CYBEREDGE GROUP

2023 Cyberthreat Defense Report

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

<< Research Sponsors >>

PLATINUM

(ISC)² Arkose Labs FORTRA HUMAN imperva MENLO SECURITY

GOLD

Delinea LOOKINGGLASS netskope Netsurion SailPoint ZEROFOX

SILVER

hackerone netwrix OffSec Phosphorus PICUS valence

Table of Contents

Introduction

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

Now in its tenth year, the CDR has become a staple among IT security leaders and practitioners by helping them gauge their internal practices and security investments according to 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 2023

Our CDR reports yield dozens of actionable insights. Here are the top five takeaways from this year's installment:

1. **Pressure on IT security teams may be easing – finally.** The percentage of organizations compromised by at least one successful cyberattack peaked at 86.2% in our 2021 report. But after rising for years, it dipped slightly last year to 85.3%, and again in this report to 84.7% (see page 7). The percentage of organizations victimized by six or more successful attacks fell from 40.7% to 39.2% over the last year. Finally, the percentage of organizations expecting to be compromised in the coming year dropped a substantial 4.3% since our last report, from 76.1% to 71.8% (page 9). It is too early to be certain, but it seems like we may have turned a corner.

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**

2. **Our Threat Concern Index also fell.** We asked our respondents about their level of concern with 13 types of threats, from malware, phishing, and ransomware to advanced persistent threats (APTs), DDoS attacks, and supply chain threats. Compared to last year, their level of concern decreased in 12 of the 13 categories (all except supply chain threats). We averaged the ratings across all 13 threats into a "Threat Concern Index." The index fell from 3.88 in the last survey to 3.82 in this one (page 18). This implies that IT security professionals are starting to become more confident about their ability to defend against attacks.

3. **Double or more extortion ransomware is real, and very common.** Once "ransomware" was synonymous with encrypting files. Now it can involve one, two, or more threats on top of that, such as publicly releasing exfiltrated data and launching DDoS attacks to amplify pressure on the victims. In fact, it usually does. Only 21.6% of ransomware attacks last year involved encryption alone. A second threat is involved in 40.9% of attacks, while 30.4% include three threats, and 7.2% incorporate four (page 25).

4. **IT security leaders do have a seat at the table – with the board.** In organizations that have a board of directors, IT security leaders engage with them in some fashion 97.1% of the time. About half provide periodic cyber risk assessment reports, and almost as many present regularly at board meetings. More than a third share measurements of the maturity of their security programs (page 48).

Introduction

5. **Zero trust is cropping up everywhere.** Zero trust concepts are driving a lot of investment in technologies like multi-factor authentication (MFA), endpoint detection and response (EDR), privileged account management (PAM), and email and network encryption (page 44). Almost four out of five organizations say they are using or implementing zero trust network access (page 53). Zero trust frameworks are becoming core organizing models for many IT security programs.

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 hope to help IT security decision makers and practitioners gain a better understanding of how their perceptions, concerns, priorities, and defenses stack up against those of their peers around the world. IT security teams can use the data, analyses, and findings to shape answers to many important questions, such as:

- Where do we have gaps in our cyberthreat defenses relative to other organizations?
- Have we fallen behind in our defensive strategy to the point that our organization is now the "low-hanging fruit" (i.e., likely to be targeted more often due to its relative weaknesses)?
- Are we on track with both our approach and progress in continuing to address traditional areas of concern while 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 that should be added to supplement existing defenses

Introduction

Section 2: Perceptions and Concerns

In this section, our exploration of cyberthreat defenses shifts from establishing baseline security postures to determining the types of cyberthreats and obstacles to security that most concern today's organizations. The survey respondents weigh in on the most alarming cyberthreats, barriers to establishing effective defenses, and high-profile issues such as ransomware and security for hybrid cloud environments. 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, and security management and operations. 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 technologies they are using to support zero trust, how they are increasing security awareness among employees, and how IT security leaders are engaging with their board of directors. We also look at new technologies that organizations are using to defend against sophisticated threats and improve the performance of their security program.

Navigating This Report

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

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

Contact Us

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

Research Highlights

Current Security Posture

- **The cybersecurity battle may have reached a turning point.** The percentage of organizations compromised by successful attacks declined for the second year from 85.3% to 84.7% (page 7).
- **Optimism about the year ahead.** The percentage of security professionals who think a successful attack is likely or very likely fell 4.3%, to 71.8%, a big change from recent years (page 9).
- **ICS and IoT are concerns.** Among security domains, respondents are least confident about their ability to protect industrial control systems and IoT devices (page 11).
- **IAM is good, but attack surfaces are too large.** Organizations are relatively happy with their capabilities for identity and access management, but they are not making progress in attack surface reduction (page 13).
- **Security job openings are still hard to fill.** Demand for security talent vastly exceeds supply, and recent layoffs in high tech won't make much difference (page 15).

Perceptions and Concerns

- **Threat Concern Index declines.** IT security professionals are still concerned about a lot of threats…but less concerned than they were last year (page 17).
- **Web and mobile attacks.** Among web and mobile application threats, PII harvesting, account takeover, and payment fraud attacks continue to be most concerning (page 19).
- **Good and bad news on ransomware.** Successful attacks are up, ransom demands are bigger, but the percentage of organizations paying ransoms fell (page 21).
- **Double and triple extortion ransomware is now the norm.** More than three-quarters of ransomware attacks (78.4%) now include two or more threats (page 24).
- **Shortage of skilled personal handicaps security teams.** Lack of skilled personnel is the greatest barrier to IT security success, and low security awareness among employees is number two (page 26).
- **Gains from unified app and data security.** Improving cloud security posture and enhancing incident investigation are the biggest reasons to integrate application and data security on the same platform (page 28).
- **Hybrid cloud environments aren't easy.** Respondents list several challenges they face when transitioning applications to multiple cloud platforms (page 30).
- **Respect tops money as motivation for security certifications.** Why work on IT security certifications? Knowledge, credibility, and job satisfaction lead the list (page 32).

Current and Future Investments

- **Security spending is still strong.** A very solid 87.7% of respondents expect their IT security budget to increase this year, with average growth of 5.3% (page 34).
- **Network security workhorses.** Advanced threat protection, secure email gateways, and secure web gateways are the most frequently installed network security solutions (page 36).
- **New technologies for endpoint security.** Security teams are looking hard at deception technology and browser/internet isolation to add new capabilities to their endpoint defenses (page 38).
- **Hot topics for app and data security.** Most organizations have invested in API gateways and protection products, database firewalls, and web application firewalls (WAFs). Bot management is on the shopping list for this year (page 40).
- **Security management and operations covers a lot of ground.** We discuss the latest "in use" and "must have" tools for improving security programs (page 42).

Practices and Strategies

- **Technologies supporting zero trust.** MFA and EDR play the most significant roles in zero trust initiatives, but other technologies are almost as important (page 44).
- **How do you increase security awareness?** The vast majority of organizations are working to increase security awareness among employees, but methods differ (page 46).
- **IT meets the BOD.** IT security leaders are now engaging with their board of directors in a surprising number of ways (page 48).
- **Sophisticated defenses against sophisticated threats.** IT teams are depending on network behavior analysis, deception technology, and artificial intelligence (AI) to counter the most sophisticated attacks (page 50).
- **Use cases for XDR.** Extended detection and response solutions are helping organizations identify hidden cyberthreats, improve productivity, and accelerate incident response (page 52).
- **Way past hype.** Six relatively new technologies and architectures are in use or being implemented by at least 70% of organizations (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?

Has the cybersecurity battle reached a turning point? It's too early to say for sure, but after years of losing ground, this year's CDR provides evidence that IT security professionals are becoming more optimistic. Evidence of that hopeful trend starts with the first two questions of our survey, about successful cyberattacks in the past year and the likelihood of successful cyberattacks in 2023.

While one year does not a trend make, two years sometimes does. After a long upward movement, the percentage of organizations that were compromised by at least one successful cyberattack fell from 86.2% two surveys ago, to 85.3% in last year's survey, to 84.7% in this one. In addition, the portion of organizations reporting six or more successful attacks over the past 12 months fell for the first time in five years, from 40.7% in the last survey to 39.2% (see Figure 1).

Those findings shouldn't cause anyone to let down their guard. Both figures about successful attacks in the past year are the third highest in the history of our survey, exceeding the figures for all the years between 2014 and 2020. A large number of organizations are being compromised multiple times (see Figure 2). But as we will see later in this report, several indicators are pointing toward slightly more confidence that today's cybersecurity defenses can hold off the myriad cyberthreats facing today's commercial enterprises and government agencies.

What do we think has led to this more positive attitude? One factor is the relaxation of some of the challenges created (or at least heightened) by COVID-19. Relative to the peak times of the pandemic, people are spending fewer days working from home, where they are more vulnerable, and more working in offices, where data and applications are easier to protect. Similarly, workers are relying somewhat less on personally owned devices (BYOD) and more on company laptops and smartphones with more controls.

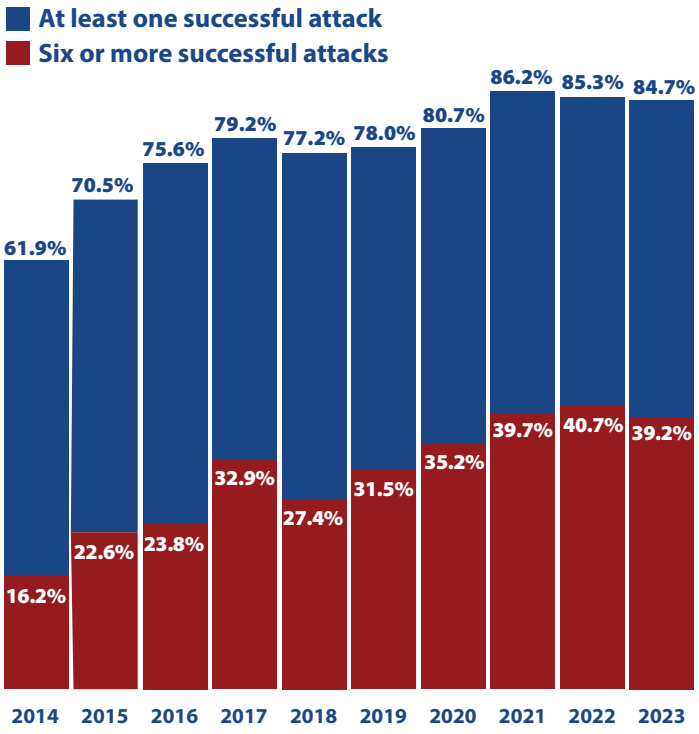

Figure 1: Percentages compromised by at least one successful attack and by six or more successful attacks.

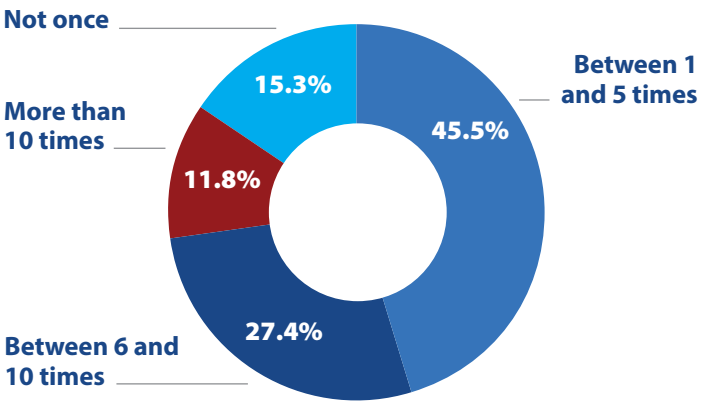

Figure 2: Frequency of successful cyberattacks in the last 12 months.

Section 1: Current Security Posture

But of even more importance for the long term, we think organizations are finally seeing returns on investments made during the pandemic. These include deploying technologies and practices such as machine learning, security analytics, network monitoring, deception, and zero trust network access. ROI also results from efforts to improve cybersecurity awareness among users and create closer working relationships between IT security teams and top executives and boards of directors. We will be discussing these factors throughout this report.

There are a few interesting variations in the rates of compromise reported. Of the seven major industries surveyed for this report, the most often victimized were finance (95.7%) and telecom & technology (88.9%). These were followed by retail (85.6%) and healthcare (79.2%). Things seemed to have improved in education, which declined from 90.5% in the last survey to 78.9% in this one. The major industries compromised the least were manufacturing (77.5%) and government (74.4%) (see Figure 3).

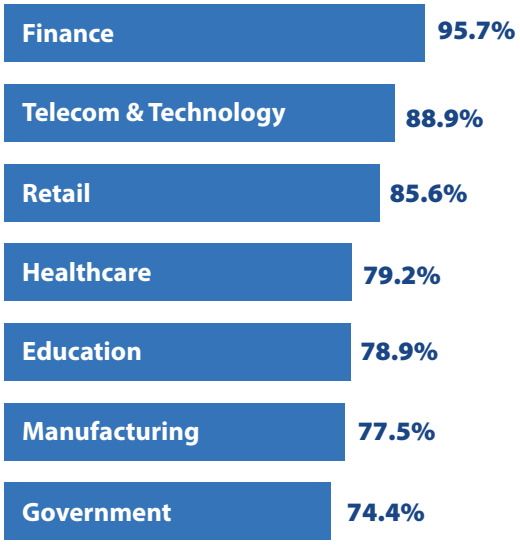

*Figure 3: Percentage compromised by **at least one** successful attack in the past 12 months, by industry.*

"...organizations are finally seeing the return on investments made during the pandemic. This includes…machine learning, security analytics, network monitoring, deception, and zero trust network access. It also results from efforts to improve cybersecurity awareness among users..."

Looking globally, there were three countries where more than half of the organizations reported six or more successful cyberattacks during the year: Mexico (56.3%), Australia (55.1%), and Germany (52.0%). In the United States, the number was just under half (48.6%). Which countries had the fewest organizations with six or more successful attacks? The answer: Japan (15.6%), France (16.5%), Colombia (20.0%), Italy (22.0%), Brazil (22.6%), and China (24.0%) (see Figure 4).

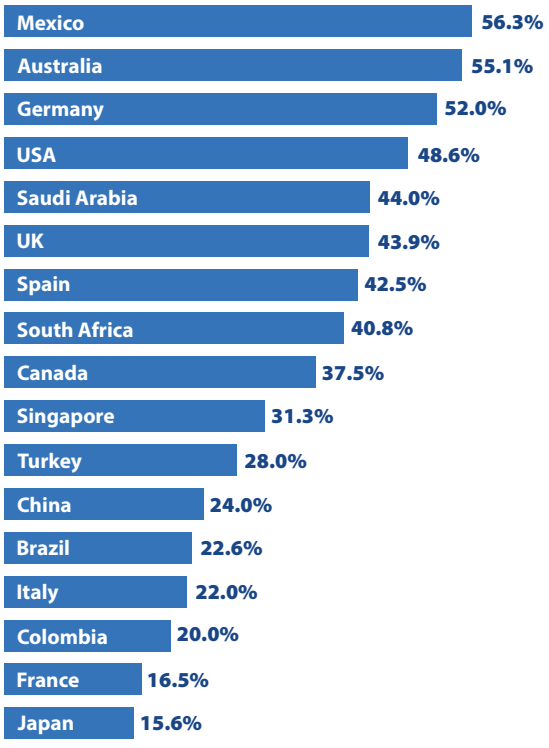

*Figure 4: Percentage compromised by **six or more** successful attacks*

Section 1: Current Security Posture

Future Likelihood of Successful Cyberattacks

What is the likelihood that your organization's network will become compromised by a successful cyberattack in 2023?

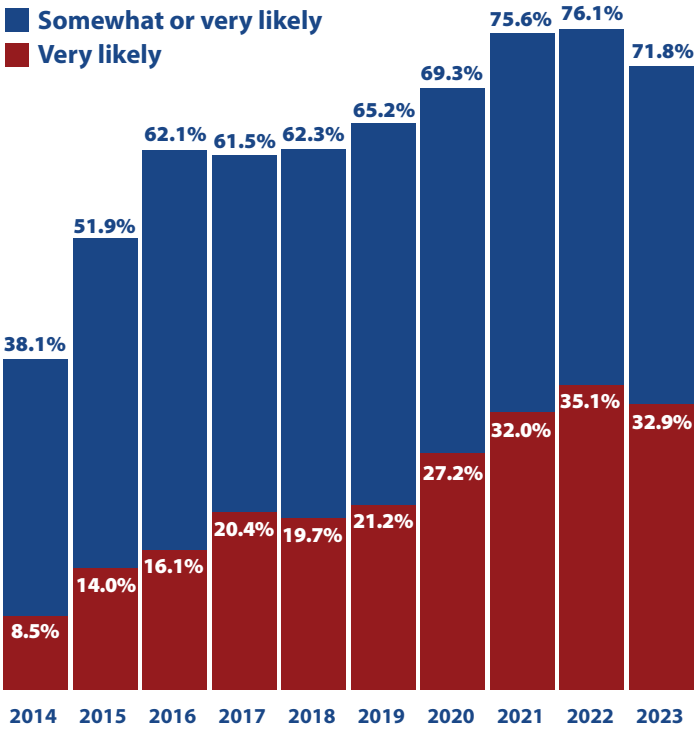

Figure 5: Percentage indicating compromise is "more likely to occur than not" in the next 12 months.

The idea that the cybersecurity battle has reached a turning point after so many years of bad news is supported by respondents' perspectives on the coming year. The portion saying it was somewhat or very likely that their organization would suffer a successful cyberattack in the year ahead grew steadily from 61.5% in 2017 to 76.1% in our 2022 survey. This year, however, that figure fell 4.3%, a significant drop, to 71.8%.

The same pattern is evident if you look only at the percentage who answered "very likely." That number rose continuously from 19.7% in 2018 to 35.1% four years later, but declined to 32.9% in this survey. This drop shows a definite gain in confidence.

As we mentioned in the previous section, we think the turnaround is due to a combination of factors, including fewer days of work at home, less use of unmanaged BYOD devices, the payoff from security investments made during the pandemic, and increased cybersecurity awareness among users.

An interesting dynamic we have noticed every year is the tendency for respondents to be optimistic that the coming year will be better than the past one. That trend carried over to this year, with 84.7% reporting that their organization had suffered at least one successful attack the previous year (see Figure 1), versus the 71.8% who think it somewhat or very likely that they will be compromised in the 2023. But perhaps there is more reason for optimism this year than in the past!

"The idea that the cybersecurity battle has reached a turning point after so many years of bad news is supported by respondents' perspectives on the coming year. The portion saying it was somewhat or very likely that their organization would suffer a successful cyberattack... fell 4.3% to 71.8%, a significant drop."

Section 1: Current Security Posture

The respondents predicting the highest rate of successful cyberattacks were in China (86.0%), Australia (82.0%), and Saudi Arabia (80.0%). In the middle of the pack: the United States (74.2%), Germany (73.3%), Canada (73.0%), Italy (72.4%), and the United Kingdom (72.2%). The optimists were in France (63.9%), South Africa (62.0%), Brazil (53.0%), and Turkey (at 46.0%, the country with the least worried survey participants for the second year in a row) (see Figure 6).

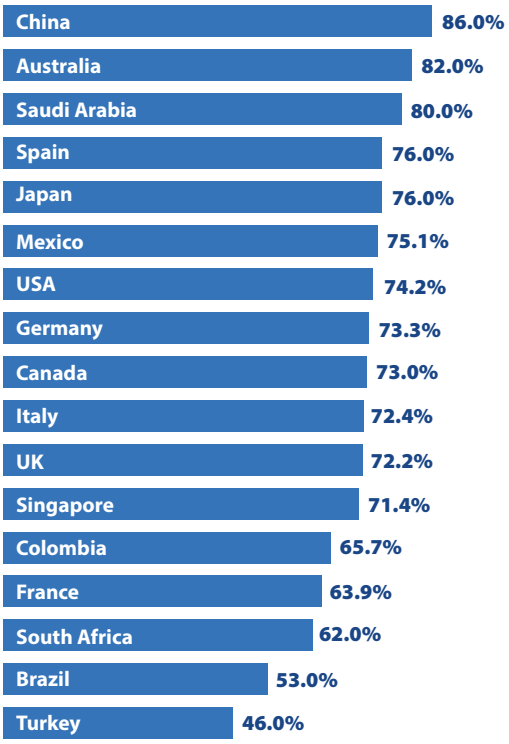

Figure 6: Percentage indicating compromise is "more likely to occur than not" in the next 12 months, by country.

By industry, respondents from finance are the most certain of successful attacks (84.5%), followed by those from retailers (75.6%), telecom & technology companies (73.8%), and educational institutions (70.2%). Only around two-thirds of participants from manufacturers (66.7%), healthcare organizations (65.7%), and government agencies (64.6%) are expecting to be compromised (see Figure 7).

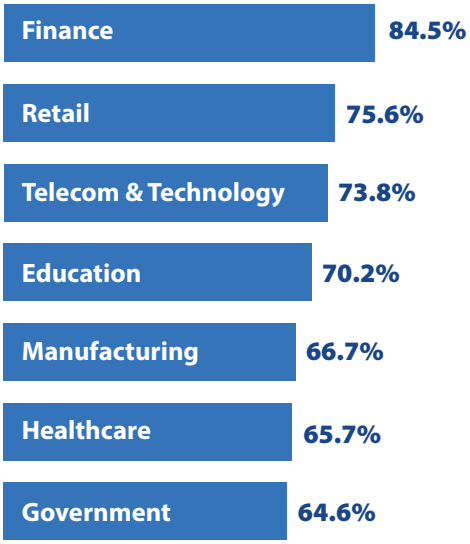

Figure 7: Percentage indicating compromise is "more likely to occur than not" in the next 12 months, by industry.

Section 1: Current Security Posture

Security Posture by IT Domain

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

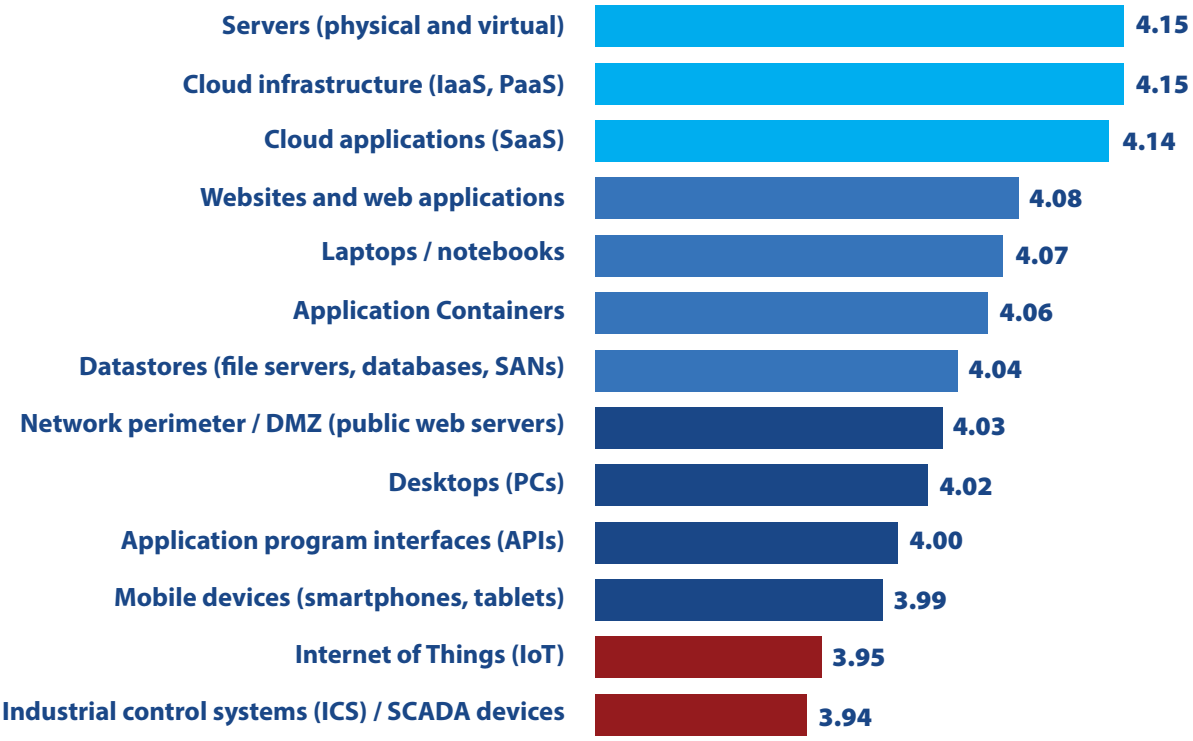

Figure 8: Perceived security posture by IT domain.

In every survey we ask security professionals to assess how well their organization is prepared to defend 13 different IT domains. This year, the story seems to be that the rich are getting richer and the poor are becoming poorer, or more accurately, that the safe are getting safer and the less secure are becoming even more worrying.

Examples of the safe getting safer? Security posture ratings rose for the top two domains in last year's survey. The score for physical and virtual servers increased from 4.12 to 4.15 (on a scale of 1 to 5, with 5 being the best overall security posture), and the score for SaaS cloud applications edged up from 4.13 to 4.14.

Section 1: Current Security Posture

But the biggest winner this year was cloud infrastructure, in the form of infrastructure as a service (IaaS) and platform as a service (PaaS) offerings. Last survey they were in the middle of the pack, in seventh place with a score of 4.08. This year they jumped into a tie for first place at 4.15. This represents a milestone for IaaS and PaaS vendors. Security professionals now are just as confident about the security of applications running on those cloud platforms as in the security of apps running on servers in corporate data centers and offices.

Examples of the less secure becoming even more worrying? The two IT domains at the bottom of our list are Internet of Things (IoT) and industrial control systems (ICS)/supervisory control and data acquisition (SCADA) devices. Ratings of the security posture of both of these areas fell a substantial .06 since last year, to 3.95 and 3.94, respectively.

IoT devices and industrial systems are becoming a focus of concern for several reasons:

- The astounding proliferation of internet-connected devices in offices, factories, homes, vehicles, cities, utilities, transportation networks, etc., etc.
- The emergence of new threats against these devices, such as the Mirai botnet and the Verkada hack, from military organizations and state-sponsored attackers as well as cybercriminals
- The success of supply chain-based attacks such as the SolarWinds hack that affect hundreds of organizations at one time

Clearly this is an area where IT security professionals feel at risk and are hoping for better solutions from the cybersecurity vendor community.

"This year, the story seems to be that the rich are getting richer and the poor are becoming poorer. Or more accurately, that the safe are getting safer and the less secure are becoming even more worrying."

Two other IT domains that make security professionals nervous: application programming interfaces (APIs) and mobile devices.

Organizations and software vendors are releasing more cloud applications made up of many modular services. These services depend on APIs to interact with hundreds of other services. Most organizations do not have a lot of experience creating and managing secure APIs. Threat actors have recognized that these APIs represent a large and growing attack surface. No wonder APIs are a growing area of concern!

Mobile devices continue to be a touchy area for IT organizations. Workers and customers want to use them for more and more business and personal transactions, yet these devices can't support the same security controls as conventional computers. In addition, threat actors have realized that by compromising mobile devices they can defeat some multifactor authentication (MFA) solutions and gain wide access to corporate networks and applications. We have seen a lot of progress in security tools to protect and monitor mobile devices, but IT security professionals are definitely not yet comfortable with what their organizations have in place.

Section 1: Current Security Posture

Assessing IT Security Functions

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

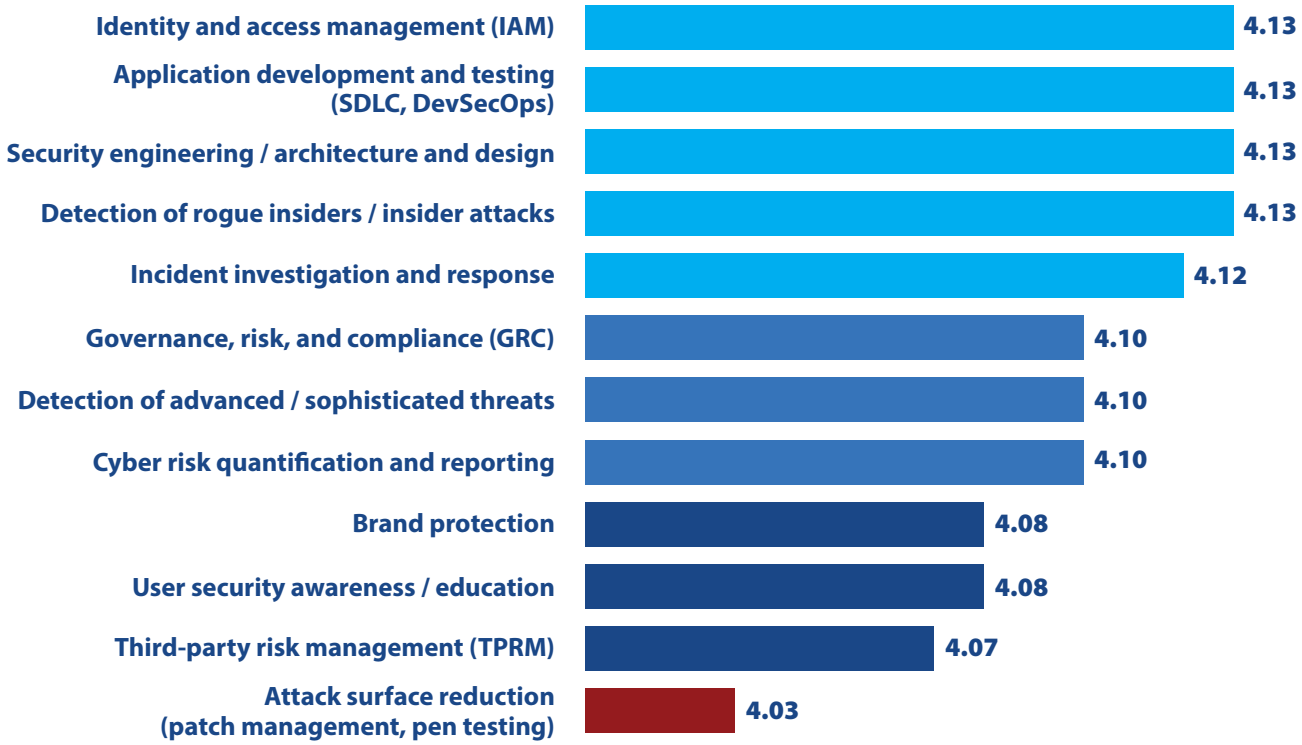

Figure 9: Perceived adequacy of functional security capabilities.

We turn our attention now to how our respondents rate the adequacy of their organization's capabilities across 12 IT security functions. Which ones do they think are strongest, and which ones might need some improvement?

The scores and the rankings of most of the functional areas were very similar to last year's results. However, a few did move up or down on the list.

For example, many organizations think they have gotten better at detecting shenanigans by insiders. Detection of rogue insiders/insider attacks moved up from ninth on the list in the last survey to fourth in this one (the score rose from 4.09 to 4.13 on a scale of 1 to 5, with 5 being most capable). We believe this is due to better monitoring of data and network activity (including the use of AI to detect unusual activity by employees and contractors) and more-effective application of least privilege and other zero trust principles.

Section 1: Current Security Posture

On the other hand, the assessment of governance, risk, and compliance moved in the other direction, dropping from a tie for first place in 2022 to a three-way tie for sixth place now (4.14 to 4.10). We suspect that the causes of this decline have less to do with any weakening of capabilities, and more to do with increasing demands for better governance and risk management.

Two other functional areas that dropped a bit over the year: detection of advanced/sophisticated threats (from third place to a tie for sixth) and brand protection (from a tie for sixth to ninth). Again, this is probably the result of new threats and rising expectations outpacing current capabilities.

The assessments of most of the other security functions remain broadly the same as last year. Organizations are most comfortable with their people and processes in the areas of identity and access management, application development and testing, security engineering, architecture and design, and the aforementioned detection of rogue insiders/insider attacks (all 4.13). Incident investigation and response is only slightly behind, at 4.12.

At the other end of the scale, respondents were least confident about their organization's capabilities for brand protection (4.08), user security awareness/education (also 4.08), third-party risk management (4.07), and attack surface reduction (4.03).

Is it surprising that attack surface reduction has been at the bottom of this list for two years running? Yes and no. It is surprising in that most of the activities that go into attack surface reduction, such as patch management, penetration testing, and network segmentations, have been around for a long time and don't involve any great leaps in technology or knowledge. However, it is less surprising when we think about how attack surfaces have expanded over the last few years with the increase in home and remote work, the movement of applications to dispersed cloud data centers, the explosion of IoT devices, and the integration of manufacturing and operational technology (OT) into IT networks, among other developments.

"As Wonderland's Queen of Hearts said to Alice: 'Now, here, you see, it takes all the running you can do, to keep in the same place. If you want to get somewhere else, you must run at least twice as fast as that!'"

Attack surface reduction is one of those areas where you work harder and harder, but the task keeps expanding to offset your improvements. As Wonderland's Queen of Hearts said to Alice: "Now, here, you see, it takes all the running you can do, to keep in the same place. If you want to get somewhere else, you must run at least twice as fast as that!"

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.)

A serious shortage of skilled IT security professionals has been a theme of our survey for quite a while. In fact, for the past seven years it has been the #1 or #2 factor inhibiting organizations from adequately defending themselves against cyberthreats (see page 26).

As this report was being written in early 2023, the news media was detailing massive layoffs in high tech. Industry leaders that have announced employee reductions of a thousand or more include Alphabet (Google's parent company), Amazon, Dell, IBM, Meta (the parent company of Facebook), Microsoft, PayPal, Salesforce, Twitter, and Zoom. So, will a flood of laid-off tech industry employees fill the gap in the market for IT security personnel? Almost certainly not.

First, while high tech companies are cutting staff in areas like marketing, sales, product management, and human resources, most are holding onto their security professionals. Well, with the exception of Twitter, which has jettisoned workers across the board. We'll see how that works out.

Second, security people moving from tech companies will hardly make a dent in the massive shortage of skilled professionals. According to the 2022 (ISC)² Cybersecurity Workforce Study, the global cybersecurity workforce gap is about 3.4 million, including 436,080 in North America, 515,879 in Latin America, 317,050 in Europe and the Middle East, and 2,163,468 in Asia. (Full disclosure: (ISC)² is a sponsor of this report).

With that out of the way, let's look at our data.

As in most recent years, the greatest shortage is IT security administrators. Just over 40% of our respondents reported that their organization is currently experiencing a shortfall in that area (see Figure 10).

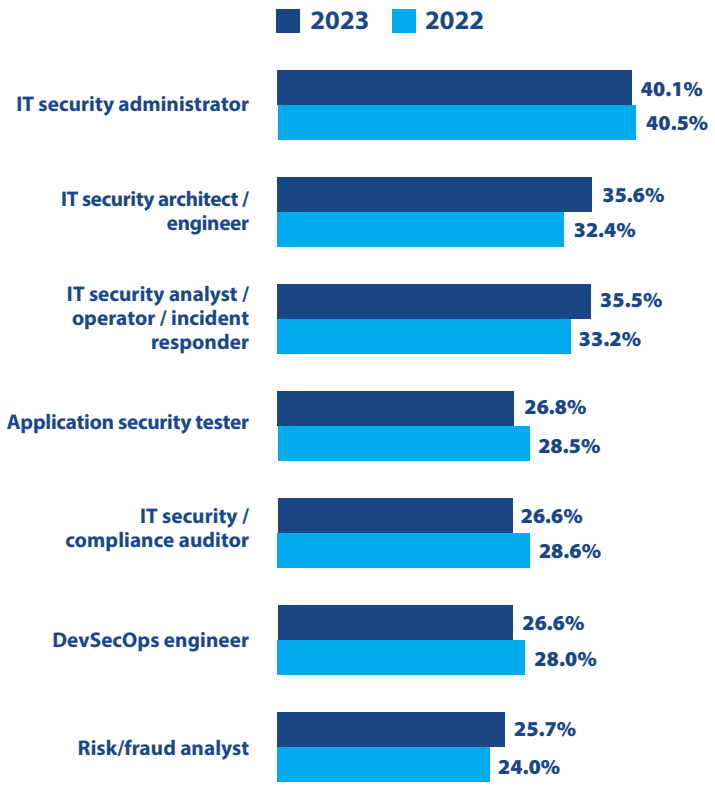

Figure 10: Cybersecurity skills shortage, by role.

Section 1: Current Security Posture

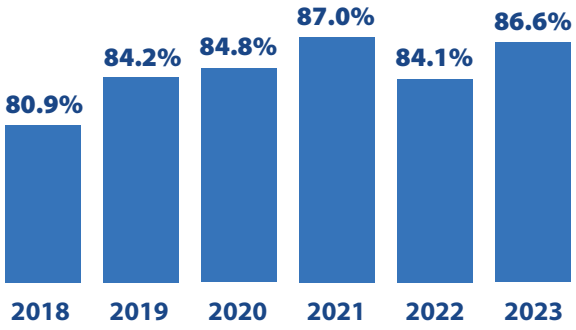

Figure 11: Percentage of organizations experiencing a shortfall of skilled IT security personnel in at least one role.

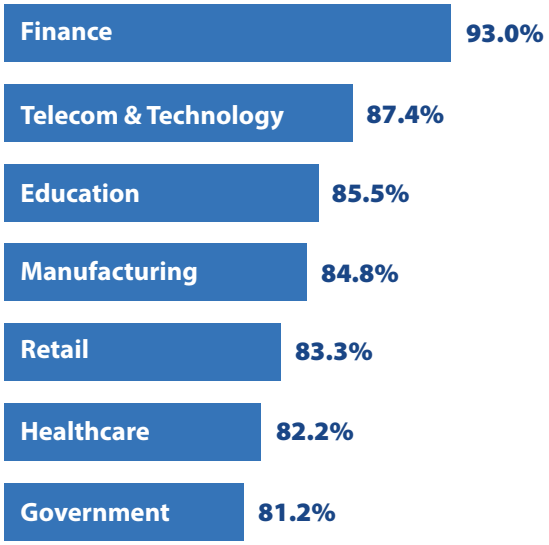

Figure 12: Cybersecurity skills shortage, by industry.

The second and third places are held by IT security architect/engineer (35.6%) and IT security analyst/operator/incident responder (35.5%).

Demand also greatly exceeds supply for application security testers (26.8%), IT security/compliance auditors (26.6%), DevSecOps engineers (also 26.8%), and risk/fraud analysts (25.7%).

The percentage of organizations experiencing a shortfall in at least one role was 86.6%, a tad higher than last year and the second highest in the history of our survey (see Figure 11).

By industry, shortages are most acute in finance (93.0%), followed by telecom & technology (87.4%) and education (85.5%) (see Figure 12).

"...will a flood of laid off tech industry employees fill the gap in the market for IT security personnel? Almost certainly not."

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.

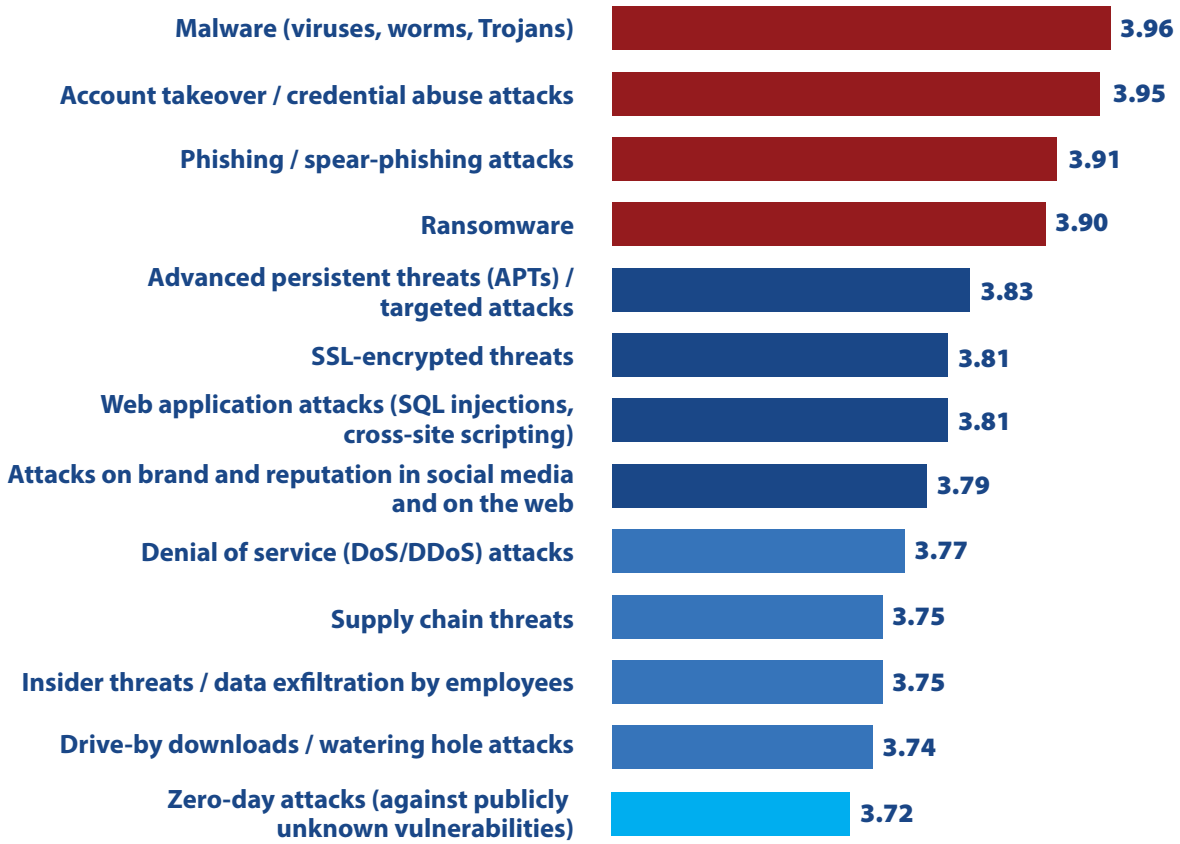

Figure 13: Relative concern for cyberthreats by type.

Here is additional evidence that IT security professionals are becoming more confident. Our respondents know they must remain vigilant about a wide range of cyberthreats. However, compared with last year, the level of their concern decreased in 12 of 13 cyberthreat categories. The only exception was supply chain threats, which was unchanged at 3.75 (on a scale of 1 to 5, with 5 being the highest level of concern).

In fact, the scores decreased between .05 and .10 for six types of cyberthreats: malware, ransomware, attacks on brand and reputation, DDoS, insider threats, drive-by downloads and watering-hole attacks, and zero-day attacks. While .05-.10 may not sound like much, for this type of survey it is a pretty significant change in one year, and we very rarely see multiple items in one question moving that much.

Section 2: Perceptions and Concerns

Each year we average these scores to create what we call our Threat Concern Index. As shown in Figure 14, this index fell from 3.88 in the last survey, a tie for the record, to 3.82 in this one. While that is not the largest change in the index ever, it is a notable one, especially since it breaks the rising trend of the past few years.

The two cyberthreats causing the greatest concern are the same as last year: malware (3.96, down from 4.01 in the previous survey) and account takeover/credential abuse attacks (3.95, down slightly from 3.97) (see Figure 13). Malware has been at the top of the list since 2016, no doubt because it is not only a threat in itself but also a common element of many types of attacks, including ransomware, APT, and zero-day attacks.

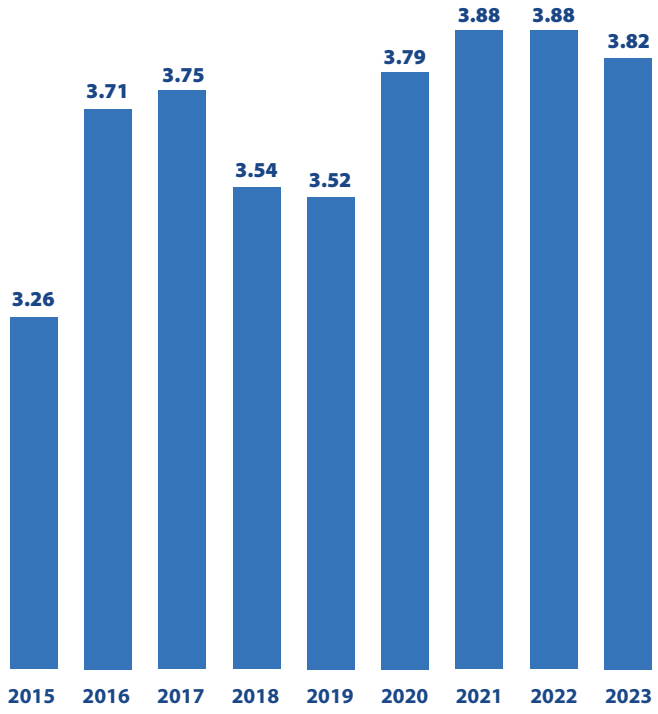

Figure 14: Threat Concern Index, depicting overall concern for cyberthreats.

Phishing and spear phishing attacks are now in third place (3.91, slightly down from 3.93). Humans remain the weakest link in IT security, and a lack of security awareness among employees remains a pressing concern, as we discuss on page 26.

Ransomware slipped from third place last year to (just) behind phishing (3.90, down from 3.96). With all the attention given to ransomware recently, it might seem surprising that it dropped a notch. Perhaps security teams are slightly more confident because of the investments they have been making in detecting ransomware and in backing up data. Or perhaps they are heartened by governments and law enforcement agencies starting to take more-aggressive actions to rein in ransomware gangs.

At the other end of the spectrum, our respondents are least concerned about drive-by downloads/watering hole attacks (3.74) and zero-day attacks (3.72). As a matter of fact, since the last survey, the score for zero-day attacks decreased by .10, the largest drop of any of the cyberthreats mentioned in this question. We think this is the result of improvements in security tools that monitor activities on networks and endpoints, and use machine learning and AI to identify malicious actions early enough so that security teams can respond to and contain exploitation.

"Here is additional evidence that IT security professionals are becoming more confident... Compared with last year, the level of their concern decreased in 12 of 13 cyberthreat categories."

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.)

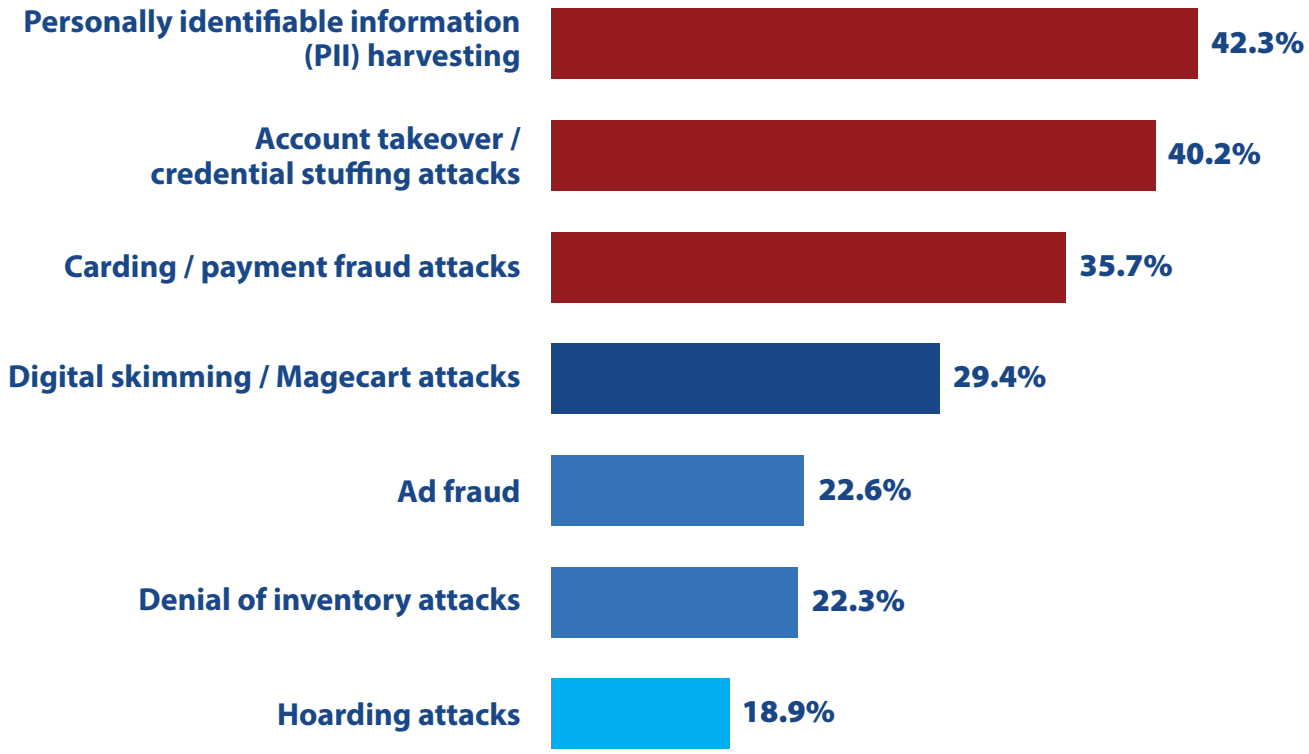

Figure 15: Most-concerning web and mobile application attacks.

Web and mobile attacks are a significant threat to ecommerce companies, financial institutions, and basically any organization that advertises or sells products on the web or through mobile apps. In addition, because an unfortunate number of people reuse the same passwords across personal and work accounts, some of these attacks can also be used to acquire credentials from just about any commercial or government organization.

Starting with last year's survey, we have asked our respondents to select the three types of web and mobile attacks that most concern them. The rankings were unchanged from last year. The top two, by a significant margin, are the harvesting (i.e., stealing) of personally identifiable information (PII), cited by 42.3% of our respondents, and account takeover (ATO) and credential stuffing attacks, selected by 40.2% (see Figure 15).

Not surprisingly, carding and payment fraud attacks are also up there, named by more than a third of the IT security professionals (35.7%). The selection rate was even higher for participants from companies in finance, retail, and entertainment and leisure.

Section 2: Perceptions and Concerns

Denial of inventory and hoarding attacks were issues for 22.3% and 18.9% of organizations, respectively. These are essentially application-level DDoS attacks. Typically, an attacker programs bots to go to an ecommerce site and put a large quantity of in-demand items into shopping carts, or to go to a travel site and temporarily lock up "inventories" of airline seats or hotel rooms. This tactic denies the items or inventory to legitimate buyers, preventing sales and harming the reputation of the merchants. The techniques has also been known to be used by scalpers who have previously secured quantities of the items and want to drive up the price.

We added one new category to this year's survey: ad fraud. This typically involves cybercriminals setting up websites, arranging to have advertising networks display ads on these sites, manufacturing a blizzard of clicks on the ads, then collecting per-click fees from the advertising network. The clicks can come from botnets, people in offshore "click farms," or techniques such as "click hijacking" (redirecting a click from a real person on a real ad to one of the ads on the cybercriminal's website). Ad fraud turns out to be a major concern for a non-trivial 22.6% of the organizations in our survey.

Responses also showed the pervasiveness of web and mobile attacks. A full 91.5% of organizations are affected by at least one of them (see Figure 16).

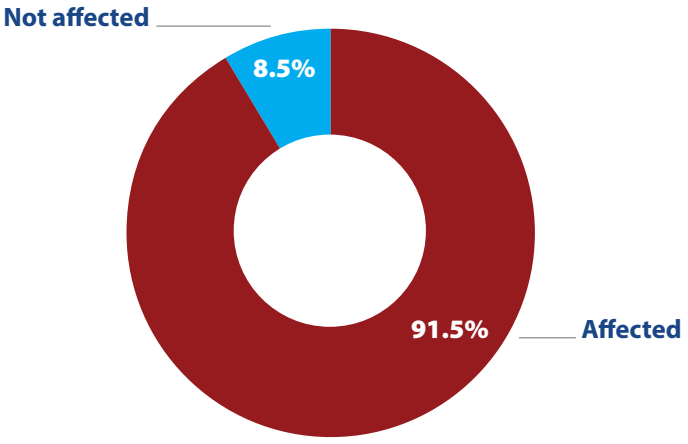

Figure 16: Organizations affected by a web or mobile application attack.

As you might expect, these attacks affected almost every company in finance (97.2%) and retail (94.1%) (see Figure 17). Organizations in education and manufacturing were affected less often – but not that much less often (91.1% and 86.0%, respectively).

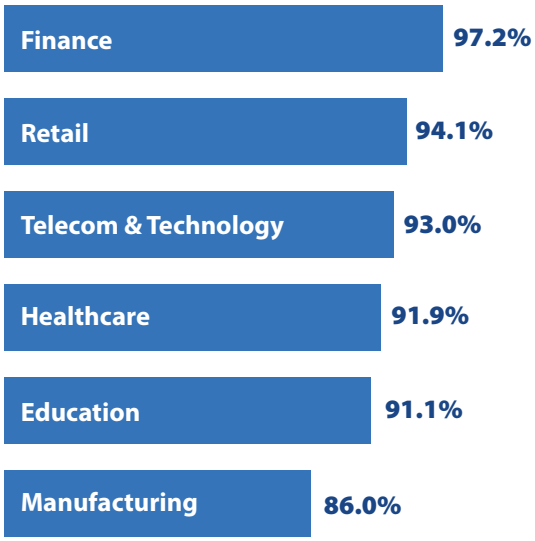

Figure 17: Organizations affected by a web or mobile application attack, by industry.

"Responses showed the pervasiveness of web and mobile attacks. A full 91.5% of organizations are affected by at least one of them."

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?

It's been another very busy year in the world of ransomware. In many respects, negative trends have continued to play out. However, the percentage of organizations that paid ransoms actually declined, and there are other signs that the dynamics of the ransomware "market" might be changing. Let's look at the details.

The percentage of organizations affected by ransomware increased yet again, from 71.0% in the last survey to 72.7% in this one, reaching a new high (see Figure 18).

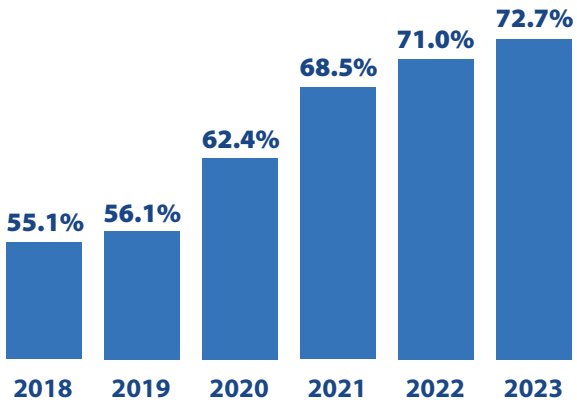

Figure 18: Percentage of organizations victimized by ransomware.

We see several factors driving the continuing spread of ransomware in recent years, most importantly:

- Increased targeting of certain industries, such as healthcare and education. Ransomware gangs continue to refine their methods for terrorizing these organizations, such as encrypting patient records (interfering with life-and-death medical procedures) and student records (creating havoc for both enrollment and graduation).
- New targets and new methods, such as attacking supply chain participants (e.g., Kaseya and EMC) to compromise many downstream customers with one exploit, and developing ransomware attacks against OT and IoT devices.
- Perfecting double and triple extortion ransomware attacks (which we discuss at length in conjunction with the next question).
- Continuing increases in average ransomware payments (see data from Coveware in Figure 19), which provide incentives for more ransomware activity.

But one very important pattern may be reversing. The percentage of organizations that experienced a ransomware attack and paid the ransom declined 3.2%, from 62.9% to 59.7% (see Figure 20). Before this year, the percentage grew steadily from 38.7% in 2018 to 62.9% last year, with only one small (0.7%) annual decrease in that period.

What might have caused this reversal? Here are some of the possibilities:

- Organizations investing more in backup and recovery processes, giving them confidence that they could recover data from saved copies.
- The emergence of decryption and data recovery service providers and the development of ransomware-specific decryption tools that enable victims to decrypt data without paying a ransom. One recent example is the release by the U.S. Federal government's Cybersecurity and Infrastructure Security Agency (CISA) of a ransomware recovery script that counteracts the ESXiArgs ransomware.
- Some cyber insurance providers tightening their policies and the terms under which they will reimburse organizations for ransomware payments.
- Laws and regulations prohibiting ransom payments under certain circumstances.

Section 2: Perceptions and Concerns

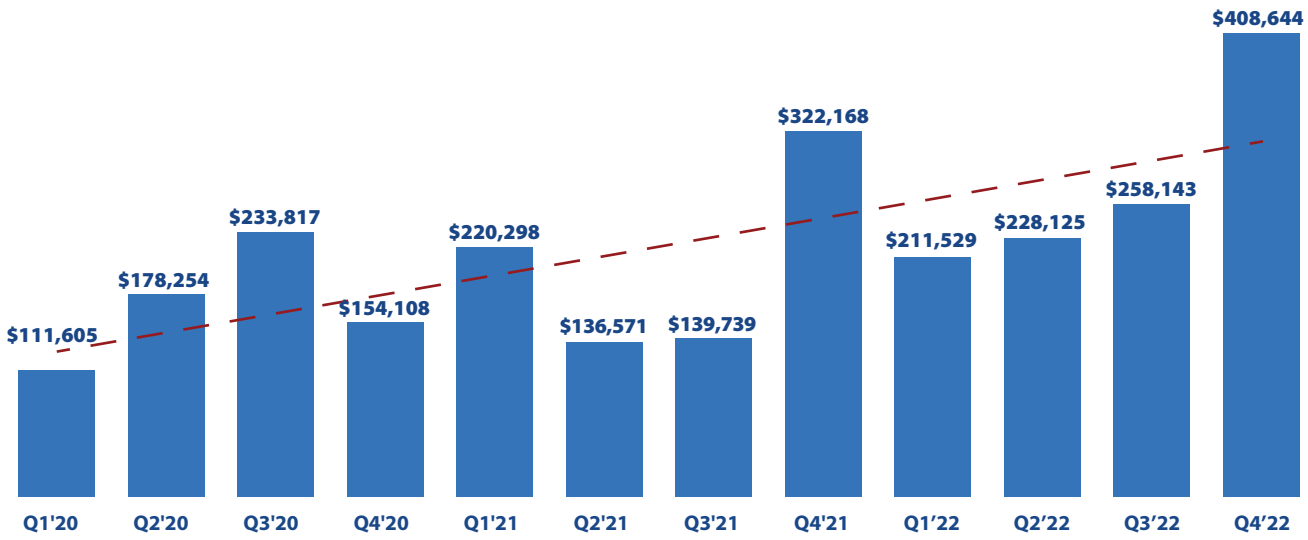

Figure 19: Average ransom payments, by quarter (data source: Coveware Quarterly Ransomware Reports).

Legal and regulatory issues are becoming especially important for some organizations. Law enforcement agencies have been discouraging ransomware payments for some time, on the grounds that they fund criminal activity and encourage more attacks. Now they are going even farther.

For example, an advisory from the U.S. Treasury Department's Office of Foreign Assets Control (OFAC), issued in 2020 and updated in 2021, warns that an organization that pays ransom to an entity that has been sanctioned by OFAC for criminal or terrorist activities "may be held civilly liable even if it did not know or have reason to know it was engaging in a transaction with a person that is prohibited under sanctions laws and regulations administered by OFAC." The same applies to "Companies that facilitate ransomware payments to cyber actors on behalf of victims, including *financial institutions, cyber insurance firms, and companies involved in digital forensics and incident response* [emphasis added]."

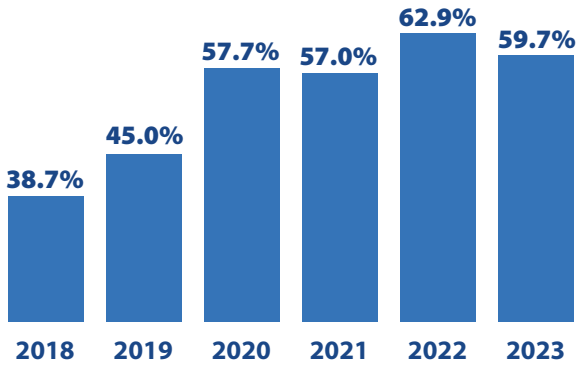

Figure 20: Percentage of victimized organizations paying ransoms.

Meanwhile, authorities in the European Union and United Kingdom have made forceful statements against paying ransoms, and the EU Networks & Information Systems Directive (NIS Directive) gives EU members the right to impose fines on ransom payers.

Are these statements just a bluff from anxious bureaucrats? We are not aware of any case being brought against ransomware payers, but there certainly have been cases involving companies paying conventional ransoms to sanctioned terrorist organizations.

In short, while companies victimized by ransomware continue to face very unpleasant decisions about whether to pay or not pay, the pressures against paying have become stronger and may be reversing the trend to give in.

Section 2: Perceptions and Concerns

Back to our data.

The percentage of organizations that elected to pay ransoms and did recover their data rose slightly from 72.2% to 72.7% (see Figure 21). The high percentage reflects the incentive for ransomware gangs to deliver on their promises to encourage future victims to pay up.

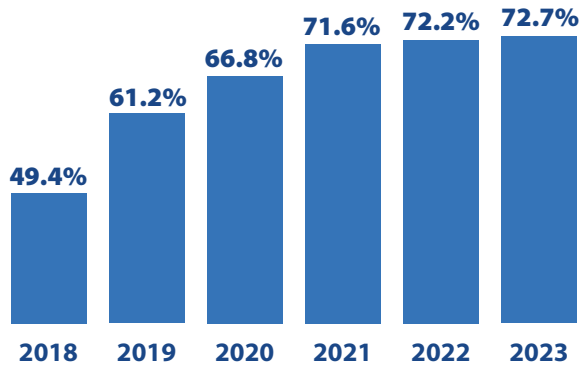

Figure 21: Percentage of ransom payers that recovered data.

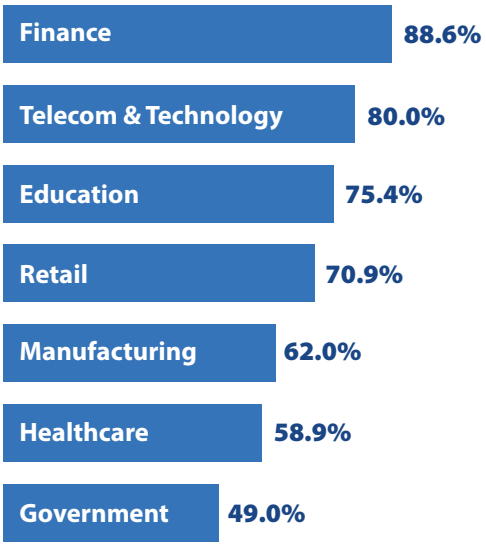

Figure 22: Percentage of organizations victimized by ransomware in the last 12 months, by industry.

Among major industries, the ranking was exactly the same as last year (see Figure 22). The most frequently victimized were finance, telecom & technology, and education (88.6%, 80.0%, and 75.4%, respectively). The least affected were healthcare (58.9%) and government (49.0%).

As shown in Figure 23, the countries experiencing the most ransomware attacks were Germany (81.1%), Saudi Arabia (80.0%), China (also 80.0%), Spain (79.2%), and the United States (75.6%). Brazil (64.7%), France (63.5%), Canada (62.5%), and Japan (53.1%) were the most fortunate.

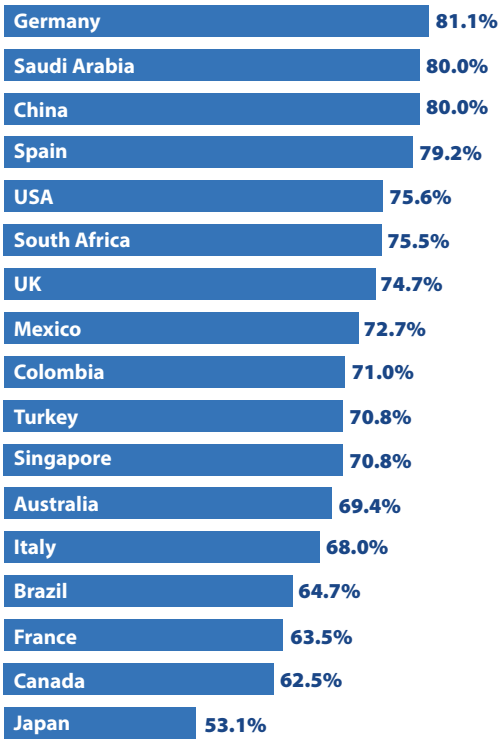

Figure 23: Percentage of organizations victimized by ransomware in the last 12 months, by country.

Section 2: Perceptions and Concerns

Double or More Extortion Ransomware

If victimized by ransomware in the past 12 months, which of the following threats did the attacker make in addition to encrypting your data and/or systems if your organization failed to pay the ransom?

One of the most important developments in ransomware is the widespread adoption of double, triple, and even quadruple extortion varieties.

Until recently, ransomware was defined as malware that encrypted files on a computer and displayed a message demanding a payment in return for a key to decrypt the files. Now that definition is almost quaint. While there are still a significant number of "ransomware classic" attacks, there are many more that involve one, two, or even three threats on top of losing your data. Most of these involve exfiltrating copies of files to a server controlled by the attacker before the original files are encrypted on the target computers (see Figure 24 for an example of a "triple extortion" ransom demand).

How many attacks involve more than one threat, and what threats are most common? That's exactly what we wanted to know. So we asked respondents whose organization had been victimized by ransomware whether the attack included any of three additional threats:

- To release exfiltrated data (allowing it to fall into the hands of cybercriminals and others)
- To notify customers and the media of the breach (potentially undermining trust in the organization)
- To commit a DDoS attack against the organization (applying additional pressure to pay the ransom quickly rather than dragging out negotiations)

The results are shown in Figure 25. About two out of five ransomware attacks (39.8%) included a threat to release data publicly. Slightly more included threats to notify customers or the media of the data breach (41.5%) or apply pressure through a DDoS attack (41.9%).

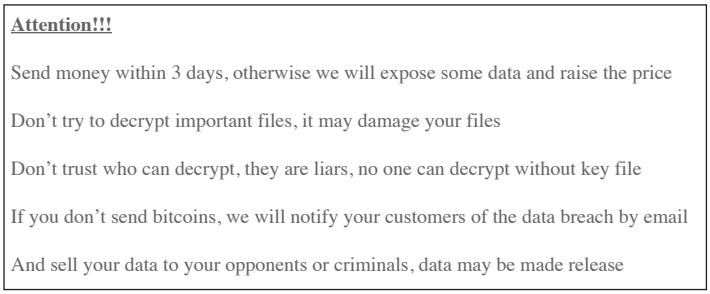

Figure 24: Excerpt from a triple extortion ransomware attack threatening encryption, customer notification, and release of data.

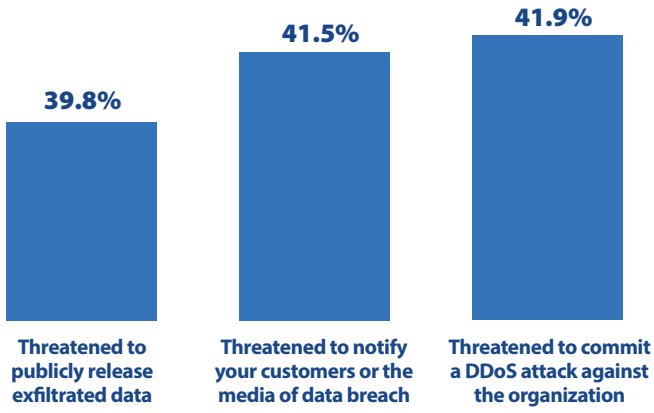

Figure 25: Threats made in ransomware attacks in addition to losing encrypted data.

"While there are still a significant number of 'ransomware classic' attacks, there are many more that involve one, two, or even three threats on top of losing your data."

Section 2: Perceptions and Concerns

Inquiring minds also want to know how many attacks are still the plain vanilla, you-will-lose-your-data variety, and how many qualify as double extortion, triple extortion, and even quadruple extortion attacks.

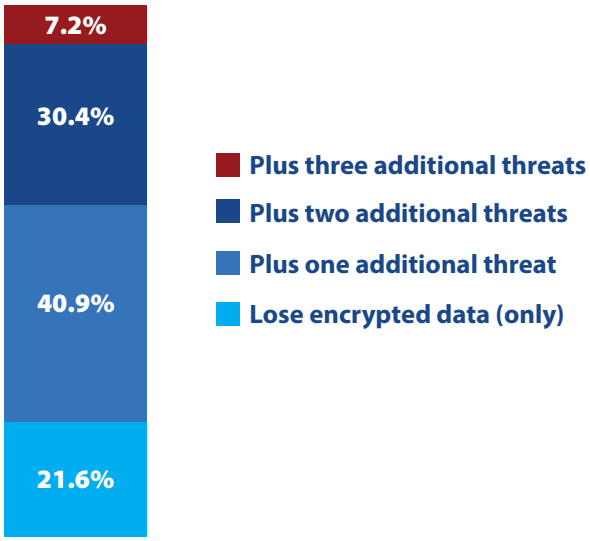

Figure 26: Number of threats made as part of a ransomware attack.

You can see the answers in Figure 26. Only 21.6% of the reported attacks were ransomware classic threats of losing encrypted data. The sweet spots for ransomware gangs were clearly one additional threat (40.9%) or two additional threats (30.4%). Three additional threats on top of encryption were relatively rare: only 7.2%. Which is good, because "quadruple extortion ransomware" sounds more like a difficult figure skating jump than a cyber menace.

"Three additional threats on top of encryption were relatively rare: only 7.2%. Which is good, because 'quadruple extortion ransomware' sounds more like a difficult figure skating jump than a cyber menace."

Section 2: Perceptions and Concerns

Barriers to Establishing Effective Defenses

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

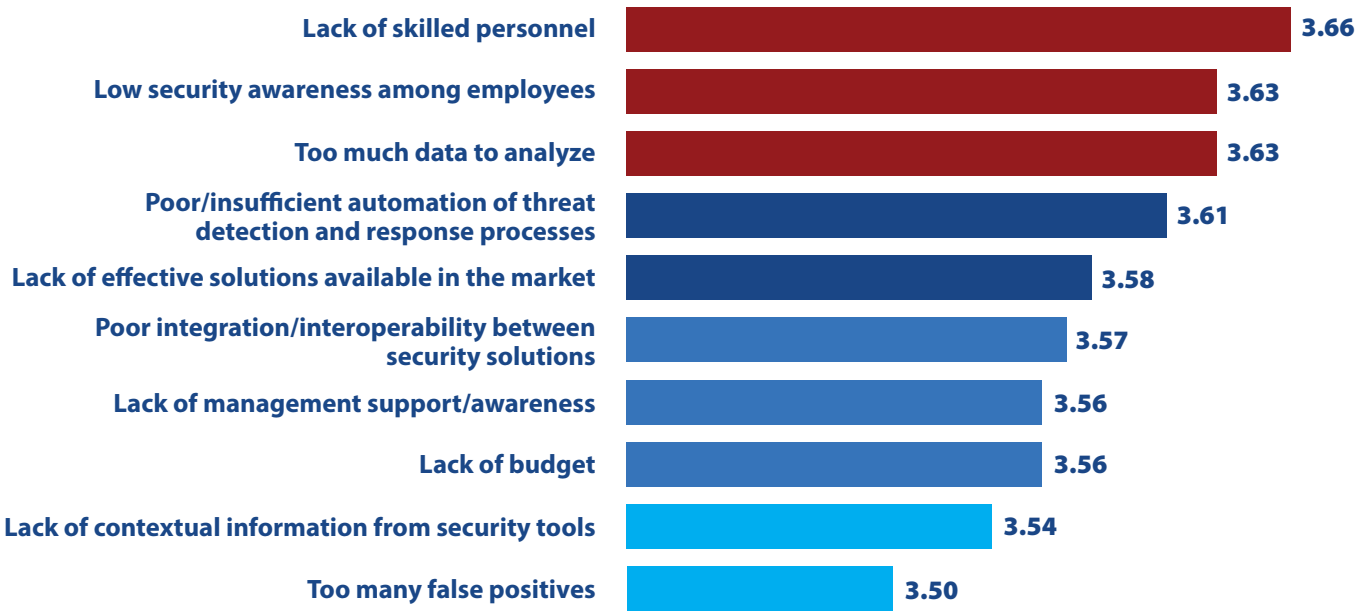

Figure 27: Inhibitors to establishing effective cyberthreat defenses.

We all know that it is important to set goals. But once you have a goal, often the next question is, "What is preventing us from reaching it?" Since one of the fundamental goals of IT security professionals is defending against cyberthreats, we asked our respondents what factors are inhibiting their organization from reaching that objective.

Figure 27 shows that the biggest inhibitor this year is, once again, lack of skilled personnel, with a score of 3.66 (on a scale of 1 to 5, with five highest). In fact, you have to go back to our 2017 edition to find a year when lack of skilled personnel was not first or second. As we saw on page 16, all but a mere 14% of organizations have a hiring shortfall in at least one cybersecurity job category.

Low security awareness among employees tied for second place , at 3.63. It has been in the first or second position for several years. If you are interested in this topic, skip to page 46 to see what training organizations are offering to improve security awareness.

The other factor in this second-place tie, too much data to analyze, moved up from fifth place in the previous survey. This is an example of too much of a good thing. Network monitoring tools, database monitoring tools, EDR solutions, and various types of firewalls and gateways are spitting out unprecedented quantities of security data, telemetry, risk signals, indicators of compromise (IoCs), and what have you. A lot of security teams are feeling overwhelmed.

Section 2: Perceptions and Concerns

It's encouraging to see that poor integration/interoperability between security solutions dropped from third place in 2022 to sixth place now. Today, security vendors are offering more and better integrations between their products and other technologies in the security infrastructure.

It's interesting to note which barriers to effective defenses are of relatively less concern to our respondents. Lack of management support and lack of budget are both near the bottom of this list. We think this reflects both the increased visibility of IT security to top management, and the fact that IT security leaders now are interacting with executives and boards of directors on a regular basis (see page 48).

The bottom two factors in this survey are lack of contextual information from security tools and too many false positives. Why should that be? Most likely the increasing use of security analytics and tools with AI capabilities is automating the work involved in correlating data from different sources and triaging alerts.

Now back to a theme that has been cropping up again and again in our data. The rating for every one of the 10 "inhibitors" included in this question declined between the last survey and this one. And when we average those ratings to calculate our "Security Concern Index," we see that number fall from 3.65 two years ago and 3.64 last year to 3.58 this year (see Figure 28). That's another clue that the tide may be turning in favor of IT security professionals feeling more confident.

"It's encouraging to see that poor integration/interoperability between security solutions dropped from third place in 2022 to sixth place now. Today, security vendors are offering more and better integrations between their products and other technologies in the security infrastructure."

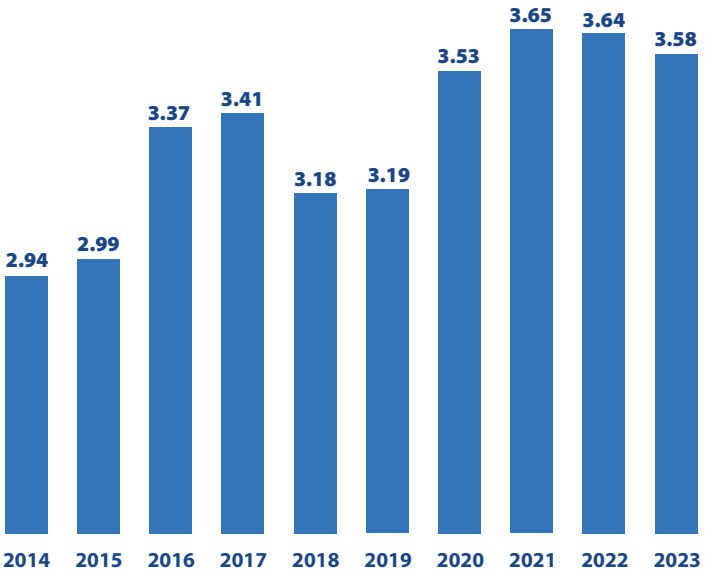

Figure 28: Security Concern Index, depicting the average rating of security inhibitors.

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 29: Benefits achieved by unifying application and data security defenses.

When looking at the data from the previous question, we noted that poor integration/interoperability between security solutions is becoming less of a challenge for IT security professionals. Part of that improvement comes from security vendors integrating their products with each other, and part from vendors integrating more technologies within their own solutions.

In this question we look at an example of the latter: vendors providing a unified platform for application and data security defenses such as WAFs, DDoS protection, runtime application self-protection (RASP), API security, risk analytics, and database security. What are the biggest benefits of leveraging an integrating offering in this space?

"The benefit most often mentioned is improved cloud security posture... As organizations migrate more workloads to the cloud, keeping them safe becomes a higher priority and a bigger challenge. Unifying related security technologies in a single platform can pay big dividends."

Section 2: Perceptions and Concerns

The benefit most often mentioned is improved cloud security posture, cited by 49.1% of our respondents (see Figure 29). As organizations migrate more workloads to the cloud, keeping them safe becomes a higher priority and a bigger challenge. Unifying related security technologies in a single platform can pay big dividends.

Another benefit, mentioned almost as often (46.1%), is enhanced security incident investigation. Fast, accurate incident response is obviously another key goal of IT security teams. Unified platforms take a lot of the work and delay out of assembling and analyzing contextual data to identify, contain, and reconstruct attacks.

Following close behind are simplified security rules management (43.7%) and improved customer support experience (40.8%), showing that the advantages of integrated security technologies extend to security architects and administrators and to customer support staffs.

What major industries are making the most use of unified platforms for application and data security? The adoption rate is 95% or above in telecom & technology, retail, and finance (see Figure 30).

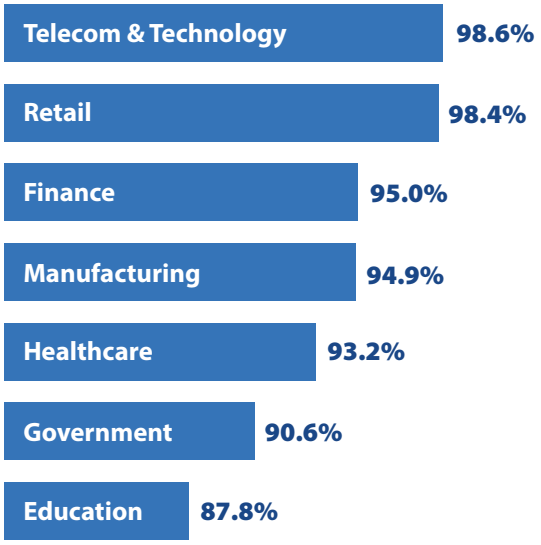

Figure 30: Organizations that have implemented a unified platform for application and data security, by industry.

Section 2: Perceptions and Concerns

Hybrid Cloud Security Challenges

Which of the following hybrid cloud security challenges are most concerning? (Select up to three.)

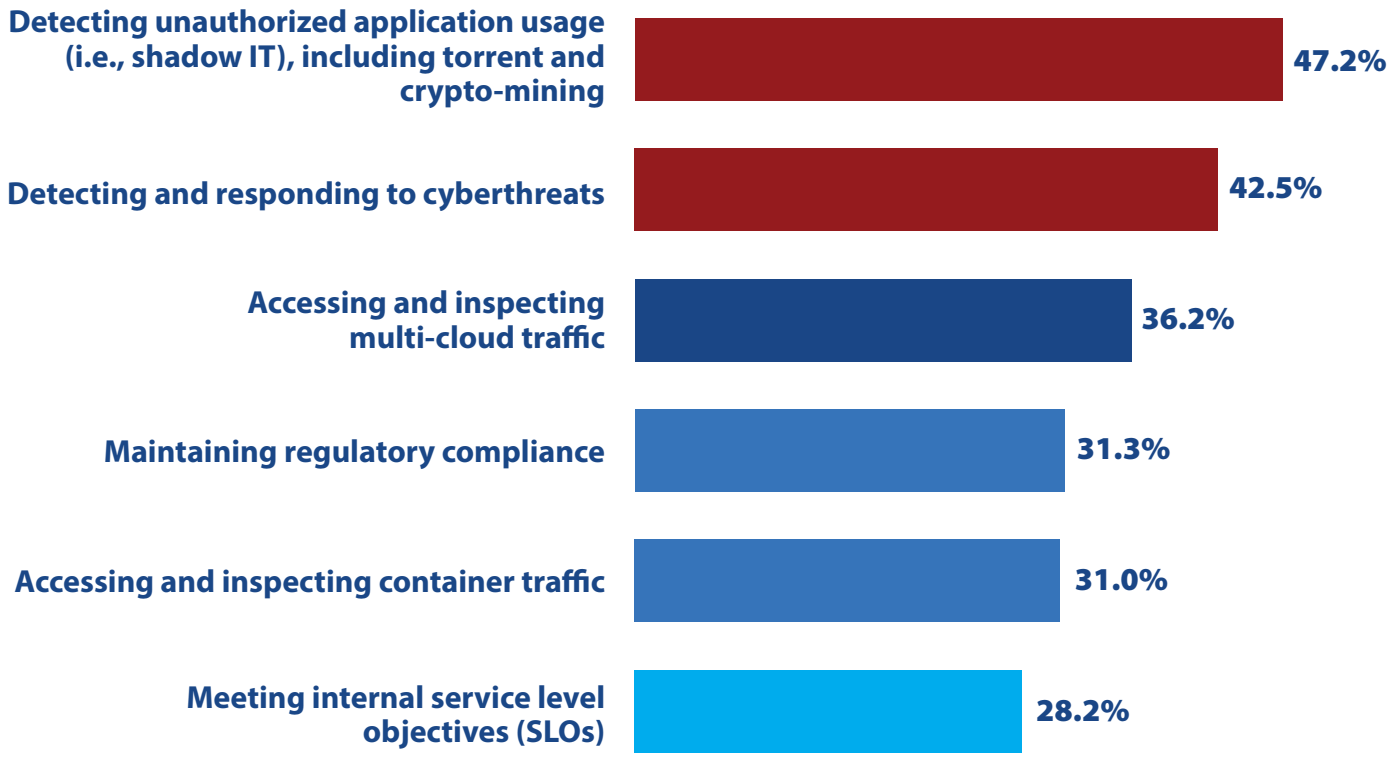

Figure 31: Most concerning hybrid cloud security challenges.

Transitioning all your applications to one cloud platform can simplify your life. Someone else (the cloud platform provider) takes care of deploying and managing the infrastructure!

But the vast majority of organizations today (96%, according to our survey) work in some kind of hybrid cloud environment. That means applications are spread across data centers and private clouds, as well as public cloud platforms hosted by Amazon, Microsoft, Google, Alibaba, IBM, and others. This complexity creates a host of challenges for IT security teams.

Which hybrid cloud security challenges are most concerning? We're glad you asked.

As shown in Figure 31, respondents from almost half of all organizations (47.2%) surveyed are very worried about detecting unauthorized application usage. They need to cope with departments that contract directly for cloud resources and services without informing IT, creating "shadow IT" activities without proper controls. They know that tech-savvy employees are using encryption and specialized protocols to exchange

Section 2: Perceptions and Concerns

"The vast majority of organizations today (96%, according to our survey) work in some kind of hybrid cloud environment. That means applications are spread across data centers and private clouds, as well as public cloud platforms... This complexity creates a host of challenges for IT security teams."

files and view suspicious sites on the dark web without being monitored. They have seen dedicated gamers tie up a lot of computing power without authorization. And they need to guard against unscrupulous employees who appropriate computing resources to mine cryptocurrencies or to run personal businesses on the side.

Next, 42.5% of survey respondents are concerned about their ability to detect and respond to cyberthreats. Some types of threats can only be detected by correlating data from across the enterprise – which is very hard to do in a hybrid cloud environment. Although cloud service providers are now offering very good security and network monitoring tools, most of them only cover the environment managed by that service provider.

Other significant challenges include accessing and assessing multi-cloud network traffic (36.2%), maintaining regulatory compliance (31.3%), and accessing and inspecting container traffic (31.0%).

Section 2: Perceptions and Concerns

Benefits of Achieving IT Security Certifications

Which of the following benefits have you experienced as a result of achieving one or more IT security professional certifications?

Figure 32: Benefits experienced as a result of achieving one or more IT security professional certifications.

IT security professionals clearly see a lot of value in studying for and obtaining certifications. But we wondered to what degree achieving IT security professional certification is motivated by the promise of job advancement and higher compensation, a desire for more knowledge, or other factors.

Well, according to our respondents, the biggest drivers are related to self-esteem, not material gain. As shown in Figure 32, the two benefits cited most often are expanded knowledge of IT security (49.3%) and increased credibility and respect (47.7%).

Third place on this list went to another non-material reward: improved job satisfaction (44.6%).

That's not to say that IT security professionals behave entirely out of a sense of selfless altruism. Almost 43% mentioned the value of certifications for employment and advancement, and 36.0% said certification helped increase their compensation.

"As a headline appearing some years ago on the website of the Association for Psychological Science said: 'Respect Matters More Than Money for Happiness in Life.'"

Section 2: Perceptions and Concerns

Still, it's reassuring that the guardians of IT security take at least as much pleasure in improving their skills and being recognized for their work as they do in getting raises. That preference may not be as rare as we think. And there is scientific research behind it: the website of the Association for Psychological Science stated: "Respect Matters More Than Money for Happiness in Life." (You can read that report at https://www.psychologicalscience.org/news/releases/respect-from-friends-matters-more-than-money-for-happiness-in-life.html.)

It is interesting to note that the ranking of these factors has been stable over time. We last asked this question in the 2020 Cyberthreat Defense Report, and the benefits of IT security certifications were listed in exactly the same order then as they are now.

The data shows some interesting differences between countries. As you can see from Table 1, expanded knowledge was the benefit selected most often in eight of the countries in the survey. Increased credibility and respect was at the top in five countries, improved job satisfaction led in one, and increased opportunities for employment and advancement was at the head of the list in three.

One more finding from the survey: of the respondents who don't currently have an IT security professional certification, almost two-thirds plan to pursue one.

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

Table 1: Benefit experienced most often as a result of achieving IT security professional certifications, by country.

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 2023?

Our survey paints a positive financial picture for IT security groups in 2023. The percentage of organizations whose budgets increased reached a new record of 87.7% (see Figure 33). In addition, as shown in Figure 34, the size of the average increase reached a new high, 5.3%, compared with 4.6% last year.

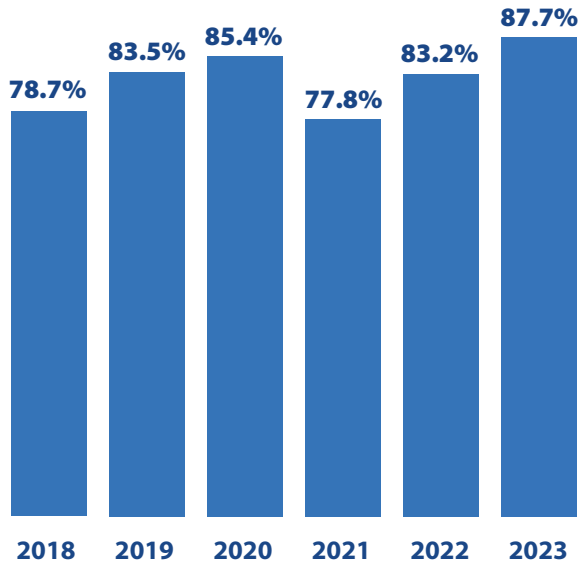

Figure 33: Percentage of organizations with rising security budgets.

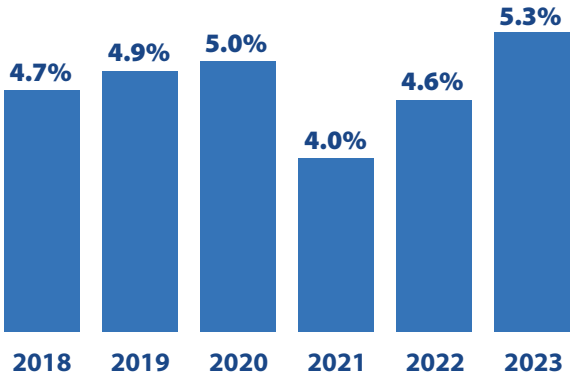

Figure 34: Mean annual increase of IT security budgets.

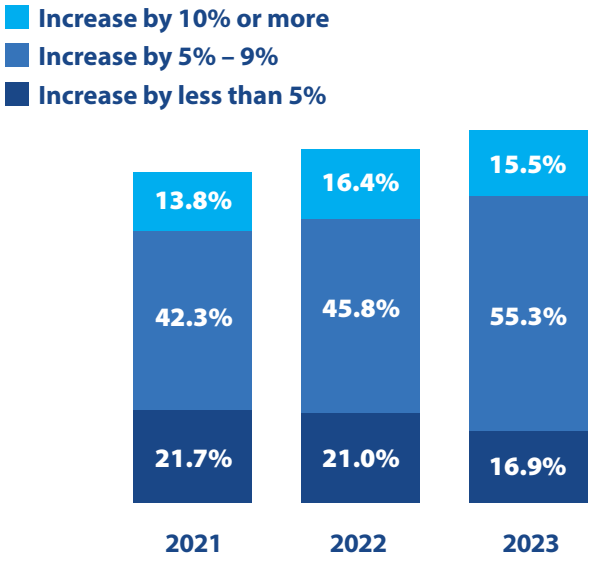

Figure 35: Breakdown of annual increase in IT security budgets by size of increase.

These increases reflect greater management awareness of the importance of strong defenses and rapid response. Another factor may be management's realization that international conflicts and rivalries could prompt malicious state-sponsored hackers to seek to disrupt commercial and government organizations of all types and sizes. On the positive side, increased spending may also reflect the success of IT leadership in communicating cybersecurity issues with top executives and boards of directors (see page 48).

Figure 35 breaks down the data for organizations expecting an increase. The sweet spot continues to be budget increases in the 5%-9% range. More than half of all organizations (55.3%) fell in that range. Only 15.5% are enjoying increases of 10% or more, while 16.9% are getting increases of less than 5%.

Section 3: Current and Future Investments

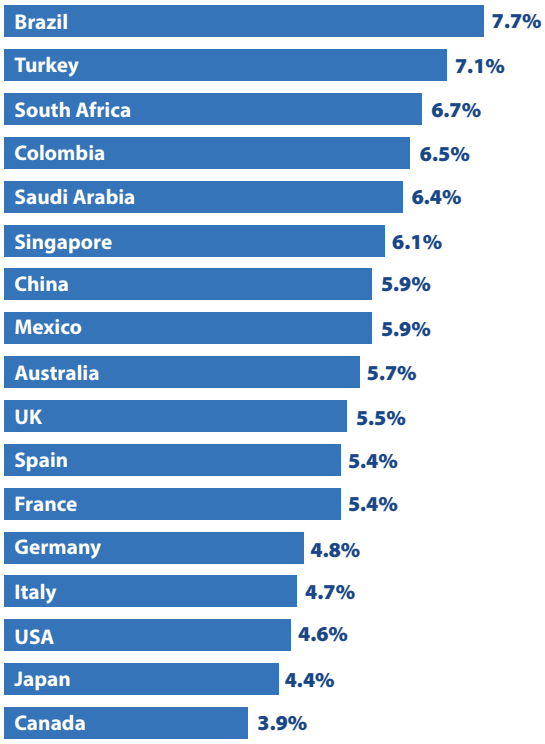

Figure 36: Mean security budget increase, by country.

"Our survey paints a positive financial picture for IT security groups in 2023. The percentage of organizations whose budgets increased reached a new record of 87.7%."

Of course, not everyone is seeing their budget go up: 7.4% of budgets are staying about the same and 4.9% are decreasing.

Which brings us to a big caveat. This information is based on 2023 budgets as they were being formulated at the end of 2022. If a recession materializes in 2023, or even if top management simply becomes more cautious about expenses, these budgets could be cut during the year. We will have to wait and see.

Meanwhile, Figure 36 shows budgets increases by country. The averages range from around 7% at the top, for Brazil, Turkey, and South Africa; to the 4%-5% range at the bottom, for Germany, Italy, the United States, Japan, and Canada.

The average increase for major industries is shown in Figure 37. Finance and manufacturing are seeing the biggest average increases (6.0% and 5.9%, respectively), and telecom & technology and education the lowest (4.7% and 4.6%).

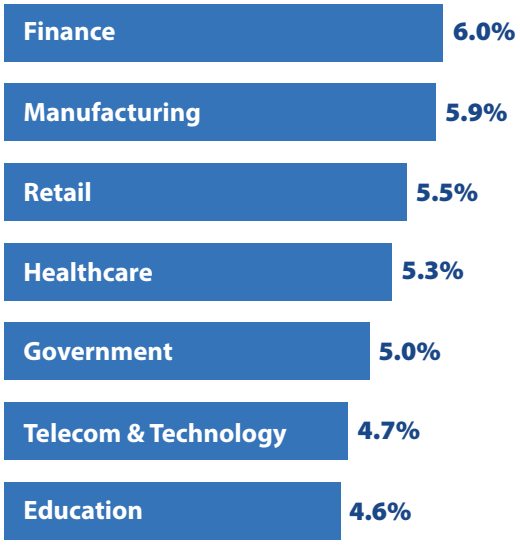

Figure 37: Mean security budget increase, by industry.

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 threat prevention (sandboxing, ML/AI)	56.8%	32.2%	11.0%
Secure email gateway (SEG)	55.6%	31.8%	12.6%
Secure web gateway (SWG)	53.6%	35.4%	11.0%
Intrusion detection / prevention system (IDS/IPS)	53.1%	32.9%	14.0%
SSL/TLS decryption appliances / platform	51.3%	36.4%	12.3%
Data loss / leak prevention (DLP)	51.2%	38.6%	10.2%
Network access control (NAC)	50.9%	36.3%	12.8%
Denial of service (DoS/DDoS) prevention	48.1%	39.6%	12.3%
Network behavior analysis (NBA) / NetFlow analysis	45.2%	37.5%	17.3%
Next-generation firewall (NGFW)	42.1%	43.6%	14.3%
Deception technology / distributed honeypots	39.0%	39.9%	21.1%

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

Network security has always been a core element of IT security. In fact, until a few years ago, it seemed like most of IT security centered on keeping bad stuff outside of the network perimeter with firewalls, secure gateways, intrusion detection products, antimalware solutions, etc., and keeping confidential stuff from leaking from inside the network perimeter, with technologies such as data loss prevention (DLP).

Today we are adapting to a perimeterless, zero trust, "assume you have been breached" world. But that doesn't mean that network security is any less important. On the contrary, it means you must inspect and filter the packets flowing within your corporate network as well as the traffic entering and leaving your premises.

So what network security solutions are the workhorses and must-haves of IT security groups today? Which up-and-coming technologies are your peers planning to acquire and deploy?

Since we first asked those questions in the 2015 CDR, the network security solution most often in use has been advanced threat prevention or one of its predecessor technologies, such as network antivirus. That remains true today, with advanced threat prevention deployed in 56.8% of organizations (see Table 2). While earlier versions of this solution focused on identifying malware signatures, current products typically combine signature recognition with sandboxing, AI-based pattern recognition and analysis, and other advanced technologies.

Section 3: Current and Future Investments

"Today we are adapting to a perimeterless, zero trust, 'assume you have been breached' world. But that doesn't mean that network security is any less important. On the contrary, it means you must inspect and filter the packets flowing within your corporate network as well as the traffic entering and leaving your premises."

Other network security solutions have moved up in the world. Over the past two years, secure email gateway (SEG) and secure web gateway (SWG) have advanced from the number 3 and number 7 positions to numbers 2 and 3, deployed in 55.6% and 53.6% of organizations, respectively.

Four other network security technologies are in use in at least half of all organizations: intrusion detection/prevention systems (IDS/IPS) at 53.1%, SSL/TLS decryption at 51.3%, data loss (or leak) prevention (DLP) at 51.2%, and network access control (NAC) at 50.9%.

The "Planned for Acquisition" category was led by next-generation firewalls (NGFWs). A significant 43.6% of organizations are planning to invest in one this year, either as a new technology or to replace an older NGFW product currently in use.

Another leader in planned investment (39.9%) is deception technology and distributed honeypots. We expect to see many deception solutions deployed in the next few years. Not only do they divert attackers away from real targets, but they also help security teams understand and defend against the tactics, techniques, and procedures (TTPs) of active threat actors.

Finally, denial of service (DoS/DDoS) prevention solutions are planned for acquisition in 39.6% of the organizations. This is an area where defenses need to be upgraded regularly to account for new techniques (Memcached DDoS attacks, anyone?) and ever-increasing volumes. Also, the emergence of DDoS attacks as elements in ransomware campaigns (see page 24) may be prompting organizations to improve their defenses against this menace.

Next: endpoint security technologies in use and planned for acquisition (page 38).

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)	72.6%	22.2%	5.2%
Data loss / leak prevention (DLP)	56.1%	32.4%	11.5%
Endpoint detection and response (EDR)	54.5%	34.3%	11.2%
EPP / Advanced anti-virus / anti-malware (machine learning, behavior monitoring, sandboxing)	52.8%	36.9%	10.3%
Disk encryption	51.4%	36.7%	11.9%
Browser or Internet isolation / micro-virtualization	50.9%	39.1%	10.0%
Digital forensics / incident resolution	48.8%	36.4%	14.8%
Deception technology / honeypot	41.4%	43.2%	15.4%

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

Table 3 shows deployments and plans for endpoint security technologies. As you may have noticed, darker shades of blue indicate a higher frequency of adoption and more frequent plans for acquisition, and lighter shades the opposite.

Basic anti-virus/anti-malware technology (that is, a product that focuses on identifying malware using threat signatures) remains by far the #1 endpoint security technology, installed in 72.6% of organizations. This is a good example of a product category that is not considered hot, but still serves an important purpose. Those thousands of malware variants are still out there in the wild!

The second and third most often installed endpoint security technologies, DLP and EDR, remain the same, although their order has switched.

Data loss (or leak) prevention (DLP) is currently in use at 56.1% of organizations, showing that it is an established workhorse. Clearly, there is a lot of benefit in stopping end users from emailing or transferring documents or files that contain sensitive information, and most DLP products today can even flag or block outgoing text strings that contain keywords related to confidential data.

Section 3: Current and Future Investments

Endpoint detection and response (EDR) products are also in widespread use (54.5% of organizations). They alert security teams to IoCs on endpoints and help block malicious activities there. EDR products are seen as playing an important role in zero trust security frameworks (see page 44). Also, they are now being integrated with other security solutions to create extended detection and response (XDR) solutions that are relevant for many use cases and offer a wide range of benefits (see our discussion of this topic on page 52).

Other technologies in use in half of organizations are endpoint protection platforms (EPP), disk encryption, and browser or internet isolation solutions (52.1%, 51.4%, and 50.9%, respectively). EPP solutions are cousins of EDR but have additional remediation capabilities. Disk encryption is, of course, a longstanding best practice for endpoints that contain sensitive information. And as we will discuss on page 51, browser or internet isolation solutions allow users to visit websites and open emails and documents without giving threat actors access to their workstations or smartphones.

What endpoint security technologies are planned for acquisition this year? The leaders are deception technology/honeypot (planned at 43.2% of organizations) and browser or internet isolation (39.1%).

Now let's see what your peers think about application and data security solutions (page 40).

"What endpoint security technologies are planned for acquisition this year? The leaders are deception technology/honeypot (planned at 43.2% of organizations) and browser or internet isolation (39.1%)."

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	60.6%	30.9%	8.5%
Database firewall	60.1%	29.0%	10.9%
Web application firewall (WAF)	55.4%	35.8%	8.8%
Database activity monitoring (DAM)	51.7%	36.1%	12.2%
Application container security tools/platform	50.8%	40.1%	9.1%
Cloud access security broker (CASB)	50.2%	35.4%	14.4%
Application delivery controller (ADC)	50.2%	33.7%	16.1%
Runtime application self-protection (RASP)	49.3%	35.8%	14.9%
File integrity / activity monitoring (FIM/FAM)	46.4%	39.9%	13.7%
Third party code analysis	45.1%	35.3%	19.6%
Static/dynamic/interactive application security testing (SAST/DAST/IAST)	44.6%	41.2%	14.2%
Bot management	35.9%	43.6%	20.5%

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

There are two must-haves in the application and data security category: API gateway/protection and database firewall (see Table 4).

API gateway/protection is the application and data security solution installed in the largest percentage of organizations (60.6%), and is the leader for the fourth year running. API gateways enforce authorization and encryption policies and limit the impact of DDoS attacks. API protection solutions go even farther. They can map an organization's attack surface to uncover rogue and forgotten APIs, track and analyze attacker behaviors, and correlate API-related data across hybrid- and multi-cloud environments. As more organizations move to modular, services-based cloud applications whose access is typically routed through APIs, security teams need tools to detect and respond to attacks targeting those APIs.

Database firewalls have moved up to the second position in this category (in use in 60.1% of organizations), after occupying third place for the past two years. They are among the few application and data security solutions whose installations increased in the past two years, rising from 58.1% to 60.1%. This increase is consistent with the trend of protecting data where it resides rather than trying to block attacks at the enterprise perimeter.

Section 3: Current and Future Investments

Bot management is not installed as often as the other applications in this sector, but new deployments are coming. It is the leader in planned acquisitions, at 43.6%. Controlling traffic from bots is a priority because of their use in ransomware, spam, and DDoS attacks and other threats.

Application security testing (SAST/DAST/IAST) is in second place in planned acquisitions, at 41.2%. Agile organizations are committed to developing software faster, but know they need more automated testing to make this safe.

Application container security tools/platforms has the distinction of being near the top of both currently in use (50.8%) and planned for acquisition (40.1%) lists. This reflects the increasing use of container technology for cloud-based applications.

"API gateway/protection is the application and data security solution installed in the largest percentage of organizations (60.6%), and is the leader for the fourth year running."

Last, but not least, we turn to our final table in this survey for data on current use and planned acquisition of security management and operations technologies (page 42).

Section 3: Current and Future Investments

Security Management and Operations 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
Active Directory protection	61.6%	28.9%	9.5%
Cyber risk quantification/scorecard	54.6%	32.4%	13.0%
Security configuration management (SCM)	52.6%	33.8%	13.6%
Patch management	50.5%	34.3%	15.2%
Advanced security analytics (e.g., with machine learning, AI)	49.6%	41.1%	9.3%
Security information and event management (SIEM)	48.8%	38.3%	12.9%
Vulnerability assessment/management (VA/VM)	48.5%	40.3%	11.2%
Security orchestration, automation and response (SOAR)	47.8%	36.9%	15.3%
Penetration testing / attack simulation software	46.7%	39.0%	14.3%
Threat intelligence platform (TIP) or service	45.8%	40.0%	14.2%
User and entity behavior analytics (UEBA)	44.1%	37.1%	18.8%
Full-packet capture and analysis	41.6%	43.5%	14.9%

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

Our Security Management and Operations category covers a lot of ground. It includes technologies related to basic security hygiene (vulnerability assessment and patch management), to automating IT security activities (SOAR and SCM), to collecting and analyzing security data (SIEM, UEBA, and advanced security analytics), and to other activities that strengthen an organization's security program (cyber risk quantification, Active Directory protection, and threat intelligence) (see Table 5).

As it happens, the four solutions most often in use this year are exactly the same four, and in the same order, as last year.

Leading the list is Active Directory protection, in use at 61.6% of organizations. Security teams need to prevent identity information in Active Directory from being stolen or used by attackers practicing privilege escalation. It is also useful for finding and fixing accounts that are special targets of threat actors, such as accounts that are over-permissioned or no longer used by a legitimate employee or contractor.

Section 3: Current and Future Investments

Cyber risk quantification tools and risk scorecards are also popular, deployed in 54.6% of organizations. They help IT groups calculate and track cyber risks, so they can focus security activities on the threats that can do the most damage. They also help IT groups communicate with top management and boards of directors about risks and justify security investments. If you refer to Figure 40 on page 48, you will see that almost half of all organizations (45.5%) provide board members with access to their cyber risk quantification or scorecard tool.

Security configuration management (SCM) and patch management continue to be old reliables, installed in about half of all organizations (52.6% and 50.5%, respectively). Maintaining the configurations of security tools and key software like database management systems is essential to maintain the effectiveness of defenses. Keeping systems patched is a critical process that needs no explanation. Both of these solutions can be managed with spreadsheets (sort of), but tools designed for these tasks save time and reduce errors.

"Our 'security management and operations' category covers a lot of ground... As it happens, the four solutions most often in use this year are exactly the same four, in the same order, as last year."

In the planned for acquisition column, the leaders are full packet capture and analysis (on the agenda for 43.5% of organizations) and advanced security analytics (41.1%). They are followed closely by vulnerability assessment/management (VA/VM) and threat intelligence platform (TIP) or service (40.3% and 40.0%, respectively).

Section 4: Practices and Strategies

Technologies Playing a Role in Zero Trust Security

Which three of the following security technologies play the most significant roles in your organization's zero trust security framework? (Select up to three.)

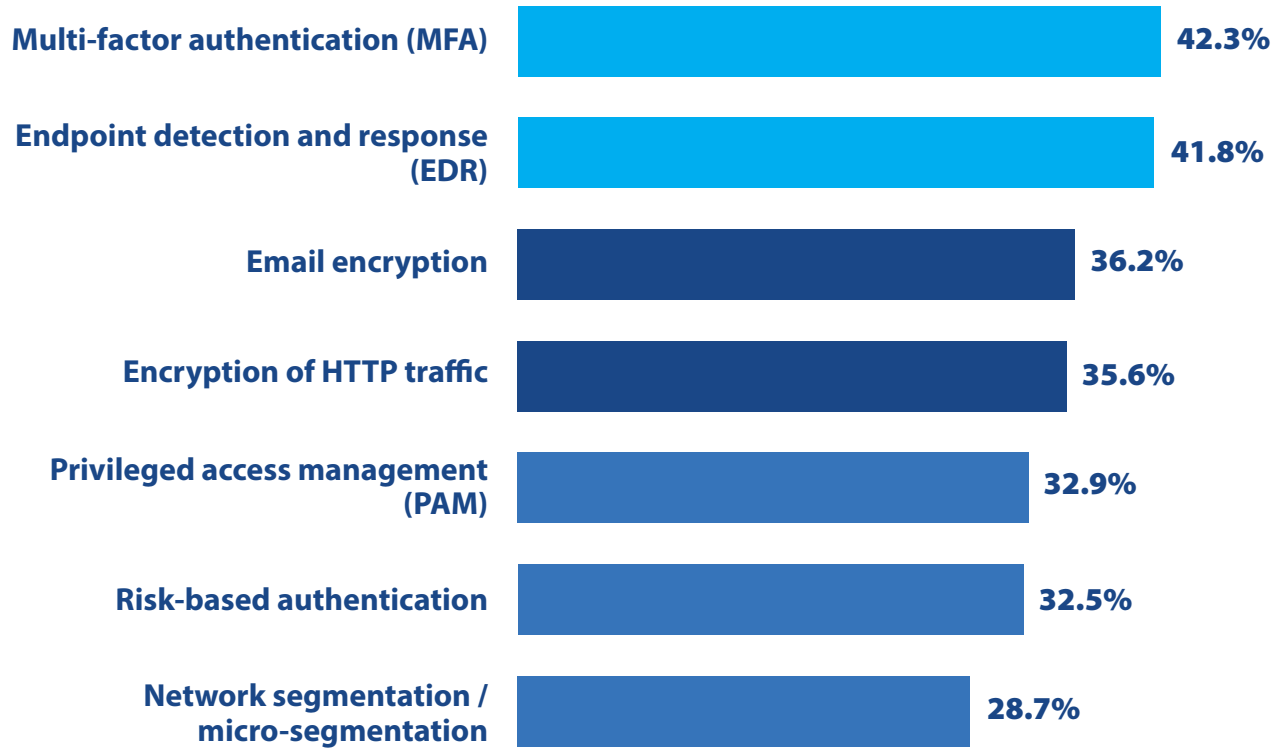

Figure 38: Technologies playing the most significant role in the organization's zero trust security framework.

Today, zero trust concepts are driving a lot of technological innovation and investment by IT organizations. But the "zero trust" label can be applied to many ideas. They include:

- Improving authentication (to make sure that every user, no matter where they attach to the network, is identified and validated as the person they claim to be)
- Rigorously enforcing the principle of least privilege (to ensure that users only have access to the specific resources they need to do their jobs)
- Applying micro-segmentation (to prevent threat actors from moving laterally inside networks)
- All sorts of other things, depending on the organization's vision of zero trust

So, we added a new question to this year's survey to see what security technologies organizations are using to support their zero trust security initiatives (see Figure 38).

Section 4: Practices and Strategies

The two technologies playing the largest roles in zero trust frameworks today are multi-factor authentication (MFA), cited by 42.3% of respondents, and endpoint detection and response (EDR), selected by 41.8%.

MFA certainly deserves a prominent place on this list. It gives organizations confidence that users requesting access to resources are not threat actors who have guessed, stolen, or bought passwords and other credentials. Most cybersecurity experts consider MFA a must-have for any secure environment. For example, the U.S. Office of Management and Budget is requiring all U.S. Federal agencies to adopt MFA for most types of applications by the end of 2024 (you can read the memo at: https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf).

EDR solutions are also a key component of a zero trust architecture. They provide data to help security teams make sure endpoints have not been compromised in ways that might allow threat actors to capture passwords, or even defeat MFA. They also enforce security policies on endpoints.

"We added a new question to this year's survey to see what security technologies organizations are using to support their zero trust security initiatives."

Next on the list of technologies widely used to support zero trust initiatives are email encryption (36.2%) and encryption of HTTP traffic (35.6%). They make it much harder for threat actors to tamper with emails and network traffic, for example, by inserting phishing links or capturing passwords, passcodes, and security tokens as they traverse a network.

Privileged access management (PAM) also received a lot of attention; it was cited by 32.9% of respondents. PAM enables security and identity management teams to control the permissions of IT and security administrators, top executives, and others who in the past were often granted almost unlimited access to an organization's information assets. It's not that IT security professionals don't *want* to trust these users completely, it's that they *can't* trust them completely. Many apparently trustworthy people turn out to be rogue insiders. Also, organizations don't want threat actors who have captured the credentials of privileged users to have free run of their entire computing environment.

One surprise is that network segmentation and micro-segmentation came in last on this list, at 28.7%. In most descriptions of zero trust models, segmentation is highlighted as an absolutely critical element. We believe most organizations recognize its importance, but because of the difficulty and effort of implementing granular segmentation, they are holding off until late in their zero trust roadmap. In other words, many organizations are starting by implementing a version of zero trust "lite" without making a big investment in segmentation, but will address it in a later stage of their zero trust program.

Section 4: Practices and Strategies

Increasing Security Awareness Among Employees

Which of the following does your organization offer to increase security awareness and train employees on avoiding phishing and other cyberthreats?

Figure 39: What organizations offer to increase security awareness and train employees on avoiding phishing and other cyberthreats.

Security awareness among employees has already come up several times in this report, most notably as an IT security function that organizations are not confident about (page 13) and as one of two powerful factors inhibiting them from adequately defending against cyberthreats (page 26).

IT security groups know very well that the smartest threat actors target end users. As cryptographer Bruce Schneier once said: "Amateurs hack systems, professionals hack people."

So, what are organizations doing about it? What types of employee security education are they offering (or requiring) to address this problem?

The first notable finding is that an overwhelming 98.3% of organizations currently provide some form of security awareness training for their employees (although we might wonder what leaders in the remaining 1.7% are thinking).

Section 4: Practices and Strategies

"IT security groups know very well that the smartest threat actors target end users. As cryptographer Bruce Schneier once said: 'Amateurs hack systems, professionals hack people.'"

As shown in Figure 39, a large majority of organizations are providing security training for employees during onboarding. For some (47.3%), this training is conducted by a live instructor, and for others (41.0%), it's provided through pre-recorded videos or lessons.

Organizations have also recognized the importance of reinforcing security lessons. Slightly more than half (52.1%) conduct security awareness training for all employees at least annually, and 40.4% make videos or training modules available on demand.

Simulations of phishing attacks and other threats are additional tools for reinforcing the lessons employees learn during their training sessions. Security simulations must be implemented very carefully. If mishandled, they can create anxiety or cause employees to feel that they are being spied on or tested with an eye to punishment. Presented in the right context, however, they can make security concepts memorable in a way that is hard to duplicate in a classroom setting or with a video. Our data shows that these simulations have really caught on and are being used in 44.0% of organizations.

Do you think wall signs and motivational posters are tacky? Have you seen the Demotivator® posters that poke fun at them? (Samples: "MEETINGS: None of us is as dumb as all of us," and "YOU ARE SPECIAL: If you require additional affirmation, get a puppy. The rest of us are trying to work")? Well, despite that, wall signs can be effective when they convey accurate, usable information. That's why signs with reminders on how to avoid phishing and other cyberthreats are pinned or taped to the walls at 41.9% of organizations.

Section 4: Practices and Strategies

Security Leaders Engaging with Boards of Directors

How do your IT security leaders engage with your organization's board of directors?

Figure 40: How IT security leaders engage with their organization's board of directors.

You can find many articles in the press about how boards of directors are now taking a strong interest in IT security. But is that true? And if it is, how do they interact with the security experts in their organization? To find out, we added a question to our survey.

The most common form of interaction is providing monthly, quarterly, or annual cyber risk assessment reports to the board. Slightly more than half of the organizations (50.7%) mentioned this best practice (see Figure 40). Reporting means board members get a picture of the organization's business risks regularly. That information helps them understand the threats to the organization and the activities of the security team to meet those threats. It also gives the board members a basis to approve or modify IT security budgets. This kind of sharing is one reason why IT security budgets are continuing to grow at the rates shown in Figure 34 on page 34.

Almost half of all organizations (45.5%) give board members access to a cyber risk quantification or scorecard system. This implies a level of interaction beyond merely handing over printed reports. Presumably, it allows board members who are interested to dig deeper into the details of how security groups assess the strengths and weaknesses of their different IT security functions and what IT leadership is doing to reduce business risks.

Section 4: Practices and Strategies

The survey also confirms that today, IT leaders interact directly with board members. A solid 41.0% of respondents report that their IT security leaders present regularly at board meetings.

Another very striking result: IT security leaders in 43.1% of the organizations participate in a cyber risk assessment committee chaired by a board member. This suggests a very active role of at least some board members in deciding (and hopefully approving) security plans. It implies a huge increase in board interaction from a few years ago.

"The Syms clothing chain promoted itself with the slogan: 'An educated consumer is our best customer.' Perhaps we can paraphrase that to: 'An educated board is IT security's best supporter.'"

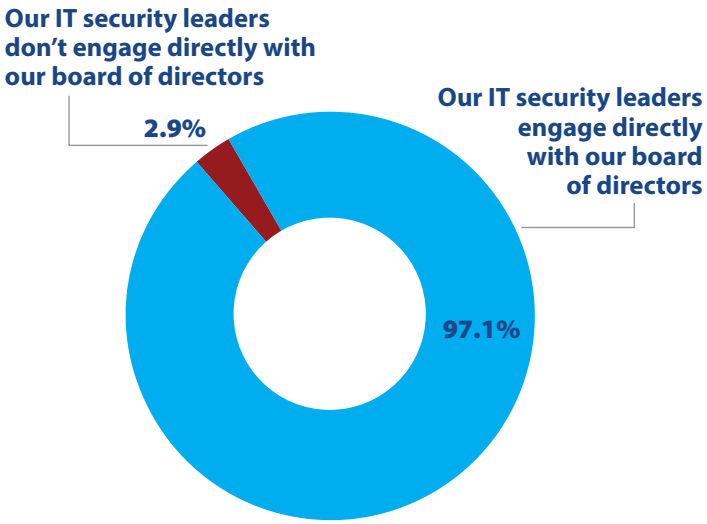

Figure 41: IT security leaders who engage with the board of directors.

Finally, a significant number of organizations track the maturity of their IT security programs (37.8%) or work with third parties to conduct independent cyber risk assessments (37.4%). These practices help IT security teams focus energies and funds on the security functions that need the most improvement – and show executives and board members where progress has been achieved.

Another important finding from our data is that engagement between IT security leaders and board members is almost universal. Of organizations that have a board of directors, only a small minority (2.9%) said their IT leaders didn't have any interaction with the board (see Figure 41).

Interaction with the board means that security leaders must be able to talk the language of business as well as technology by measuring risk and explaining the business benefits of investments in security. On balance, however, high levels of engagement are very good news. For many years, the Syms clothing chain promoted itself with the slogan: "An educated consumer is our best customer." Perhaps we can paraphrase that to: "An educated board is IT security's best supporter."

Section 4: Practices and Strategies

Technologies Playing the Biggest Roles Against Sophisticated Threats

Which of the following signature-less technologies play the biggest roles in your organization for protecting against sophisticated threats, such as ransomware, phishing, and zero day attacks? (Select up to three.)

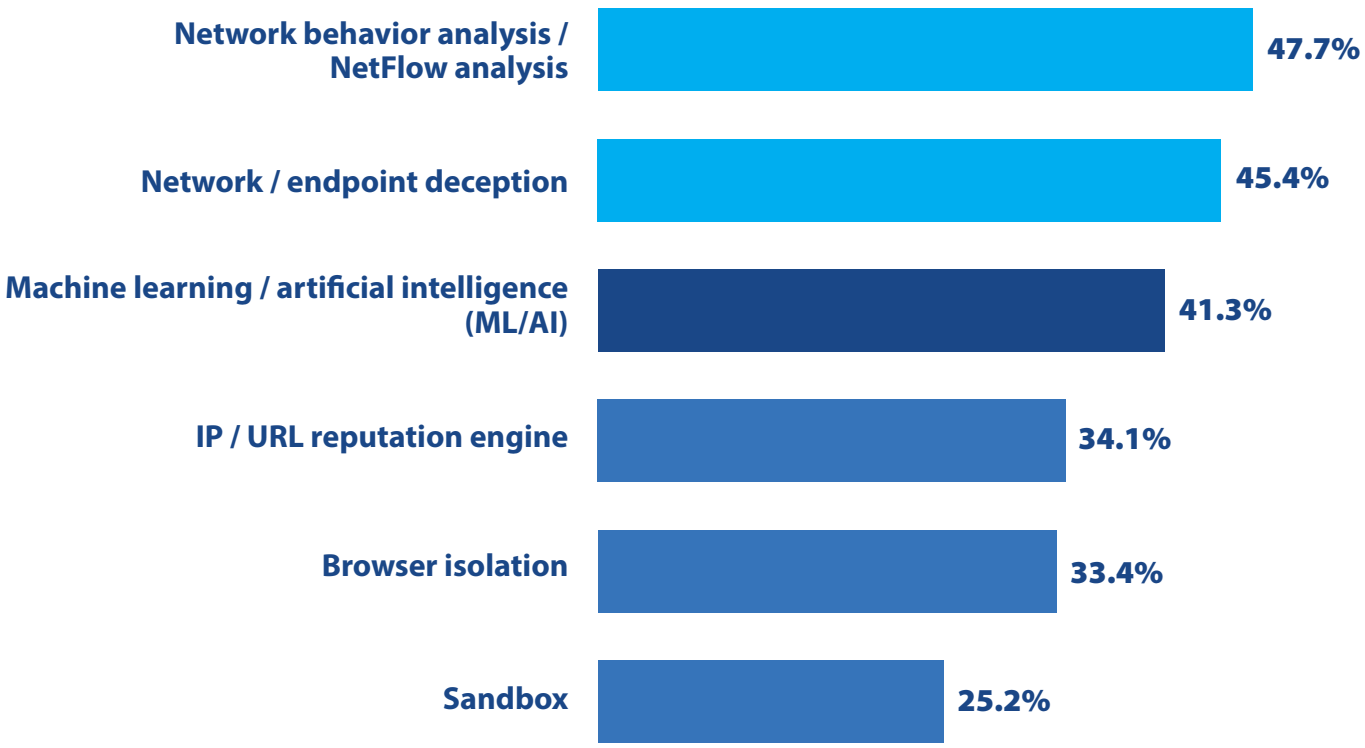

Figure 42: Signature-less technologies playing the biggest roles protecting against sophisticated threats such as ransomware, phishing, and zero day attacks.

This is another new question in our survey. We asked about the adoption of some relatively new technologies that are getting a lot of attention as innovative methods of preventing or detecting threats, such as ransomware, phishing, and zero day attacks that don't involve files with easily recognizable signatures.

The most widely used of the technologies on this list are network behavior analysis and NetFlow analysis, which play a significant role in 47.7% of organizations (see Figure 42). Security groups use them to identify unusual behaviors in network flows that are associated with threat actors searching networks for targets, accessing databases and sensitive files, and exfiltrating stolen data. The same analysis can also reveal suspicious activity by insiders and supply chain partners.

Network and endpoint deception technologies are almost equally popular and are being used by 45.4% of organizations.

Section 4: Practices and Strategies

They create decoy networks and systems that lure attackers away from real assets. The goal is to detect malicious activity, confuse and slow attackers, and learn the tactics, techniques, and procedures (TTPs) of threat actors. Deception technologies have an unusual advantage: almost no false positives. Employees and customers have no reason to access fake systems, so alerts generated by decoys are almost certainly the result of activity by threat actors.

Machine learning and AI are widely touted as powerful tools to identify malicious behaviors. What should we make of our findings that they play a big role in the defenses of 41.3% of organizations? We'd say that number indicates adoption is fairly wide, but not universal.

"Deception technologies have an unusual advantage: almost no false positives. Employees and customers have no reason to access fake systems, so alerts generated by decoys are almost certainly the result of activity by threat actors."

IP and URL reputation engines allow enterprises to block network traffic from or to websites and systems known to host malware or to be involved with ransomware, spam, phishing attacks, and other dangerous activities. They have also achieved a significant level of adoption, at 34.1%.

Another up-and-coming security technology is browser isolation, now used in exactly one-third of the organizations surveyed (33.4%). Browser isolation allows employees to perform activities like accessing websites, opening emails, and downloading documents in an isolated environment in the cloud. They can do their work just as they would from a regular browser, but any malware, ransomware, and other bad things in the websites, emails, and documents they access can't reach their systems – or anywhere else outside of the isolated browser session. Another key aspect of browser isolation is that it improves security without affecting the end user's experience at all. We think you'll be hearing more about this type of technology in the future.

What about sandbox technology? It's been around a long time as a key defense against malware (it executes suspicious files in an isolated environment to see if they perform malicious actions). Yet only a quarter of our respondents (25.2%) rated it as playing a major role in their organization's defenses.

Section 4: Practices and Strategies

Use Cases for Extended Detection and Response (XDR)

Extended detection and response (XDR) unifies endpoint detection and response (EDR) with popular network security tools, often sourced from the same vendor. Which of the following (XDR) use cases are most important to your organization? (Select up to three.)

Figure 43: Extended detection and response (XDR) use cases most important to the organization.

Extended detection and response (XDR) solutions collect and correlate data from a wide range of sources, including networks, endpoints, and cloud platforms, to help organizations detect and understand attacks more completely and accurately and respond to them faster. They represent a convergence of network monitoring, log management and analysis (SIEM), and endpoint detection and response (EDR) technologies. We found that almost all organizations have embraced XDR (see Figure 44 in the next section). But why?

The number one use case, not surprisingly, is identifying hidden cyberthreats, cited by 43.1% of the recipients (see Figure 43). Ransomware attacks, APTs, and most other major cyber menaces start with compromised endpoints. Detecting IoCs on endpoints as quickly and completely as possible is obviously an extremely high priority for IT security groups and a major motivation to invest in XDR solutions.

The next three important use cases are improving the productivity of security personnel (39.9%), accelerating incident investigation and response (39.6%), and reducing false positives (32.5%). These are priority goals in a world where IT security personnel are a scarce resource (see page 15) and a fast response to threats can avoid massive damage to an organization's revenue and reputation.

Our findings show that XDR is as widely deployed for reducing product acquisition costs (28.0%) or mitigating alert fatigue (24.3%).

Section 4: Practices and Strategies

Emerging IT Security Technologies and Architectures

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

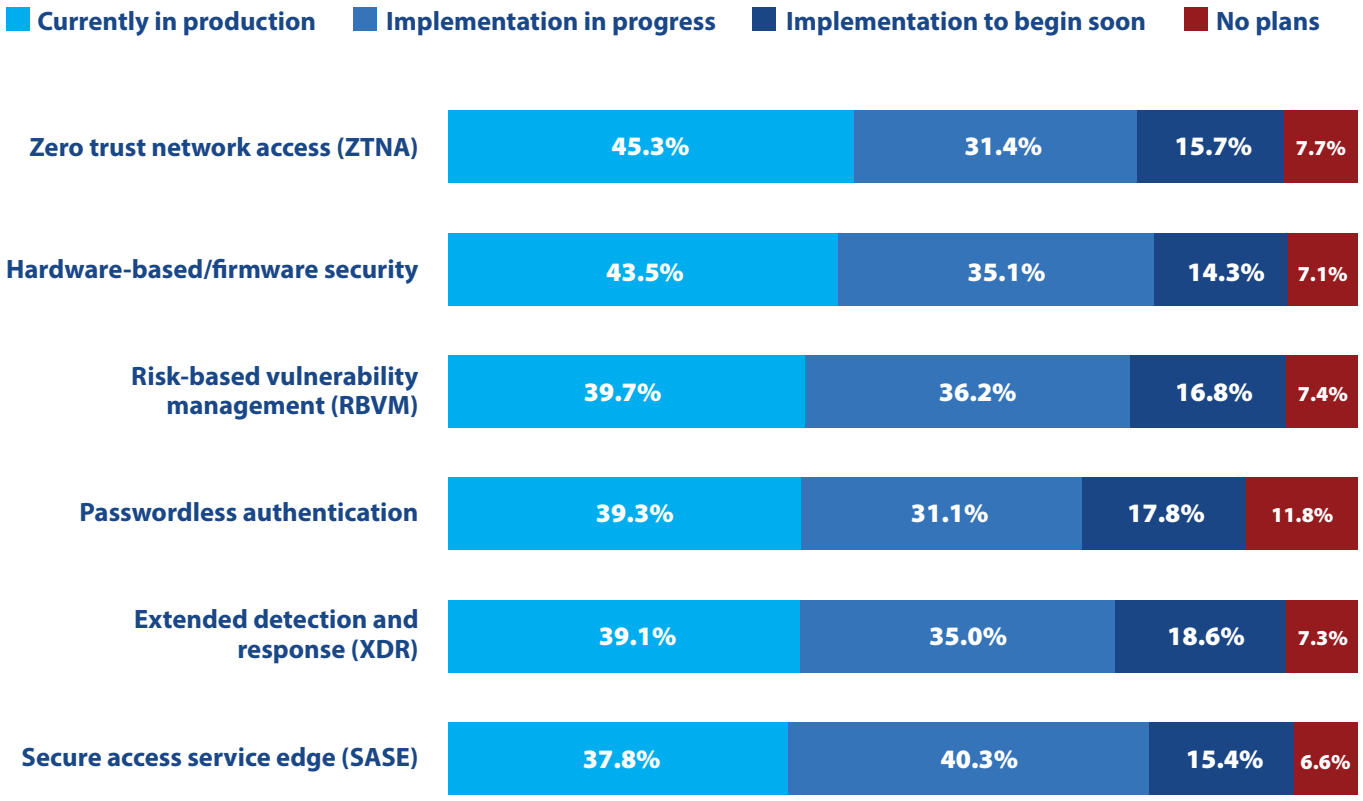

Figure 44: Plans for implementing emerging IT security technologies and architectures.

The final question in our survey examines where organizations stand on deploying six emerging IT security solutions. Some can be deployed as a single product, while others typically involve several products that work toward the same goals (e.g., secure access service edge, or SASE).

Figure 44 shows the six solutions ranked by the percentage of organizations that have them in production. You may notice, however, that the ranking would be different if we added together "currently in production" and "implementation in progress." Our takeaway is that:

- The percentage of organizations committed to each of these solutions is roughly the same.
- All of them are seen as worthwhile investments by almost everyone; the percentage having "no plans" to implement ranges from 11.8% to only 6.6%.

Of these six leading-edge solutions, the one in production most often is zero trust network access (ZTNA) at 45.3% of organizations. An additional 31.4% have begun to implement ZTNA, and 15.7% more have plans. This reflects how pervasive zero trust security ideas have become.

Section 4: Practices and Strategies

It is interesting to note that over two years the ratios of in production and being implemented for ZTNA have basically reversed: from 30.2% and 44.3% two surveys back to 45.3% and 31.4% now. This suggests that over that period, somewhere between 13% and 15% of organizations moved from implementing to using successfully.

Hardware- and firmware-based security, added to the survey last year, showed the second highest level of deployment: 43.5% in production. Implementation in progress is also high, at 35.1%. We believe this is an up-and-coming solution area. Security data and software embedded in hardware and firmware are far harder to compromise or disrupt than security data and software that can be accessed in memory or on disk.

Risk-based vulnerability management (RBVM) is also popular. It is in production in 39.7% of organizations, and is being implemented in another 36.2%. The idea behind RBVM is that organizations must not only identify as many vulnerabilities as possible across their attack surface, but they should also prioritize remediation based on factors such as the likelihood of the vulnerability being exploited by threat actors and the impact on the business if the exploitation is successful. There are far too many vulnerabilities to fix all at once, so it is essential to understand which are critical so they can be remediated first.

What about passwordless authentication, currently in production in 39.3% of organizations? Today it is widely agreed that passwords are so easy to guess, phish, steal, or buy that they can't be relied on for authentication. Instead, security teams are deploying MFA solutions that give passwords either a minor role or none at all. Biometrics play an important part in this area. The FIDO Alliance (https://fidoalliance.org/) champions standards that will eliminate sticky notes. Well, not *all* of them. But authentication solutions using FIDO standards will slash sticky note sales by getting rid of passwords.

XDR solutions are in production in 39.1% of organizations and are being implemented in an additional 35.0%. As we discussed regarding our previous question, organizations are employing XDR to identify hidden cyberthreats, improve the productivity of security personnel, and accelerate incident investigation and response, among other use cases.

Secure access service edge (SASE) solutions are in production or being implemented in almost four out of five organizations (78.1%). They are a key response to the challenges of remote work that peaked during the COVID pandemic.

"The FIDO Alliance champions standards that will eliminate sticky notes. Well, not *all* of them. But authentication solutions using FIDO standards will slash sticky note sales by getting rid of passwords."

The Road Ahead

Zero Trust Expands Even as COVID Recedes

In some ways, the rapid dissemination of zero trust principles is a legacy of COVID-19. In 2023, zero trust models are having an increasingly powerful impact on IT security, even as COVID is receding.

Zero trust concepts were introduced in 2010 and slowly gained traction during the next decade. However, it was COVID's far-reaching impact on working conditions in 2020 and 2021 that caused zero trust ideas to take off. As the pandemic took hold, IT security groups were challenged to support vast numbers of employees working at home, using an array of new communications and collaboration tools hosted on cloud platforms, over more types of networks, often with personal, unmanaged devices. Zero trust frameworks provided guidance for dealing with the most pressing issues they faced, such as requiring strong authentication for everyone, enforcing consistent access control policies everywhere, and limiting access resources on a "need to use" basis.

Now that COVID is gradually becoming a serious but manageable health issue, and as workers return to their offices (at least part time), is the zero trust wave going to subside? It doesn't look that way. Organizations still need to protect people, data, and applications that are widely distributed across locations and computing platforms. New threats make strong MFA a bigger need than ever. More-granular access control and network segmentation are needed to combat threat actors who continually develop new ways to penetrate networks and move laterally.

Over the next couple of years, there will be plenty of debate about what exactly is required for a real zero trust environment, and whether the term has been stretched to the point where it doesn't mean anything in particular. Nevertheless, we expect to see a lot more organizations implementing zero trust principles so they can walk the walk as well as talk the talk.

Is All Cybercrime Becoming Ransomware?

In our Road Ahead section last year, we wondered if the ransomware industry might have peaked. After all, organizations of all kinds were becoming more vigilant; governments were promoting measures to prevent attacks and imposing penalties for paying ransoms; law enforcement agencies were having occasional successes taking down ransomware gangs; and security solution vendors were introducing new defenses. And indeed, what we are calling "ransomware classic" has tapered off. Ransomware attacks that involve only encrypting files are way down, as we discussed on pages 24 and 25.

One take on the current situation is that ransomware has reinvented itself by morphing into double extortion or triple extortion variants that combines multiple threats. Threats to release exfiltrated information, notify customers and the media of breaches, and conduct DDoS attacks make ransom demands even harder to resist. This Darwinian adaptation has enabled overall ransomware attacks to stay at high levels and average ransom payments to rise (see Figures 18 and 19).

However, there is another way of looking at these developments. Let's say you are a cybercriminal who specializes in breaching employee databases and exfiltrating names and Social Security numbers. Once you succeed, it takes a lot of work to turn that information into cash by setting up credit card accounts, making purchases, reselling the goods to obtain currency, etc. Of course, you can just sell the data to someone else on the dark web, but you might only get a few dollars per number. Then you realize you can make the same money or better with a lot less work by demanding a ransom for not using the information. So, you partner with a ransomware gang and launch a double extortion ransomware attack.

In other words, we may be seeing cybercriminals of many types deciding to monetize their activities by demanding ransoms, rather than using or selling the information they steal.

This would not necessarily be good news, but it might point to new ways to protect against and respond to ransomware attacks. The more complex the attack, the more chance of errors by the attackers.

The Road Ahead

The Menace of AI Chatbots and Deepfakes

While this is being written in early 2023, security experts are starting to assess the potential dangers of bad guys using the ChatGPT chatbot and other AI-based tools. They are concerned that threat actors might use these tools to:

- Generate grammatically perfect, polished phishing messages
- Create highly customized phishing emails that correctly use terminology specific to industries or roles, perhaps even replicating the style of individuals such as a firm's CEO
- Obfuscate existing malware variants
- Write new malicious code

Deepfakes are also a major threat. There have already been a few attempts to use simulated voices (typically of CEOs) to persuade subordinates to transfer funds to the account of a fabricated supplier, as well as primitive attempts to literally put words in the mouths of political figures in phony videos.

As deepfake technology improves, we will undoubtedly see more and better examples employed for both cybercrime and ideological and political ends. It's not hard to imagine the possibilities:

- Launch phishing attacks by having fake celebrity endorsers announce sales and send customers to fake websites to capture credit card information
- Sow confusion by having fake versions of corporate executives announce product recalls or accidents caused by the company's products
- Manipulate stocks by releasing fake videos of CEOs announcing strongly positive or negative news
- Manipulate elections by releasing fake videos of political candidates making controversial statements, exhibiting physical or mental infirmities, or issuing phony endorsements
- Demand ransoms for not doing any of the above (see "Is All Cybercrime Becoming Ransomware?" above)

At this time, threats from AI-based tools and deepfakes are mostly speculative. However, because it is the nature of AI technologies to improve over time, we are very likely to see an ongoing arms race between threat actors, who are finding new uses for AI-based chatbots and deepfake tools, and IT security vendors, who are developing solutions to detect and block them.

IT Security Leaders Talking Risks and Returns

A new question in this year's survey asked whether IT security leaders engage with their board of directors. In case anyone had doubts, the responses showed that such interaction is almost universal and takes many forms. They include providing risk reports, presenting at board meetings, and working together on cyber risk assessment committees. A significant number of IT security teams also share measurements of the maturity of their security programs or the results of cyber risk assessments conducted by third parties (see pages 48 and 49).

We can describe the security team's interaction with boards as an evolution from zero engagement to multi-faceted involvement, as shown by this progression:

1. We never talk to them.
2. We talk to them only when we are forced to because of a data breach, disruption of business, or some other major crisis.
3. We tell them how many vulnerabilities we've remediated and how many attacks we've stopped and ask for additional funding so we can do more of that kind of thing.
4. We discuss how our programs align with organizational goals and support priority initiatives.
5. We describe current risks to the business, explain what we are doing to mitigate them, and discuss the financial return on investments in security based on losses prevented and revenues increased.

The Road Ahead

We'd say that some organizations are stuck at the third level, and most have established themselves on the fourth. Only a handful have advanced to the fifth level. But now that IT security leaders are getting face time and sharing metrics with board members, they are going to have to do a lot more talking about risks and returns.

An Opportunity to Hire IT Security Talent?

Year after year, our survey has found that a shortage of skilled IT security personnel is the biggest factor inhibiting organizations from adequately defending themselves against cyberthreats. That didn't change this year (see Figure 27).

As we pointed out on pages 15 and 16, job seekers from the current wave of layoffs in high tech won't come near to filling this gap. However, this may be a good time for organizations to make an extra effort to find and recruit some of the refugees from respected technology companies that are cutting back. Perhaps consider offering cybersecurity training and certification as a recruitment tool. After all, training and certification are not just about the Benjamins (page 32).

It may also be a good time to think creatively about finding smart people with certain backgrounds and training them to fill IT security roles. For example, good coders can become application security professionals, and financial analysts with the right mindset might make good risk and fraud analysts.

Appendix 1: Survey Demographics

This year's report is based on survey results obtained from 1,200 qualified participants hailing from 17 countries (see Figure 45) across six major regions (North America, Europe, Asia Pacific, Latin America, the Middle East, and Africa). Each participant has an IT security job role (see Figure 46). This year, 47.5% of our respondents held CIO, CISO, or other IT security executive positions.

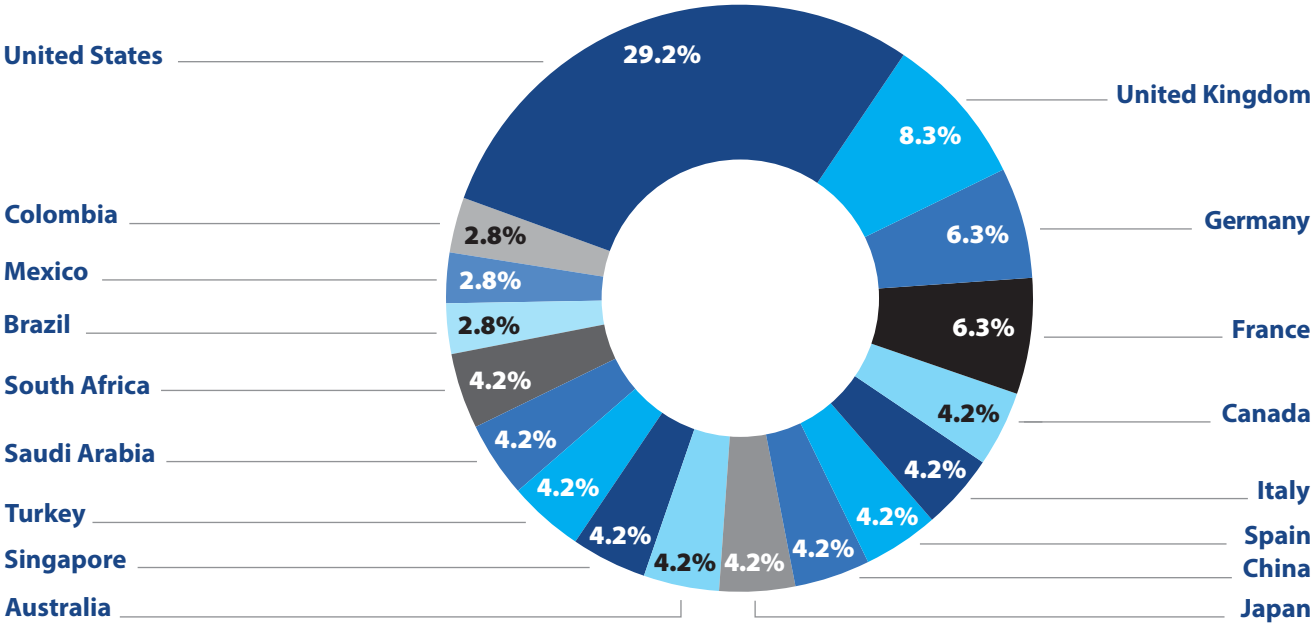

Figure 45: Survey participation by country.

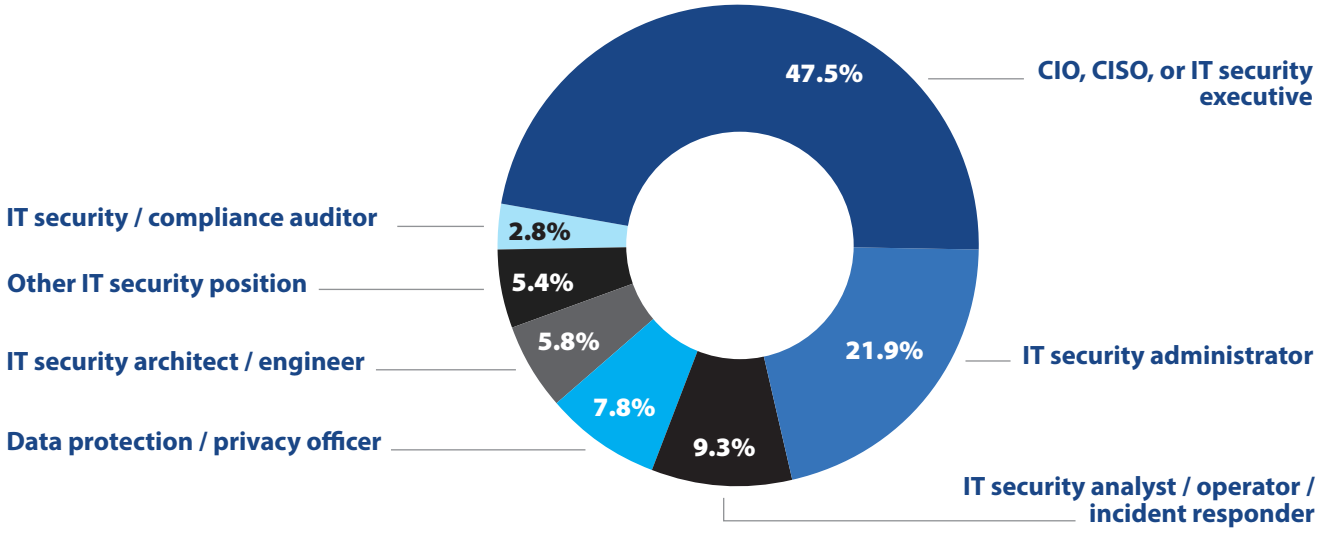

Figure 46: Survey participation by IT security role.

Appendix 1: Survey Demographics

This study addresses perceptions and insights from research participants employed with commercial and government organizations with 500 to 25,000+ employees (see Figure 47). A total of 19 industries (plus "Other") are represented in this year's study (see Figure 48). Seven industries – education, finance, government, healthcare, manufacturing, retail, and telecom & technology – accounted for 62% of all respondents. No single industry accounted for more than 15.5% of participants.

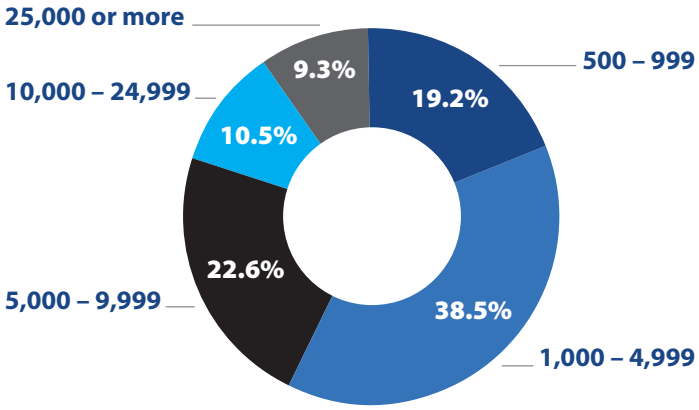

Figure 47: Survey participation by organization employee count.

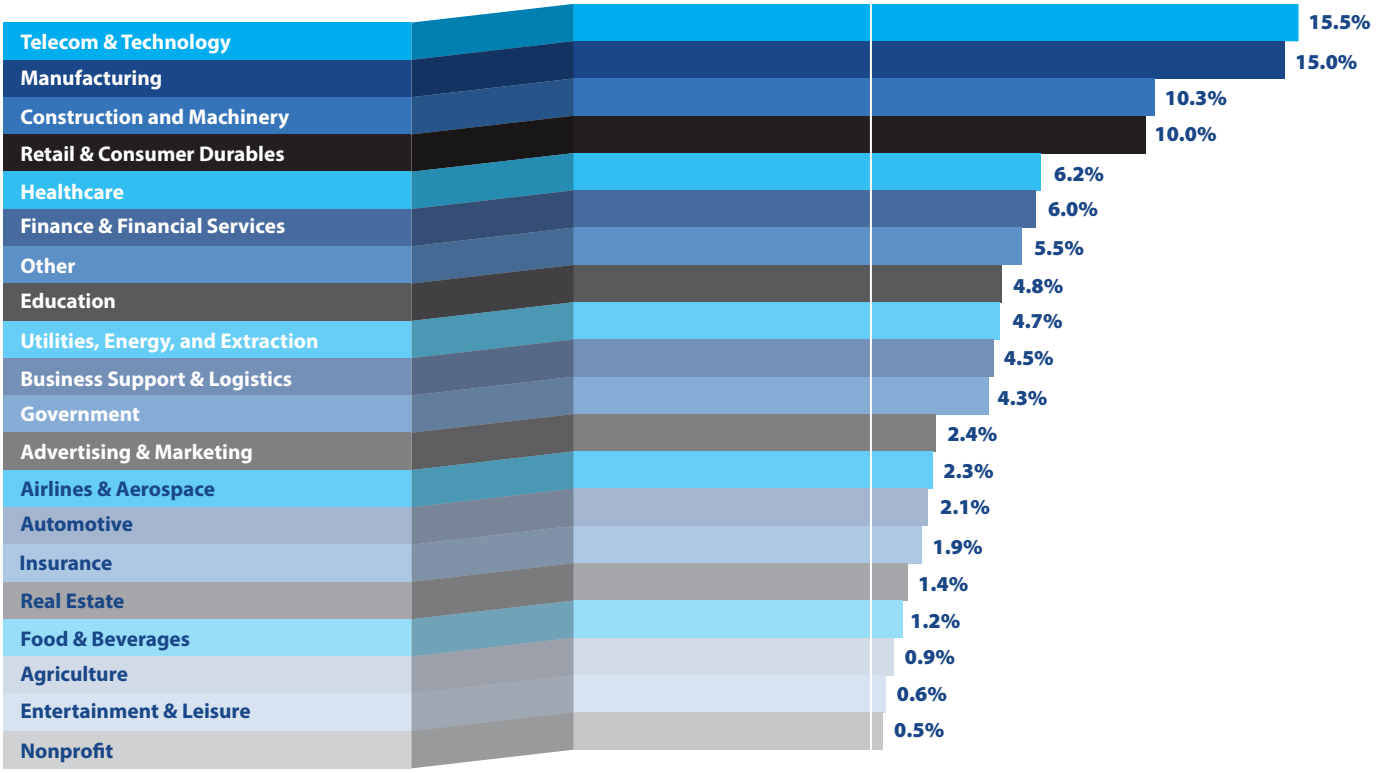

Figure 48: Survey participation by industry.

Appendix 2: Research Methodology

CyberEdge developed a 27-question, web-based, vendor-agnostic survey instrument in partnership with our research sponsors. The survey was completed by 1,200 IT security professionals in 17 countries and 19 industries in November 2022. The global 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 our 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 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, pragmatic approach to security. Our association of candidates, associates and members, nearly 330,000 strong, is made up of certified cyber, information software and infrastructure security professionals who are making a difference and helping to advance the industry. Our vision is supported by our commitment to educate and reach the general public through our charitable foundation – The Center for Cyber Safety and Education™.

Arkose Labs | www.arkoselabs.com

Arkose Labs is the global leader in bot management and account security, and its mission is to create an online environment where all consumers are protected from malicious activity. Its AI-based platform combines powerful risk assessments with dynamic attack response that undermines the ROI behind attacks while improving good user throughput. The company offers the world's first and only $1 Million Credential Stuffing Warranty™. Headquartered in San Mateo, CA with offices in Brisbane and Sydney, Australia, San Jose, Costa Rica, and London, UK, the company ranked as the 106th fastest-growing company in North America on the 2022 Deloitte Fast500 list.

Fortra | www.fortra.com

Fortra's Digital Risk and Email Protection provide comprehensive solutions for your toughest email security and brand integrity challenges. Through our digital risk protection solutions, we provide curated threat intelligence and complete mitigation of external threats across web, social, and mobile channels. While our email security and anti-phishing solutions protect emails, brands, and data from sophisticated phishing attacks, insider threats, and data loss.

HUMAN Security | www.humansecurity.com

HUMAN is a cybersecurity company that protects organizations by disrupting digital fraud and abuse. We leverage modern defense to disrupt the economics of cybercrime by increasing the cost to cybercriminals while simultaneously reducing the cost of collective defense. Today we verify the humanity of more than 20 trillion digital interactions per week across advertising, marketing, e-commerce, government, education and enterprise security, putting us in a position to win against cybercriminals. Protect your digital business with HUMAN.

Imperva | www.imperva.com

Imperva is a cybersecurity leader whose mission is to protect data and all paths to it. We protect customers from cyber attacks through all stages of their digital transformation. Imperva Research Labs and our global intelligence community enable Imperva to stay ahead of the threat landscape and seamlessly integrate the latest security, privacy and compliance expertise into our solutions.

Menlo Security | www.menlosecurity.com

Menlo Security protects organizations from cyberattacks by eliminating the threat of malware and evasive web threats from documents, email, and the single biggest productivity tool – the web browser. Menlo's patented 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, eight of the ten largest global financial services institutions, and large governmental institutions. Menlo Security is headquartered in Mountain View, California.

Appendix 3: Research Sponsors

Gold Sponsors

Delinea | www.delinea.com

Delinea is a leading provider of Privileged Access Management (PAM) solutions for the modern, hybrid enterprise. The Delinea Platform seamlessly extends PAM by providing authorization for all identities, granting access to an organization's most critical hybrid cloud infrastructure and sensitive data to help reduce risk, ensure compliance, and simplify security. Delinea removes complexity and defines the boundaries of access for thousands of customers worldwide. Our customers range from small businesses to the world's largest financial institutions, intelligence agencies, and critical infrastructure companies.

LookingGlass | www.lookingglasscyber.com

The LookingGlass Platform is purpose-built to see the entire internet, enabling national, industrial, and enterprise-scale decisions with unparalleled curated threat intelligence on critical assets, risks, and sectors. LookingGlass delivers actionable insights and advanced analytics to support attack surface intelligence, third party risk management, and national-scale cyber missions.

Netskope | www.netskope.com

Netskope, a global SASE leader, is redefining cloud, data, and network security to help organizations apply zero trust principles to protect data. Fast and easy to use, the Netskope platform provides optimized access and real-time security for people, devices, and data anywhere they go. Netskope helps customers reduce risk, accelerate performance, and get unrivaled visibility into any cloud, web, and private application activity. Thousands of customers, including more than 25 of the Fortune 100, trust Netskope and its powerful NewEdge network to address evolving threats, new risks, technology shifts, organizational and network changes, and new regulatory requirements.

Netsurion | www.netsurion.com

Netsurion® delivers complete cybersecurity confidence through wider attack surface coverage, deeper threat detection, and faster incident response. Netsurion's Managed XDR solution combines our 24x7 SOC and our Open XDR platform in a co-managed service that gives you the ultimate flexibility to adapt and grow while maintaining a secure environment. Headquartered in Ft. Lauderdale, FL with a global team of security analysts and engineers, Netsurion is a leader in Managed Extended Detection & Response (MXDR).

SailPoint Technologies | www.sailpoint.com

SailPoint is a leading provider of identity security for the modern enterprise. Using a foundation of artificial intelligence and machine learning, the SailPoint Identity Security Platform delivers the right level of access to the right identities and resources at the right time—matching the scale, velocity, and environmental needs of today's cloud-oriented enterprise. Our intelligent, autonomous, and integrated solutions put identity security at the core of digital business operations, enabling even the most complex organizations across the globe to build a security foundation capable of defending against today's most pressing threats.

ZeroFox | www.zerofox.com

ZeroFox (Nasdaq: ZFOX) is an enterprise software-as-a-service leader in external cybersecurity. The ZeroFox platform combines advanced AI analytics, digital risk and privacy protection, full-spectrum threat intelligence, and a robust portfolio of breach, incident and takedown response capabilities to expose and disrupt phishing and fraud campaigns, botnet exposures, credential theft, impersonations, data breaches, and physical threats that target your brands, domains, people, and assets. Join thousands of customers, including some of the largest organizations in the public sector, finance, media, technology, retail and manufacturing, to address the entire lifecycle of external cyber risks.

Appendix 3: Research Sponsors

Silver Sponsors

HackerOne | www.hackerone.com

HackerOne closes the security gap between what organizations own and what they can protect. HackerOne's Attack Resistance Management blends the security expertise of ethical hackers with asset discovery, continuous assessment, and process enhancement to find and close gaps in the ever-evolving digital attack surface. This approach enables organizations to transform their business while staying ahead of threats. Customers include Citrix, Coinbase, Costa Coffee, General Motors, GitHub, Goldman Sachs, Google, Hyatt, Microsoft, PayPal, Singapore's Ministry of Defense, Slack, the U.S. Department of Defense, and Yahoo. In 2021, HackerOne was named as a 'brand that matters' by Fast Company.

Netwrix | www.netwrix.com

Netwrix makes data security easy. Since 2006, Netwrix solutions have been simplifying the lives of security professionals by enabling them to identify and protect sensitive data to reduce the risk of a breach, and to detect, respond to and recover from attacks, limiting their impact. More than 13,000 organizations worldwide rely on Netwrix solutions to strengthen their security and compliance posture across all three primary attack vectors: data, identity and infrastructure.

OffSec | www.offsec.com

OffSec is the leading provider of continuous professional and workforce development, training, and education for cybersecurity practitioners. OffSec's distinct pedagogy and practical, hands-on learning help organizations fill the infosec talent gap by training their teams on today's most critical skills. With the OffSec Learning Library featuring 6,000 hours of content, 1,500 videos, 2,500 exercises, and 900 hands-on labs, OffSec demonstrates its commitment to empowering individuals and organizations to fight cyber threats with indispensable cybersecurity skills and resources. OffSec also funds and maintains Kali Linux, the leading operating system for penetration testing, ethical hacking, and network security assessments.

Phosphorus Cybersecurity | www.phosphorus.io

Phosphorus Cybersecurity is the leading xIoT Breach Prevention platform for the xTended Internet of Things. Designed to secure the growing and unmonitored Things across the enterprise xIoT landscape, our Enterprise xIoT Security Platform delivers Attack Surface Management across every vertical, providing Active Discovery & Assessment, Hardening & Remediation, and Detection & Response to bring xIoT security to every cyber-physical Thing in your environment. With xIoT intelligent active discovery and posture assessment, Phosphorus automates the remediation of the most significant IoT, OT, and Network device vulnerabilities—including unknown and inaccurate asset inventory, out-of-date firmware, default credentials, risky configurations, and out-of-date certificates.

Picus Security | www.picussecurity.com

Picus Security helps security teams of all sizes to continuously validate and enhance organizations' cyber resilience. Our Complete Security Validation Platform simulates real-world threats to automatically evaluate the effectiveness of security controls, identify high-risk attack paths to critical assets, and optimize threat prevention and detection capabilities. As the pioneer of Breach and Attack Simulation, we specialize in supplying the actionable insights our customers need to be threat-centric and proactive. Via our online Purple Academy, we give back to the community by providing free training about the latest offensive and defensive security approaches.

Valence Security | www.valencesecurity.com

Valence Security offers collaborative remediation workflows that engage with business users to contextualize and reduce SaaS data sharing, supply chain, identity, and misconfiguration risks. With Valence, security teams can secure their critical SaaS applications like Microsoft 365, Google Workspace, Salesforce, and Slack and ensure continuous compliance with internal policies, industry standards and regulations, while accelerating business productivity and the speed of SaaS adoption. Valence is backed by leading cybersecurity investors like Microsoft's M12 and YL Ventures, and is trusted by leading organizations.

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 & 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 & 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 & Event Management (SIEM)
- Security Orchestration, 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) & 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 about CyberEdge 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: 2023 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 at https://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.

Web browsers are a focal point for cyber attacks.

Threat actors have taken advantage of the shift to remote work and are targeting workers where they spend a majority of their time—the web browser. Through a new class of threats called Highly Evasive Adaptive Threats (HEAT) that easily bypass multiple layers of detection in prominent security technology, these attacks result in malware, compromised credentials, and many times, ransomware.

Find out today if your organization is susceptible to HEAT attacks with a simple HEAT Check.

menlosecurity.com/heatcheck

MENLO SECURITY