It makes perfect sense that cloud security is the specialty security certification most sought after today by IT professionals (51.2%)."

Section 2: Perceptions and Concerns

felt their IT security professional certifications better equipped them to meet the cybersecurity challenges they faced during the pandemic.

So, being proponents of IT security training and certification, we asked the 1,200 respondents to this year's CDR to select up to three of nine cybersecurity certification types that they believe would be beneficial to their career paths. Nearly all of our respondents (99%) acknowledged that achieving at least one cybersecurity certification would help their career (see Figure 22).

It makes perfect sense that cloud security is the specialty security certification most sought after today by IT professionals (51.2%). One of the most notable paradigm shifts in the IT security industry in recent years is the move from on-premises applications and security packages to cloud-hosted applications and cloud-native security solutions. In last year's COVID-19 impact study, a whopping 75% of respondents said the pandemic affected their preferences for cloud-based security solutions. Later in this report, we'll see that the percentage of security applications and services delivered via the cloud increased substantially from a year ago (see page 47).

The second most sought-after specialty cybersecurity certification is software security (50.0%), which relates to another paradigm shift in cybersecurity thinking. Eliminating vulnerabilties during coding is an extremely cost-effective way to reduce your attack surface.

In third place is security administration (38.3%), which is particularly timely since the IT security role in greatest demand this year is IT security administrator (see page 16). Beyond that, the six remaining specialty certifications, while relevant to specific job roles and industries, rate between 12.8% (health care) and 23.1% (management).

Section 3: Current and Future Investments

IT Security Budget Allocation

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

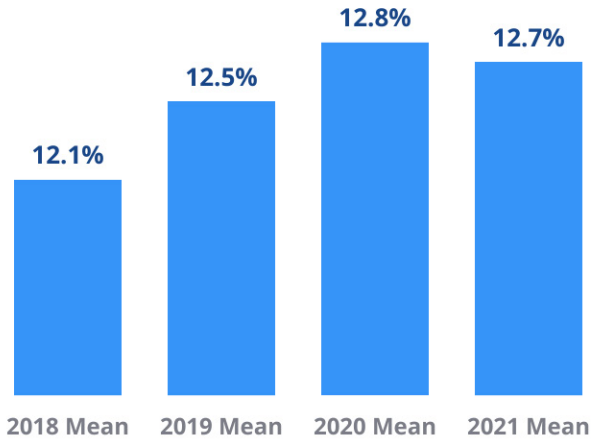


Figure 23: Percentage of IT budget allocated to information security, by year.

Each year we ask our CDR respondents to specify the percentage of their employer's overall IT budget that is allocated to information security. For the first time since we asked this question, four years ago, the percentage of IT budget allocated to security has gone down rather than up (see Figure 23). Globally speaking, that percentage is 12.7%, down from 12.8% a year ago. Now, we're only talking about one-tenth of one percent. But the fact that this is our first-ever decline is noteworthy.

We think the explanation for this change lies in the non-security operational costs of supporting so many new remote workers created by COVID-19. Yes, organizations have increased their budgets for IT security (see page 31), but they are also spending more on laptops, network connections, help desk support, and

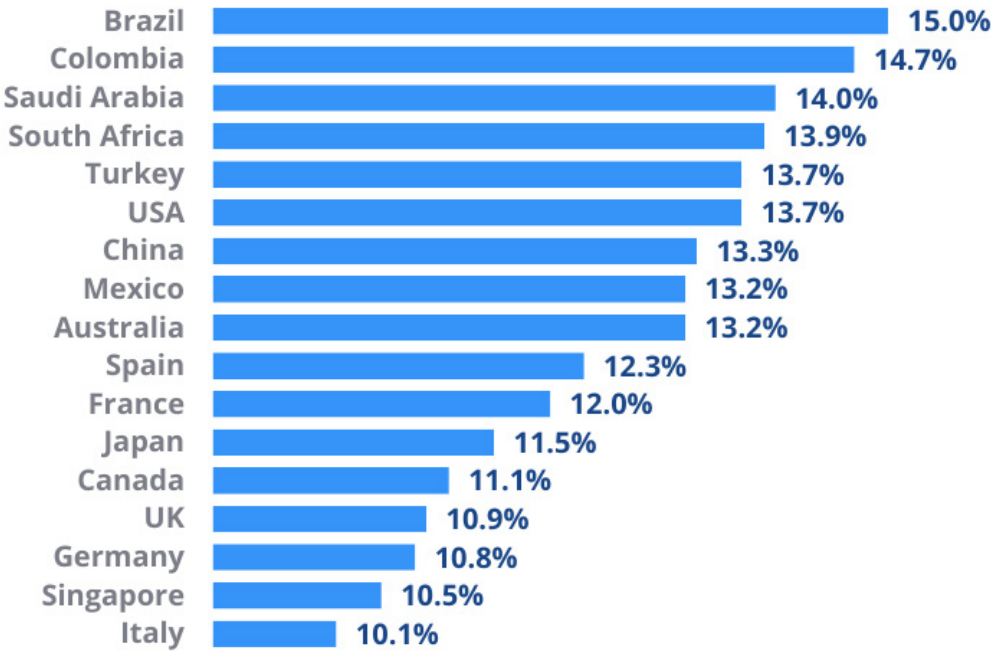


Figure 24: Percentage of IT budget allocated to security, by country.

Section 3: Current and Future Investments

other costs related to remote work. We don't think the flattening of this trend represents less commitment to security, but rather a host of unavoidable expenses related to provisioning and supporting WFH and BYOD.

Of course, the portion of IT budgets consumed by security varies by country, by industry, and by organization size. Let's review statistics from each of these perspectives.

Geographically speaking, organizations from Brazil (15.0%), Colombia (14.7%), and Saudi Arabia (14.0%) dedicate the largest portions of their respective IT budgets to security, while organizations from Italy (10.1%), Singapore (10.5%), and Germany (10.8%) assign the smallest. The United States, at 13.7%, is a full percentage point higher than the global mean of 12.7% (see Figure 24).

From an industry perspective, education (13.7%), telecom and technology (13.2%), and finance (12.8%) are above the global mean. Health care (11.7%), government (11.8%), manufacturing (11.8%), and retail (12.6%) are below it (see Figure 25).

Finally, from a size perspective, smaller organizations with 500-999 employees (13.4%) dedicate the largest portion of IT budget to security, while mid-size enterprises with 5,000-9,999 employees (12.2%) and 10,000-24,999 employees (12.1%) dedicate the smallest (see Figure 26).

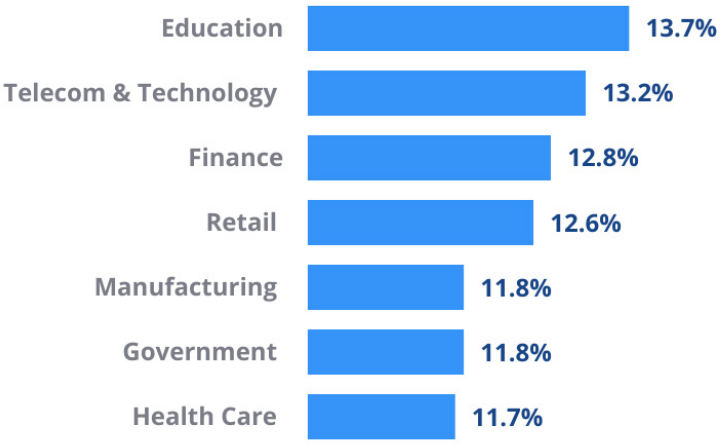


Figure 25: Percentage of IT budget allocated to security, by industry.

"For the first time since we asked this question, the percentage of IT budget allocated to security has gone down rather than up."

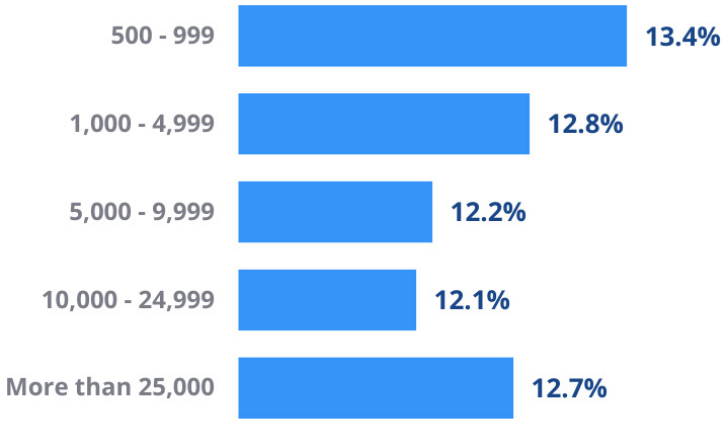


Figure 26: Percentage of IT budget allocated to security, by employee count.

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 2021?

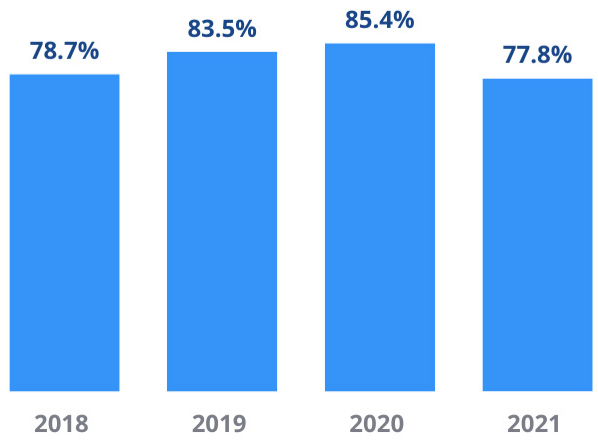


Figure 27: Percentage of organizations with rising security budgets.

Every year for eight consecutive years, CyberEdge has asked IT security professionals whether their operating budgets were increasing or decreasing in the coming year, and by how much. For the first time in our CDR history, we've seen a decline in the percentage of organizations whose security budgets are rising (see Figure 27).

Furthermore, this is a first-ever decline in the amount of IT security budget increases (see Figure 28). Over the preceding three years, IT security budgets have gone up by 4.7%, 4.9%, and 5.0%, respectively. This year, the average IT security budget is "only" going up by 4.0%.

Now, before we all hit the panic button, let's put this into perspective. First, we're still in the midst of a global pandemic. Despite the progress that nations have made in distributing COVID-19 vaccines, it's not over yet. And some industries (e.g., hospitality and retail) have been harder hit by the pandemic than others (e.g., government and utilities). Second, we're not saying that the average IT security budget has shrunk this year. Quite the contrary. In fact, more than three-quarters (77.8%) of IT security budgets have increased this year. It's just that these budgets, on average, aren't growing as fast as they have in the past.

From a regional perspective, IT security budgets in Brazil (+5.8%), South Africa (+5.0%), and Mexico (+4.8%) aren't as adversely affected. However, IT security budgets in Spain (+2.8%), Canada (+2.9%), and Germany (+3.0%) have been harder hit. In the United States, average IT security budgets are rising by 3.8% this year, just under the +4.0% global mean (see Figure 29).

Looking at our seven major industries, healthcare (+4.8%), telecom and technology (+4.5%), and government (+4.2%) are all above the global mean. Retail (+4.0%) and finance (+4.0) align with the global mean. Education (+3.2%) and manufacturing (+3.9%) are both below the global mean (see Figure 30).

Organization size does not appear to be a major influencer with regard to 2021 IT security budget changes. Mid-size enterprises with 5,000-9,999 employees seem to have the most IT security budget growth (+4.5%), while the very largest enterprises with 25,000 or more employees (+3.5%) are experiencing the smallest IT security budget growth (see Figure 31).

In short, although the growth of IT security budgets has slowed, the IT security profession is a great place to be from a job security perspective.

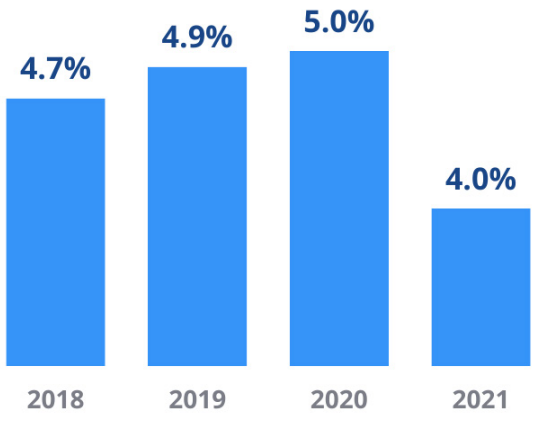


Figure 28: Mean annual increase in IT security budgets.

Section 3: Current and Future Investments

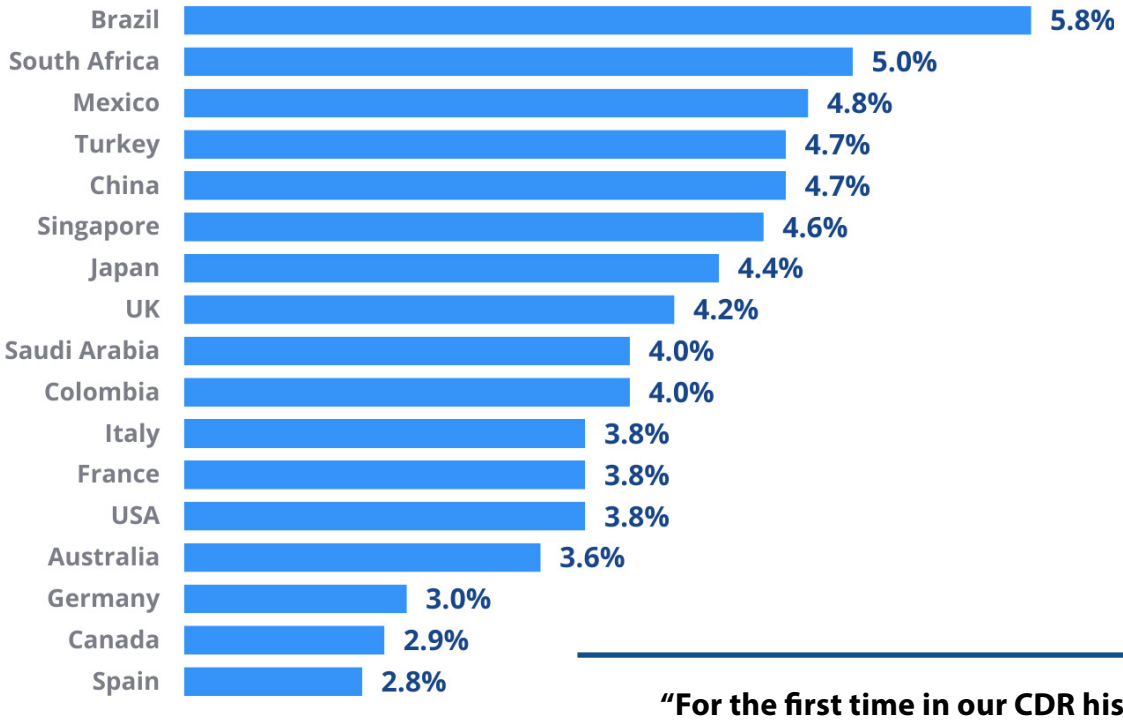


Figure 29: Mean security budget increase, by country.

"For the first time in our CDR history, we've seen a decline in the percentage of organizations whose security budgets are rising."

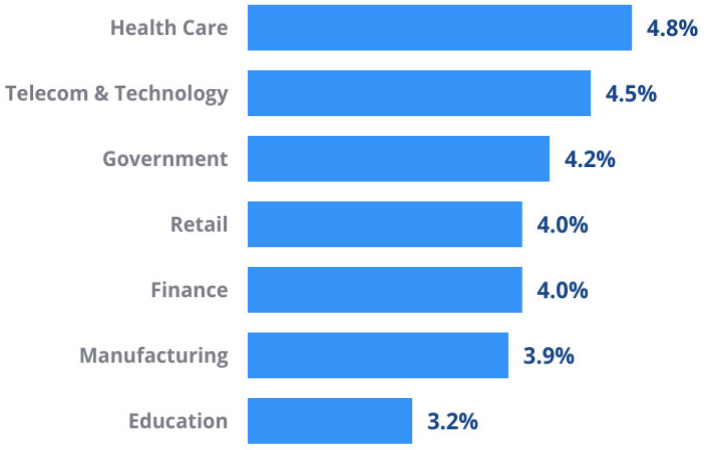


Figure 30: Mean security budget increase, by industry.

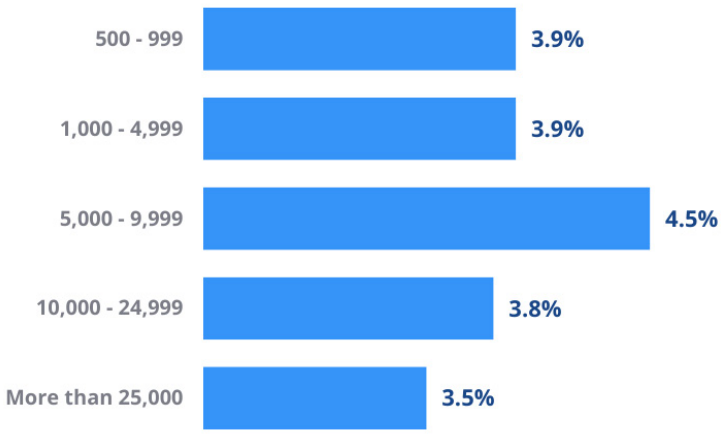


Figure 31: Mean security budget increase, by employee count.

Section 3: Current and Future Investments

COVID-19 Effects on IT Security Purchase Priorities

How has the COVID-19 pandemic affected your organization's priorities for acquiring new IT security products and services?

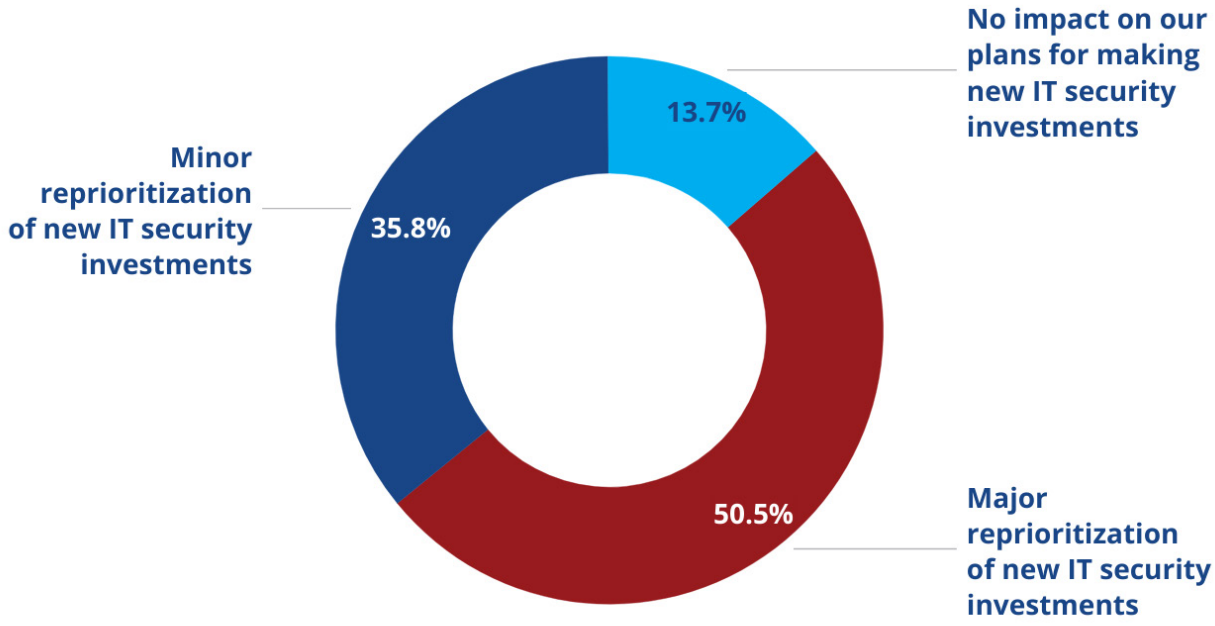


Figure 32: Effects of the COVID-19 pandemic on IT security spending priorities.

The COVID-19 pandemic turned all of our lives upside down—both personally and professionally. From an IT security perspective, security teams had just finished budget planning at the end of 2019 and were starting to execute their plans in the first quarter of 2020. Then all hell broke loose.

Once again, last year's "The Impact of COVID-19 on Enterprise IT Security Teams" yielded many valuable insights (see page 55), including:

- 114% average increase in remote workers
- 59% increase in BYOD policies
- Insufficient remote access capacity
- Massive increase in cyberthreats and security incidents
- 75% of respondents have increased their preference for cloud-based security solutions

One question that we didn't ask in that report is how the pandemic affected the big picture with regard to IT security spending priorities. As you can imagine, the pandemic had a significant effect (see Figure 32). In fact, just over half (50.5%) of organizations said the pandemic triggered a major re-prioritization of new IT security investments, while 35.8%

Section 3: Current and Future Investments

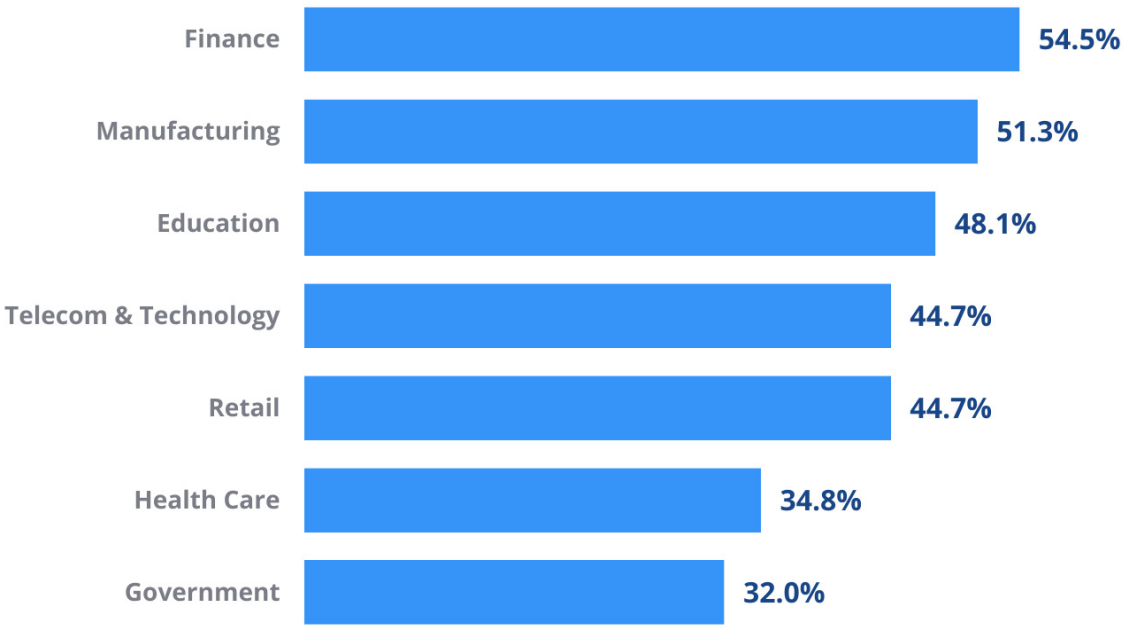


Figure 33: Organizations where COVID-19 caused a major reprioritization of IT security investments, by industry.

reported some spending re-prioritization. Only 13.7% – we'll call them the lucky ones – felt the pandemic had no impact on their IT security spending priorities.

From an industry perspective, the organizations where major re-prioritization was required were more common in finance (54.5%) and manufacturing, while organizations in the government (32.0%) and healthcare (34.8%) sectors were not as impacted (see Figure 33).

From a geographical perspective, organizations in Turkey (68.0%), Mexico (66.7%), Colombia (60.6%), and the United States (60.2%) experienced the highest incidence of major changes in spending priorities. Organizations in Canada (30.6%), the United Kingdom (31.6%), and Germany (35.1%) were not as affected as much.

No matter which way you slice it, the vast majority (86.3%) of IT security organizations had to alter their IT security spending priorities last year to accommodate a massive increase in remote workers, to secure a plethora of unmanaged personal devices, and to deal with a massive increase in cyberthreats and other security risks. Let's all be grateful that the end of this pandemic is near so life can return to at least some semblance of normalcy.

"No matter which way you slice it, the vast majority (86.3%) of IT security organizations had to alter their IT security spending priorities last year."

Section 3: Current and Future Investments

Network Security Deployment Status

Which of the following network security technologies are currently in use or planned for acquisition (within 12 months) by your organization?

	Currently in use	Planned for acquisition	No plans
Advanced malware analysis / sandboxing	58.9%	32.8%	8.3%
Data loss / leak prevention (DLP)	53.5%	35.8%	10.8%
Secure email gateway (SEG)	53.3%	33.6%	13.1%
Intrusion detection / prevention system (IDS/IPS)	51.8%	35.9%	12.3%
Network access control (NAC)	51.4%	36.4%	12.2%
SSL/TLS decryption appliances / platform	51.3%	35.3%	13.4%
Secure web gateway (SWG)	51.2%	36.5%	12.3%
Denial of service (DoS/DDoS) prevention	50.0%	38.6%	11.4%
Network behavior analysis (NBA) / NetFlow analysis	48.0%	36.5%	15.5%
Next-generation firewall (NGFW)	46.7%	40.3%	13.0%
Deception technology / distributed honeypots	43.3%	37.2%	19.6%

Table 1: 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 enable you to compare your organization's current and planned usage of common security technologies against those of 1,200 of your peers around the globe – starting with network security technologies.The first column depicts the percentage of responding organizations that are currently using each technology in production. The middle column portrays organizations that are planning to acquire the technology this year. The last column reflects organizations that haven't firmed up their plans yet.

To make the results easier to absorb, we color-coded the cells. 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.

Let's start by examining which network security technology is most widely used these days. In Table 1 we see only one dark blue cell, corresponding to advanced malware analysis/ sandboxing (58.9%), in the top spot for the second consecutive

Section 3: Current and Future Investments

year. We can remember when sandboxing first emerged as an enterprise-class product, initially within on-premises, purpose-built appliances. But rapidly, sandboxing became a commoditized feature. It was often provided as an inexpensive cloud-based add-on to next-generation firewalls (NGFWs), secure web gateways (SWGs), and secure email gateways (SEGs). Then, of course, the "bad guys" found ways to evade sandboxing analysis by suppressing malicious routines in files until a human later triggered them.

That's about the same time when security products featuring ML and AI algorithms designed to detect advanced and zero-day threats arrived on the scene. Nowadays, organizations can't afford to rely on network security technologies that feature signature-based detection alone. That's why advanced malware analysis boasts the highest combined adoption percentage (91.7%) of organizations that are planning to acquire this technology or are already using it in production. This certainly augers well, as malware is the number-one class of cyberthreat on the minds of security professionals this year (see page 17).

Shifting gears, let's examine which network security technology is at the top of most shopping lists this year. Once again, we've got one dark blue cell. This time, it's NGFW. Although NGFWs have been around for more than a decade, not all organizations have realized the benefits of integrating firewall, intrusion prevention system (IPS), and application control technologies into one unified, single-pass architecture. One potential "political" concern is firewall admins from network teams feeling they might lose administrative control to their security counterparts. But that really shouldn't be an issue, especially since modern NGFWs provide role-based access control so network and security personnel can maintain control over the NGFW settings and data that are most relevant to their respective roles.

In second place this year is DoS/DDoS prevention technology (38.6%), which also represents the biggest year-over-year gainer with regard to acquisition plans. It wouldn't surprise us at all if demand for DDoS prevention solutions spiked after Amazon Web Services was hit by a gigantic DDoS attack in February 2020. Plus, have you heard about "extortion DDoS attacks" yet? It's like ransomware meets DDoS. Thousands of organizations received emails last year from cybercrime syndicates demanding that Bitcoin ransoms be paid or else full-scale DDoS attacks would follow. Some demonstrated their capabilities by committing pre-emptive DoS attacks. While most organizations that rejected the ransom payment were unaffected, some were victimized by multivector DDoS floods, which peaked at around 200 Gbps.

"It wouldn't surprise us at all if demand for DDoS prevention solutions spiked after Amazon Web Services was hit by a gigantic DDoS attack in February 2020."

In third place is deception technology/distributed honeypots (37.2%). If you haven't looked at this technology yet, do yourself a favor and check it out. It's a smart and fairly easy way to uncover infiltration attempts by detecting would-be invaders as they move laterally across your network or a simulated replica of your network. You gain not only valuable intelligence on your cyber-adversaries, but also the ability to sever their connections to your network mid-attack.

That wraps up this year's network security buying intentions. Next up is endpoint security (see page 37).

Section 3: Current and Future Investments

Endpoint Security Deployment Status

Which of the following endpoint security technologies are currently in use or planned for acquisition (within 12 months) by your organization?

	Currently in use	Planned for acquisition	No plans
Basic anti-virus / anti-malware (threat signatures)	70.5%	22.2%	7.3%
Data loss / leak prevention (DLP)	58.1%	30.4%	11.5%
Advanced anti-virus / anti-malware (machine learning, behavior monitoring, sandboxing)	56.8%	36.1%	7.1%
Application control (whitelist / blacklist)	55.1%	32.9%	12.0%
Disk encryption	54.0%	34.4%	11.6%
Digital forensics / incident resolution	51.3%	35.8%	13.0%
Browser / internet isolation and micro-virtualization	48.2%	38.3%	13.5%
Deception technology / honeypot	41.8%	41.3%	16.9%

Table 2: 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 2). As with Table 1, percentages in dark blue correspond to a higher frequency of adoption and acquisition plans, while those in light blue correspond to a lower frequency.

Once again, let's start out by focusing our attention on the first column in the table and identify which endpoint security technology is most widely used. Likely not a surprise to anyone, basic signature-based anti-virus/anti-malware (70.5%) is at the top of the list – and probably won't budge from that spot for many years to come. Although we all know that relying on signature-based defenses alone is an exercise in futility, they do play a critical role by filtering out all of the easy (i.e., known) stuff so security solutions with more-sophisticated capabilities aren't overwhelmed as they detect more-advanced threats that signature-based defenses missed.

Let's now discuss the endpoint security technology that is most sought-after in 2021: deception technology/honeypot (41.3%). As we mentioned in the network security section (see page 36), deception technology provides a smart and fairly easy way to uncover infiltration attempts by detecting would-be invaders as they move laterally across your network or a replica. Again, you not only gain valuable intelligence on your cyberadversaries, but also the ability to sever their connections to your network mid-attack. User laptop and desktop computers dramatically

Section 3: Current and Future Investments

"Demand for browser isolation technology has increased so much that it boasts the biggest 'change in use' gain among all other endpoint security technologies depicted in this study."

increase the quantity of potential "traps" that cyberattackers may fall into, improving the odds of detecting threats early.

Close behind deception technology/honeypot is browser or Internet isolation/micro-virtualization technology (38.3%). Browser isolation technology, in particular, has grown in popularity in recent years – no doubt sparked by the use of so many unmanaged devices during the pandemic. Instead of viewing content accessed via the Internet using local applications, users open content within applications in the cloud. This change is seamless to users, who view the applications as if they were running locally. This approach prevents client operating systems and applications from being accessed and compromised by malware. Because browser isolation services are cloud-based, they are a good fit for organizations that want to move more security solutions to the cloud. Demand for browser isolation technology has increased so much that it boasts the biggest "change in use" gain among all other endpoint security technologies depicted in this study.

In third place this year is advanced anti-virus/anti-malware technology (36.1%) equipped with ML, behavior monitoring, and/or sandboxing mechanisms. This technology complements traditional, signature-based endpoint defenses by detecting advanced and zero-day threats that those defenses miss. Sometimes this technology operates as a standalone endpoint detection and response (EDR) solution, while at other times it is integrated with a full-fledged endpoint protection platform (EPP) offering.

Now that we've covered endpoint security technologies most in demand this year, let's explore application- and data-centric security technologies (see page 39).

Section 3: Current and Future Investments

Application and Data Security Deployment Status

Which of the following application- and data-centric security technologies are currently in use or planned for acquisition (within 12 months) by your organization?

	Currently in use	Planned for acquisition	No plans
API gateway / protection	63.8%	29.1%	7.1%
Web application firewall (WAF)	58.5%	32.1%	9.4%
Database firewall	58.1%	31.9%	10.0%
Database encryption / tokenization	56.6%	30.5%	12.9%
Application container security tools/platform	54.1%	36.8%	9.1%
Database activity monitoring (DAM)	53.3%	35.5%	11.2%
Cloud access security broker (CASB)	52.0%	34.7%	13.3%
Application delivery controller (ADC)	50.4%	34.7%	14.9%
Static/dynamic/interactive application security testing (SAST/DAST/IAST)	48.6%	38.2%	13.2%
Runtime application self-protection (RASP)	48.2%	35.9%	15.9%
Deception technology / distributed honeypots	47.0%	36.9%	16.1%
File integrity / activity monitoring (FIM/FAM)	46.9%	39.0%	14.1%
Bot Management	40.7%	40.4%	18.9%

Table 3: 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 3). 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.

Our first observation is that API gateway/protection adoption has skyrocketed! It has gone from last place to first place in just four years. In 2018, adoption was at 45.1%. Today, it's at 63.8%. For lack of a more eloquent expression, holy cow! Organizations have come to realize the compelling security and administrative benefits of this must-have security technology.

Of course, web application firewalls (58.5%), database firewalls (58.1%), and database encryption/tokenization (56.6%) technologies also fall into the must-have category when it

Section 3: Current and Future Investments

comes to application and data security. As DevSecOps adoption continues to soar (see page 49), several other technologies on this list will gain traction, such as SAST/DAST/IAST (48.6%) and RASP (48.2%) testing tools.

With regard to what's hot on this year's application and data security shopping list, a new CDR entrant, bot management, takes the top spot (40.4%). This rising star technology protects your websites, mobile applications, and APIs from automated attacks, helping to mitigate the risk of data breaches while improving operational efficiency. It can help prevent a variety of modern cyberthreats, including account takeover attacks, carding attacks, and business logic attacks such as inventory hoarding and content scraping (see page 19).

Second on this year's list is file integrity/activity monitoring (FIM/FAM), an "oldie but goodie" in the application and data security industry. FIM provides an essential layer of defense that helps detect illicit activity across critical file systems so security teams can shut down attacks before they have a chance to cause damage. FAM discovers and monitors sensitive data (e.g., credit card numbers, Social Security numbers) on servers and can provide an early warning upon detecting a potential data breach.

In third place this year are the aforementioned SAST/DAST/IAST application security testing tools (38.2%) – staples among DevSecOps professionals. Although ranked a little lower on this year's application security wish list, demand for RASP (35.9%) is also growing. If you are unfamiliar with these acronyms, read on:

- Static application security testing (SAST), also known as "white box testing," allows developers to uncover security vulnerabilities in application source code early in the software development life cycle.
- Dynamic application security testing (DAST), also known as "black box testing," is designed to discover security vulnerabilities within a running web application after the software development life cycle is complete.
- Interactive application security testing (IAST) combines elements of both SAST and DAST approaches by placing an agent within the application that performs all of its analysis inside the app in real time at any point during the software development life cycle.
- The term "runtime application self-protection" (RASP) was coined by Gartner in 2012. It's a security technology built into the application runtime environment that is capable of controlling application execution while detecting and preventing attacks in real time.

Now that we've delved into what's hot in the application and data security space, let's now dive into the world of security management and operations technologies (see page 41).

"On this year's application and data security shopping list, a new CDR entrant, bot management, takes the top spot (40.4%)."

Section 3: Current and Future Investments

Security Management and Operations Deployment Status

Which of the following security management and operations technologies are currently in use or planned for acquisition (within 12 months) by your organization?

	Currently in use	Planned for acquisition	No plans
Patch management	56.7%	29.1%	14.2%
Advanced security analytics (e.g., with machine learning, AI)	56.1%	34.9%	9.0%
Security configuration management (SCM)	55.2%	32.3%	12.5%
Security information and event management (SIEM)	50.6%	37.3%	12.0%
Vulnerability assessment/management (VA/VM)	50.3%	38.3%	11.4%
Security orchestration, automation and response (SOAR)	49.6%	35.6%	14.8%
Full-packet capture and analysis	49.5%	38.8%	11.7%
Penetration testing / attack simulation software	47.9%	39.9%	12.1%
User and entity behavior analytics (UEBA)	46.6%	37.4%	16.0%
Threat intelligence platform (TIP) or service	43.0%	43.5%	13.5%

Table 4: Security management and operations technologies in use and planned for acquisition.

Next up, we have security management and operations. These technologies serve several important purposes, such as reducing an organization's attack surface, detecting advanced threats, and automating key security operational functions. 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.

At the last Gartner Security and Risk Management Conference that CyberEdge participated in before COVID-19 struck, one of the speakers presented three strategies for dramatically reducing cybersecurity risks – patch, patch, and patch. So, it's no wonder why patch management (56.7%) has appeared at the top of the "currently in use" column for three years running.

Advanced security analytics (56.1%) equipped with ML and/or AI threat detection engines jumped from last place in 2019 to second place in 2020. This year, it remains in second place as one of the top cyberthreat hunting solutions in the industry, while security configuration management (55.2%) remains a top-three contender for the third consecutive year.

Let's now explore the hottest security management and operations technologies planned for acquisition this year. At the tippy top of the list (sorry… had to…) for the second consecutive year is the threat intelligence platform, or TIP (43.5%). TIPs help automate, streamline, and simplify the entire process of researching, aggregating, and organizing threat intelligence data. There are multiple use cases for this compelling technology.

Section 3: Current and Future Investments

In our 2019 CDR, we asked our respondents to identify key motivations for deploying TIPs. They were:

- To improve our ability to detect cyberthreats (53.7%)
- To improve our ability to validate security alerts (52.9%)
- To improve our ability to prioritize responses to security alerts (43.3%)

In second position this year is penetration testing (39.9%), which accounts for the highest percentage increase in planned adoption this year. Penetration testing, sometimes called pen testing or ethical hacking, refers to the process of using hacking techniques to probe computer systems for vulnerabilities and security misconfigurations that hackers could exploit.

Third on the list of hottest security management and operations technologies, for the second consecutive year, is full-packet capture and analysis (38.8%). In our view, this is the "microwave oven" of security tools. Before the microwave oven came along, our parents didn't realize how life-changing this appliance would be. Similarly, once you start using a full-packet capture and analysis tool, you'll soon forget what life was like before it arrived. That's because it's such a powerful tool for detecting advanced threats, validating security incidents, and assessing the impact of a successful cyberattack.

"At the tippy top of the list (sorry… had to…) for the second consecutive year is the threat intelligence platform, or TIP (43.5%)."

That covers the highlights of security management and operations technologies. One more category to go – identity and access management (see page 43).

Section 3: Current and Future Investments

Identity and Access Management Deployment Status

Which of the following identity and access management (IAM) technologies are currently in use or planned for acquisition (within 12 months) by your organization?

	Currently in use	Planned for acquisition	No plans
Adaptive/risk-based authentication	56.3%	32.9%	10.8%
Password management / automated reset	54.6%	34.5%	10.9%
Privileged account/access management (PAM)	51.4%	34.5%	14.1%
Identity-as-a-Service (IDaaS)	51.2%	33.5%	15.4%
Tokens (hardware or software)	50.8%	34.5%	14.7%
User/account provisioning and de-provisioning	50.6%	36.4%	13.0%
Identity analytics	50.4%	36.0%	13.6%
Two-/multi-factor (2FA/MFA) authentication	49.8%	36.3%	14.0%
Single sign-on (SSO)	49.8%	36.6%	13.6%
Smart cards	46.2%	35.0%	18.9%
Federated identity management (SAML, Oauth)	44.1%	37.4%	18.6%
Biometrics	41.8%	40.1%	18.1%

Table 5: Identity and access management technologies in use and planned for acquisition.

As we hit the home stretch of security technology investments, we turn to the innovative world of identity and access management, or IAM, a staple of every IT security organization. As mentioned on more than one occasion (five, actually), percentages in dark blue correspond to a higher frequency of adoption or acquisition plans, while those in light blue correspond to a lower frequency.

Leaping to the top of the currently-in-use list, from eighth place last year to first place this year, is adaptive/risk-based authentication (56.3%), also known as step-up authentication. Unlike multi-factor authentication (still widely popular), which asks users for specific credentials whenever they log in or access corporate resources, adaptive/risk-based authentication asks for different credentials depending on the situation. A low-risk request from the user's usual device might require a single, simple form of authentication, while a high-risk transaction requested from an unusual device in a location new to the user might entail additional security questions, a code sent to a smartphone or email address, or a biometric signature. Adaptive/risk-based authentication reduces the friction for users trying to get their work done while providing additional security where appropriate.

Section 3: Current and Future Investments

Next on the currently-in-use list is password management/automated reset (54.6%), an important component of most IAM strategies for saving valuable IT administration cycles and improving user experiences. In third position is privileged account/access management (51.4%), or PAM, which helps organizations prevent insider attacks and unauthorized privilege escalation while enforcing principles of least privilege. This is particularly important, because outside attackers and malicious insiders can wreak havoc if they secure the accounts of privileged users like executives and system administrators.

"Leaping to the top of the currently-in-use list, from eighth place last year to first place this year, is adaptive/risk-based authentication (56.3%), also known as step-up authentication."

Regaining the number-one spot on IAM shopping lists from two years ago is biometrics (40.1%). Biometric technologies–such as fingerprint readers, facial recognition, iris recognition, hand geometry, and voice recognition–provide highly accurate, convenient, and hacker-proof ways to authenticate user access to systems, applications, data, and physical locations.

In second place on IAM shopping lists this year is federated identity management (37.4%), which got bumped from first place last year. This technology helps enterprises and applications share identities so subscribers can use the same credentials to access various applications. It's what enables you to log into so many websites with your Google or Facebook account.

In third place this year is single sign-on (36.6%), or SSO. SSO has been around for years, making it so much easier for workers to access disparate systems and applications using one set of credentials. SSO is tightly coupled with two-/multi-factor authentication (2FA/MFA) technology, providing an additional layer of IAM security.

Section 3: Current and Future Investments

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) and/or artificial intelligence (AI) technologies.

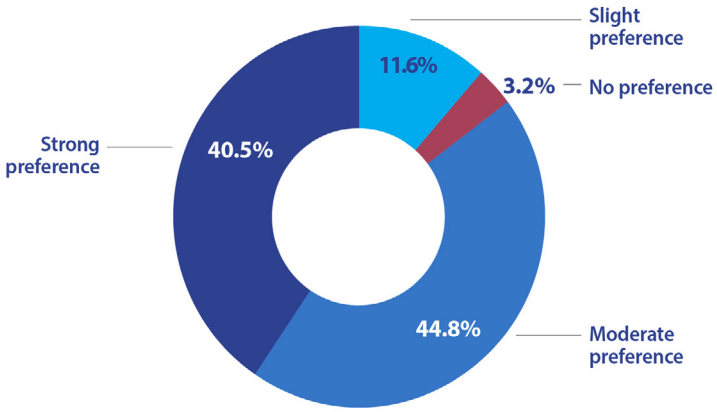


Figure 34: Preference for security products with machine learning and AI.

There's no question about it. Machine learning and artificial intelligence algorithms in cybersecurity products are here to stay. Period. But while ML and AI are often used interchangeably, they refer to different things. Let's break it down.

- AI is the ability of a system to complete tasks that are usually done by humans because they require human intelligence and discernment.
- ML is a subset of AI and, in the context of cybersecurity, is arguably the most common method for achieving AI. ML gives systems the ability to learn from experience without any explicit programming or expertise. ML relies on special algorithms, such as decision trees, neural networks, and regression.

We benefit from ML in our everyday lives and may not realize it. Gmail now has a smart reply feature that suggests brief responses to whatever mail you've received based on the content present in the email. Netflix uses ML to constantly improve movie and TV show recommendations based on what customers have watched previously. Uber uses ML to determine how long it will take for your driver to arrive. UberEATS does the same, but also factors in food preparation time based on your chosen restaurant. We could go on and on.

In the context of cybersecurity, ML and AI have improved our ability to:

- Discover new malware variants and zero-day threats
- Improve detection of phishing and spear-phishing emails
- Detect malicious network activity and stop attacks
- Uncover potential insider threats based on user behaviors
- Automate repetitive human tasks such as triaging incidents

Let's turn to the results of our survey question (see Figure 34). For the second year, we asked our respondents to gauge their overall preference for purchasing security products that feature ML and/or AI technology. And for the second straight year, the sum of those who indicated a strong preference (40.5%) and a moderate preference (44.8%) came to 85.3%, exactly. Even the industries with the most interest (telecom and technology at 90.2%) and least interest (government at 76.0%) in security products that feature ML and/or AI were the same as last year (see Figure 35). It's almost like watching Bill Murray in Groundhog Day! (Yeah, we love that movie, too.)

"There's no question about it. Machine learning and artificial intelligence algorithms in cybersecurity products are here to stay. Period."

Section 3: Current and Future Investments

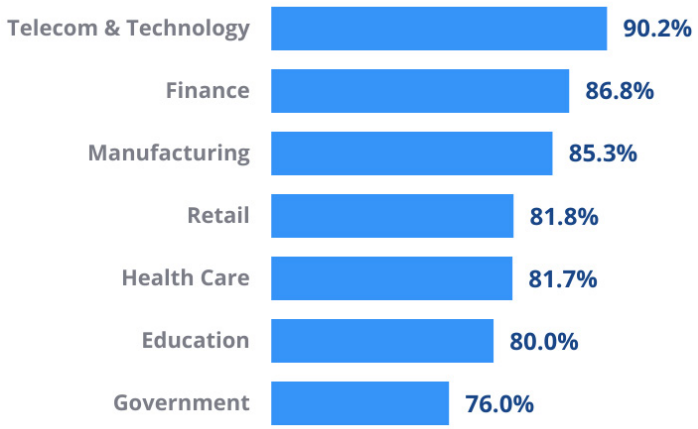


Figure 35: Strong or moderate preference for security products with machine learning and AI, by industry.

Preferences for security products that feature ML and/or AI technologies by country did change a bit this year. Last year, ML and AI were all the rage in Turkey (100%). This year, respondents from Saudi Arabia (98.0%) surpassed Turkish respondents (96.0%) for the top honors. Respondents from France (73.3%) and Germany (71.6%) were less bullish (see Figure 36).

As the results of this survey question are so close between our 2020 and 2021 CDRs, next year we'll be asking a different question about ML and AI. Sorry… no Groundhog Day sequel next year.

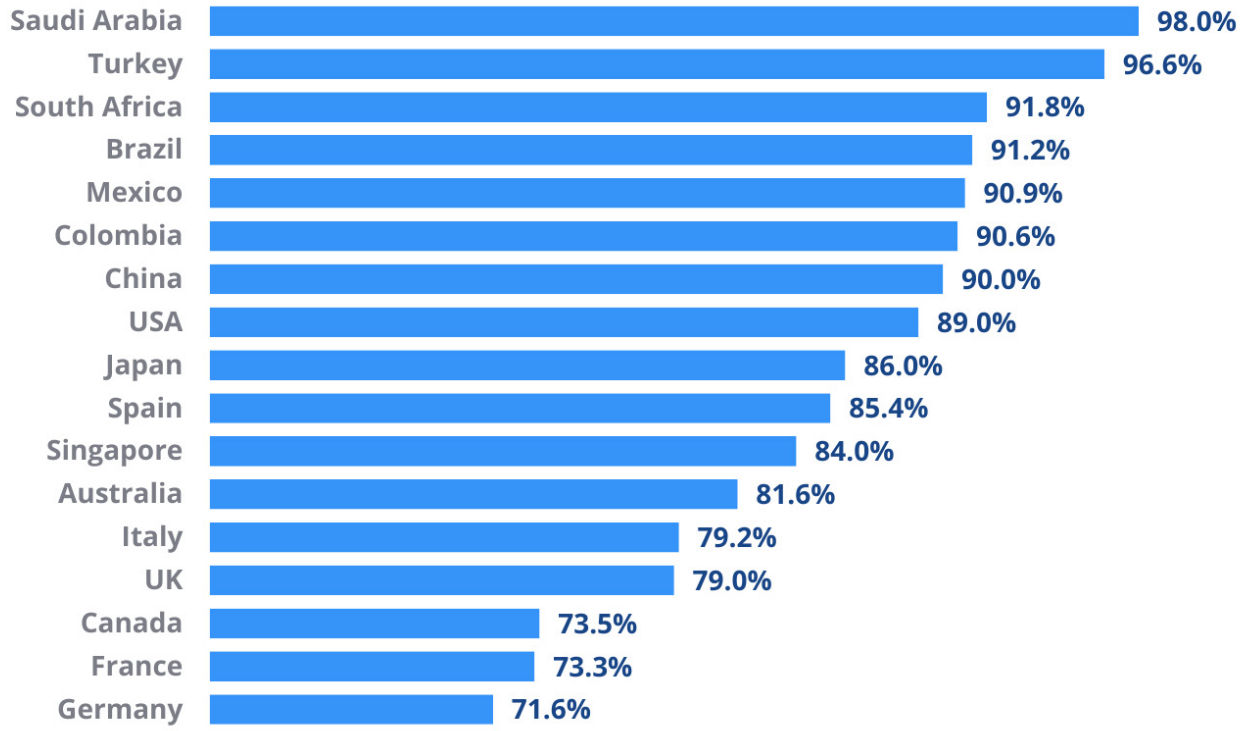


Figure 36: Strong or moderate preference for security products with machine learning and AI, by country.

Section 4: Practices and Strategies

Security Applications Delivered via the Cloud

What percentage of your information security applications and services is delivered via the cloud?

Before any of us knew what a coronavirus was, our industry was already experiencing a tidal wave of cloud-based cybersecurity solutions. Not only solutions for monitoring security in the cloud (i.e., IaaS, PaaS, SaaS), but also solutions leveraging the cloud to host security tools that monitor for risk everywhere, from cloud to core.

Before we delve into the results of the survey question referenced above, let's recap a few key statistics from last year's "The Impact

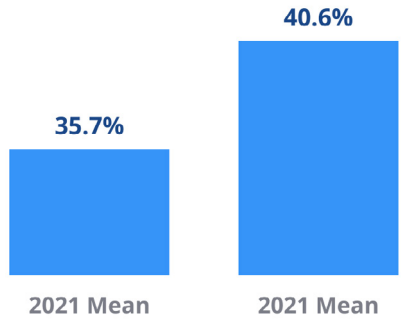


Figure 37: Percentage of security applications and services delivered via the cloud.

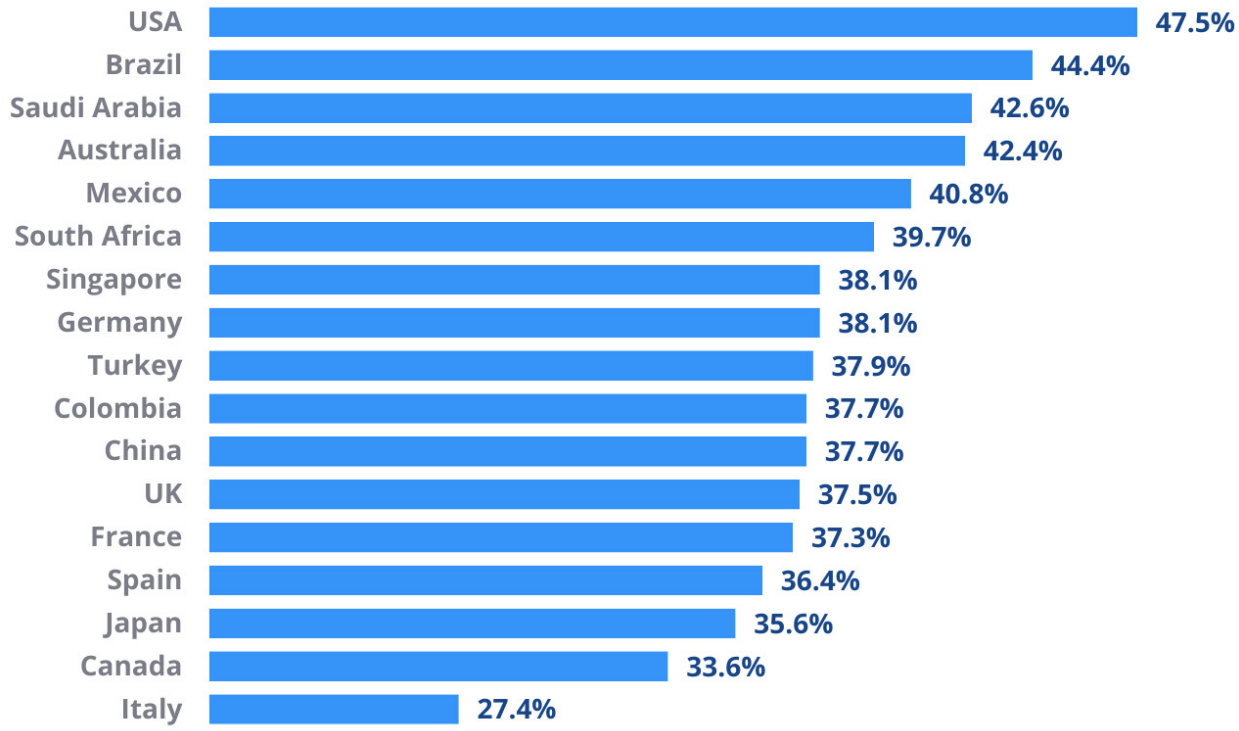


Figure 38: Percentage of security applications and services delivered via the cloud, by country.

Section 4: Practices and Strategies

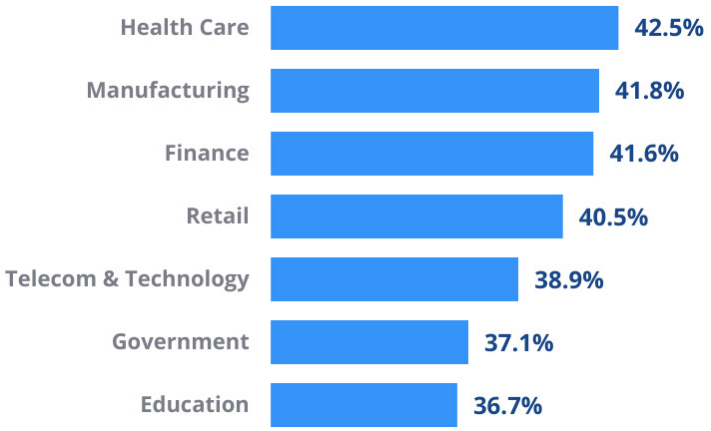


Figure 39: Percentage of security applications and services delivered via the cloud, by industry.

of COVID-19 on Enterprise IT Security Teams" survey report (see page 55). Two findings are particularly noteworthy:

- Three in four (75.1%) of the 600 IT security professionals who completed our survey last August indicated a significant or moderately increased preference for cloud-based security solutions versus traditional on-premises options.
- The top three IT security technologies that were specifically selected to address COVID-19 pandemic challenges were cloud-based SWG, cloud-based NGFW, and cloud-based SEG.

Noticing a trend here? These days, smart IT security teams are turning to cloud-based security solutions like never before. In our 2020 CDR, respondents indicated that 35.7% of their collective security applications and services were delivered via the cloud. This year, that figure has risen to 40.6%, which equates to nearly a 14% increase in just 12 months (see Figure 37).

"These days, smart IT security team are turning to cloud-based security solutions like never before."

From a geographic perspective, the United States (47.5%) has the highest adoption rate for cloud-based security solutions, with Brazil (44.4%), Saudi Arabia (42.6%), and Australia (42.4%) not far behind. Cloud-based security solutions just aren't as prevalent (yet) in Italy (27.4%), Canada (33.6%), and Japan (35.6%) (see Figure 38).

From an industry perspective, IT security professionals in the healthcare (42.5%), manufacturing (41.8%), and finance (41.6%) industries certainly have their heads in the cloud. Their counterparts in the education (36.7%) and government (37.1%) industries, not as much (see Figure 39).

Organization size doesn't seem to be a significant factor, with the range varying from 500-999 employees (45.9%) to 10,000-24,999 employees (37.4%).

Most agree that life may never return to exactly the way it was before the COVID-19 pandemic began. Once the pandemic is over and we're living in the "new normal," many believe that organizations will begin to relax restrictions that previously prevented employees from working from home, now that they've seen first-hand that remote workers can still be productive. This should entice organizations to invest even more in cloud-based security solutions – a new normal for the security industry.

Section 4: Practices and Strategies

Benefits of Embracing DevSecOps Practices

Which of the following have been the biggest benefits of DevSecOps practices for your organization? (Select up to three.)

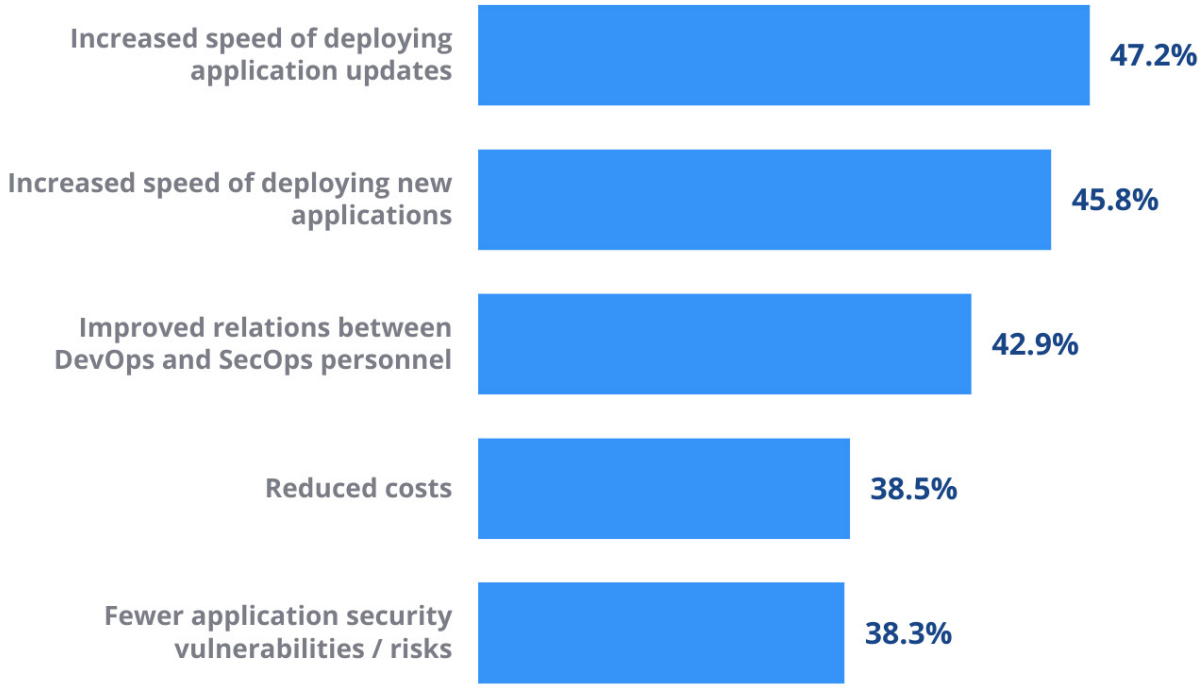


Figure 40: Most significant benefits of DevSecOps practices.

For those who aren't familiar with DevSecOps, or simply haven't jumped on the bandwagon yet, DevSecOps is a profound culture shift in the software industry that aims to bake security into the rapid-release cycles. These are typical of modern (agile) application development and deployment, also known as DevOps. Instead of securing applications after coding is finished, organizations "shift left" by baking security into the application development process from the very beginning of the software development life cycle (SDLC).

We asked our 1,200 respondents about the most notable benefits of DevSecOps practices that they've seen in their respective organizations (see Figure 40). Before we delve into the findings, it's worth noting that the benefit at the bottom of the list achieved a 38.3% rating. So, all five of these key benefits are compelling.

The top two items on the list of DevSecOps benefits are tightly coupled around the same topic–speed. Specifically, our respondents cited "increased speed of deploying application updates" (47.2%) and "increased speed of deploying new applications" (45.8%). Instead of tossing new applications and updates to existing applications over the wall to the security team to assess and approve, security is built and tested in during the development process, saving considerable time and, in many instances, accelerating business advantages.

Section 4: Practices and Strategies

If you'd like to know more about the tools that DevSecOps professionals use to embed security within modern applications, turn to page 40 to learn about SAST, DAST, IAST, and RASP.

Third on the list of DevSecOps benefits is "improving relations between DevOps and SecOps personnel" (42.9%). (We can visualize many of you shaking your heads as you read this.) Historically, tension has existed between DevOps teams and SecOps teams because they have widely divergent goals. One is focused on application features and functionality, while the other is focused on mitigating application cyber risks. This lack of cohesion between these two teams is detrimental to their IT organizations and the companies they serve.

To be clear, DevSecOps is a culture shift. Peter Drucker, widely regarded as the founder of modern management, once said, "Culture eats strategy for breakfast." What he meant is that a company's strategy, while by no means unimportant, takes a back seat to its culture. The same concept holds true within IT security teams. DevSecOps mandates continuous communication, transparency, and shared outcomes between DevOps and SecOps personnel. Suddenly, security is everyone's responsibility!

"The top two items on the list of DevSecOps benefits are tightly coupled around the same topic–speed."

This culture shift drives the next two beneficial outcomes on the list–reduced costs (38.5%) and fewer application security risks (38.3%). There's no question that implementing DevSecOps has a positive impact on a company's bottom line. Thus, DevSecOps is one of the fastest-growing segments of the IT security industry. So much that we're happy to report 93.0% of our responding organizations have already begun to implement DevSecOps practices. Of the small group that hasn't, 71.4% plan to get started soon.

Section 4: Practices and Strategies

SSL/TLS Traffic Decryption Challenges

Which of the following challenges does your organization face with regard to decrypting SSL/TLS traffic and inspecting it for threats? (Select all that apply.)

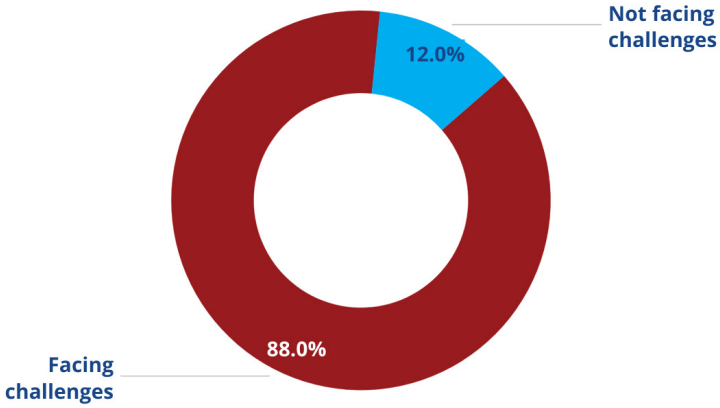


Figure 41: Percentage of organizations facing SSL/TLS traffic inspection challenges.

WARNING: Please stand back as CyberEdge steps onto the proverbial soap box and preaches for a bit.

We all have pet peeves. Last year, SurveyMonkey surveyed 544 ordinary people and asked them to rank their most significant pet peeves. The top three were leaving common spaces messy (63%), neglecting to take out the trash (45%), and talking loudly on the phone (30%). Well, we at CyberEdge have our own pet peeves about the security industry, and organizations failing to decrypt SSL/TLS traffic for inspection by security tools is one of them. It's second on our list, if you must know, right behind security vendors saying "on premise" when they really mean "on premises." But we'll save that for another day.

Last year's 2020 CDR provided an eye-opening statistic on this topic. We asked our respondents to estimate the percentage of their organization's SSL/TLS-encrypted web traffic that is actually being decrypted for inspection by network security tools. The mean response was 34.5%. That was shocking to us. With 85% or more (industry reports tend to vary between 85%-95%) of web traffic encrypted, only decrypting a third of that traffic for inspection creates an enormous blind spot for security professionals.

So, this year we wanted to understand why more organizations aren't decrypting web traffic for inspection. Specifically, we asked our respondents to select from four key SSL/TLS decryption challenges. But before we assess the rankings of those challenges, we'd like to point out a scary statistic from this year's CDR. Exactly 88% of this year's respondents indicated that their organizations are, indeed, experiencing challenges decrypting SSL/TLS web traffic (see Figure 41). What's frustrating is that we know it doesn't have to be this way. (More on that later.)

The number-one challenge our respondents face with regard to decrypting SSL/TLS web traffic is the significant decrease in performance within network security tools (44.1%) (see Figure 42). We can remember when IPS, NGFW, and SWG vendors started to build SSL/TLS decryption into their respective products about 15 years ago. In some instances, performance decreased by 90%. These days, the performance hit on typical network security appliances is still significant.

"Exactly 88% of this year's respondents indicated that their organizations are experiencing challenges decrypting SSL/TLS web traffic. What's frustrating is that we know it doesn't have to be this way."

Section 4: Practices and Strategies

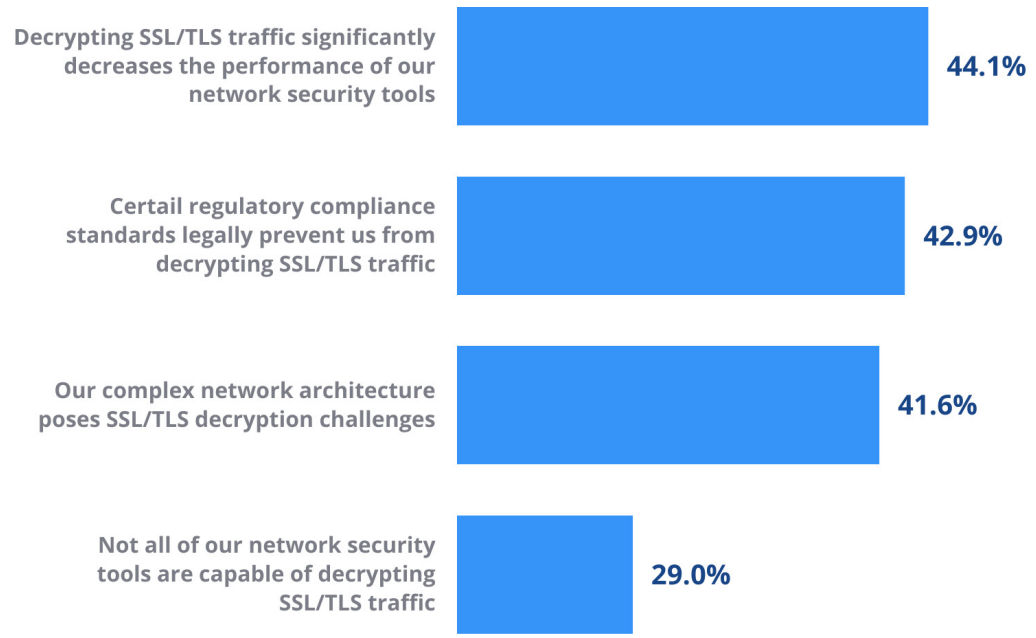


Figure 42: Challenges faced with decrypting SSL/TLS traffic for inspection.

The second-biggest challenge pertaining to decrypting SSL/TLS traffic is the potential for violating regulatory requirements, such as PCI DSS and HIPAA (42.9%). If all network traffic is decrypted, outside attackers and unauthorized employees have more opportunities to read credit card numbers, medical data, and other information protected by regulations. To prevent this, solutions need "application intelligence" so they can decrypt selectively.

The third-biggest challenge relates to the complexity of network architectures (41.5%), followed by the fact that not all network security tools are even capable of SSL/TLS decryption (29.0%).

Okay, so why is this subject such a pet peeve for CyberEdge? It's because purpose-built, dedicated SSL/TLS inspection appliances have been on the market for years and too few organizations are taking advantage of them. These appliances decrypt ingress and egress SSL/TLS traffic and direct it to a "closed loop" of network security tools (e.g., firewall, IPS, NGFW, SWG, DLP). After the traffic has been inspected and malicious traffic has been blocked, the traffic is re-encrypted before being forwarded to its final destination. Also, decryption can be selectively disabled for traffic that contains data protected by regulations.These SSL inspection appliances are so powerful that neither throughput nor latency of your Internet traffic is adversely impacted.

So, what does this mean for IT organizations? It means you can have your cake and eat it, too. By using dedicated SSL/TLS inspection appliances, you avoid performance impacts to your existing network security tools, you maintain compliance with regulatory standards, you maintain your network architecture, and you don't have to worry about security tools that are incapable of decrypting web traffic. Given that the majority of modern malware uses encryption to conceal command and control (C&C) communications, payload delivery, and data exfiltration, how can organizations afford to ignore this problem any longer?

Section 4: Practices and Strategies

Emerging IT Security Technologies

Describe your organization's deployment plans for each of the following emerging IT security technologies / architectures.

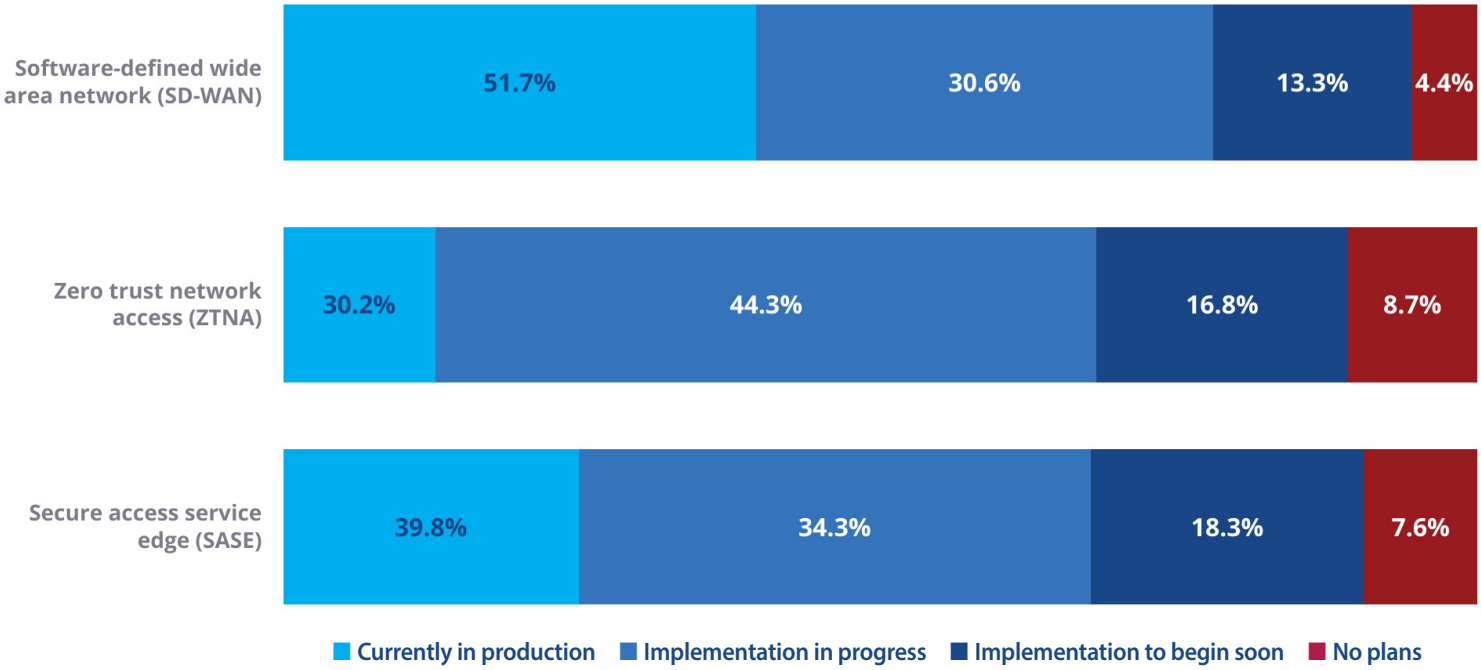


Figure 43: Plans for implementing emerging IT security technologies / architectures.

To wrap up this year's CDR findings, let's assess the extent to which IT organizations are embracing three emerging security technologies: SD-WAN, ZTNA, and SASE. For each technology, we asked our respondents whether it was already in production, if implementation was already in progress, if implementation was to begin soon, or if they had no plans at all for deployment.

Before we assess adoption rates, here's a quick primer on each of these three emerging security technologies:

- Software-defined networking (SD-WAN) is the next generation of WANs and an important step in the evolution of networking. Instead of using dozens or hundreds of individually configured routers over expensive MPLS

"If your organization hasn't already embraced any of these technologies, we hope this year's CDR will provide the evidence you need to influence change, so your organization doesn't end up at a competitive disadvantage."

Section 4: Practices and Strategies

circuits, SD-WAN simplifies network policy configuration and management while operating over broadband Internet connections, resulting in dramatically lower network costs.

- Zero trust network access (ZTNA) is a security framework that reduces network security risks by removing implicit trust and enforcing strict user and device authentication throughout the network. Unlike VPNs, which grant complete access to a LAN following user authentication, ZTNA denies access to all corporate resources with the exception of applications and systems to which the user has been explicitly granted access.
- Secure access service edge (SASE) is a cloud architecture that combines SD-WAN with key network security functions, such as firewall as a service (FWaaS), secure web gateways (SWG), cloud access security brokers (CASB), isolation, and DLP.

A common misconception is that organizations must choose between ZTNA and SASE approaches. This couldn't be further from the truth. Each solution solves different challenges. And most importantly, ZTNA is an important ingredient of a comprehensive SASE architecture.

So, with our primer complete, let's explore the results of the aforementioned survey question. And we'll do so in two ways. First, Figure 43 illustrates current adoption, with percentages that depict organizations that have already deployed each technology or are in the process of deploying it now. Here we see that 82.3% of organizations have already embraced SD-WAN, which makes sense since it's been around a few years longer. To a slightly lesser extent, 74.5% of responding organizations have implemented ZTNA and 74.1% have adopted SASE.

At the end of the day, all three of these emerging technologies play important roles in modern security architectures. If your organization hasn't already embraced any of these technologies, we hope this year's CDR will provide the evidence you need to influence change, so your organization doesn't end up at a competitive disadvantage.

The Impact of COVID-19 on the IT Security Industry

The COVID-19 pandemic and its shock to world economies have profoundly altered work environments and cybersecurity priorities. COVID-19 has prompted a massive work-from-home (WFH) movement, leading to the skyrocketing use of videoconferencing, collaboration tools, and cloud-based applications. Networks and remote access infrastructure have come under pressure. New threats targeting these technologies and pandemic-related anxieties have emerged. Meanwhile, many IT security teams are forced to do more with the same or fewer resources.

How has the COVID-19 pandemic specifically affected IT security organizations? How are they rethinking their priorities and investments? Well, thanks to research conducted by CyberEdge last year (and the generous support of our sponsors), we now have the answers.

In August 2020, CyberEdge surveyed 600 enterprise IT security professionals from seven countries and 19 industries. Our 20 survey questions were related to the following four topics:

- IT security budgets and personnel
- Work-from-home movement
- IT security challenges
- Technology investments

This culminating report is titled, "The Impact of COVID-19 on Enterprise IT Security Teams." It contains dozens of helpful insights. Here are our top five takeaways:

1. **The 2020 budget shocker.** Just when everyone thought that 2020 could finally be the year that IT security budgets stalled, we came along and are now dispelling that rumor. Our research indicates that the average enterprise IT security budget has received a 5% mid-year "boost" during the pandemic to fund additional remote access capacity, to secure personally owned devices accessing company applications and data, and to pretty much buy anything and everything that begins with the word "cloud."
2. **Remote workforce tidal wave.** Prior to the COVID-19 pandemic, about 24% of an enterprise's global workforce was working from home on a part-time or full-time basis. That number has risen to 50%, which equates to a 114% increase almost overnight. The implications of this so-called WFH movement are profound and, we believe, will influence the "new normal" for enterprises moving forward.
3. **Spike in BYOD adoption.** Before the pandemic, about 42% of enterprises employed bring-your-own-device (BYOD) policies that enable employees to use their home computers, smartphones, and tablets to access company applications and data. That number has spiked to 66%, equating to a 59% increase in a matter of months.
4. **Not enough aspirin for these headaches.** Every IT security team in every enterprise is feeling the effects of this global pandemic, including dealing with an increased volume of cyberthreats (37%), insufficient remote access and VPN capacity (35%), and increased risks stemming from unmanaged devices (35%). 73% of our respondents are also experiencing increases in third-party risks.
5. **A cloudy forecast.** Three out of four (75%) IT security professionals now prefer cloud-based security solutions to traditional on-premises security solutions–and with good reason. This makes perfect sense as the top-three IT security technology investments made specifically to address new challenges stemming from the COVID-19 pandemic begin with the "c-word."

To download the full report to review all of the research findings, click here: http://cyber-edge.com/2020-COVID-19-Impact-Report

The Road Ahead

COVID-19 Has Transformed the Workplace and Security Priorities

In most of our Cyberthreat Defense Reports, "The Road Ahead" section highlights the most critical emerging threats for the coming year–advanced malware, APTs, phishing, DDoS attacks, ransomware, etc.–and the latest security technologies being developed to meet them.

In 2021, however, we are obliged to take a different approach and focus on how the COVID-19 pandemic has created new security challenges by profoundly altering workplaces. The percentage of the global workforce working from home on a part-time or full-time basis has more than doubled, to roughly half of all workers. One direct effect has been a 59% surge in the number of enterprises implementing BYOD policies. Work from home and BYOD are likely to remain the new normal for most organizations.

This transformation of the workplace has had a profound effect on the goals of security teams. Many of them now must protect far more remote and mobile workers than in the past, as well as their devices and the data on them. For once, emerging threats have been overshadowed by the imperative to upgrade the security of remote and mobile workers (while maintaining application performance and controlling network and support costs).

Let's look first at how this new imperative is likely to play out for security organizations and security vendors in 2021.

Improving security and ease of use for remote workers: zero trust network access

Balancing security and ease of use for remote workers has always been a challenge for IT security organizations. But pre-COVID, the limited number of remote and mobile workers meant that getting the balance right was just not a top priority. Today, with half of employees working remotely at least part-time and BYOD part of the new normal, security organizations must focus on strengthening security for remote workers while making their lives easier (or at least not harder).

That's why this year we are looking for a big push toward implementing zero trust network access. Zero trust technologies aim at enforcing user and device authentication consistently across remote and headquarters-based workers, while tightly controlling access to applications and systems in data centers and cloud platforms on a "need to know" basis. Our survey data on page 53 shows very strong intent to implement and improve zero trust network access, and we expect this to continue to be a top priority for security organizations throughout 2021 and beyond.

Combining security and network management: SASE, SD-WANs, NPBs, and more

The surge in remote work also has profound implications for the interaction between security and networking. In the past, enterprises could afford to backhaul all network traffic to corporate data centers for inspection and cleaning by on-premises security tools. But with many more remote workers, far higher volumes of unpredictable network traffic, and more applications hosted in the cloud, that architecture becomes very problematic. When applications reside on cloud platforms:

- Backhauling large volumes of traffic via VPNs and MPLS circuits is expensive.
- Routing traffic through corporate data centers instead of directly to the cloud degrades application performance.
- It is much more difficult to take advantage of the new security tools designed to work on cloud platforms.

These factors are causing enterprises to examine how managing security and networks together can reduce costs, improve performance, and strengthen protection for remote workers. For example, SASE architectures, along with technologies such as SD-WANs, network packet brokers (NPBs), and secure web gateways (SWGs) facilitate secure, direct-to-web connections for remote workers and branch offices, thereby reducing backhauling over VPNs and MPLS connections. They support capabilities like routing high-priority applications over the

best-performing network links and providing automatic failover when a link goes down. They also allow to traffic to be sent directly to cloud-based security solutions that are integrated with cloud-hosted applications.

These architectures and technologies were being implemented before COVID, but we believe the pandemic has greatly accelerated their adoption.

Security applications delivered via the cloud

As we related on page 47, over the past year the percentage of information security applications and services delivered via the cloud leapt almost 5%, from 35.7% to 40.6%. This transition has been going on for years but was accelerated by the pandemic. The higher the percentage of remote workers in an organization, the greater the incentive to connect them directly to cloud-based security solutions rather than backhauling network traffic to data centers for inspection by on-premises security products. We think that security organizations, and IT security vendors, will maintain a rapid march toward cloud-based security in 2021 and beyond.

New Threats and New (and Improved) Technologies

Although the transformation of the workplace wrought by COVID-19 has had the biggest impact on IT security directions, we should still note the influence of emerging threats and the new and improved technologies being developed to meet them.

Unified monitoring across platforms featuring machine learning

We have discussed for many years the disappearance of the hard perimeter for keeping threats out of the enterprise. Over time, the emphasis of security teams has evolved toward monitoring networks and systems to quickly detect and stop malicious activity. Now that task has become more challenging because your computing environment may now be spread across on-premises data centers, SaaS applications, and cloud platforms such as Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform. Detecting malicious activity requires monitoring and correlating tens of thousands of security events on all those platforms.

How are security vendors responding? First, by creating new monitoring tools or extending existing ones to capture security events and data across on-premises, SaaS, and cloud platforms. Second, by embedding into their solutions improved ML tools that can sift through vast quantities of data to detect patterns correlated with attacks and emerging threats. The survey data on page 45 confirms the overwhelming preference of organizations for security products that feature ML or AI. We think this preference will continue to feed an ever-stronger trend toward greater use of ML and AI across more-comprehensive security data sets.

It *is* your problem: third-party risk management and brand protection

Traditionally, groups dedicated to third-party risk management (if they existed at all) operated separately from IT security, often in purchasing or in governance, risk, and compliance (GRC) departments. In a similar way, brand protection programs, assigned to scan social media and ecommerce sites for scams and negative references that could damage an enterprise's brand, often belonged solely to marketing.

But enterprises are worried that these siloed approaches increase risk. On page 13 you can see that of 11 security functions, respondents are least confident about the adequacy of their organization's third-party risk management (TPRM) capabilities. Brand protection is close behind as a major concern.

We believe forward-thinking executives will increasingly realize that IT security organizations should share responsibility for third-party risk management and brand protection. Security organizations at larger enterprises need to help their suppliers and other third parties find vulnerabilities and improve security processes. Likewise, the experience and skills of security groups are needed to help marketing groups detect brand-related scams, fraud, counterfeit goods, and misleading information on websites and social media platforms.

The Road Ahead

This trend will offer new job options for IT security team members, and will also create new opportunities for GRC, threat intelligence, and brand protection vendors to tailor their solutions for a more diverse customer base.

More innovative technologies

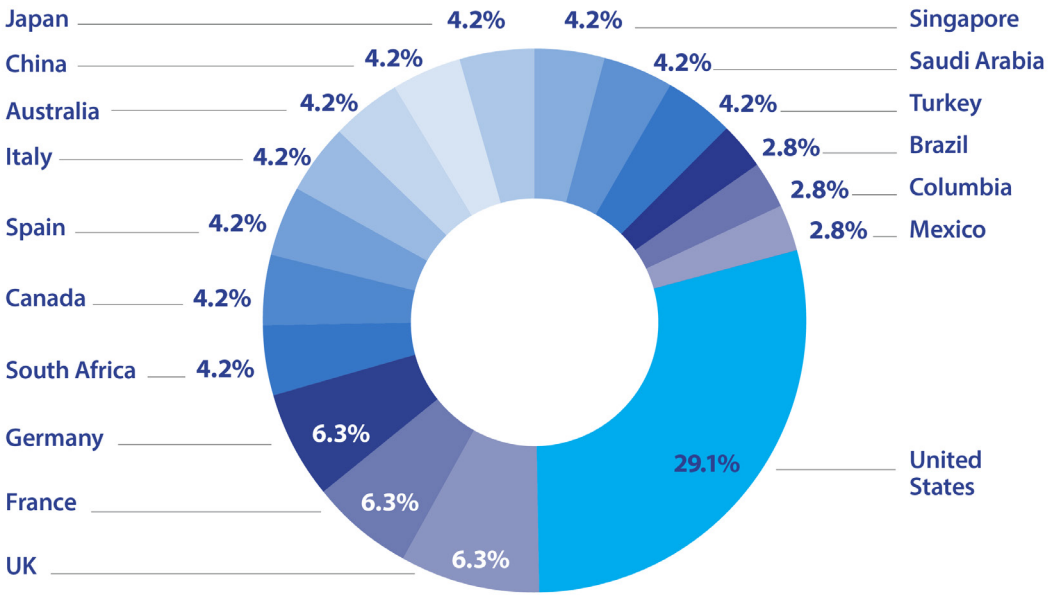
Here are some of the other innovative concepts and technologies we see becoming more prominent in 2021 and beyond:

- **Security automation, orchestration, and response (SOAR)** solutions will play an increasingly important role in managing and integrating security products on highly automated cloud platforms.
- **DevSecOps** concepts and products will help ensure that new applications are systematically tested for vulnerabilities and security policy violations.
- **Browser isolation technology** continues to improve and gain acceptance in large enterprise environments, and we see growing adoption ahead.
- **Continuous security validation** technology will help organizations confront evolving threats and changing attack surfaces. Instead of waiting for an attack to test security controls, this technology launches simulated attacks across an organization's networks and systems, validating that controls are performing as expected in production, and facilitating incident response exercises and purple teaming (a technique where red and blue teams work together to challenge and remediate defenses).
- **Threat intelligence platforms (TIPs) and services** enable organizations to identify and prioritize indicators of compromise (IoCs) and other clues about ongoing attacks faster and more accurately. We are seeing improvements in these solutions that will widen their applicability, such as the ability to correlate open-source threat data with events on an enterprise's network and to initiate automatic scans based on new threat data. Page 41 shows that 43.5% of organizations plan to implement a threat intelligence platform or service in 2021, the highest "planned for acquisition" rate of any single technology in our survey.

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 44) across six major regions (North America, Europe, Asia Pacific, Latin America, the Middle East, and Africa). Each participant has an IT security job role (see Figure 45). This year, 45% of our respondents held CIO, CISO, or other IT security executive positions.

Figure 44: Survey participation by country



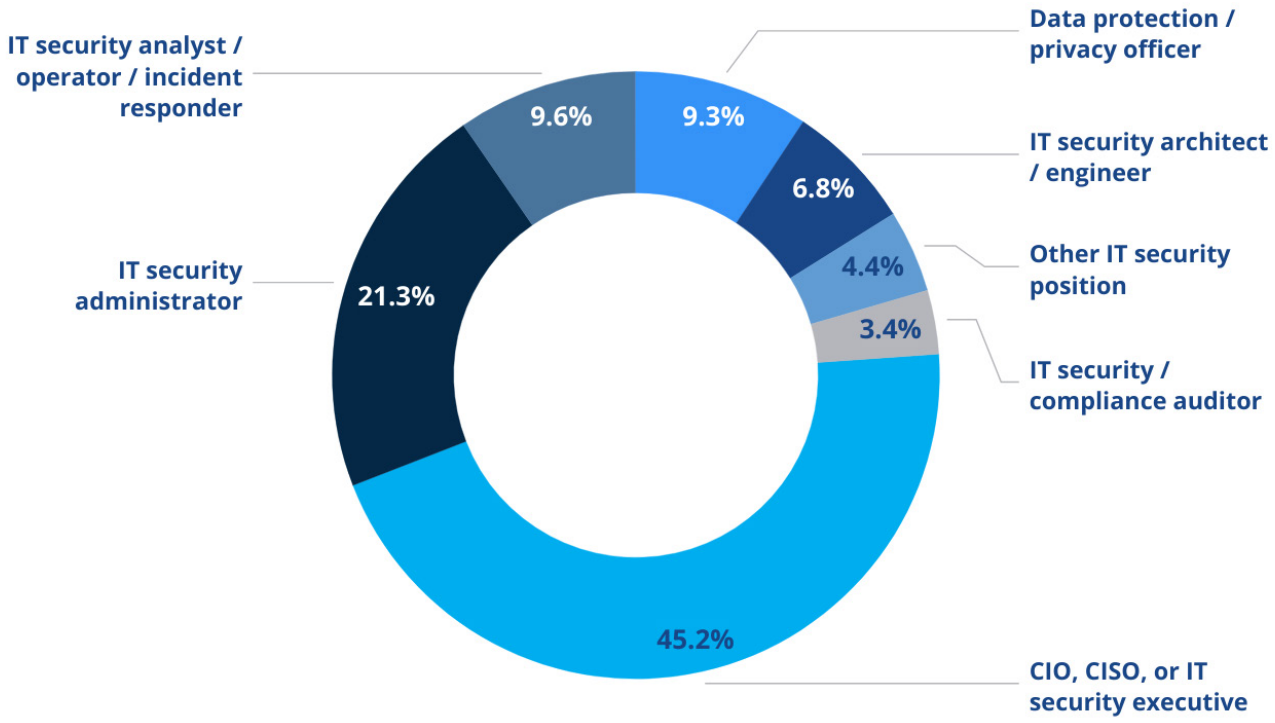


Figure 45: Survey participation by IT security role.

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 46). A total of 19 industries (plus "Other") are represented in this year's study (see Figure 47). The big 7 industries – education, finance, government, healthcare, manufacturing, retail, and telecom and technology – accounted for nearly two-thirds of all respondents. No single industry accounted for more than 15.3% of participants.

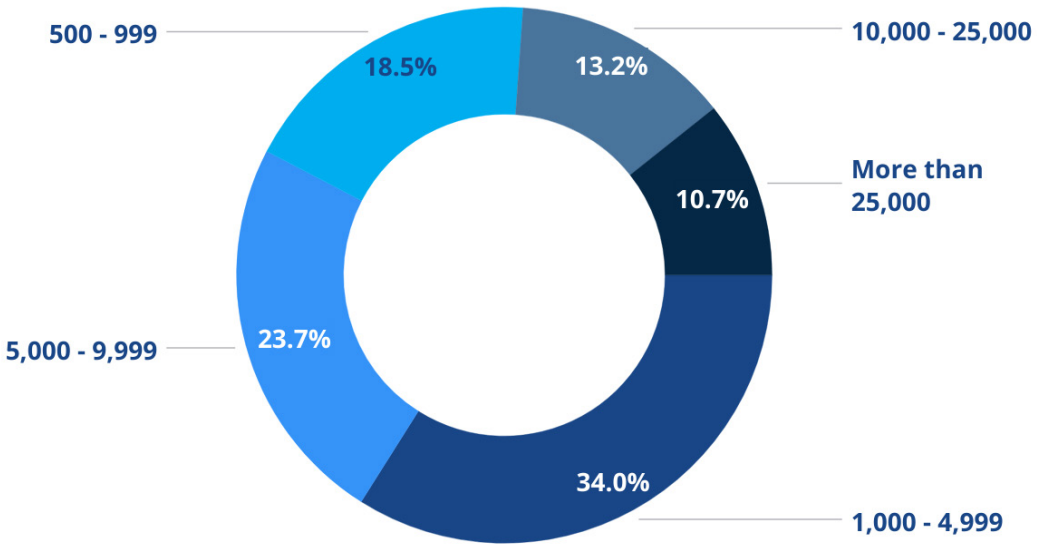


Figure 46: Survey participation by organization employee count.

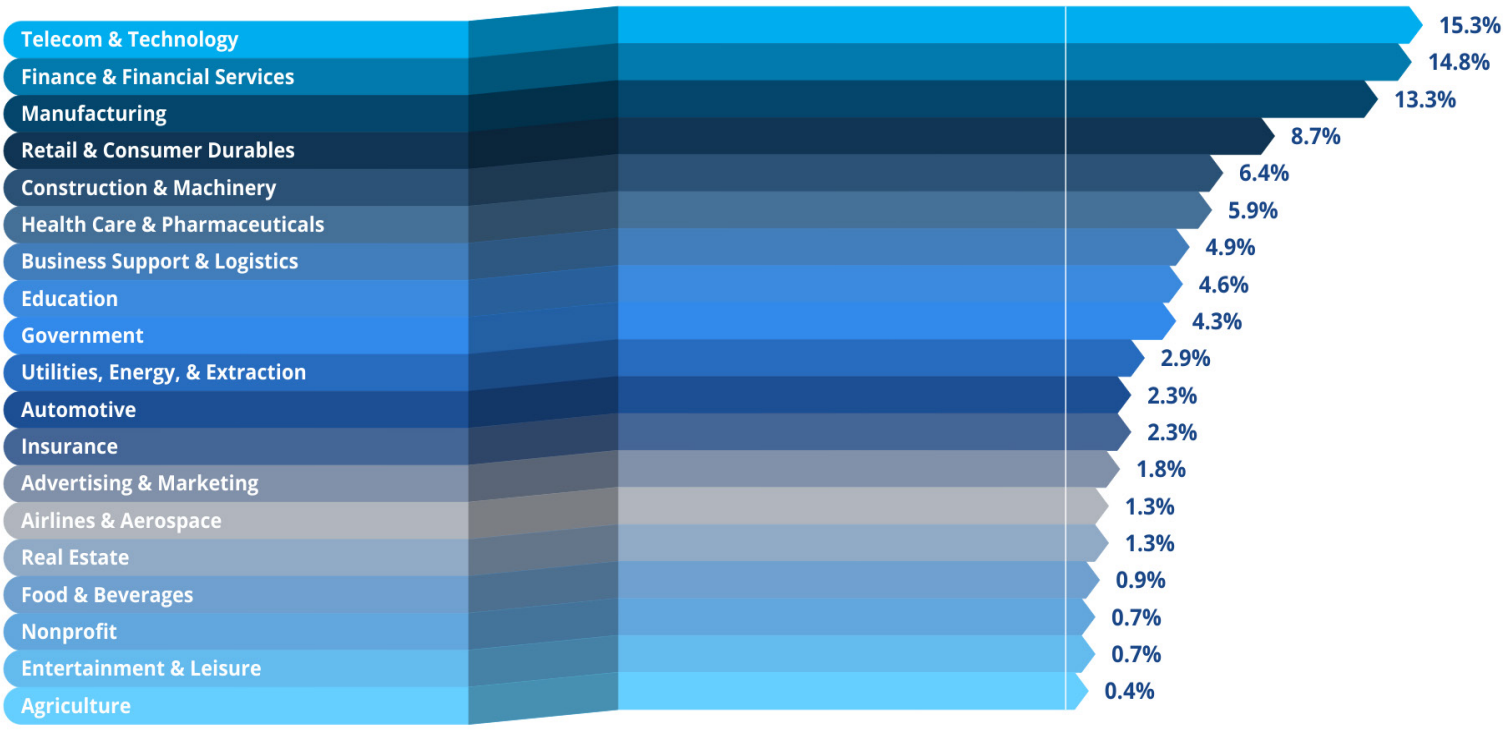


Figure 47: Survey participation by industry.

Appendix 2: Research Methodology

CyberEdge developed a 27-question, web-based, vendor-agnostic survey instrument in partnership with our research sponsors. The survey was promoted via email to 1,200 IT security professionals in 17 countries and 19 industries in November 2020. The global survey margin of error for this research study (at a standard 95% confidence level) is 3%. All results pertaining to individual countries and industries should be viewed as anecdotal as their sample sizes are much smaller. CyberEdge recommends making actionable decisions based on global data only.

All respondents had to meet two filter criteria: (1) they had to have an IT security role and (2) they had to be employed by a commercial or government organization with a minimum of 500 global employees.

At CyberEdge, survey data quality is paramount. CyberEdge goes to extraordinary lengths to ensure its survey data is of the highest caliber by following these industry best practices:

- Ensuring that the "right" people are being surveyed by (politely) exiting respondents from the survey who don't meet the respondent filter criteria of the survey (e.g., job role, job seniority, company size, industry)
- Ensuring that disqualified respondents (who do not meet respondent filter criteria) cannot restart the survey (from the same IP address) in an attempt to obtain the survey incentive
- Constructing survey questions in a way that eliminates survey bias and minimizes the potential for survey fatigue
- Only accepting completed surveys after the respondent has provided answers to all of the survey questions
- Ensuring that respondents view the survey in their native language (e.g., English, German, French, Spanish, Japanese, Chinese)
- Randomizing survey responses, when possible, to prevent order bias
- Adding "Don't know" (or comparable) responses, when possible, so respondents aren't forced to guess at questions they don't know the answer to
- Eliminating responses from "speeders" who complete the survey in a fraction of the median completion time
- Eliminating responses from "cheaters" who apply consistent patterns to their responses (e.g., A,A,A,A and A,B,C,D,A,B,C,D)
- Ensuring the online survey is fully tested and easy to use on computers, tablets, and smartphones

CyberEdge would like to thank our research sponsors for making this annual research study possible and for sharing their IT security knowledge and perspectives with us.

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, programmatic 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 public through our charitable foundation – The Center for Cyber Safety and Education™.

Gigamon | www.gigamon.com

Gigamon delivers the industry's first elastic visibility and analytics fabric addressing the critical visibility gap across your hybrid infrastructure. We close this gap by enabling cloud tools to see the network and network tools to see the cloud. With elastic scale-out and scale-up visibility and delivery of critical security and operational analytics across the hybrid cloud, Gigamon has helped thousands of the world's leading organizations run fast, stay secure and accelerate innovation while simplifying and securing IT operations.

Imperva | www.imperva.com

Imperva is the cybersecurity leader whose mission is to protect data and all paths to it. Customers globally trust Imperva to protect their applications, data, and websites from cyberattacks. An integrated approach combining edge, application, and data security protects all stages of the digital journey. Imperva technology delivers defense-in-depth to secure websites, mobile applications, and APIs from automated attacks, and threats outside the network core while providing comprehensive security to support the data lifecycle. Imperva Research Labs and our global intelligence community enable Imperva to remain ahead of the threat landscape by integrating security, privacy, and compliance expertise into solutions.

Menlo Security | www.menlosecurity.com

Menlo Security protects organizations from cyberattacks by eliminating the threat of malware from the web, documents, and email. Menlo Security's isolation-powered cloud security platform scales to provide comprehensive protection across enterprises of any size, without requiring endpoint software or impacting the end user-experience. Menlo Security is trusted by major global businesses, including Fortune 500 companies and eight of the ten largest global financial services institutions, and is backed by Vista Equity Partners, Neuberger Berman, General Catalyst, American Express Ventures, Ericsson Ventures, HSBC, and JP Morgan Chase. Menlo Security is headquartered in Mountain View, California.

PerimeterX | www.perimeterx.com

PerimeterX is the leading provider of solutions that protect modern web apps at scale. 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. PerimeterX is headquartered in San Mateo, California.

Appendix 3: Research Sponsors

Gold Sponsors

ConnectWise | www.connectwise.com

People depend on you to keep infrastructure running and critical assets secure, not only today but also for the future. However, the chaos of rapidly changing technology and evolving cyber threats can create frustrating obstacles. Whether solving for a specific technology challenge or complex requirements, ConnectWise, a community of peers, thought leaders, and experts are here to help. Your access to educational resources, conferences, in-depth training, and community-based events will deepen your knowledge and expertise. When combined with over 160 available product solutions designed to do more with less, you'll have everything you need to make sense out of chaos, improve client outcomes and position your business for ongoing success.

Herjavec Group | www.herjavecgroup.com

Robert Herjavec founded Herjavec Group in 2003 to provide cybersecurity products and services to enterprise organizations. We have been recognized as one of the world's most innovative cybersecurity operations leaders, and excel in complex, multi-technology environments. Our service expertise includes Advisory Services, Technology Architecture & Implementation, Identity Services, Managed Security Services, Threat Management, and Incident Response. Herjavec Group has offices and Security Operations Centers across the United States, United Kingdom, Canada and India.

KnowBe4 | www.knowbe4.com

KnowBe4, the provider of the world's largest security awareness training and simulated phishing platform, is used by more than 35,000 organizations around the globe. KnowBe4 helps organizations address the human element of security by raising awareness about ransomware, CEO fraud and other social engineering tactics through a new-school approach to awareness training on security. Organizations rely on KnowBe4 to mobilize their end users as the last line of defense, enabling them to make smarter security decisions, every day.

Micro Focus | www.microfocus.com

Micro Focus helps organizations run their business and transform it. Our software provides the critical tools they need to build, operate, secure, and analyze their enterprise. By design, these tools bridge the gap between existing and emerging technologies – enabling faster innovation, with less risk, in the race to digital transformation. More info: www.microfocus.com.

Thycotic | www.thycotic.com

Thycotic is a global leader in Privileged Access Management, a critical layer of IT security that protects an organization's data, devices and code across cloud, on-premise and hybrid environments. Recognized as a leader by every major industry analyst group, our modern cloud-ready PAM solutions dramatically reduce the complexity and cost of securing privileged access, providing more value and higher adoption than any alternative. Thycotic is trusted by over 12,500 leading organizations around the globe, including 25% of the Fortune 100.

Appendix 3: Research Sponsors

Silver Sponsors

AppGuard | www.appguard.us
AppGuard is a cyber security company on a mission to set a new standard: true cyber protection for all. AppGuard's patented technology prevents compromises before they happen by disrupting malware activity from causing harm without having to recognize it. Unlike detection-based solutions, AppGuard outsmarts malicious actors to ensure businesses can do what they need to do, and malware can't do what it wants to.

Binary Defense | www.binarydefense.com
Binary Defense is a managed security services provider and software developer with proprietary cybersecurity solutions that include SOC-as-a-Service, Managed Detection & Response, Security Information & Event Management, Counterintelligence and Threat Hunting. Many companies lack the time, budget and staff to properly focus on security. Binary Defense acts as an extension of clients' teams to help businesses optimize budget, reduce cyber risk and stay protected. Recognized as a "Leader" on The Forrester Wave™: Managed Detection and Response, Q1 2021 report, the Ohio-based organization earned high marks for threat hunting and threat intelligence.

Britive | www.britive.com
Britive is a cloud-native security solution built for the most demanding cloud-forward enterprises. The Britive platform empowers teams across cloud infrastructure, DevOps, and security functions with dynamic and intelligent privileged access administration solutions for multi-cloud environments. Britive helps organizations implement cloud security best practices like just-in-time (JIT) access and zero standing privileges (ZSP) to prevent security breaches and operational disruptions, while increasing efficiency and user productivity.

Cymulate | www.cymulate.com
For companies that want to assure their security against the evolving threat landscape, Cymulate SaaS-based Continuous Security Validation deploys within an hour, enabling them to challenge, assess and optimize their cyber-security posture simply and continuously end-to-end across the MITRE ATT&CK® framework. The platform provides out-of-the-box, customizable, expert and threat intelligence-led risk assessments that are simple to use for all skill levels and constantly updated. It also provides an open framework for ethical hackers to create and automate red and purple team exercises and security assurance programs tailored to their unique environment and security policies. Cymulate, for security professionals that want to know and control their dynamic environment.

EclecticIQ | www.eclecticiq.com
EclecticIQ is a global threat intelligence, hunting and response technology provider. Its clients are some of the most targeted organizations, globally. To build tomorrow's defenses today, they have to understand the threats against them – and align their efforts and investments to mitigate their risks. EclecticIQ helps governments, large enterprises and service providers manage threat intelligence, create situational awareness and adopt an intelligence-led cybersecurity approach. EclecticIQ extended its focus towards hunting and response with the acquisition of Polylogyx's endpoint technology in 2020. Founded in 2014, EclecticIQ operates globally with offices across Europe, North America, and via value-add partners.

Interos | www.interos.ai
Interos protects the world's largest enterprises, their reputation, and operations from supply chain attacks by nation states and criminal organizations; disruption from pandemics, tech, and trade wars; and compromise from unethical labor, financial distress, and sustainability challenges. The Interos business relationship graph contains millions of businesses, billions of relationships, and countless attributes. Using machine learning and natural language processing, we detect entities, infer relationships, monitor events, and assess risk – instantly and continuously.

Appendix 4: About CyberEdge Group

Founded in 2012, CyberEdge Group is the largest research, marketing, and publishing firm to serve the IT security vendor community. Today, approximately one in six IT security vendors (with $10 million or more in annual revenue) is a CyberEdge client.

CyberEdge's highly acclaimed Cyberthreat Defense Report (CDR) and other single- and multi-sponsor survey reports have garnered numerous awards and have been featured by both business and technology publications alike, including The Wall Street Journal, Forbes, Fortune, USA Today, NBC News, ABC News, SC Magazine, DarkReading, and CISO Magazine.

CyberEdge has cultivated its reputation for delivering the highest-quality survey reports, analyst reports, white papers, and custom books and eBooks in the IT security industry. Our highly experienced, award-winning consultants have in-depth subject matter expertise in dozens of IT security technologies, including:

- Advanced Threat Protection (ATP)
- Application Security
- Cloud Security
- Data Security
- Deception Technology
- DevSecOps
- DoS/DDoS Protection
- Endpoint Security (EDR and EPP)
- ICS/OT Security
- Identity and Access Management (IAM)
- Intrusion Prevention System (IPS)
- Managed Security Services Providers (MSSPs)
- Mobile Application Management (MAM)
- Mobile Device Management (MDM)
- Network Behavior Analysis (NBA)
- Network Detection and Response (NDR)
- Network Forensics
- Next-generation Firewall (NGFW)
- Patch Management
- Penetration Testing
- Privileged Account Management (PAM)
- Risk Management/Quantification
- Secure Access Service Edge (SASE)
- Secure Email Gateway (SEG)
- Secure Web Gateway (SWG)
- Security Analytics
- Security Configuration Management (SCM)
- Security Information and Event Management (SIEM)
- Security Orch., Automation, and Response (SOAR)
- Software-defined Wide Area Network (SD-WAN)
- SSL/TLS Inspection
- Supply Chain Risk Management
- Third-Party Risk Management (TPRM)
- Threat Intelligence Platforms (TIPS) and Services
- User and Entity Behavior Analytics (UEBA)
- Unified Threat Management (UTM)
- Virtualization Security
- Vulnerability Management (VM)
- Web Application Firewall (WAF)
- Zero Trust Network Access (ZTNA)

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**.