CYBEREDGE GROUP

2026 Cyberthreat Defense Report

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

<< Research Sponsors >>

PLATINUM

Google Cloud Security

ISC2

rubrik

SentinelOne

GOLD

COLORTOKENS

hackerone

VERACODE

XBOW

SILVER

cynet

KEEPER

mitiga

wallarm

MEDIA SPONSOR

SECURITY BUZZ

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.

More than a decade after its first edition, 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 2026

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

1. **Last year was basically a draw.** We start each Cyberthreat Defense Report (CDR) with a question: "How many times do you estimate that your organization's global network has been compromised by a successful cyberattack within the past 12 months?" Answers to this question provide a high-level view of the continuing arms race between threat actors and cybersecurity teams. The bad guys were clearly pulling ahead between the 2018 and 2021 CDRs (see Figure 1 on page 7). In the 2022 – 2024 reports, the good guys made up some of that ground. In the 2026 CDR we see… more or less a tie. The percentage of organizations experiencing one or more successful attacks edged downward from 81.6% last year to 80.7%, but among those, the number suffering from six or more attacks edged up from 28.7% to 30.4%. The impact of new threats and security challenges appears to have been almost exactly offset by the impact of improvements in security technologies and processes.

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. **This year, confidence and concern coexist.** Regarding the year ahead, our data shows a curious blend of optimism and pessimism. Survey respondents report greater confidence than ever before in security posture by IT domain (pages 12-13) and by IT security function (pages 14-15). However, they are more pessimistic than they were last year about the likelihood that their organization will be compromised by successful cyberattacks in the coming year (pages 10-11). What accounts for this seeming contradiction? We think it is the result of continuing improvement in the security tools and processes deployed to defend *existing* IT systems being balanced by threat actors finding more ways to manipulate users and exploit *new areas* of organizations' attack surfaces.
3. **AI is changing many games.** This report includes findings on what AI-enabled threats are most concerning to organizations. The most common responses: adaptive and evasive malware, improved attacks on passwords, improved targeting of employees, and more effective phishing emails (see pages 27-28). But today's cybersecurity professionals need to be aware of AI-related developments in many areas. These include (a) challenges in creating custom applications that incorporate AI, including AI-specific vulnerabilities, a lack of AI security knowledge, and issues with hallucinations and biases (see pages 29-30), (b) the desirably AI skills for new hires in IT security, from experience using AI to improve security workflows, to methods of evaluating risks in AI

Introduction

models and tools, to the ability to minimize hallucinations (see pages 31-32), and (c) how fast AI will impact the number of people in IT security job roles (faster than you might think – see pages 33-34).

4. **Identity security is becoming strategic.** At one time, a lot of security professionals thought identity security was about fiddling with job roles and resetting passwords. Not anymore. Identity security has been moving to center stage because identities and their credentials are spread across a wider range of environments (data center, cloud, hosted applications). They must be created and managed for huge new groups of entities (including software workloads, IoT devices, and AI agents), and they drive critical access control and authentication technologies (see pages 23-24). In fact, identity security now overlaps with nearly every other IT security domain.

5. **IT security leaders are hanging out with the board of directors (kind of).** Gone are the days when security leaders did an occasional "dog and pony show" at board meetings and then left the room. Today, they are interacting with members of boards of directors not only more often, but also at a much deeper level. That involvement includes sharing more security information with board members at regular intervals and having them participate in (and sometimes lead) cyber risk assessments (see pages 53-54).

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 organizations face in mitigating their risks
- The adequacy of organizations' security postures and their internal security practices
- The organizational factors that present the most significant barriers to establishing effective cyberthreat defenses
- Current investments in security technologies and those planned for the coming year
- The health of IT security budgets and the interaction of security leaders with boards of directors

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 CDR's 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 our resolute security professionals.

Introduction

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 and judge their organization's security posture in specific IT domains and security functions. 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

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 the role of AI in cybersecurity. These appraisals will help readers think about how their own organization can best improve cyberthreat defenses going forward. We also look at how IT security training and professional certification can help enterprises address the serious shortfall in skilled IT security staff.

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 how they are deploying leading-edge technologies and services such as AI-enabled security tools and how organizations are preparing for future challenges such as those relating to quantum computing.

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@cyberedgegroup.com.

Research Highlights

Current Security Posture

- **Good and evil in balance.** The percentage of organizations experiencing successful cyberattacks has stayed about the same for the third year in a row (page 7).
- **A gloomier outlook.** Expectations of future compromises edged up from last year (page 10).
- **Confidence in security postures.** Overall ratings of security postures by IT domain reached a record high (page 12).
- **Security awareness is shaky.** Respondents continue to have doubts about user security awareness/education (page 14).

Perceptions and Concerns

- **Phishing is BAD.** Phishing and spear phishing have replaced malware as the greatest concern among types of cyberthreats (page 16).
- **Ransoms are being paid.** The number of firms victimized by ransomware has been steady, but those paying ransoms jumped (page 18).
- **Cybersecurity skills still in demand.** Lack of skilled cybersecurity personnel continues to be the biggest factor preventing adequate defenses against cyberthreats (page 21).
- **Identity security to center stage.** Protecting identities and credentials is a bigger issue than ever before (page 23).
- **R-E-S-P-E-C-T.** Security team members want professional certifications more for knowledge and respect than for compensation (page 25).
- **AI for evil.** Among AI-enabled threats, organizations are most concerned about evasive malware, improved attacks on passwords, and improved targeting of employees (page 27).
- **Challenges in creating AI apps.** Roadblocks to creating AI-enabled apps include security vulnerabilities, lack of skills, and the potential for hallucinations and bias (page 29).
- **AI skills for new hires.** Hiring managers are looking for new employees with a variety of AI-related skills and experience (page 31).
- **AI taking jobs?** 80% of survey respondents think AI will reduce demand for people to perform their role; 46% believe that reduction will start within two years (page 33).

Current and Future Investments

- **Budgets up again.** Nine of 10 organizations expect their IT security budget to increase this year – a record (page 35).
- **MDR service providers delivering.** Speed, efficiency, expertise, and time savings are driving decisions to use MDR service providers (page 37).
- **Stop that leak!** Data loss/leak prevention is the rising star among network security technologies (page 39).
- **Endpoint security leaders.** Basic anti-malware products are installed on the most endpoints, but browser or internet isolation is moving up the list of endpoint security solutions (page 41).
- **APIs and bots.** Among application and data security technologies, API protection is the most popular, but bot management is most frequently planned for acquisition (page 43).
- **Protect the identity store.** Active Directory protection is in use in more organizations than any other security management and operations technology (page 45).

Practices and Strategies

- **Cloud security priorities.** Top priorities for improving cloud security include identity management, visibility into VMs, and monitoring of apps across multiple cloud platforms (page 47).
- **AI-enabled security tools are here.** At least 75% of organizations are either using or implementing AI-enabled tools for multiple security tasks (page 49).
- **Is quantum computing on your radar?** 96% of organizations have started to prepare for quantum computing cyber risks, but most haven't gotten far (page 51).
- **The BOD and me.** IT security leaders are engaging more often and more deeply with boards of directors than ever before (page 53).
- **Progress report on emerging technologies.** We show data on the implementation status of 10 emerging IT security technologies and architectures (page 55).

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?

It was not the best of times. It was not the worst of times. It was neither the year of triumph over cyberthreats, nor the year of defeat. It was not the zenith of AI harnessed for good, nor the nadir of AI employed for evil. Security professionals could not afford to become complacent, but neither did they need to despair.

Our apologies to Charles Dickens for that paragraph. What we mean to say is that last year was more or less a draw between attackers and defenders.

On the crucial question of how many of the more than 1,000 organizations participating in our survey were compromised by at least one successful cyberattack in the previous 12 months, our data shows a slight improvement over last year. The percentage edged down from 81.6% in the 2025 CDR to 80.7% in this one. On the other hand, the proportion of organizations experiencing six or more successful attacks crept up from 28.7% to 30.4% (see Figures 1 and 2).

In fact, although those percentages rose sharply between our 2018 and 2021 surveys and then declined significantly from the 2021 to the 2024 edition, they have been relatively stable since.

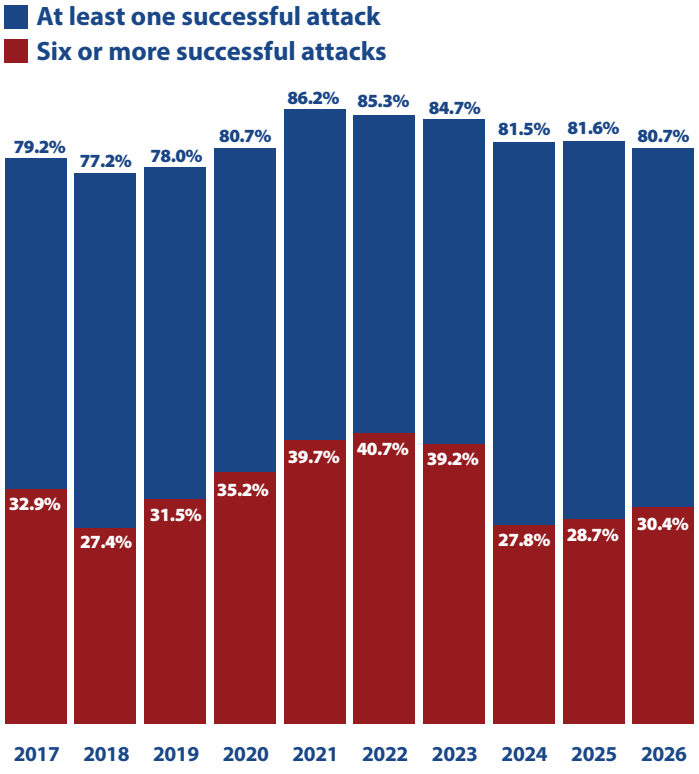

Figure 1: Percentage of organizations experiencing at least one successful attack and those experiencing six or more.

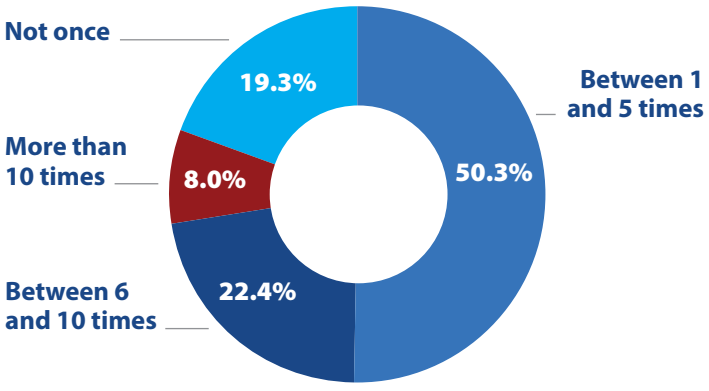

Figure 2: Frequency of successful cyberattacks in the past 12 months.

Section 1: Current Security Posture

How could there be such a balance between demons and angels when the world of cybersecurity is changing so fast, in so many ways? It could be attributed to the intervention of Saint Offset (the patron saint of forecasters and statisticians) or to factors pushing strongly in opposite directions that largely counteract each other.

Factors creating serious new challenges for security teams over the last three years include:

- The growth of dark web marketplaces and ecosystems offering sophisticated malware, tools, infrastructure, and information
- Ransomware gangs multiplying their leverage by exfiltrating data and adding the threat of public disclosure to the threat of encryption and loss
- Sophisticated state-sponsored hackers diversifying their activities to target individuals and enterprises with money-raising scams
- Exponentially more information assets (and identities) to protect due to the explosion of software workloads, internet of things (IoC) devices, cloud platforms and services, and most recently, AI agents
- New requirements to manage and protect data to comply with privacy and governance as well as security standards
- And, of course, threat actors utilizing AI tools to find more vulnerabilities, improve phishing and social engineering, and manage complex, multi-phase, cross-domain attacks that make yesterday's "advanced persistent threats" look like first-year coding class exercises

To balance those out, however, we have seen developments such as:

- Continuing increases in IT security budgets (see page 35-36)
- Payoffs from post-COVID epidemic investments in network and cloud security tools.
- Adoption of Zero Trust principles and best practices embodied in industry standards, government regulations, and incentives from cyber insurance firms
- Increasing use of standards, APIs, and security platforms to capture, correlate, and analyze alerts and data across multiple security domains for faster and more-accurate attack detection and response
- Investment in workflow automation and SOAR (security orchestration, automation, and response) tools to accelerate attack containment and remediation
- Heightened attention to security fundamentals such vulnerability scanning and patching, identity security, security awareness training for users, and ongoing education of cybersecurity professionals
- And, of course, vendors and security teams utilizing AI tools to eliminate vulnerabilities, identify and thwart phishing and social engineering attacks, and detect anomalous behaviors with a level of accuracy that makes yesterday's version of "behavior analytics" look like a high school science fair project

In the rest of this report we will see how many of these factors, negative and positive, have been playing out.

"How could there be such a balance between demons and angels? It could be attributed to the intervention of Saint Offset... or to factors pushing strongly in opposite directions that largely counteract each other."

Section 1: Current Security Posture

Returning to the details of the survey data on organizations reporting successful cyberattacks over the past 12 months, the results vary significantly across the globe. As shown in Figure 3, the percentage experiencing at least one exceeded 90% in five countries (Turkey, Colombia, Saudi Arabia, Singapore, and South Africa), while falling below 70% in three (Australia, Italy, and Japan).

Results by industry also varied. In most industries, more than 80% of organizations were affected by a successful attack, but the rate was significantly lower in government (70.2%) and healthcare (63.0%).

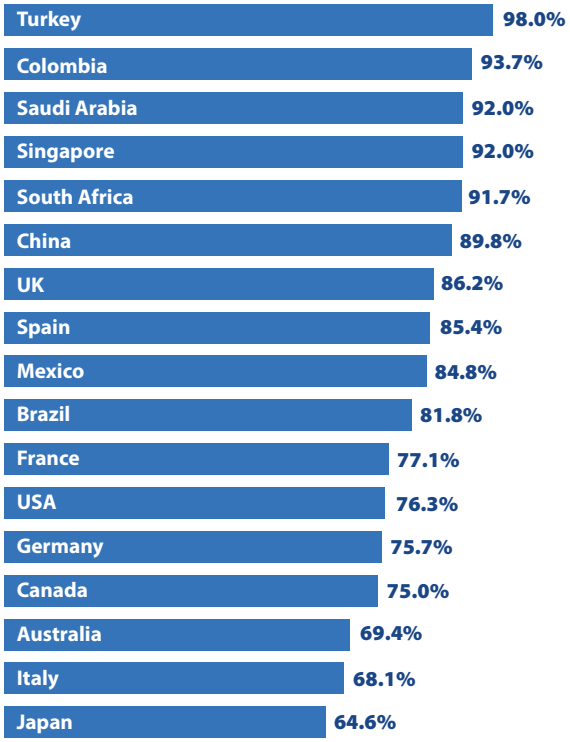

Figure 3: Percentage of organizations compromised by at least one successful attack in the past 12 months, by country.

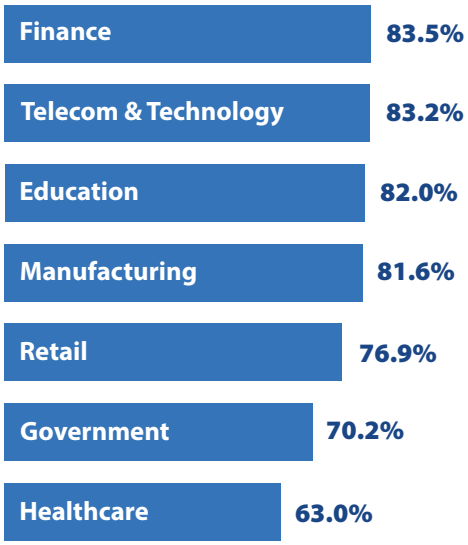

Figure 4: Percentage of organizations compromised by at least one successful attack in the past 12 months, by industry.

Future Likelihood of Successful Cyberattacks

What is the likelihood that your organization's network will become compromised by a successful cyberattack in 2026?

Looking ahead, the portion of respondents saying a successful attack in the coming year is "very likely" jumped from 20.9% in the 2025 CDR to 25.0% in this one. If we add "somewhat likely" to those, the total increased from 64.0% to 67.1% (see Figure 5). Those figures indicate a slightly gloomy view of the near future.

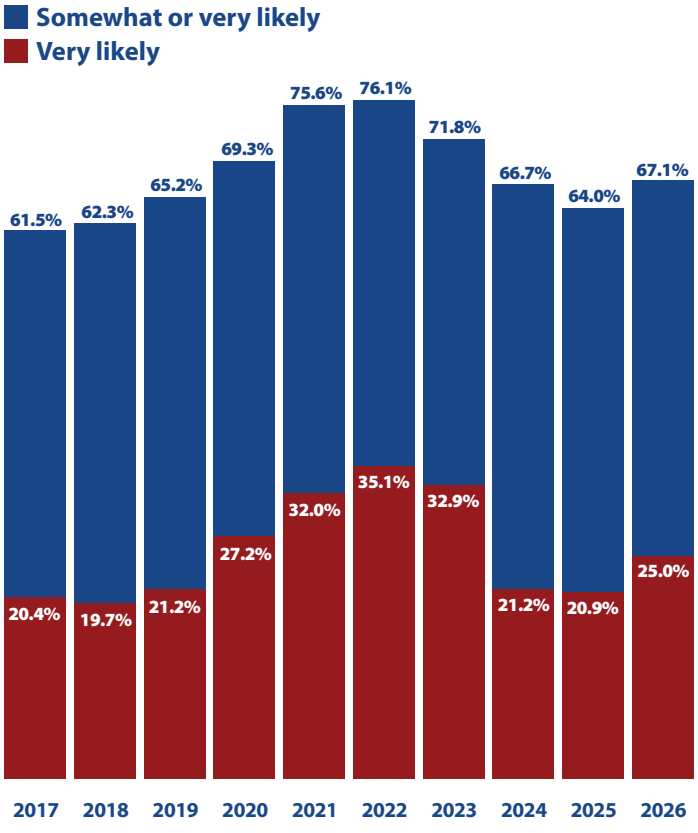

Figure 5: Percentage of organizations indicating that compromise by a successful cyberattack in 2026 is somewhat or very likely.

We think this greater pessimism among security professionals is fueled largely by uncertainty about their ability to defend against novel AI-fueled attacks. If you skip to page 27 you will see a discussion of the AI-enabled threats that most concern organizations today, such as improved attacks on passwords, better targeting of employees, and accelerated vulnerability discovery and reconnaissance by threat actors. On page 29 you'll find additional security challenges that face organizations creating custom applications that incorporate AI. These include information leaking through AI prompts and exposure to prompt injection and large language model (LLM) poisoning. These are relatively novel risks, and it's no wonder that security professionals are apprehensive.

To be sure, nobody is panicking. The "somewhat or very likely" figure of 67.1% is well below the peak levels of 2021 (75.6%), 2022 (76.1%), and 2023 (71.8%). Those peaks were driven in a large part by the surge in at-home and remote work driven by the COVID pandemic.

The combined picture from this and the previous question shows survey respondents are apprehensive that threat actors will gain a couple of steps on cybersecurity defenders this year, but the effect will not be as dire as the situation caused by the unprecedented surge in remote work a few years ago.

The percentage of respondents predicting at least one successful attack in 2026 (67.1%) is smaller than the percentage who experienced attacks in the past year (80.7%). In other words, a significant number of organizations who were victimized in 2025 think they won't be compromised in the year ahead. That's probably not realistic. However, it is consistent with data from our previous surveys. As the poet wrote: "Hope springs eternal in the human breast."

Section 1: Current Security Posture

When looking at predictions by country, we find respondents in Turkey, Singapore, Mexico, and Germany to be the most pessimistic (or perhaps the most realistic?) and those in Australia, France, Saudi Arabia, and Italy to be the least dejected (see Figure 6).

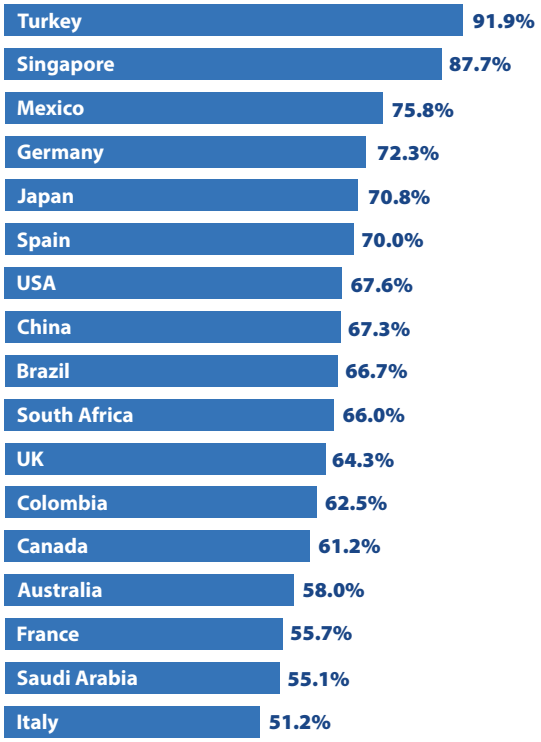

Figure 6: Percentage of organizations indicating that compromise by a successful cyberattack in 2026 is somewhat or very likely, by country.

The differences by company size are interesting. Security teams in mid-sized organizations are more apprehensive than those in both smaller and larger entities. A successful attack is thought to be somewhat or very likely in 74.6% of organizations with 5,000-9,999 employees, versus readings between 59.0% and 68.5% everywhere else (see Figure 7). This may reflect the fact that small organizations don't protect enough data or have deep enough pockets to make them enticing targets, while large enterprises are guarded by defenses in depth and specialized security staff that mid-sized organizations can't afford.

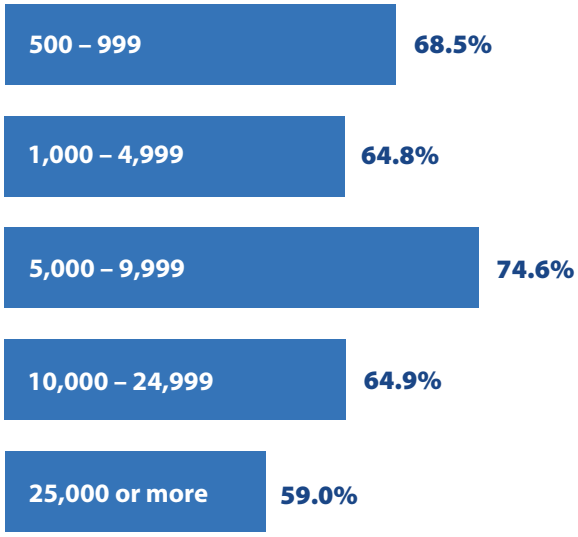

Figure 7: Percentage of organizations indicating that compromise by a successful cyberattack in 2026 is somewhat or very likely, by number of employees.

"We think this pessimism among security professionals is fueled largely by uncertainty about their ability to defend against novel AI-fueled attacks."

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:

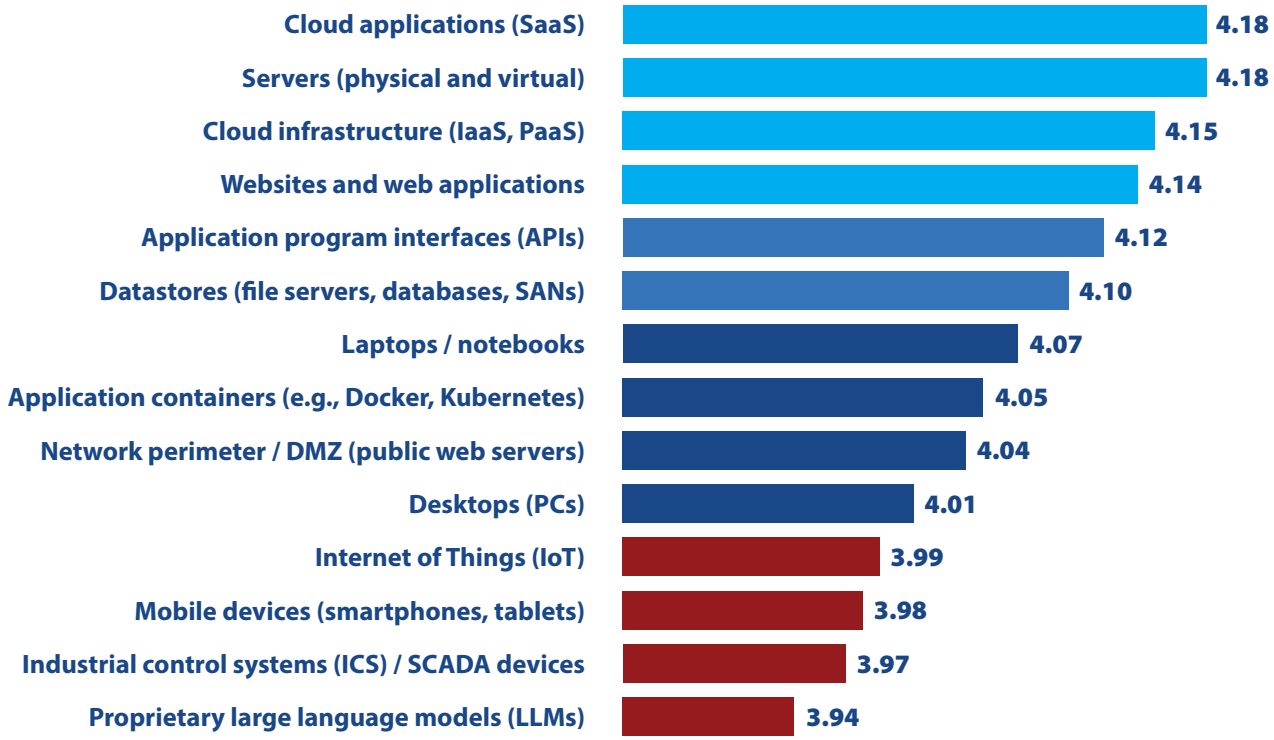

Figure 8: Perceived security posture by IT domain.

It's no secret that the attack surface of the average organization has expanded rapidly over the last few years to encompass a wide variety of physical and virtual devices, software services, and infrastructure environments. That expansion has led to a proliferation of security solutions tailored to each area. We asked survey respondents to rate their organization's security posture in 14 of those domains (see Figure 8).

As it turns out, the five domains ranked highest for security posture in the last survey where also ranked highest in this one, and their scores increased significantly. Their average rating on a scale of 1 to 5, with 5 being highest, jumped from 4.07 to 4.18 (+.11) for "Cloud applications (SaaS)," from 4.06 to 4.18 for "Servers (physical and virtual)" (+.12), from 4.02 to 4.15 for "Cloud infrastructure (IaaS, PaaS)" (+.13), from 3.93 to 4.14 for "Websites and web applications" (+.21), and from 4.0 to 4.12 for "Application programming interfaces (APIs)" (+.12). All of these are much larger movements than we normally see in this survey.

Section 1: Current Security Posture

Even the domains where security postures were rated comparatively low saw significant improvements. The rating for "Internet of Things (IoT)," a perpetual source of concern, rose from 3.90 to 3.99 (+.09). The average for "Mobile devices (smartphones, tablets)" improved from 3.87 to 3.98 (+.11), and for "Industrial control systems (ICS)/SCADA devices" from 3.88 to 3.97 (+.11).

Reflecting this positivity, CyberEdge's Security Posture Index (an average of the ratings of all the domains in the question) rose from 3.97 in the last survey to an all-time high of 4.07 in this one (+.10) (see Figure 9).

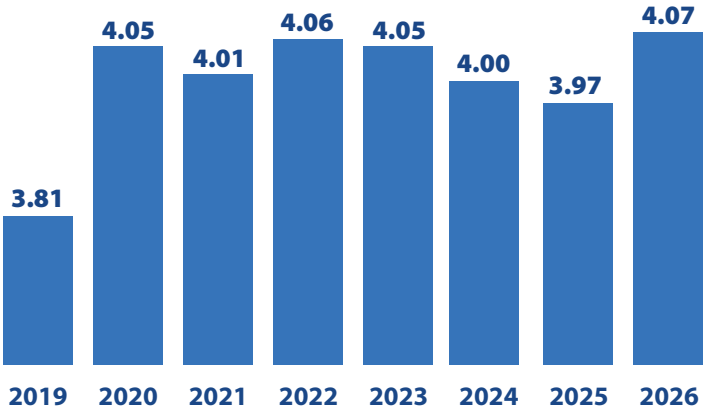

Figure 9: The Security Posture Index.

Why the increase in confidence in all the security domains, across the board, at this time? The major cause, we believe, is the maturing of AI capabilities for attack detection, automated triage of incidents and alerts, incident investigation, and rapid containment, together with increased integration and automation of security workflows.

"But wait!" you say. "What about the comment in the previous section that survey respondents have a gloomy view of the coming 12 months? How do you square that pessimism about security outcomes with this apparent increase in confidence about defenses protecting security domains?"

Here is what we think is going on:

- Security tools and processes to defend existing IT components continue to improve.
- But at the same time, threat actors are devising more ways to manipulate users and exploit new areas of the attack surface.

To suggest a medieval analogy, we are finding ways to make the individual pieces of our suit of armor stronger, but the bad guys keep finding gaps between the pieces, and it takes us a while to fill those gaps.

For example, organizations are starting to develop AI-enabled applications. This year we expanded this question by asking respondents to rate their security posture for "Proprietary large language models (LLMs)." The answer is: low (3.94). In fact, that's the lowest score of all the security domains listed in this question. So, while organizations are feeling better about their defenses for established IT security domains, they recognize that they're facing new areas of exposure, and it takes a while to address them. (For more about security risks inhibiting the creation of custom applications that incorporate AI, see pages 29-30).

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:

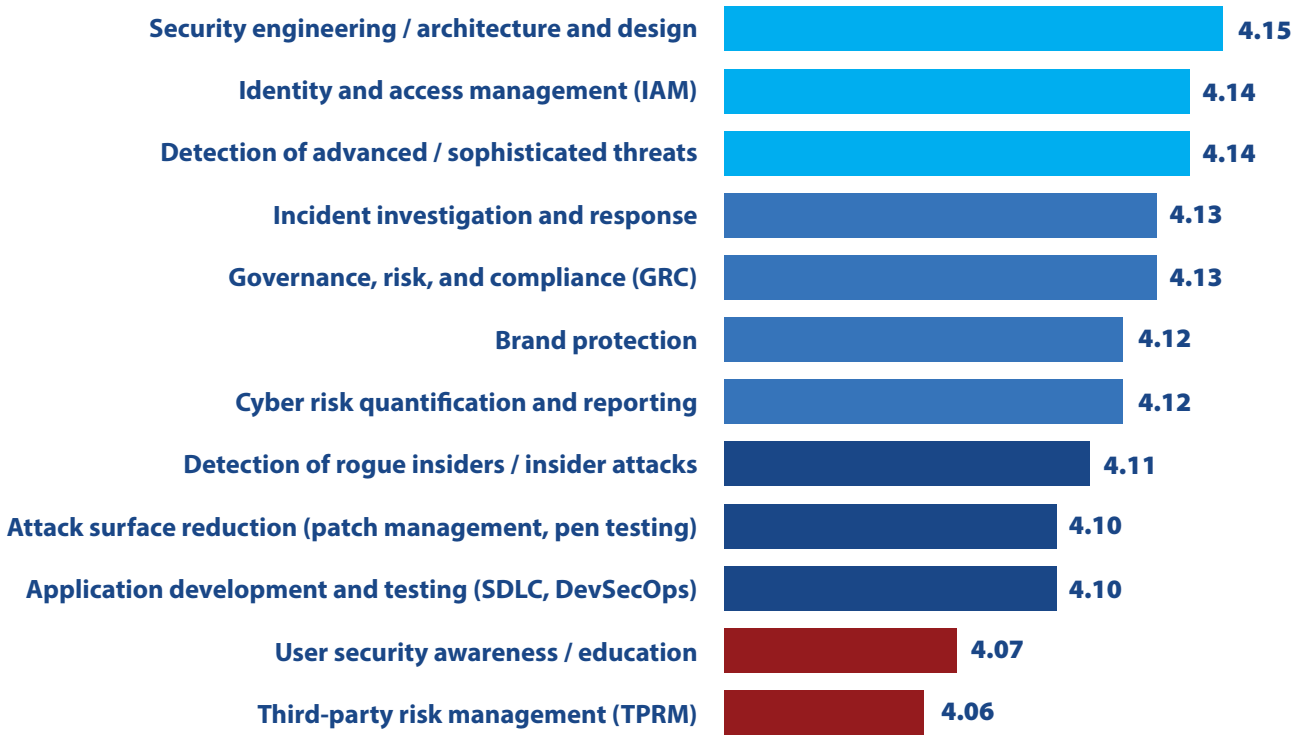

Figure 10: Perceived adequacy of security capabilities by functional area.

We also asked respondents to rate the adequacy of their organization's capabilities (in terms of people and processes) across 12 functional areas of IT security (see Figure 10).

Not surprisingly, respondents are most confident about the functional areas that are the most mature and/or have received the most attention and funding over the past few years. Those are: "Security engineering/architecture and design" (rated 4.15 on a scale of 1 to 5 with 5 highest), "Identity and access management (IAM)" (4.14), "Detection of advanced/sophisticated threats" (4.14%), "Incident investigation and response" (4.13%), and "Governance, Risk, and Compliance (GRC)" (4.13%).

Things get a more interesting a little farther down the list.

"Detection of rogue insiders/insider attacks" remains an area of concern (4.11), despite the fact that theft and disruption by insiders have been a massive problem since the invention of commerce. Why haven't organizations put more resources into stamping out these threats?

Section 1: Current Security Posture

Probably because it has been hard to distinguish between legitimate and malicious actions by employees and because security teams are hyper conscious of the personal and organizational consequences of mistakenly blocking legitimate activities. But that is exactly the kind of challenge that AI is best at addressing. AI can sort through huge volumes of data to distinguish between behaviors that are normal and those that are anomalous and have been associated with rogue activity in the past. And it looks like that may be happening. The rating for capabilities to detect rogue insiders jumped from 3.97 in the last survey to 4.11 in this one. That gain of 0.14 was the largest increase of any of the responses to this question.

Security professionals gave their organizations even lower ratings for "Attack surface reduction (patch management, pen testing) (4.10%), "Application development and testing (SDLC, DevSecOps)" (4.10%), "User security awareness/education" (4.07%), and "Third-party risk management (TPRM)" (4.06%).

The fact that organizations have the least confidence in their capabilities for user security awareness and supply chain security doesn't mean they are ignoring these areas completely. Rather, these functions mostly involve changing people's behavior, and cybersecurity groups are generally much more comfortable with technology than psychology.

Unfortunately, many security groups view programs for user security awareness and supply chain security as *useful,* or even *important,* but not as *urgent*. We think that is a mistake. To refer to our previous topic, threat actors recognize that people (both at targeted enterprises and at third parties that work with them) represent gaps in our technology-based security armor and are putting more and more effort into exploiting them. Failure to treat these areas with urgency gives the bad guys a big running start toward the center of our digital estates.

"Unfortunately, many security groups view programs for user security awareness and supply chain security as *useful,* or even *important,* but not as *urgent*. We think that is a mistake... Not to treat these areas with urgency is to give the bad guys a running head start toward the center of our digital estates."

Section 2: Perceptions and Concerns

Concern for Cyberthreats

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

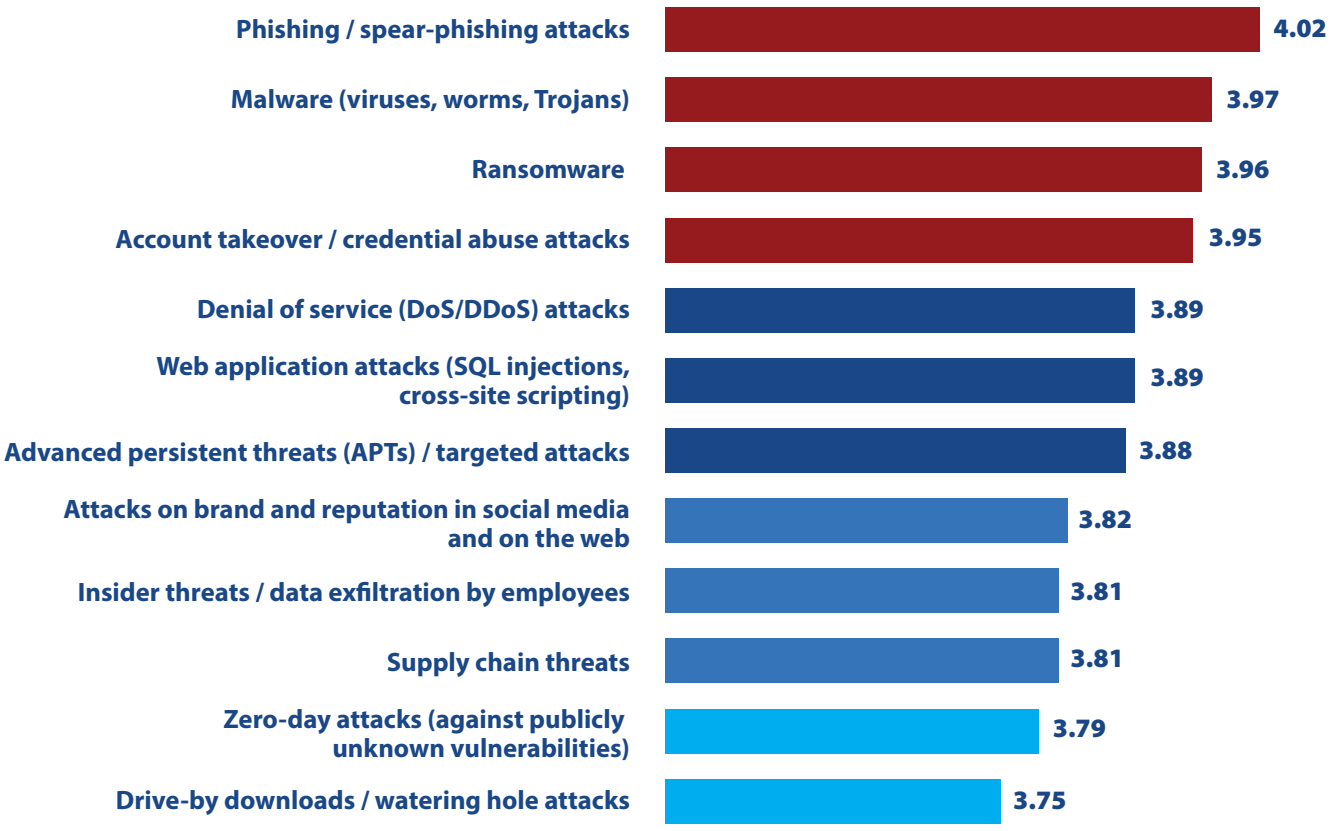

Figure 11: Relative concern for cyberthreats.

With all the types of cyberthreats out there, it's worth knowing which ones are the biggest concerns for cybersecurity professionals.

For the past 10 years the distinction of being the number one concern has gone to malware. But this year we have a new top dog, or should we say a new nemesis: "Phishing/spear-phishing attacks," rated at 4.02 on a scale of 1 to 5 (see Figure 11).

Phishing/spear-phishing has been steadily climbing up the list, from fourth place in the 2022 CDR, to third place in the 2023 edition, to second place in the 2024 and 2025 surveys, to number one now. Why? First, because phishing is becoming an element in more and more types of attacks. Second, because generative AI is making it easier for threat actors to produce perfectly crafted

Section 2: Perceptions and Concerns

emails. (In the 2024 CDR we suggested that bad grammar in a message was a tip-off that it might be a phishing email, whereas today, perfect grammar may be the tip-off.)

Phishing campaigns allow threat actors to implant malware on endpoints to gain footholds on networks. They send people to fake forms on counterfeit websites to capture credentials. They trick employees into transferring information or funds to external systems and taking actions that compromise their organization's defenses. And as discussed earlier, security teams that strengthen technical defenses every year don't always feel a strong sense of urgency to defeat social engineering.

Of course, "Malware (viruses, works, Trojans)" is still very much a threat. It only dropped to second position on the list, with a score of 3.97.

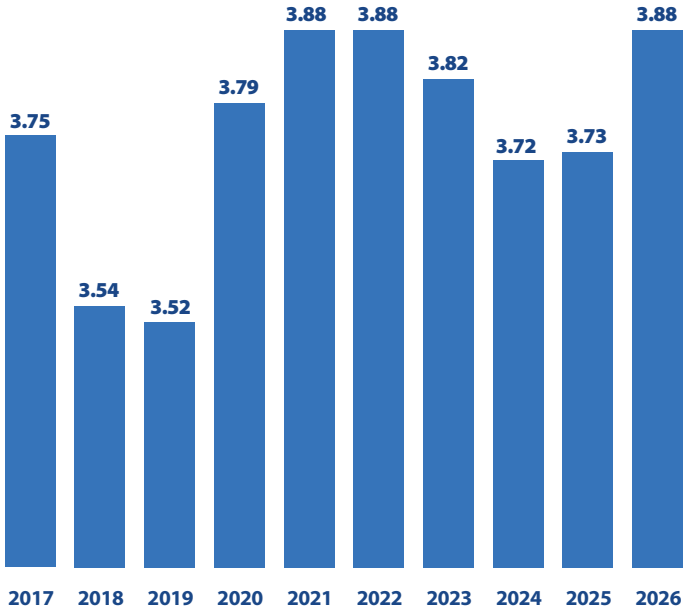

Figure 12: Threat Concern Index, depicting overall concern for cyberthreats.

"This year we have a new top dog, or should we say a new nemesis: 'Phishing/spear-phishing attacks,' rated at 4.02 on a scale of 1 to 5."

The next three most concerning cyberthreats remained in the same position as in the last survey: "Ransomware" (3.96%), "Account takeover/credential abuse attacks" (3.95%), and "Denial of service (DOS/DDOS) attacks" (3.89%).

The next two switched places, with "Web application attacks (SQL injections, cross-site scripting" (3.89%) ending just a smidgen above "Advanced persistent threats (APTs)/targeted attacks" (3.88).

But although the relative rankings of these cyberthreats have been stable for the most part, the level of concern increased from the previous survey for every one of them. That across-the-board increase is reflected in the jump in CyberEdge's Threat Concern Index, the average of the ratings for all the responses in this question. As shown in Figure 12, the index climbed from 3.73 in the 2025 CDR to 3.88 in this one, and is tied with the peak years of 2021 and 2022.

The driving factors include challenges such as low security awareness among employees, a shortage of skilled cybersecurity personnel, too much data to analyze, and AI helping threat actors increase the volume and sophistication of their campaigns. These and other barriers to establishing effective defenses will be discussed on pages 21-22.

Section 2: Perceptions and Concerns

Responding to Ransomware

If victimized by ransomware in the past 12 months, did your organization pay a ransom to recover data?

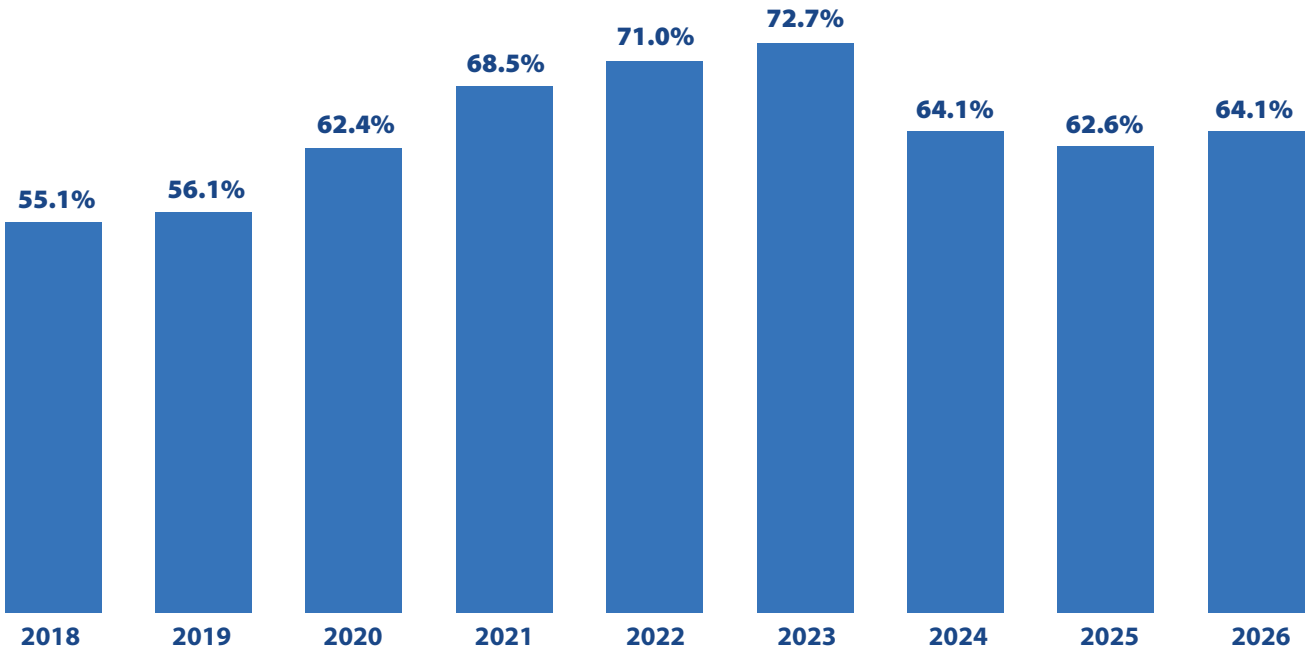

Figure 13: Percentage of organizations victimized by ransomware.

The percentage of organizations affected by ransomware climbed steadily from the 2108 CDR through the 2023 edition, peaking at 72.7%. But the number of victimized organizations fell substantially in 2024, to 64.1%, and has remained essentially unchanged since (see Figure 13).

Why the drop? Ransomware gangs, which had enjoyed years of growth and steady profits, began to encounter headwinds. Law enforcement agencies around the world investigated and took down some of the leading gangs, along with groups providing supporting infrastructure for what has been called "Ransomware as a Service." Governments put pressure on victimized enterprises not to pay ransoms. And organizations invested in better backups and more security tools, which undermined efforts of less-sophisticated ransomware groups.

Why the plateau, rather than a continuing decline? Better-resourced gangs found profitable new targets, particularly mid-sized organizations in industries like healthcare, business services, and local government, where there were often gaps in defenses and disruptions could be extremely costly (and in healthcare, even life threatening). Also, new players were joining the ransomware game (notably state-sponsored hacking groups in North Korea and elsewhere), and the majority of ransomware groups added extortion on top of (and sometimes instead of) the threat of lost data.

Section 2: Perceptions and Concerns

But despite the reappearance here of Saint Offset (see page 8), this year saw major changes in how victimized organizations responded. Specifically, the percentage of organizations affected by ransomware that paid ransoms skyrocketed 14.3%, from 40.7% to 55.0% in the past year (see Figure 14).

Why this abrupt reversal of the previous trend of declining payment rates? Our data shows that the propensity to pay the ransom jumped in specific industries, notably healthcare, retail, and manufacturing, and in companies with between 500 and 10,000 employees.

We note two commonalities across these groups that make them particularly promising targets:

- Disruption to operations can have a potentially disastrous impact on profits that may be unsustainable for small and medium-sized organizations with limited resources.
- Many have expanding attack surfaces with many more cloud-hosted software workloads and internet-connected things, including medical devices, mobile devices, kiosks, sensors, cameras, and operational and industrial systems (which, as we saw on page 12, have among the weakest security postures).

Also, ransomware gangs may have decided that it is good business to ensure that payers can actually recover their data, and are trying to supply better decryptors. Supporting this hypothesis is the fact that the percentage of organizations that paid ransoms and subsequently recovered their data rose substantially over the last year, from 54.3% to 60.8% (see Figure 15).

It is also worth noting that the threat of ransomware is not receding. The size of ransomware payments can jump around quite a bit from quarter to quarter because of a few major incidents, but the trend continues steadily upward, as shown by data from Coveware pictured in Figure 16.

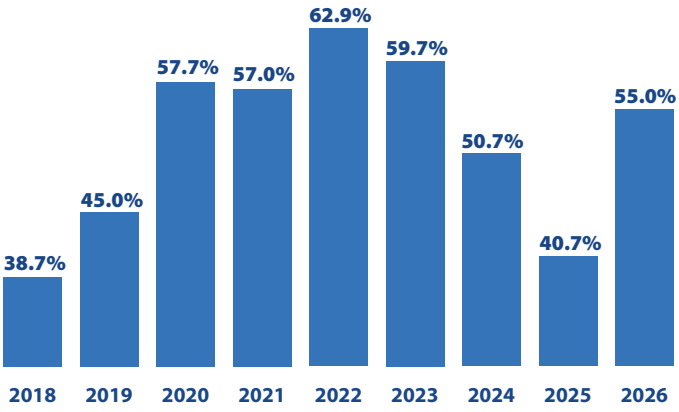

Figure 14: Percentage of victimized organizations paying ransoms.

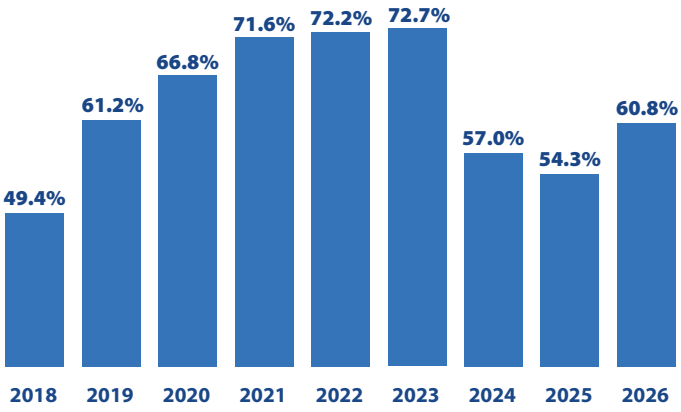

Figure 15: Percentage of ransom payers that recovered data.

Section 2: Perceptions and Concerns

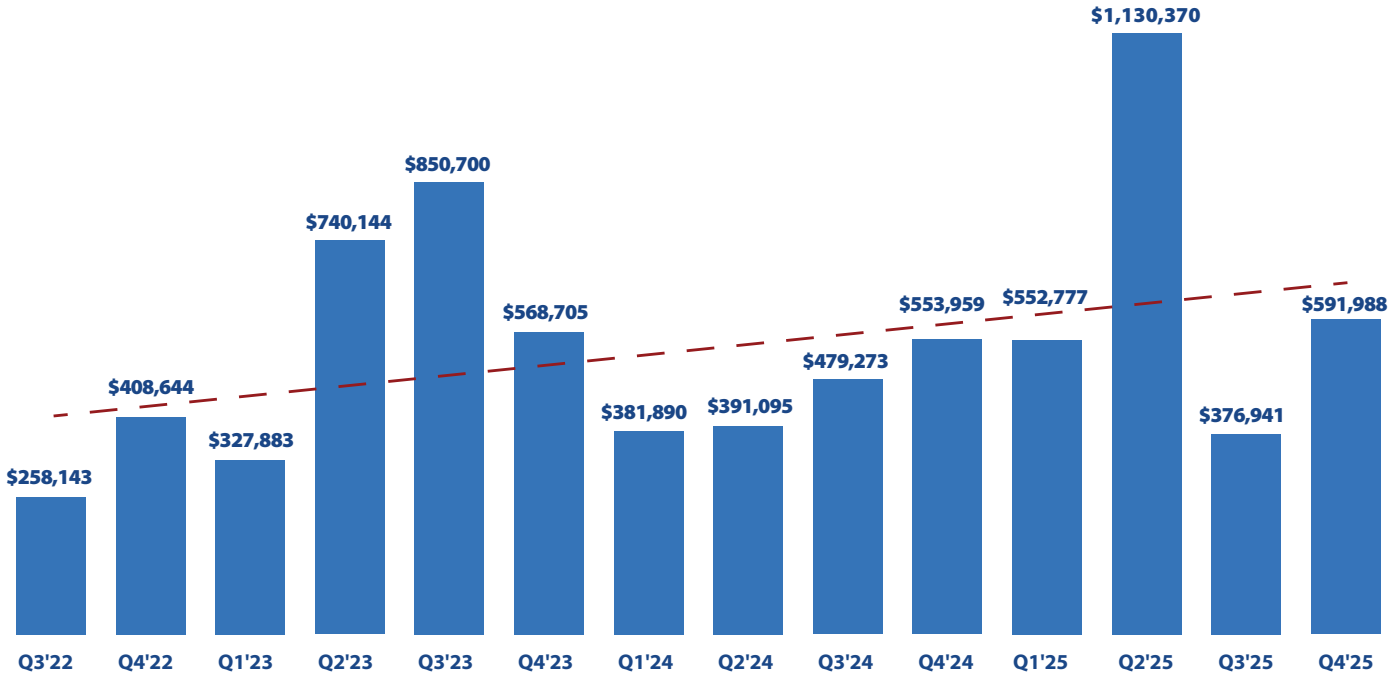

Figure 16: Average ransom payments by quarter (data source: Coveware Quarterly Ransomware Reports).

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.

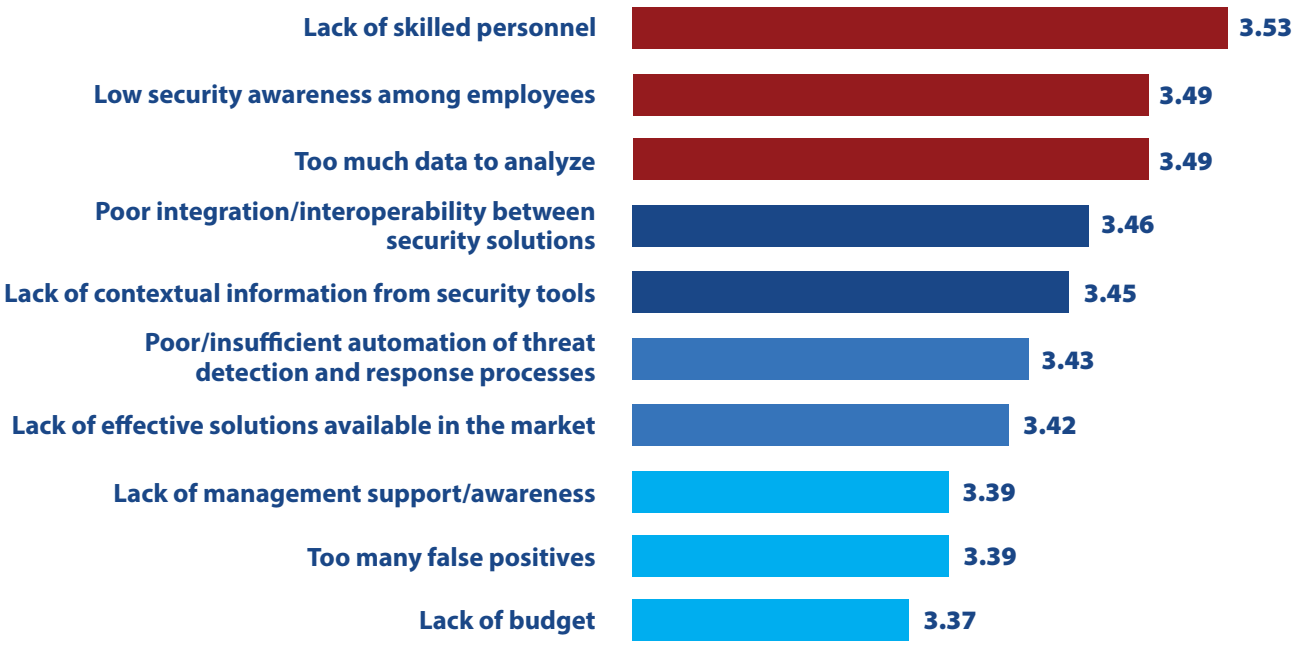

Figure 17: Inhibitors to establishing effective defenses against cyberthreats.

On the key question of what factors are inhibiting organizations from adequately defending themselves against cyberthreats, not much changed from last year. However, we think we may be on the brink of some big changes over the next year or two, mostly driven by AI.

First, looking back, we find exactly the same issues that were at the top of the list last year. They are: "Lack of skilled personnel" (3.53 on a scale of 1 to 5), "Low security awareness among employees" (3.49), "Too much data to analyze" (also 3.49), "Poor integration/interoperability between security solutions" (3.46), and "Lack of contextual information from security tools" (3.45) (see Figure 17).

At the bottom of the list, where the least troublesome factors reside, it is encouraging to see that "Lack of management support/awareness" (3.39) and "Lack of budget" (3.37) continue to be (relative) non-problems. This finding is consistent with other data in this survey. For example, security budgets have been rising and are anticipated to show a healthy increase this year (see pages 35-36). Also, IT security leaders are engaging more than ever with top executives and boards of directors (see pages 53-54). Generally speaking, management is standing behind security teams and securing the funding they need.

Section 2: Perceptions and Concerns

The impression of year-to-year stability is reinforced by the steadiness of CyberEdge's Security Concern Index, an average of the scores of the responses in this question, which is essentially unchanged from the two previous surveys (see Figure 18).

So why do we think big changes are coming? Mostly because AI is likely to have a major impact on some of them in the very near future.

For example, a shortage of experienced cybersecurity professionals has been rated the #1 or #2 barrier to effective defense for the last nine editions of the CDR. AI could potentially alter that situation significantly by:

- Automating routine tasks so security professionals have more time to work on high-value tasks and projects
- Providing data, analysis, and recommendations that effectively "upskill" junior and mid-level analysts, incident responders, threat hunters, etc., so they can work faster and make better decisions with a much shorter learning curve

Security teams could get more work done, at a higher level of effectiveness, without needing to hire more people or compete for hard-to-get specialists.

Of course, it's not that simple. There is a significant risk that some organizations will overestimate the effectiveness of today's AI tools and underestimate the challenges of using them safely (see pages 29-30 for a discussion of some of those challenges). If security staffs become too lean as a result, stress and overwork could decrease effectiveness and even lead to increased turnover. We'll have to see how that plays out.

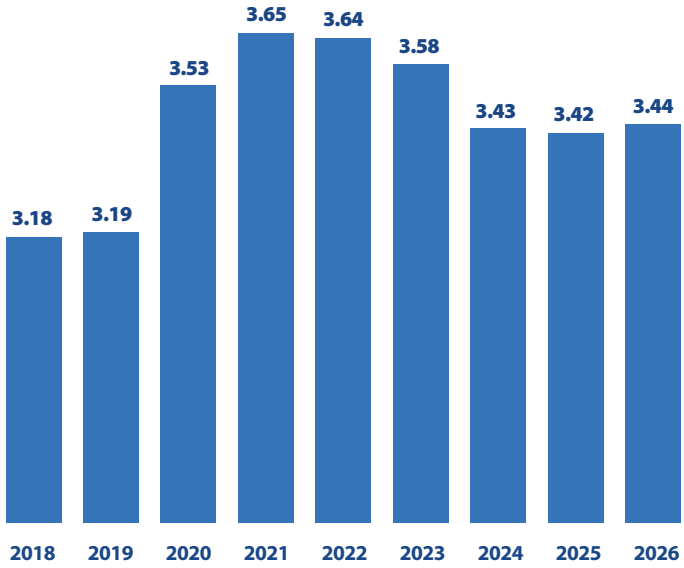

Figure 18: The Security Concern Index, representing the average rating of security inhibitors.

Several other responses to this question will also be affected by the increasing use of AI-enabled security tools, which are already being applied to analyze large volumes of security data and events, automatically gather and organize contextual information from many sources, and automate attack detection and response (see pages 49-50 for details on the deployment of AI for a variety of security tasks).

Our survey shows that changes in these areas are almost inevitable and probably coming very soon. As you can see on pages 33-34, 80% of survey respondents believe AI will reduce the number of people needed to perform their current role, and more than half of those think the impact will start within one or two years.

Section 2: Perceptions and Concerns

Concerns About Identity Security Risks

What are your biggest concerns about identity security risks? (Select up to five.)

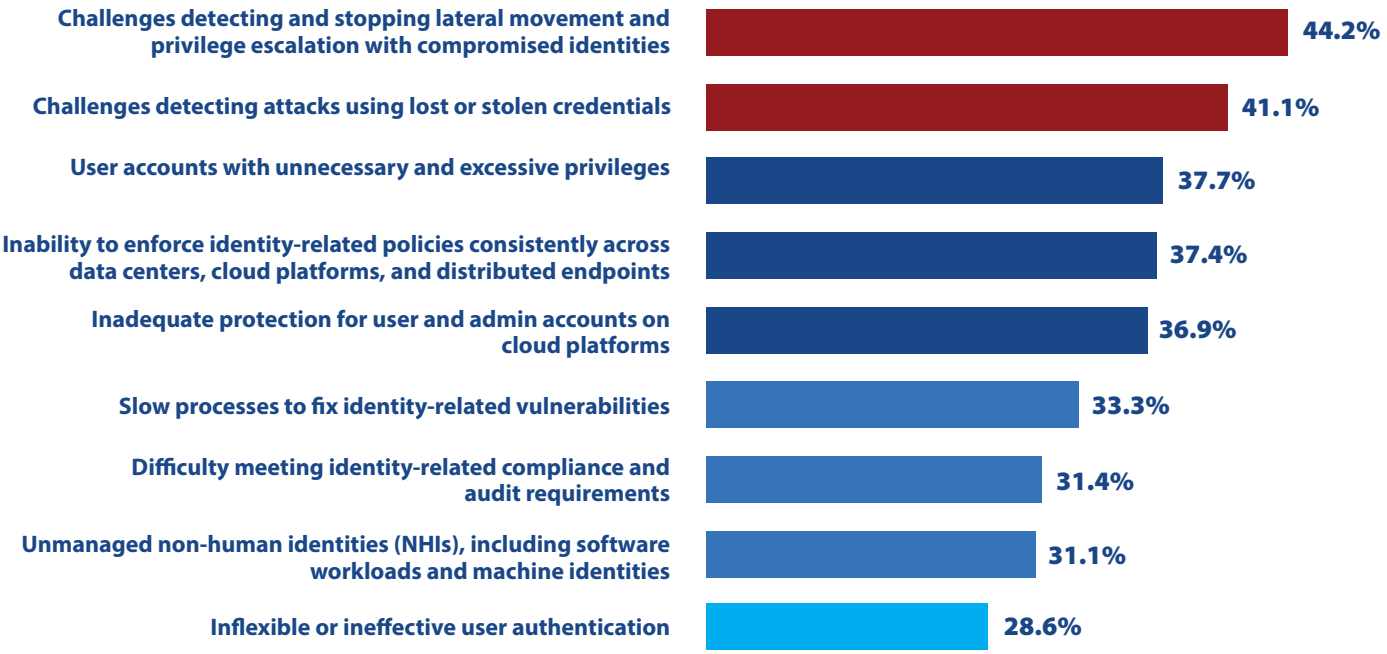

Figure 19: Most-concerning identity security risks.

This is a new question in the CDR. Identity security has been a core discipline of cybersecurity for many years. However, in the past, security teams often viewed it largely as a realm for administrative types to define and redefine roles and their appropriate access rights and for help desk staffs to endlessly reset passwords.

But times have changed! Identity security has grown in importance to become a critical discipline that interacts with almost every cybersecurity domain.

Factors that have moved identity security to center stage include imperatives to:

- Manage identities across a wider range of environments, including corporate data centers, multiple cloud platforms, and hosted software services
- Create and control identities for whole new classes of entities beyond people, sometimes called non-human identities, or NHIs. These include dynamic software workloads, IoT devices, industrial and operational systems, and most recently, AI agents
- Use identities and associated privileges to drive advanced access control and authentication technologies, including multi-factor authentication

Section 2: Perceptions and Concerns

One reason to assign an identity and permissions to a printer, a software workload, or an AI agent is to make it easier to manage and protect those entities. But an even more important goal of identity security is *to protect everything else from unauthorized access by those entities and millions more like them.* You don't want a badly programmed printer to reach out and take down a critical network controller, or a software workload compromised by a threat actor to access an entire cloud environment, or an autonomous AI agent to manipulate an unlimited number of other agents and applications. To prevent those behaviors, every NHI needs to be assigned just the access rights needed to do its job.

A maxim on the dark web goes: "Why break down the door if you can steal the key?" And indeed, as shown in Figure 19, our respondents' biggest concerns related to identity security involve limiting the potential damage from stolen credentials and keys. "Challenges detecting and stopping lateral movement and privilege escalation with compromised identities" was selected as one of the top five identity security concerns by 44.2%, and "Challenges detecting attacks using lost or stolen credentials" was picked by 41.1%.

The next two greatest concerns in this area involve reducing the "blast radius" (the potential extent of damage) from compromised identities. Respondents highlighted the need to minimize "User accounts with unnecessary and excessive privileges" (37.7%) so that, for example, the credentials of a system admin for one application couldn't be used to access data in other applications. They also lamented their "Inability to enforce identity-related policies consistently across data centers, cloud platforms, and distributed endpoints" (37.4%). That concern is related to situations where policies correctly limiting the permissions of a user or NHI in one area (say, in the corporate data center) are not applied in others (such as applications hosted on web platforms).

Respondents also indicate that "Inadequate protection for user and admin accounts on cloud platforms" is a major challenge for many of them (36.9%).

Our data confirms that identity security is now a top-of-mind topic now for security teams. No less than 96.6% of respondents indicated a concern about one or more of the challenges on our list. Only 3.4% stated their organization had none of these concerns (see Figure 20).

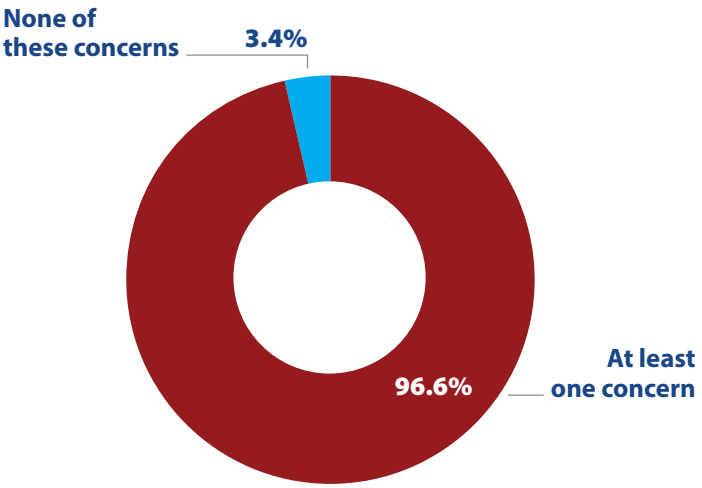

Figure 20: Organizations concerned about one or more identity security risks.

"You don't want a badly programmed printer to reach out and take down a critical network controller, or a software workload compromised by a threat actor to access an entire cloud environment, or an autonomous AI agent to manipulate an unlimited number of other agents and applications."

Section 2: Perceptions and Concerns

Benefits of IT Security Professional Certifications

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

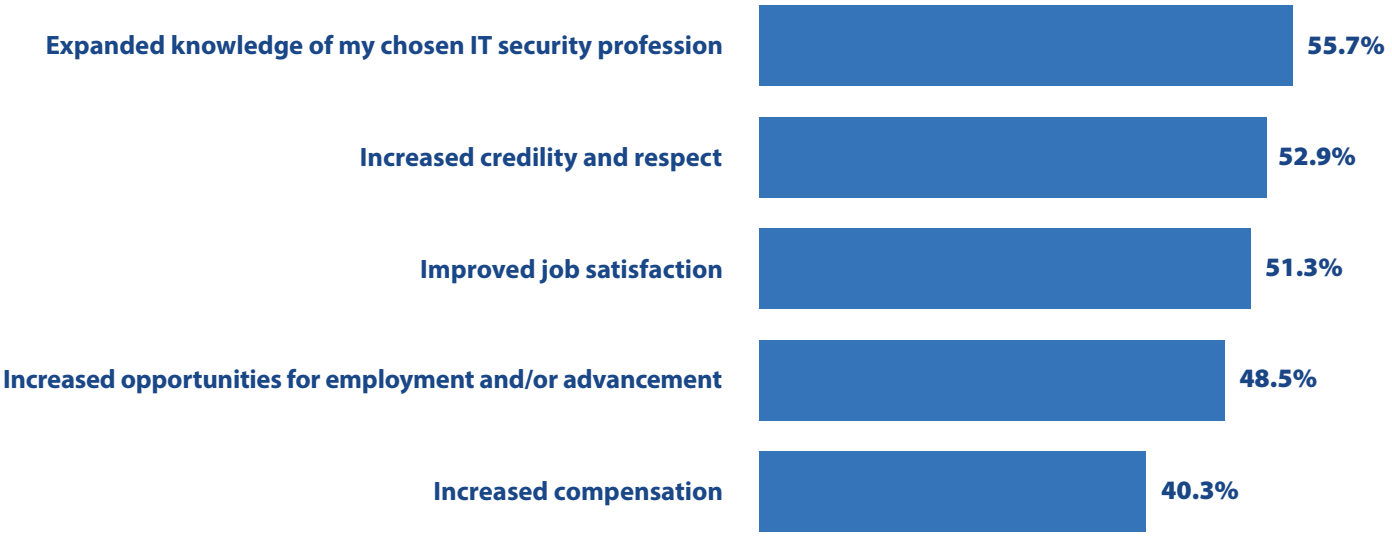

Figure 21: Benefits experienced as a result of achieving one or more IT security professional certifications.

Money isn't everything. Sometimes the knowledge that you are doing good work and earning the respect of your peers is more important. At least that's what our data says (see Figure 21).

When asked about reasons for obtaining IT security professional certifications, respondents most often selected "Expanded knowledge of my chosen IT security profession" (55.7%). Many of us are cynics, but most of us really do want to do a good job. In cybersecurity, keeping up skills is a key part of that.

During his Oscar acceptance speech, Cary Grant said: "Probably no greater honor can come to any man than the respect of his colleagues." Many security professionals feel the same way.

"Increased credibility and respect" was highlighted as a motivation by 52.9% of the survey respondents. "Improved job satisfaction," a feeling that often that comes with the respect of colleagues, wasn't far behind; it was cited by 51.3%.

"Many of us are cynics, but most of us really do want to do a good job. In cybersecurity, keeping up skills is a key part of that."

Section 2: Perceptions and Concerns

By the way, scientific research confirms the importance of respect. A post on the website of the Association for Psychological Science states: "Respect Matters More Than Money for Happiness in Life." You can view it here.

Of course, material motivations do play a part in decisions to obtain professional certifications. "Increased opportunities for employment and/or advancement" was selected by 48.5% of the respondents, and "Increased compensation" by 40.3%.

These priorities have been very stable. When we asked the same question in the 2020 and 2023 CDRs, six and three years ago, the order of the responses was exactly the same.

A final finding: pretty much everyone perceives that IT professional security certifications have significant value. Almost 96% of respondents already have one or more, and of the remaining 4%, two-thirds plan to get one (see Figure 22).

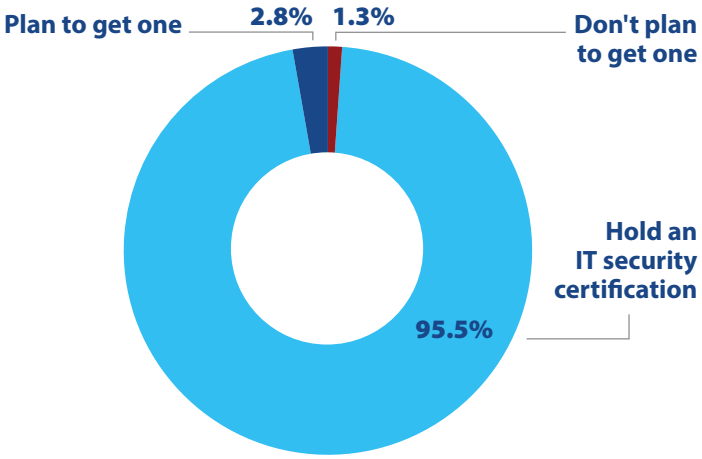

Figure 22: Respondents who hold an IT security professional certification.

Section 2: Perceptions and Concerns

Most Concerning AI-enabled Threats

What AI-enabled threats are most concerning for your organization? (Select up to four.)

Figure 23: Most-concerning AI-enabled threats.

This is one of four new AI-related questions that we added to the 2026 CDR. Experts have been talking for a while now about potential AI-enabled threats, but this is one of the first survey questions to collect data on which of these threats most concern security professionals.

Almost half (45.5%) of respondents cite "Higher volumes of adaptive and evasive malware" as one of their top four concerns in this area (see Figure 23). Adaptive AI-enabled malware learns from the target organization's environment in real time and creates new strategies to prevent being recognized as malicious. For example, if it spots the presence of certain security tools, it might modify its own code so its signature won't match any in threat signature databases and its behaviors will differ from patterns associated with previous attacks. Evasive malware uses techniques like fileless execution and delayed activation to fool conventional anti-malware tools.

Second on this list is "Improved attacks on passwords (e.g., brute force attacks)" (43.1%). Exploiting weak passwords is already a tried-and-true hacker approach for breaking into networks, but now some of the techniques can be supercharged by AI.

Section 2: Perceptions and Concerns

AI-enabled tools test possible passwords faster, home in on the most likely weak passwords for given types of users, and can potentially automate gathering of personal data from social media accounts that users might be tempted to include in passwords.

(A thought: maybe it's a good time to remind users not to incorporate into passwords any personal data that might be available on social media. That includes family birthdays, names of relatives and pets, current and past addresses, favorite sports team, favorite Disney princess, favorite character from the MCU, lyrics from Bad Bunny, Taylor Swift, Drake, or "the Boss," etc.)

In fact, AI can use information from social media, corporate websites, and other online sources not only to crack passwords, but also to target employees with access to high-value information and fool them into disclosing data or credentials. That's why organizations are worried about "Improved targeting of employees based on data scraping from social media and corporate websites" (39.7%) and "More effective phishing emails" (also 39.7%).

Just as AI can automate and accelerate cybersecurity workflows for tasks such as vulnerability detection, triage, and incident investigation, it can automate threat actor processes, increasing concerns about "Accelerated vulnerability discovery and reconnaissance by threat actors" (38.7%) and "Accelerated automation and orchestration of multi-step attacks" (37.4%).

"Deepfake voice and video cloning for impersonation" came in at the bottom of this list, with a rating of 37.1%. That's probably because deepfakes used for cyberattacks are still relatively rare. However, there have been several serious, successful, and very visible attacks using deepfakes (look up the $25 million Arup incident, for example, or the North Korean remote IT worker schemes). We anticipate their numbers will ramp up considerably this year.

"Maybe it's a good time to remind users not to incorporate into passwords any personal data that might be available on social media... family birthdays, names of relatives and pets, current and past addresses, favorite sports team, favorite Disney princess, favorite character from the MCU, etc."

Section 2: Perceptions and Concerns

Challenges Creating Applications with AI Capabilities

On a scale of 1 to 5, with 5 being major challenge, rate how seriously each challenge is inhibiting your organization from creating custom applications that incorporate AI capabilities?

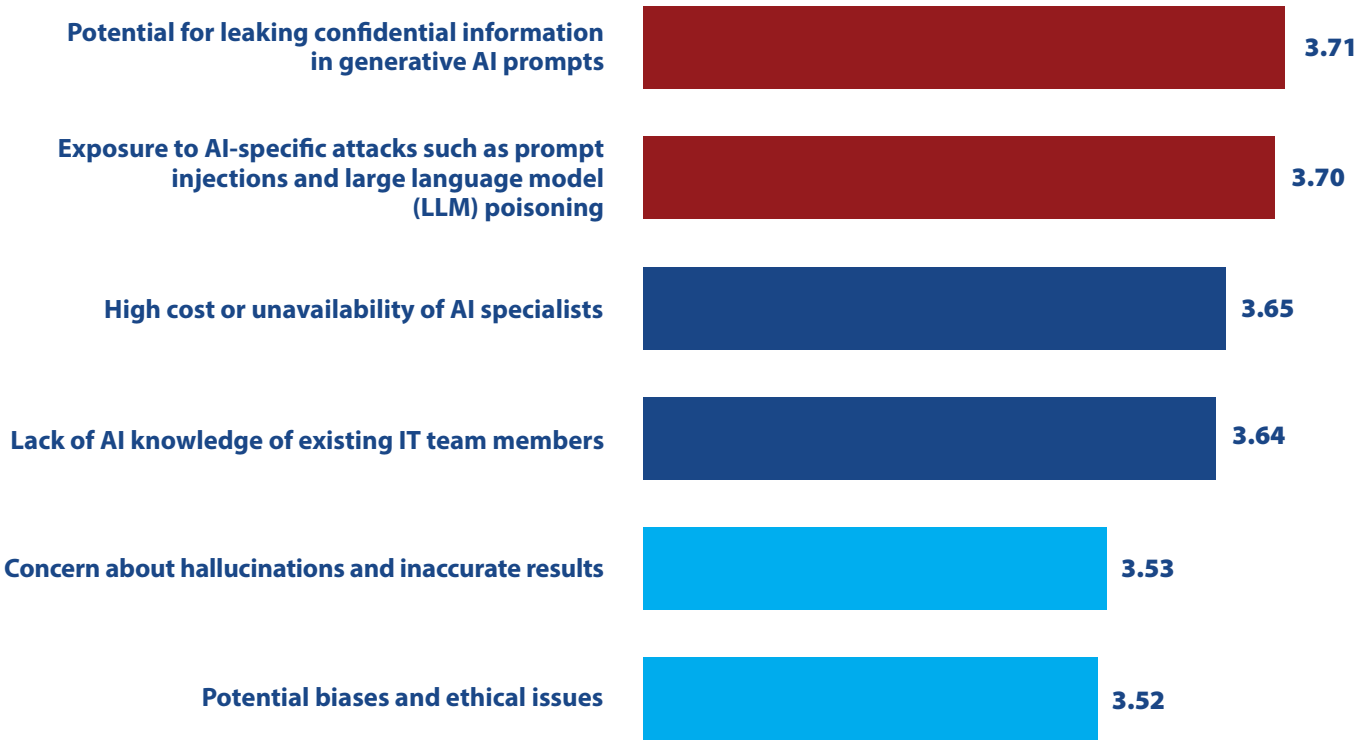

Figure 24: Challenges inhibiting the creation of custom applications that incorporate AI

As organizations have become more familiar with AI and large language models (LLMs), they have begun to develop their own custom applications with AI capabilities. However, groups deploying AI-enabled apps face a number of novel challenges. Which challenges do security and software teams think are doing the most to slow down the deployment of these applications? We added this question to the survey to find out.

The challenges we asked respondents to rate fell into three categories:

- Cybersecurity issues that could result in confidential data being captured or manipulated by threat actors
- Difficulty finding personnel with the right skill sets to develop secure AI-enabled applications
- Characteristics of AI systems that could produce inaccurate or undesirable results

Section 2: Perceptions and Concerns

Perhaps not surprisingly for a survey of security professionals, the two challenges related to cybersecurity issues are seen as the most important.

"Potential for leaking confidential information in generative AI prompts" received the highest score, 3.71 on a scale of 1 to 5 (see Figure 24). If a custom application sends prompts to public generative AI systems, outsiders may be able to see those prompts, including confidential information contained in them. This is a novel kind of data leakage, and few organizations have any experience in how to monitor or control it.

An almost equal concern is "Exposure to AI-specific attacks such as prompt injections and large language model (LLM) poisoning (3.70)." If a custom application uses an internal LLM or tool and allows prompts from outsiders (customers, researchers, business partners, etc.), threat actors may be able to submit prompts that disable the AI system's guardrails and controls, allowing the bad guys to extract confidential data, disable the application, and potentially navigate to other information assets. LLM poisoning attacks involve planting incorrect or biased information into a data source used to train a model. This can cause the AI-enabled application to produce inaccurate or skewed results.

The next two challenges on the list, "High cost or unavailability of AI specialists" and "Lack of AI knowledge of existing IT team members" received scores of 3.65 and 3.64, respectively. Giant AI vendors such as Microsoft, OpenAI, Alphabet (parent company of Google), Amazon, and Apple are giving such astronomical compensation packages to AI experts that other enterprises have little hope of recruiting them. And of course, it will take time for security and software engineering teams to upskill their existing staff. It's likely that talent acquisition will continue to be a tough job for some time. Of course, organizations can obtain *some* valuable AI skills through new hires. The next topic in this report examines the AI-related experience that organizations want to find in new employees.

The final set of challenges on our list relate to characteristics of AI systems that could produce inaccurate or undesirable results.

Mark Twain supposedly said: "It ain't what you don't know that gets you into trouble. It's what you know for sure that just ain't so." Hallucinations are a huge issue for AI systems, as you probably know. There are techniques for reducing their frequency, but as of today we can't eliminate them completely. That's why a significant number of organizations regard "Concerns about hallucinations and inaccurate results" (3.53) as a barrier to deploying custom applications with AI capabilities.

"Potential biases and ethical issues" (3.52) is at the bottom of the list, but is still a factor. Most prominent among these concerns are racial and gender biases embedded in the data sources AI models use for learning, which then manifest themselves in the systems' output. Potential problems include not only the perpetuation of offensive stereotypes, but also unfair hiring and compensation decisions, discriminatory treatment of certain groups, and seriously flawed advice on medical, legal, financial, and personal matters. Other troublesome issues include privacy violations, copyright infringement, and lack of accountability (since most AI systems are not transparent about their sources and how they reach conclusions).

We are confident that these challenges can be resolved, or at least greatly mitigated, but it will take time to work out all the ramifications.

Section 2: Perceptions and Concerns

AI-related Skills Sought in IT Security New Hires

What AI-related experience and skills are most important when seeking new hires for IT security positions? (Select up to four.)

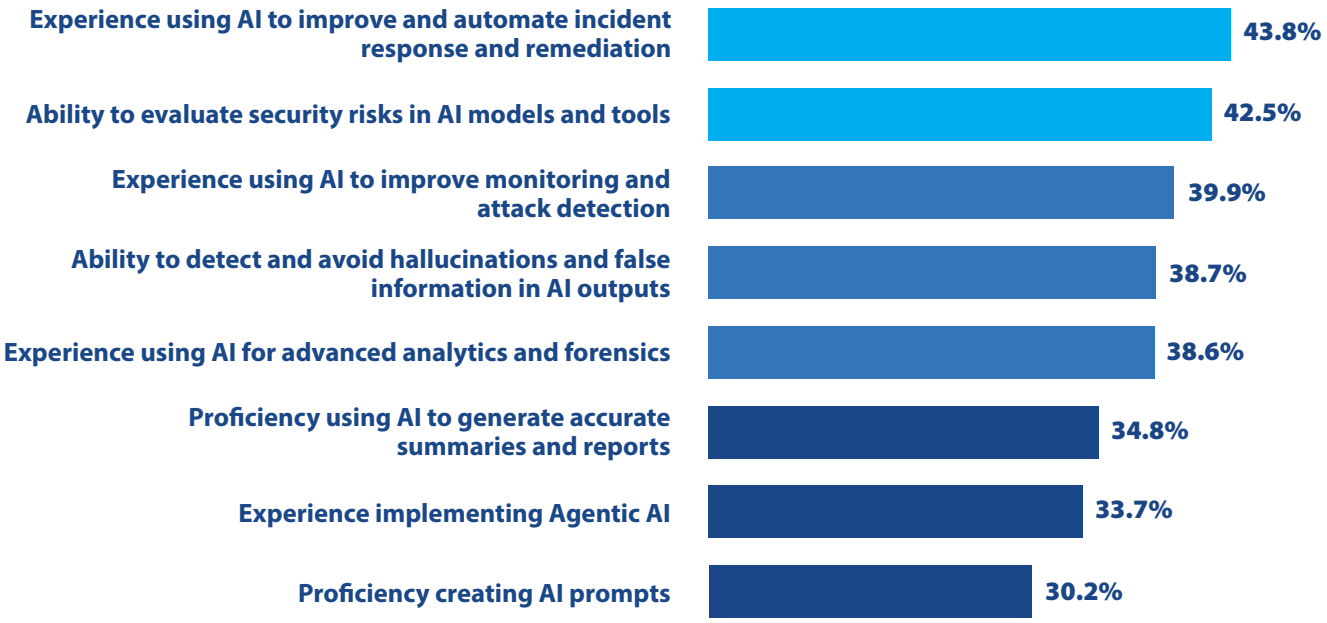

Figure 25: Most important AI skills when seeking IT security new hires.

The question of what AI-related skills organizations need is a little more complicated than it might seem at first glance. Security teams need members with AI knowledge for three different purposes:

- To use AI capabilities to improve security workflows and processes
- To understand how threat actors are using AI and how AI can be employed to counter them
- To mitigate or eliminate security risks in internally developed AI-enabled applications

That means security teams need a lot of AI-related skills. So, we added a new question to this survey asking what skills and experience they are looking for in new hires.

The #1, #3, and #6 items on their wish list are related to using AI to improve security workflows and processes. "Experience using AI to improve and automate incident response and remediation" was selected as one of the top four areas by 43.8% of the respondents. "Experience using AI to improve monitoring and attack detection" was selected by 39.9%. "Proficiency using AI to generate accurate summaries and reports" was chosen by 34.8% (see Figure 25). A preference for experience in these areas is not surprising; security leaders who aren't using AI-related tools to improve their teams' performance are falling down on the job.

Section 2: Perceptions and Concerns

The second and fourth items on the list are skills important to making internally developed AI-enabled applications secure, accurate, and unbiased. "Ability to evaluate security risks in AI models and tools" and "Ability to detect and avoid hallucinations and false information in AI outputs" were chosen by 42.5% and 38.7% of respondents, respectively.

What about skills that would help identify AI-enabled attacks? "Experience using AI for advanced analytics and forensics" was cited by 38.6% of the respondents.

"Proficiency creating AI prompts" was selected least frequently (30.2%). We suspect that is because hiring managers in cybersecurity expect smart cybersecurity professionals to be able to pick up that skill on the job or through self-study, and aren't too concerned about whether new hires bring experience in that area.

One clear takeaway from this data: all security professionals need to start acquiring AI knowledge and experience so they can start putting AI-related skills on their resumes. The vast majority of organizations (96.8%) are recruiting new hires with at least one of these skills; only 3.2% aren't (see Figure 26).

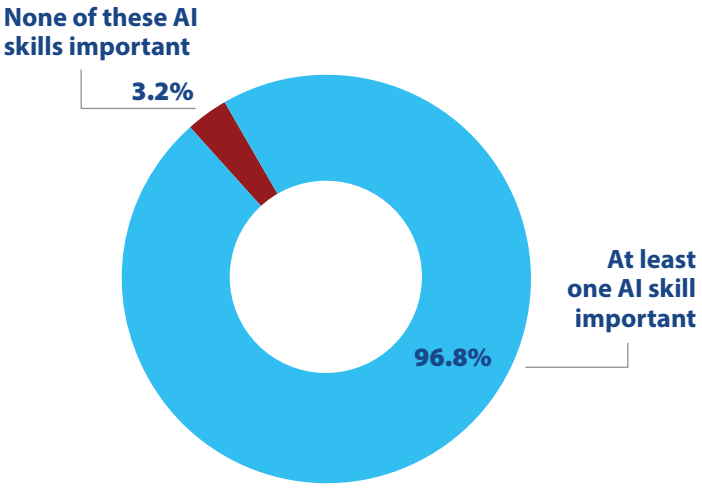

Figure 26: Organizations where at least one AI skill in new hires is important.

Section 2: Perceptions and Concerns

Belief That AI Will Reduce People in IT Security Jobs

Do you believe that AI will significantly reduce the number of people needed to perform your current job role?

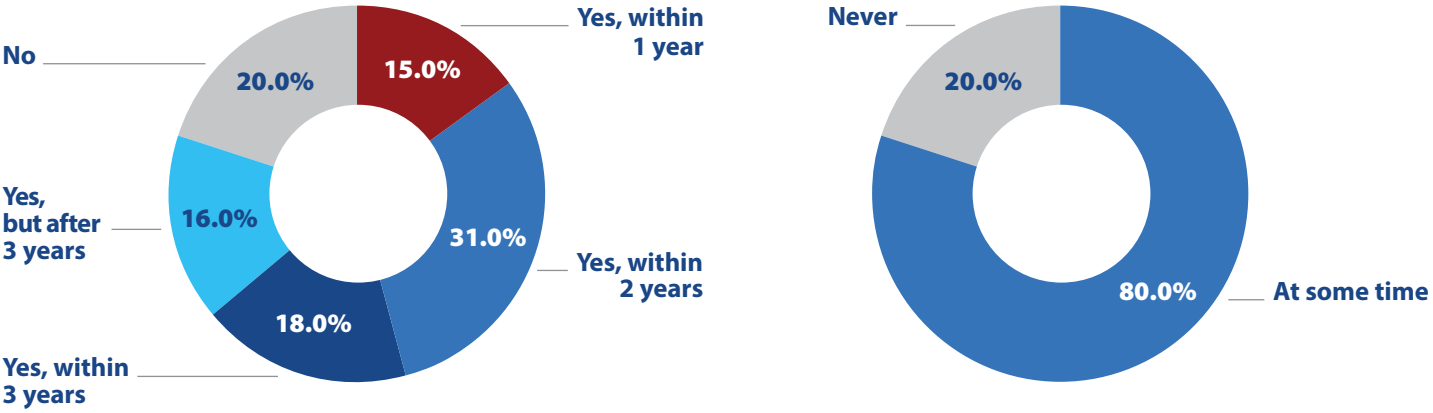

Figure 27: Respondents who believe AI will significantly reduce people needed to perform their current job.

Security professionals (like almost everyone else) are concerned that AI might reduce job opportunities in their areas of expertise. But timing can make a big difference. Do they expect the pressure from AI to start soon or not for years?

When asked when they believe AI will significantly reduce the number of people needed to perform their current role, 15% of the survey respondents predict that hiring in their job category will be affected this year, and another 31% say the effect will be felt between one and two years from now (see the left side of Figure 27). if we define "near term" as within two years, then almost half of the total survey sample (46%) foresees a significant impact in the near term.

How much less pessimistic are the other survey recipients? Well, 18.0% expect the effect to start in two to three years and another 16.0% believe it will happen sometime beyond three years. Only 20% are saying "no, that will never happen."

Another way of looking at these numbers is that no less than 80% of our security professionals that AI *will* have an impact on hiring for their roles at some point, versus only 20% who don't (see the right side of Figure 27).

"Another way of looking at these numbers is that no less than 80% of our security professionals believe that AI *will* have an impact on hiring for their roles at some point, versus only 20% who don't."

Section 2: Perceptions and Concerns

However, the percentage of respondents anticipating near-term impact (within two years) vary quite a bit across countries and industries. For example, more than 50% in Singapore, Spain and the USA expect significant near-term effects, while 37% or less hold that view in China, South Africa, Mexico, Brazil, and Canada (see Figure 28).

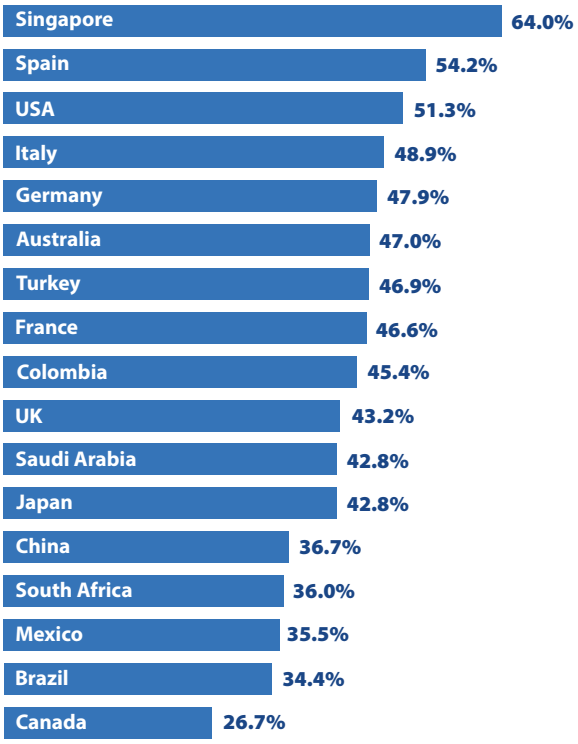

Figure 28: Respondents who believe AI will significantly reduce people needed to perform their current job within two years, by country.

Among the major industries tracked in this survey, security professionals in retail are very concerned about the next two years, while those in government are much less so (see Figure 29).

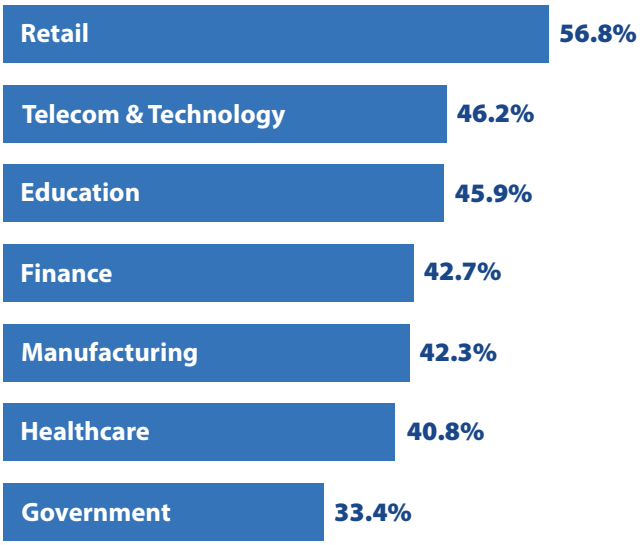

Figure 29: Respondents who believe AI will significantly reduce people needed to perform their current job within two years, by industry.

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 2026?

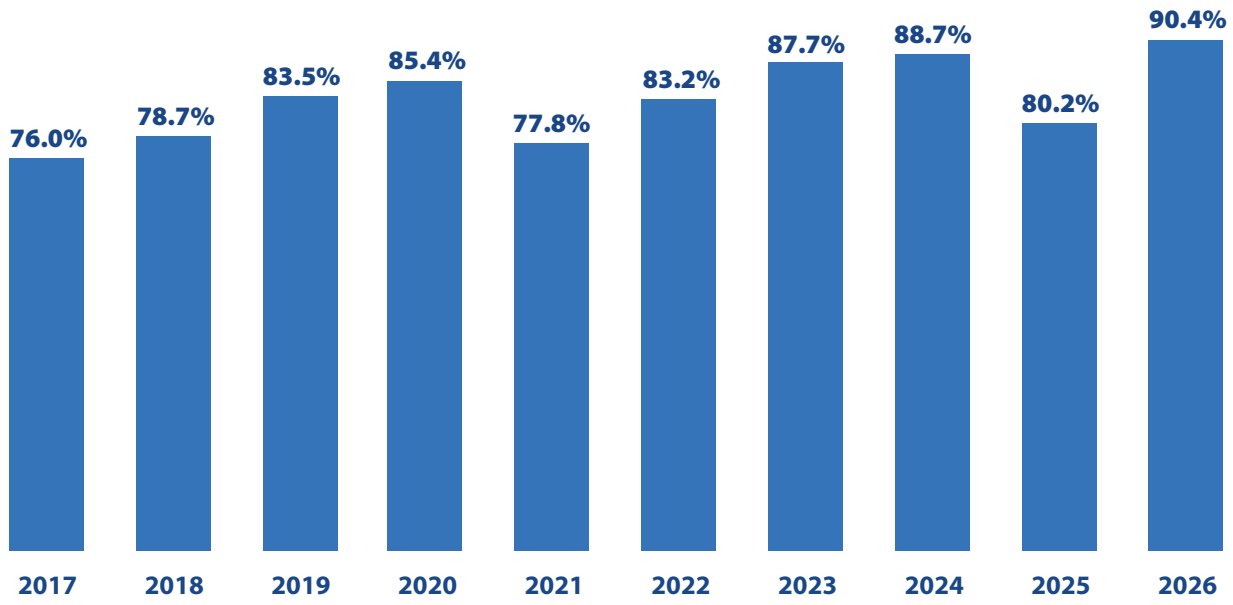

Figure 30: Percentage of organizations with rising IT security budgets.

As we saw on page 21, lack of budget is *not* a major barrier to success for most security teams. And that seems to be true more than ever now. As shown in Figure 30, the percentage of organizations expecting an increase in their IT security budget hit a new record in this survey: 90.4%. After several years of a steadily rising trend, that percentage dipped to 80.2% a year ago, but this year's jump more than made up for that dip.

The strength of budget growth is also underscored by the size of the average expected increase, from 4.3% to 5.6%. This is the second largest expected increase in the history of this survey (see Figure 31).

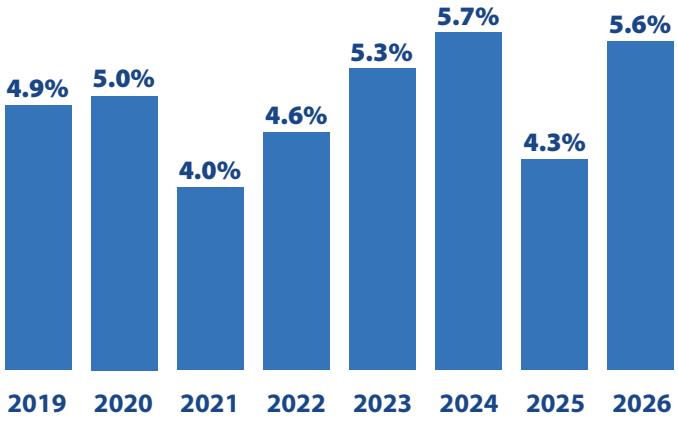

Figure 31: Mean annual increase in IT security budgets.

Section 3: Current and Future Investments

In any year, some enterprises need to cut expenses because of aggressive competition, rising interest rates, falling margins, reduced government spending, reduced consumer spending, reduced business investment, unprecedented tariffs, wars, etc. But the fact that a mere 5% of respondents are expecting a loss of funds this year shows that top executives and boards of directors have decided they must maintain their organization's ability to defend against cyber criminals and other bad actors.

If you have been doing the math, you will have figured out that the remaining 5% of respondents expect their budgets to stay about the same.

Two other interesting findings:

- Well over half (58.4%) of the respondents predicting a budget increase believe it will fall between 5% and 9% (see Figure 32).
- Expected budget increases were very consistent across organizations of all sizes, ranging from 5.3% to 5.8% (see Figure 33).

Finally, what factors do we think have been shaping these expectations about budgets? They appear to include: (a) steady economic growth in most parts of the world (at least in late 2025 and early 2026); (b) increasing realization by top management and boards that security issues can harm their personal reputations and bonuses; and (3) more investment in technologies and staff with AI capabilities.

We should mention, however, that economic and political shocks could cause a major recession that would upend these positive expectations.

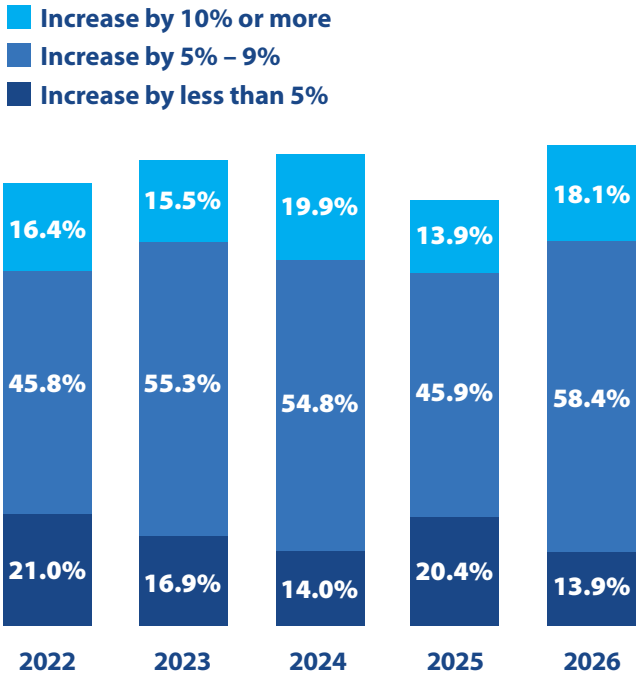

Figure 32: Breakdown of annual increase of IT security budgets (excludes organizations expecting declining or flat budgets).

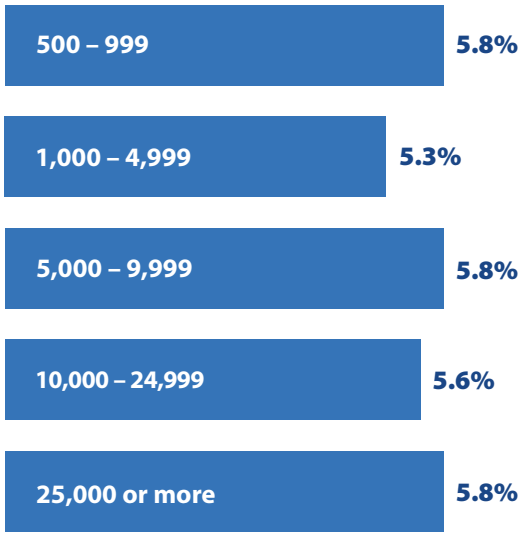

Figure 33: Mean IT security budget increase, by number of employees.

Benefits of Working with an MDR Service Provider

What are the most important benefits of working with a managed detection and response (MDR) service provider? (Select up to five.)

Figure 34: Most important benefits of working with an MDR service provider.

In the 2022 and 2025 CDRs we asked what IT security functions organizations were outsourcing to managed security services providers (MSSPs). The most widely outsourced function in both years: "Detecting and responding to advanced cyberthreats/ managed detection and response (MDR)."

This year we decided to drill down and find out exactly why MDR services are so popular. We asked security professionals in organizations that work with MDR services about the most important benefits they are receiving.

The benefit selected most often was "Improves monitoring and detection of attacks on endpoints and cloud-based applications" (46.8%) (see Figure 34). That is no surprise, since "detection" is right there in the name of the service.

The second most frequently selected benefit was "Speeds up compliance and audit reporting" (40.4%). Automating documentation and reporting don't directly improve security, but are the kinds of tasks that can be safely and easily outsourced. Taking them off the plate of internal security teams gives them a lot more time to work on in-depth investigations and improve decision making.

Section 3: Current and Future Investments

MDR service providers have specialized infrastructure for threat detection and response that many organizations lack, as well as deep expertise in those areas. Those advantages are behind the third and fourth reasons for working with them: "MDR service providers have workflows for detection, analysis, and response that are more automated than our internal ones" (38.1%) and "MDR service providers have more expertise in detection and response than our staff" (36.7%).

The importance of these capabilities is consistent with the information in Figure 17 on page 21 that "Too much data to analyze" is the third-greatest barrier to successful defense. Clearly, there is a lot of incentive to for organizations to accelerate detection and analysis any way they can.

The value of outsourcing labor-intensive tasks to outside specialists is captured in two additional reasons to work with MDR service providers: "Shields our teams from large volumes of low-priority and irrelevant alerts" and "Frees up security team members for other tasks" (both 36.5%).

It is interesting to note that although saving money was a top benefit for about a third of the respondents (31.5% cited "Reduces overall costs"), two-thirds did *not* include cost savings as one of the top five benefits of MDR services. Instead, speed, efficiency, expertise, and time savings are driving most decisions to outsource appropriate detection and response tasks.

"Although saving money was a top benefit for about a third of the respondents... speed, efficiency, expertise, and time savings are driving most decisions to outsource appropriate detection and response tasks."

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
Data loss / leak prevention (DLP)	56.0%	34.9%	9.0%
Intrusion detection / prevention system (IDS/IPS)	55.0%	34.1%	10.9%
Secure email gateway (SEG)	54.3%	32.2%	13.4%
Secure web gateway (SWG)	54.0%	34.7%	11.3%
Network access control (NAC)	53.6%	33.6%	12.7%
Advanced threat prevention (sandboxing, ML/AI)	52.2%	38.1%	9.7%
SSL/TLS decryption appliances / platform	49.3%	39.3%	11.5%
Denial of service (DoS/DDoS) prevention	48.4%	38.1%	13.6%
Next-generation firewall (NGFW)	43.3%	45.6%	11.1%
Network behavior analysis (NBA) / NetFlow analysis	42.3%	43.1%	13.6%
Deception technology / distributed honeypots	36.1%	43.0%	20.9%

Table 1: Network security technologies in use and planned for acquisition.

As organizations increase their reliance on cloud platforms and SaaS applications, network security is no longer quite the top-of-mind security area that it once was. But it still demands attention, because network security solutions continue to do incredibly important work protecting against a wide variety of malicious activities, providing early warning of attacks, and supplying critical data to help analytics and AI tools identify complex campaigns.

"Data loss/data leak prevention (DLP)" is the rising star of the network security technologies shown in Table 1. The percentage of organizations with a DLP solution currently in use increased from 55.4% in the 2025 CDR to 56.0% in this one. That increase was enough to move DLP from fifth place on last year's list to first place in this one. This technology detects and blocks the exfiltration of data and files by threat actors and rogue insiders, as well as by employees who are careless, clueless, or simply

Section 3: Current and Future Investments

unaware of corporate policies limiting the sharing of confidential information. DLP products are important for compliance as well; many government regulations and industry standards require or strongly recommend them.

However, over the past year installation rates declined for the next four network security technologies on our list. The percentage of organizations running "Intrusion detection/prevention system (IDS/IPS)" dipped from 57.2% to 55.0%. Those using a "Secure email gateway (SEG)," a "Secure web gateway (SWG)," and a "Network access control (NAC)" solution fell, respectively, from 58.4% to 54.3%, from 56.4% to 54.0%, and from 56.7% to 53.6%.

Five of the other six technologies in the table also showed declines. The exception was "Advanced threat prevention (sandboxing, ML/AI)," which increased from 50.9% to 52.2%.

But we hasten to stress that these results do not mean network security technologies are obsolete or irrelevant. Quite the contrary; six of the technologies discussed here continue to run in more than half of organizations.

In fact, most of the underlying technologies are more important than ever. It's just that many of them are being provided by broader security platforms or service offerings, rather than by free-standing products. As a result, some respondents omitted them from their response to this question.

Next: endpoint security technologies in use and planned for acquisition (page 41).

"Most of the underlying technologies are more important than ever. It's just that many of them are being provided by broader security platforms or service offerings rather than by free-standing products."

Section 3: Current and Future Investments

Endpoint Security Deployment Status

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

	Currently in use	Planned for acquisition	No plans
Basic anti-virus / anti-malware (threat signatures)	70.5%	25.5%	4.0%
Data loss / leak prevention (DLP)	59.4%	30.5%	10.1%
Endpoint detection and response (EDR)	57.1%	32.5%	10.5%
Browser or Internet isolation / micro-virtualization	55.4%	34.5%	11.1%
EPP / Advanced anti-virus / anti-malware (machine learning, behavior monitoring, sandboxing)	53.9%	36.9%	9.2%
Disk encryption	51.6%	34.0%	14.3%
Digital forensics / incident resolution	47.4%	38.5%	14.2%
Deception technology / honeypot	39.8%	42.9%	17.3%

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

"Basic anti-virus/anti-malware (threat signatures)" has been the #1 endpoint security technology for many years. It is currently in use at 70.5% of organizations, while no other technology on this list exceeds 60% (see Table 2). Although detection via signatures isn't new or sexy, organizations still rely on those techniques to catch a lot of malware.

The second and third most often installed technologies for endpoint protection are "Data loss/leak prevention (DLP)" and "Endpoint detection and response (EDR)." The percentage of organizations where they are in use increased by 2.6% over the past year for both DLP (from 56.8% to 59.4%) and for EDR (from 54.5% to 57.1%). We should point out that the DLP solutions covered here check for confidential data at the endpoints, versus the DLP products discussed in the previous section, which are blocking exfiltration over the network.

"Browser or Internet isolation/micro-virtualization," used by 55.4% of organizations, moved up from sixth place in the previous CDR to fourth place in this one. Products in this category run browser and application sessions in a controlled space that allows users to do their work, but prevents attackers from seeing or accessing the users' devices. It's a clever way of protecting endpoints from many threats and is now used in more than half of all organizations.

Section 3: Current and Future Investments

"EPP/Advanced anti-virus/anti-malware" is likewise installed in more than half of organizations (53.9%).

And so is "Disk encryption." But… disk encryption on endpoints may be falling out of favor. Its installation percentage fell 4.9% over the past year, from 56.5% to 51.6%. This may reflect that security teams are changing their emphasis toward file-level security. We will have to see whether this is a long-term trend.

Are there some additional rising stars in this category? "Digital forensics/incident resolution" and "Deception technology/honeypot," are not currently in use in as many organizations as the other technologies in this group (47.4% and 39.8%). However, their installations went up last year, and they are the leaders in the "Planned for acquisition" column of Table 2.

Next: application and data security (page 43).

"'Browser or Internet isolation/micro-virtualization'… moved up from sixth place in the previous CDR to fourth place in this one... It's a clever way of protecting endpoints from many threats and is now used in more than half of all organizations."

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	61.4%	31.5%	7.1%
Web application firewall (WAF)	61.2%	29.4%	9.3%
Database firewall	60.3%	29.5%	10.1%
Database activity monitoring (DAM)	56.1%	33.2%	10.7%
Application container security tools / platform	55.5%	36.8%	7.6%
Cloud access security broker (CASB)	50.7%	35.5%	13.7%
Application delivery controller (ADC)	50.0%	33.8%	16.2%
File integrity / activity monitoring (FIM/FAM)	49.3%	37.9%	12.8%
Static / dynamic / interactive application security testing (SAST/DAST/IAST)	45.8%	38.8%	15.4%
Runtime application self-protection (RASP)	44.5%	40.4%	15.1%
Third-party code analysis	42.6%	38.8%	16.6%
Bot management	39.8%	42.7%	17.6%

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

Among application- and data-centric security technologies, "API gateway/protection" moved from third position last year in the "Currently in use" column to first place in this one (see Table 3). Products to manage and defend APIs are installed in 61.4% of organizations. Security teams understand APIs are the gateways into cloud-based applications for threat actors as well as for legitimate application developers, and therefore need to be protected from abuse.

We usually consider that technologies installed in 60% or more of organizations have earned the designation of "must-haves." By that definition, "Web application firewall (WAF)," at 61.2% and "Database firewall," at 60.3%, are both must-haves. As the names make clear, these technologies provide special protection and policy enforcement features for two of the most critical categories of information assets.

Section 3: Current and Future Investments

Other very popular technologies for safeguarding applications and data stores are "Database activity monitoring (DAM)" products (56.1%) and "Application container security tools/ platform" (55.5%).

We also want to call attention to technologies with the highest numbers in the "Planned for acquisition" column of Table 3.

Bots and botnets provide infrastructure to launch DDoS attacks as well as ransomware, phishing, and spam campaigns. "Bot management" tools (in the purchasing plans of 42.7% of organizations) give security teams a way to throttle back traffic from bots to prevent those threats from causing damage.

"Runtime application self-protection" (RASP) technology, planned for acquisition by 40.4% or organizations, operates inside running applications to monitor them for suspicious and abnormal activities. When questionable activities are detected, RASP software can alert security and application teams or take steps to stop attacks immediately, such as by blocking malicious requests and terminating user sessions.

Application security testing tools ("SAST, DAST, and IAST") and "Third party code analysis" products evaluate software code to identify vulnerabilities, policy violations, and code sourced from third parties that might be compromised by threat actors or copyrighted. Both of these technologies are planned for acquisition by 38.8% of organizations. (Whether it is the same 38.8% of organizations or different ones, we can't say.)

We now examine the current use and planned acquisition of security management and operations technologies (page 45).

Section 3: Current and Future Investments

Security Management and Operations Deployment Status

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

	Currently in use	Planned for acquisition	No plans
Active Directory protection	56.0%	34.7%	9.3%
Security configuration management (SCM)	55.2%	33.4%	11.4%
Patch management	54.5%	33.8%	11.7%
Vulnerability assessment / management (VA/VM)	53.5%	37.8%	8.7%
Cyber risk quantification / scorecard	53.1%	32.5%	14.4%
Security information and event management (SIEM)	52.2%	36.1%	11.7%
Penetration testing / attack simulation software	51.6%	35.5%	12.9%
Threat intelligence platform (TIP) or service	48.9%	37.6%	13.5%
Advanced security analytics (e.g., with machine learning, AI)	47.6%	43.3%	9.1%
Full-packet capture and analysis	46.6%	39.5%	13.9%
Security orchestration, automation, and response (SOAR)	46.4%	40.0%	13.5%
User and entity behavior analytics (UEBA)	43.8%	41.2%	15.1%

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

With all the attention going to new technologies and processes to detect and respond to attacks, it is easy to lose sight of the importance of identifying and fixing security weaknesses to prevent attacks from taking hold in the first place. Fortunately, our survey data shows that security teams still place a lot of emphasis on doing exactly that.

Let's start with protecting identity information and credentials. Elsewhere in this report we have discussed why identity security is becoming more important and emerging as a top-of-mind topic for security leaders (see pages 23-24 and 47). Microsoft Active Directory is the system of record for identity information in many organizations. Therefore, it is no surprise that Active Directory is

Section 3: Current and Future Investments

targeted by many of the most sophisticated cybercriminals and state-sponsored hacking groups in the world. And it is also no surprise, and also very fortunate, that security teams feel it is vital to protect it. As shown in Table 4, "Active Directory protection" is the most-installed security management and operations technology on our list, in use at 56.0% of organizations.

The importance of proactively identifying weaknesses and hardening an organization's attack surface (sometimes categorized as "left of boom" security) is also confirmed by the second, third, and fourth most-installed technologies in Table 4. These are "Security configuration management (SCM)," "Patch management," and "Vulnerability assessment/management (VA/VM)." These are currently being used in 55.2%, 54.5%, and 53.5% of organizations, respectively. It is interesting to note that in the past these technologies were somewhat batch oriented, but they have been retooled to perform continuous, or at any rate very frequent, scanning and remediation and to incorporate machine learning and other AI features.

And speaking of machine learning and other AI features, the highest percentages in the "Planned for acquisition" column are "Advanced security analytics (e.g., with machine learning, AI)," in the future for 43.3% of organizations, and "User and entity behavior analytics (UEBA)," being acquired by 41.2%. Interest in these technologies is tied directly to how AI boosts their speed and analytical power.

Section 4: Practices and Strategies

Priorities for Improving Cloud Security

What are your organization's top priorities in the next 12 months for improving cloud security? (Select up to five.)

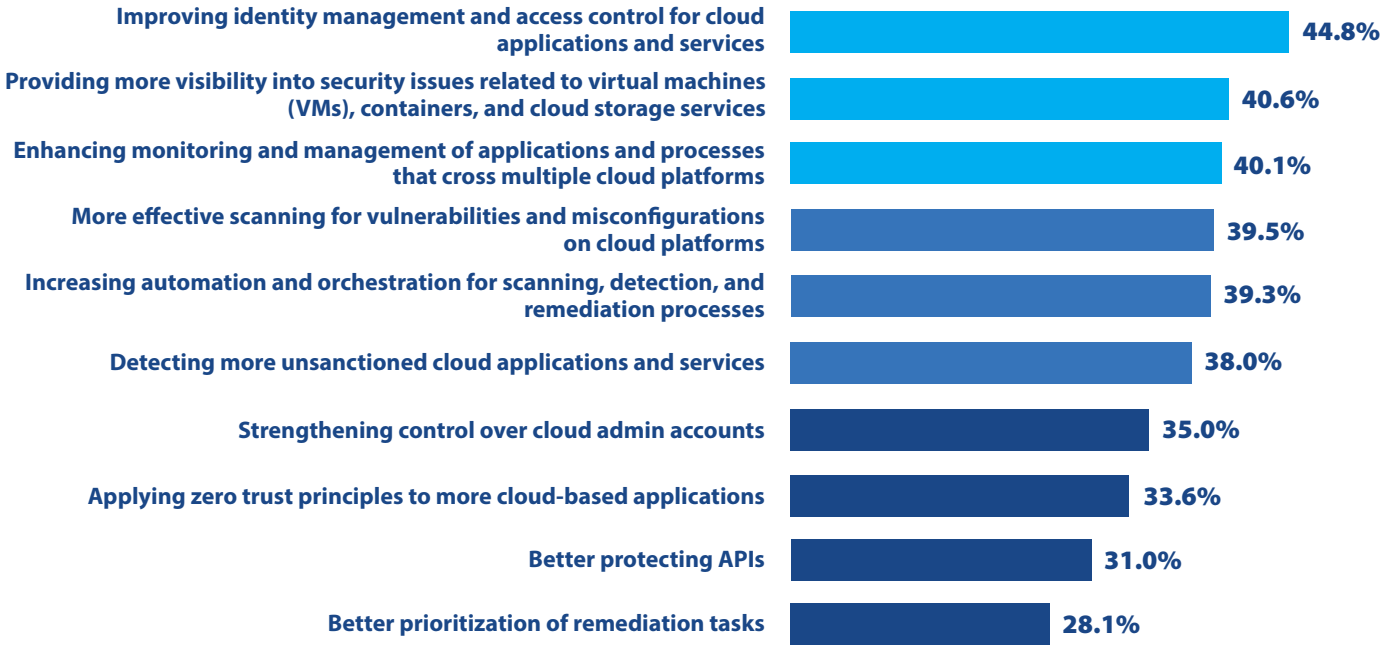

Figure 35: Top priorities for improving cloud security.

Organizations have been investing heavily to bring their cloud security up to speed. We added a question to the survey asking respondents about their organization's top five priorities for the coming year in that domain.

The clear #1 choice is: "Improving identity management and access control for cloud applications and services," which was cited by 44.8% of the respondents (see Figure 35). On pages 23 and 24 we outlined some of the factors that have made identity security a top-of-mind issue for security teams:

- The need to manage identities across a wide range of environments, including multiple cloud platforms
- The challenge of creating and controlling vast numbers of non-human identities (NHIs), many of which reside in the cloud
- The growing importance of advanced access control and authentication techniques that rely on identity information, particularly for cloud-hosted applications and services

Section 4: Practices and Strategies

Ideally, security teams would be able to identify all the accounts for each person and NHI and ensure that permissions across all of them are consistent with each other and with the principle of least privilege (PoLP). That's a really tough goal, though, and security teams are rightfully concerned that many people and cloud-based software workloads have excessive, unnecessary privileges.

Two other high priorities are "Providing more visibility into security issues related to virtual machines (VMs), containers, and cloud storage services" (40.6%) and "Enhancing monitoring and management of applications and processes that cross multiple cloud platforms" (40.1%). Today, processes and data are increasingly flowing between multiple workloads within and across cloud platforms. Without end-to-end visibility into these flows, it can be very hard for even the best AI-enabled security tools to detect and analyze sophisticated attacks.

What is behind "More effective scanning for vulnerabilities and misconfigurations on cloud platforms" (39.3%)? Security teams need to counter threat actors who are making significant investments in their own vulnerability scanning tools to identify attack points in cloud applications and platforms, often leveraging AI. They are even adding malicious features to scanning tools developed by security consultants.

"Increasing automation and orchestration for scanning, detection, and remediation processes" (39.3%) speaks to the fact that many security workflows are still too slow and labor-intensive. Organizations are actively investing in security orchestration, automation, and response (SOAR) tools and in vendor-supplied platforms with automated workflows that cross cloud platforms and security functions.

It is interesting that "Applying zero trust principles to more cloud-based applications" (33.6%) comes in as only the eighth priority on this list, despite widespread support for zero trust concepts. We suspect that (a) some organizations have already gone fairly far down the zero trust path and think they may be at the point of diminishing returns, while (b) others are holding back on zero trust initiatives until they improve security fundamentals like identity management, visibility, monitoring, and effective vulnerability scanning. Do either of these descriptions fit your organization?

Finally, data shows that everyone is concerned about cloud security. Less than 1% of organizations do not share at least one of the priorities in this question (see Figure 36).

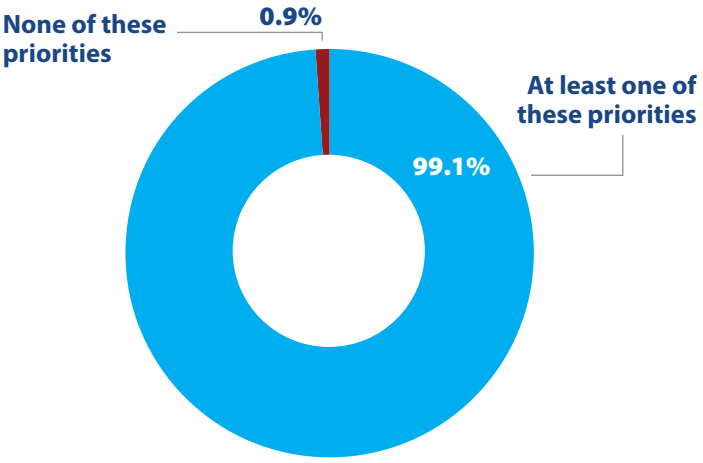

Figure 36: Organizations with at least one priority for improving cloud security in the next 12 months.

"Security teams are rightfully concerned that many people and cloud-based software workloads have excessive, unnecessary privileges."

Section 4: Practices and Strategies

Plans to Utilize AI-enabled Tools for Security Tasks

Describe your organization's plans to utilize security tools that feature AI for each of the following IT security tasks.

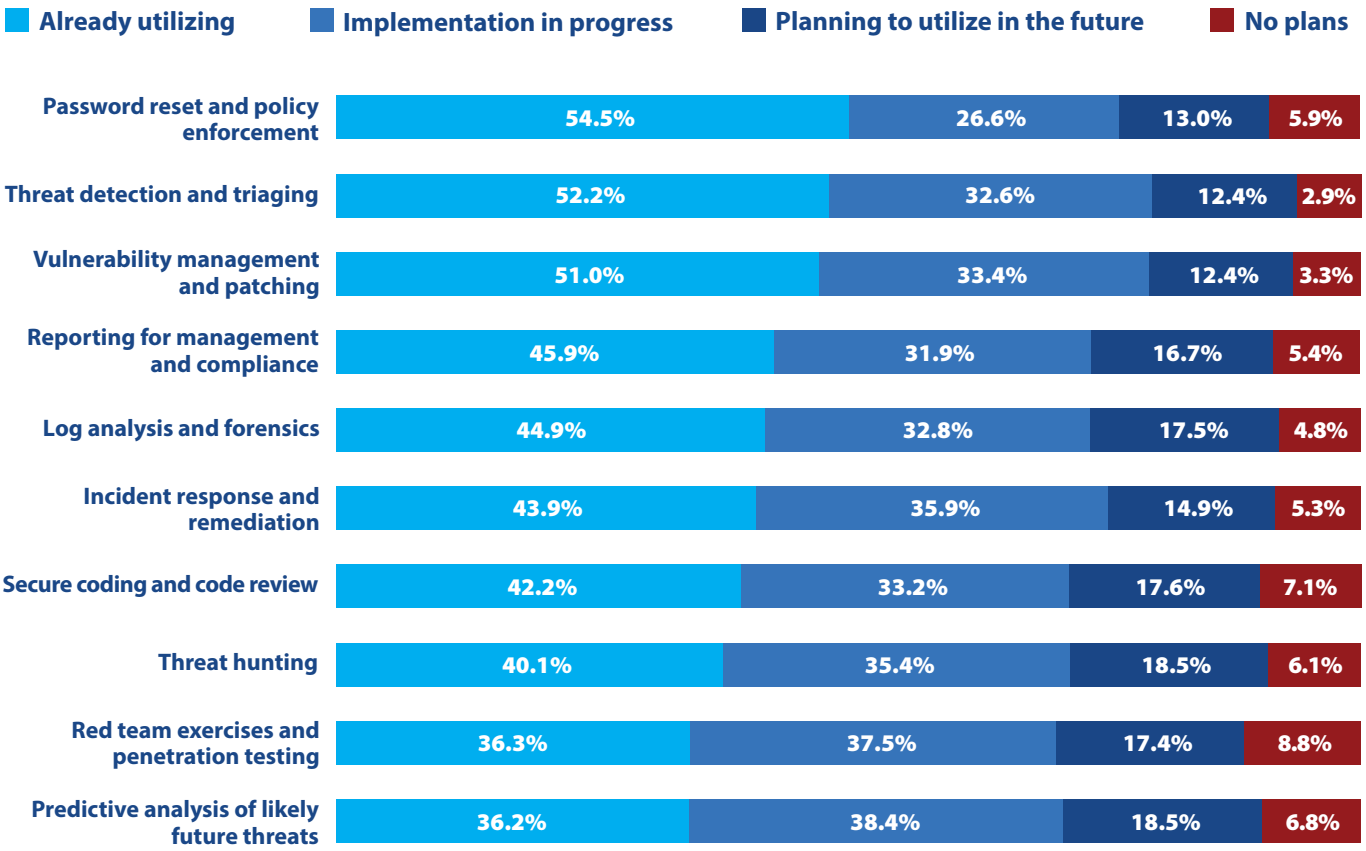

Figure 37: Implementation status of AI-enabled tools for specific security tasks.

In the 2025 CDR we asked respondents to "Select the option that best describes your organization's overall preference for purchasing security products that feature artificial intelligence (AI) technologies." It turned out that 12% had a slight preference, 47% had a moderate preference, and 35% had a strong preference. Only 6% had no preference.

This year we decided to dig a little deeper and find out exactly what tasks AI-enhanced security tools are being used for, and how far enterprises have gotten in implementation. Our first finding: organizations have committed in a BIG way to using AI-enhanced tools for almost every security task.

Section 4: Practices and Strategies

Figure 37 shows 10 areas where AI can enhance security processes. In *every one* of those 10:

- At least 75% of organizations are already committed to using AI capabilities (that is, AI features are in use or being implemented now).
- Only 9% or less don't plan to utilize them at some point

AI is supporting "Password reset and policy enforcement" in 54.3% or organizations now and is being implemented in another 26.6%. Password policies are usually fairly straightforward and reset processes are very time consuming, making this an early choice for AI adoption.

Benefits are a little different for "Threat detection and triaging" (52.2% already utilizing + 32.6% implementation in progress). AI-based tools can identify patterns in vast amounts of data, meaning that they can detect threats and triage incidents not only faster than unaided humans, but also more accurately. As an added bonus, while they triage incidents, they can also gather and organize context and create timelines that allow analysts to investigate high-priority incidents with far less effort than before.

Similar incentives apply to "Vulnerability management and patching" (51.0% + 33.4%), "Reporting for management and compliance" (45.9% + 31.9%), "Log analysis and forensics" (44.9% + 32.8%), and "Incident response and remediation" (43.9% + 35.9%). In all these processes, pattern recognition can save time, reduce effort, increase accuracy, and support human decision making with extra context and insights.

But we return to our major finding on this topic: most organizations are already fully committed to using AI features for all 10 of the IT security tasks listed here, and most likely for many others as well.

"Our first finding: organizations have committed in a BIG way to using AI-enhanced tools for almost every security task."

Section 4: Practices and Strategies

Preparations for Quantum Computing Cyber Risks

Which of the following actions is your organization taking to prepare for quantum computing cyber risks? (Select all that apply.)

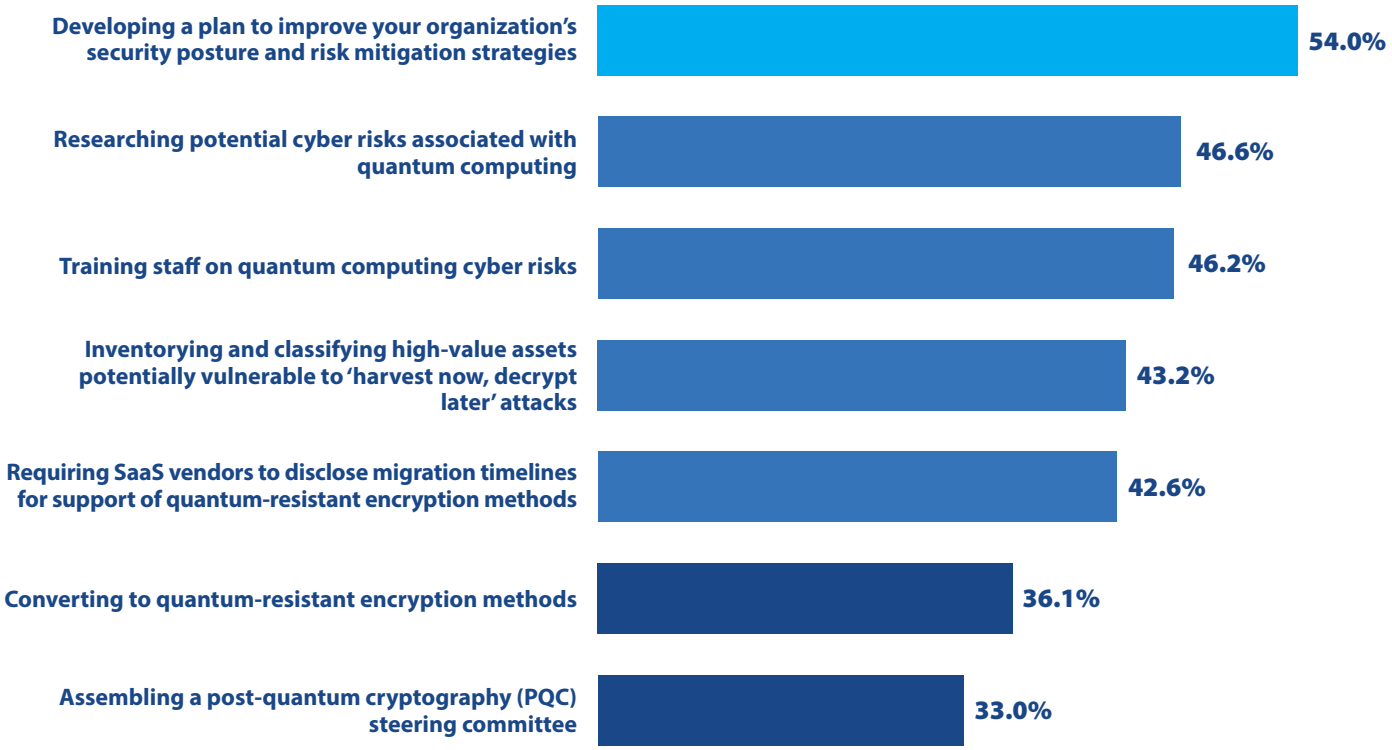

Figure 38: Actions being taken to prepare for quantum computing risks.

Is quantum computing on your radar? If not, why not?

Look, we admit that we don't understand quantum computing. Qubits? Quantum superposition? Entangled states? Quantum decoherence? (Although we know that humorist Dave Barry would say that Quantum Decoherence would be a good name for a rock band.)

We're mystified, and it's okay if you are, too. But what is *not* okay is failing to plan for the potential impacts of quantum computing on cybersecurity.

A few things security professionals needs to know now about quantum computers:

- For certain tasks, they are really, really, really, really fast (pick your benchmark: 13,000 times or 241 million times faster than a supercomputer).
- They are not ready for prime time yet, but expert opinion seems to be converging on predictions of reliable, scalable models being available sometime in the 2030s.

Section 4: Practices and Strategies

- They will not replace conventional computers for most applications, but will have massive advantages for specific tasks that could make the world a much better place, including scientific modeling, simulation, optimization, computer vision and image recognition, and training AI models.
- And, oh yes, they will be able to crack secure communications, compromise digital signatures, decrypt hundreds of millions of files we have been protecting with public key infrastructure (PKI) methods, and undermine blockchain integrity.

One of the reasons organizations need to act *now* is that threat actors are launching "harvest now, decrypt later" (HNDL) attacks. Those involve acquiring and storing vast quantities of encrypted data that they will be able to decrypt when quantum computers are available. They may not be able to get at your Social Security number now, but just wait…

So, what actions are organizations taking today to prepare for quantum computing cyber risks?

We might classify the most common activities as "learning, planning, and general preparation." Specifically, respondents pointed to "Developing a plan to improve your organization's security posture and risk mitigation strategies" (54.0%), "Researching potential cyber risks associated with quantum computing" (46.6%), and "Training staff on quantum computing cyber risks" (46.2%) (see Figure 38).

Next come two activities that might be considered as laying the groundwork for future actions: "Inventorying and classifying high-value assets potentially vulnerable to 'harvest now, decrypt later' attacks" (43.2%) and "Requiring SaaS vendors to disclose migration timelines for support of quantum-resistant encryption methods" (42.6%).

However, only about a third of organizations have gotten to the stage of rolling up their sleeves and actually "Converting to quantum-resistant encryption methods" (36.1%) and collaborating with other groups across the enterprise by "Assembling a post-quantum cryptography (PQC) steering committee" (33.0%).

Quantum-resistant encryption, also called post-quantum cryptography (PQC), involves replacing today's popular cryptographic algorithms with symmetric encryption, multivariate quadratic equations, lattice-based cryptography, and other alternatives that we also don't understand but that experts believe will remain impervious to quantum decryption.

So don't panic, but get going – especially the 6.5% of you who haven't taken any of these actions to preparre for quantum computing threats (see Figure 39).

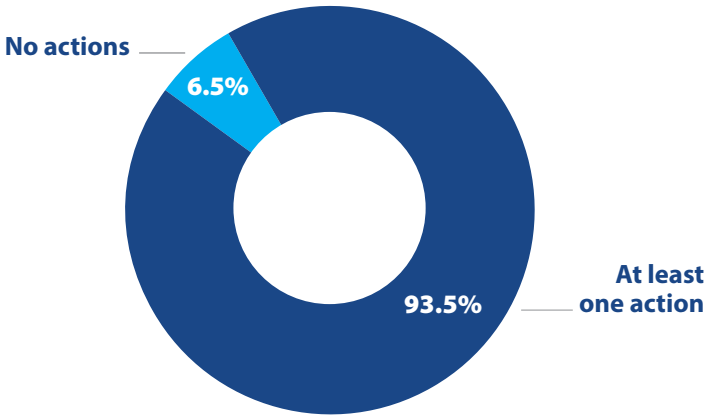

Figure 39: Organizations taking at least one action to prepare for quantum computing risks.

"We're mystified by quantum computing, and it's okay if you are too. But what is *not* okay is failing to plan for the potential impacts of quantum computing on cybersecurity."

IT Security Leader Interaction with the Board of Directors

How do your IT security leaders engage with your organization's board of directors? (Select all that apply.)

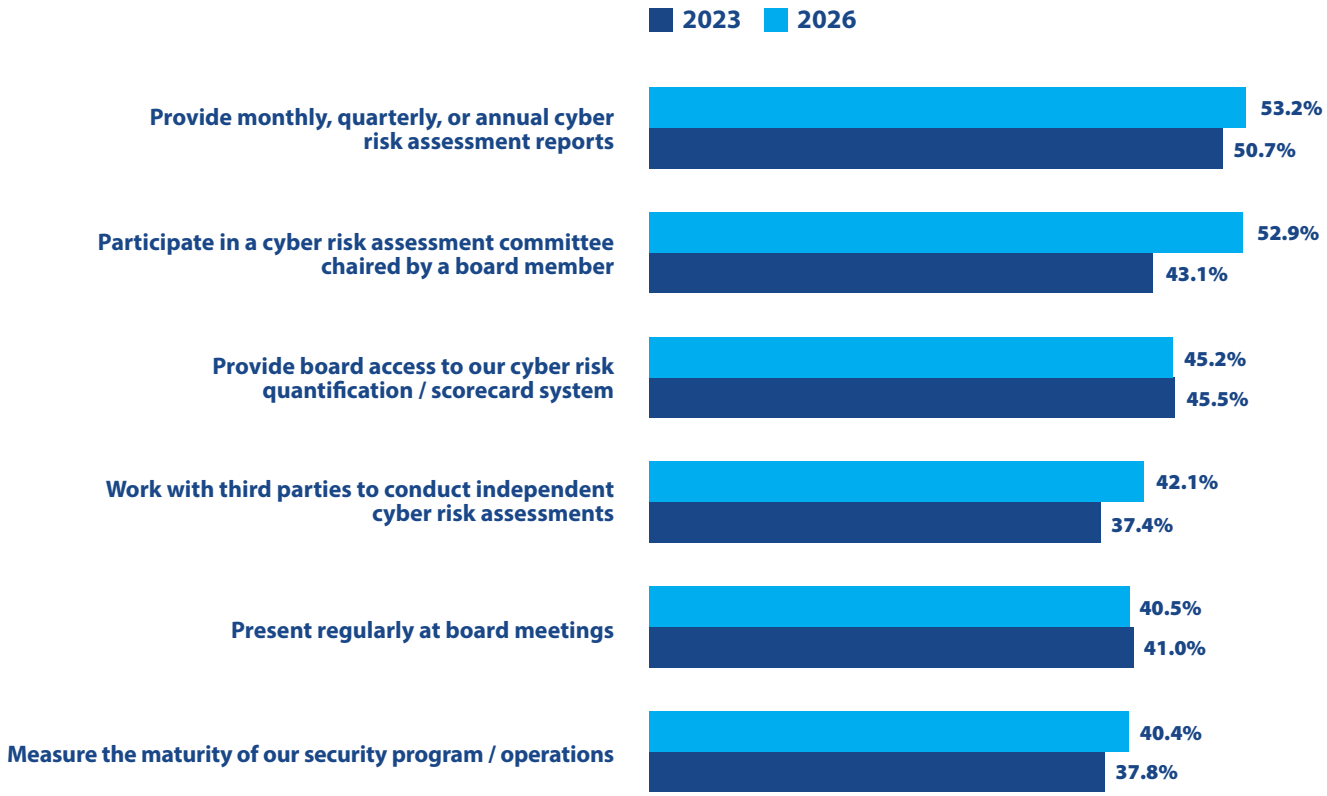

Figure 40: How IT security leaders engage with their organization's board of directors, 2023 and 2026 surveys compared.

A very noticeable trend over the last decade or so has been the steady increase of interaction between security leaders and their organization's board of directors and other executive stakeholders. In many enterprises this has progressed from little or no direct contact, to an occasional slide-based "dog and pony show" at a board meeting, to sharing in-depth information on a regular basis and collaborating outside the boardroom.

This trend toward more interaction is a very positive development. It helps align cybersecurity activities with business priorities, and it ensures continuing support for cybersecurity programs (as shown by the fact that cybersecurity budgets have grown consistently, even in many organizations that are retrenching in other areas, as we discussed on page 36).

Section 4: Practices and Strategies

Factors driving this trend include both a push from investors and customers demanding that boards take an active role in ensuring that data breaches and business disruptions don't occur on their watch, and the pull of board members with a growing interest in cybersecurity, and increasingly, experience in the field. We have some data regarding this last point: in the 2024 CDR we asked respondents whose organizations had a board of directors if at least one member had a cybersecurity background, and 62.2% said yes.

How exactly are security leaders engaging with board members? We asked in the 2023 CDR and this one, and the results are shown in Figure 40.

The most common forms of interaction are "Provide monthly, quarterly, or annual cyber risk assessment reports" (53.2%) and "Participate in a cyber risk assessment committee chaired by a board member" (52.9%).

"Board members actively participate in cyber risk discussions at more than half of organizations! And the rate of participation increased by almost 10% over the last three years!"

This last finding is very notable. Board members actively participate in cyber risk discussions at more than half of organizations! And the rate of participation increased by almost 10% over the last three years.

Furthermore, at 45.2% of organizations security leaders "Provide board access to our cyber risk quantification / scorecard system," and at 42.1% they share independent cyber risk assessments.

In short, interacting directly with the board is now the rule rather than the exception for security leaders.

Emerging IT Security Technologies and Architectures

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

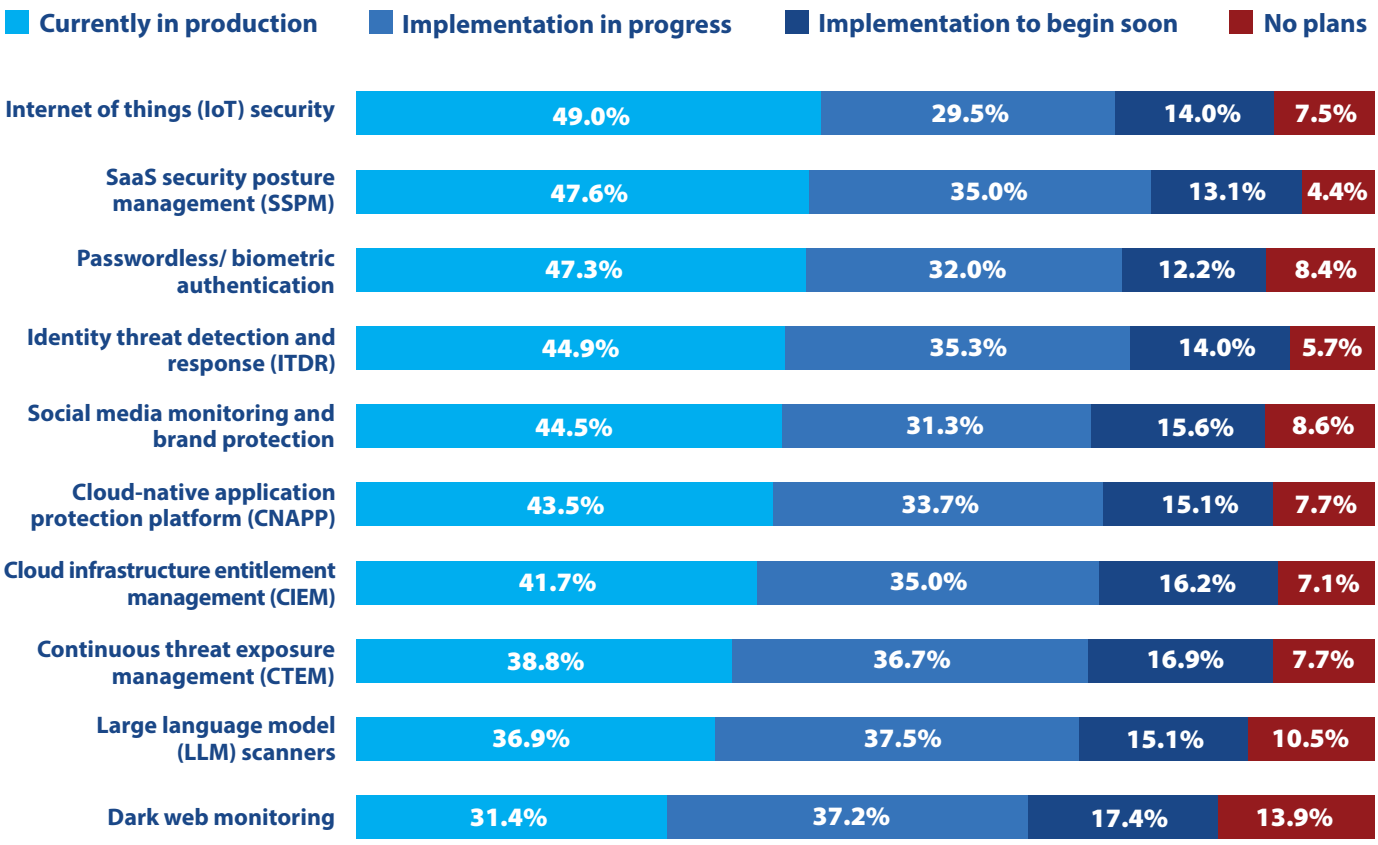

Figure 41: Plans for implementing emerging IT security technologies and architectures.

We close out the data analysis part of this report with a look at the deployment status of 10 emerging IT security technologies and architectures (see Figure 41).

Of the 10, "Internet of things (IoT) security" is currently in production in just under half (49.0%) of all organizations. High rates of deployment were reported not only by manufacturing, utility, and logistics companies, but also by firms in construction, finance, and agriculture. That's right, down on the farm you'll find an awful lot of internet-connected things: soil and crop sensors, livestock monitoring collars, smart pumps and irrigation controls, smart greenhouses, smart silos, and autonomous tractors and robots. IoT security is a challenge everywhere.

Section 4: Practices and Strategies

Also very popular: technology for "SaaS security posture management (SSPM)" (47.6%) and for "Passwordless/ biometric authentication" (47.3%). As organizations make increasing use of multiple hosted applications, it becomes more important, and more difficult, to find and remediate misconfigurations, exposed data, user accounts with excessive permissions, and compliance policy violations across SaaS platforms. As threat actors increasingly focus on capturing and exploiting legitimate employee and customer credentials, organizations are depending more and more on advanced authentication technologies to prevent bad guys from accessing online resources.

As we have mentioned several times in this report, both human and non-human identities are proliferating wildly, making it harder to pinpoint identity security weaknesses and to detect attacks that leverage those weaknesses. "Identity threat detection and response (ITDR)" products, currently in production in 44.9% of organizations, help with those.

Other technologies and architectures included on this list similarly help security teams identify and remediate vulnerabilities and detect malicious actions across a range of IT domains.

"That's right, down on the farm you'll find an awful lot of internet-connected things: soil and crop sensors, livestock monitoring collars, smart pumps and irrigation controls, smart greenhouses, smart silos, and autonomous tractors and robots. IoT security is a challenge everywhere."

We added one new technology in this CDR: "Large language model (LLM) scanners." It is in production only in 36.9% of organizations, but another 37.5% are in the process of implementing it. The growing interest in this form of scanning reflects the fact that organizations are starting to deploy AI features in more custom, internally developed applications (as discussed on pages 29-30). At the moment, LLMs are the domain where security teams are less confident about their defenses (see pages 12-13).

The Road Ahead

AI – How Big?

The 2025 CDR had just one question focused on artificial intelligence and its impact on cybersecurity. You may have noticed that there are five in this report. That's because discussions about AI in cybersecurity have expanded well beyond "How are the bad guys going to improve their attacks with AI, and how can we use AI to detect those attacks?" Now cybersecurity professionals also need to think carefully about how AI can fundamentally transform our cybersecurity workflows, our processes, our goals, and our roles. And questions like these appear in even larger form in discussions about the world economy and global job markets.

So, of course, AI is big and getting bigger. But how big can it get? We look at this question in terms of two sets of forces pushing for acceleration or deceleration, toward revolution or evolution.

Factors pushing toward revolution include:

- AI's astounding track record dramatically increasing the speed and accuracy of tasks of all kinds.
- An extremely rapid rate of improvement in AI models and tools.
- Vast, immense, colossal, monumental, economy-shifting, galactic-scale investment in AI technologies and the infrastructure to support them.

Reasons why the pace of change may be slowed to mere rapid evolution include:

- AI models may run out of new high-quality data to improve their performance (there is evidence that this is starting to happen).
- Most AI systems are non-deterministic, opaque, biased, and subject to hallucinations (that is, they give different answers to the same question, you can't tell why, the answers might be skewed by incomplete data, and some answers might be flat out wrong).
- The AI investment boom may turn out to be a bubble, causing massive retrenchment and bankruptcies in the AI industry.

We're not going to predict which set of forces will prevail, but readers should keep in mind that both are possible and watch for signs.

AI – How Autonomous?

Returning to cybersecurity, "agentic AI" has become a thing, and we will need to see how far and how fast it develops. For example, autonomous AI agents that detect suspicious behavior can act at machine speed to force password resets, or block connections to IP addresses on the web, or isolate compromised systems. That is usually a good thing. However, there is a risk that, without a human in the loop, autonomous agents could block legitimate transactions or worse. To prevent that, security teams need to design effective guardrails for the agents and enable autonomy in stages (perhaps by starting with alerts and gradually permitting more types of actions to be taken autonomously).

AI – How Secure?

We think security for AI-enabled applications is going to emerge as a big topic in the next year or two. So far, discussions of the "AI attack surface" have been mostly speculative. But security and development teams are starting to recognize security as a challenge to creating custom AI applications (see pages 29-30). And elevating AI security to a hot-button issue may only take two or three highly visible incidents: a couple of major breaches or disruptions of AI-enabled applications, or AI tools generating software code with critical vulnerabilities, or poisoned data leading to damaging outputs from AI. In fact, issues with AI security could end up being one of the factors that turn the AI revolution into the AI evolution.

AI – How About Me?

Maybe it's a good time to develop expertise in AI security. Seriously.

AI-based tools are already having an impact on the job prospects of some software coders. Most cybersecurity teams are partly insulated from those pressures by a persistent lack of skilled cybersecurity personnel (see page 21). However, almost half of the respondents in this survey are predicting that AI will affect hiring for their role within two years (pages 33-34).

The Road Ahead

To prepare for that future, cybersecurity professionals should consider:

- Staying on top of their field, particularly in areas where experience and human judgment will continue to trump the advantages of AI tools
- Developing expertise to position themselves as AI security experts with their current employer
- Acquiring skills that would enable them to seek employment with AI-oriented vendors, service providers, and consulting firms

Cyberwar – How Bad?

At the time this is being written, the role of cyberattacks in the war of the United States and Israel against Iran has been relatively minor. And while cyberattacks have been employed in the war between Russia and Ukraine, they haven't had a major impact on the conflict. Do those facts indicate that fears of cyberwar have been overblown?

No, we don't think so. In fact, we'd argue that the danger has increased. One lesson that small and medium-sized nations may have learned from Iran's experience is that countries overmatched by their enemies in conventional arms should invest heavily in weapons for "asymmetric warfare." That is, weapons that are relatively cheap and don't require extensive infrastructure… like cyber weapons.

Cybersecurity Platforms – How Good?

Oh my, we keep getting away from everyday cybersecurity. So, let's conclude with a trend a little closer to home. We are seeing more cybersecurity "platforms" that collect and analyze data from multiple security domains (networks, endpoints, email and messaging systems, corporate data centers, cloud platforms, SaaS applications, etc.). Many of these platforms also automate and orchestrate containment and remediation actions across these environments.

We expect to see more of these platforms being released by vendors and deployed by enterprises. That's because threat actors are creating more-sophisticated, multi-stage attacks that can only be identified and contained by correlating data from multiple environments (preferably with AI).

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 42) 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 43). This year, 40.1% of our respondents held CIO, CISO, or other IT security executive positions.

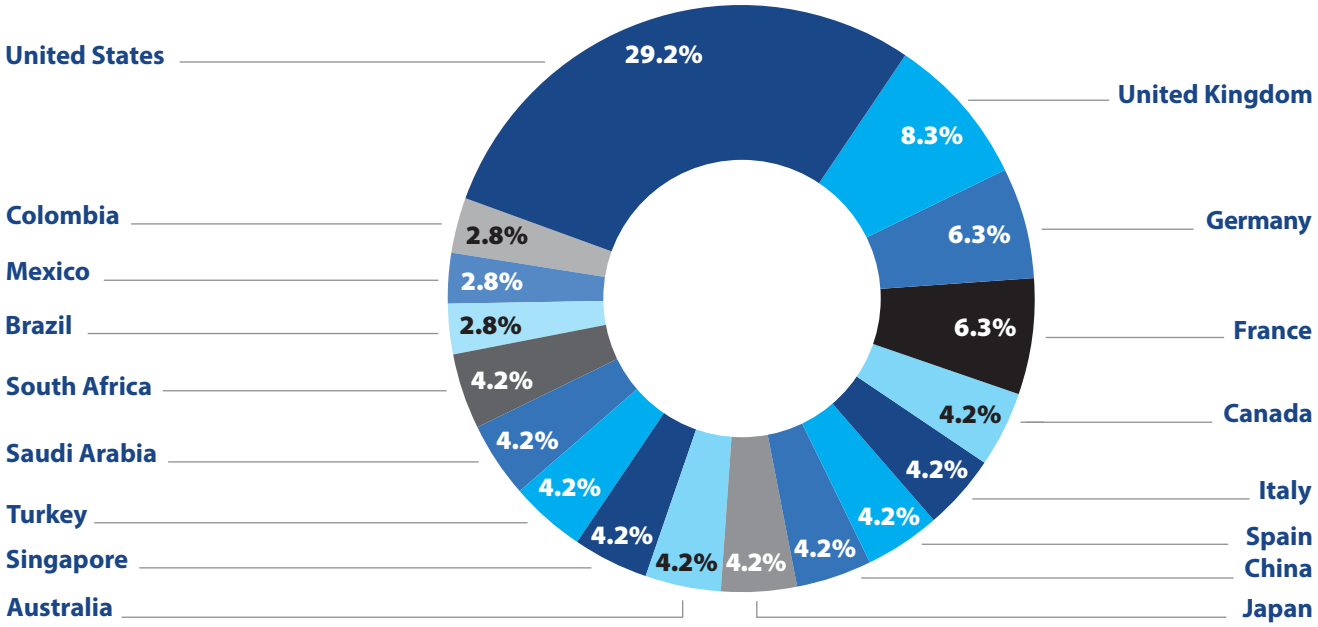

Figure 42: Survey participants by country.

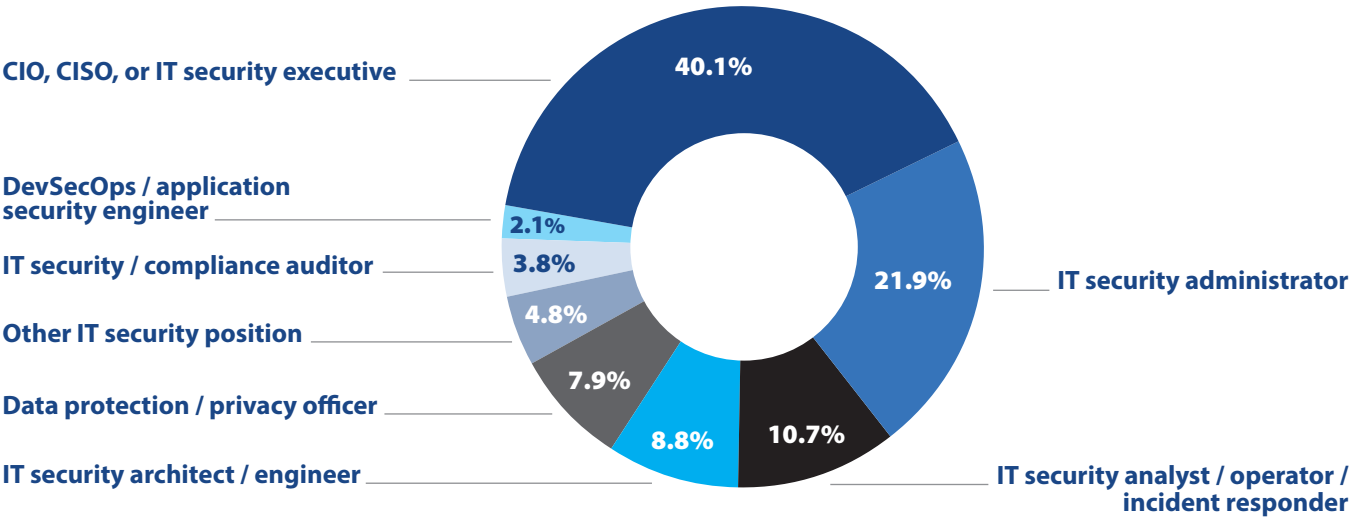

Figure 43: Survey participants by IT security role.

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 44). A total of 19 industries (plus "Other") are represented in this year's study (see Figure 45). The big 7 industries – education, finance, government, healthcare, manufacturing, retail, and telecom & technology – accounted for 68.0% of all respondents. No single industry accounted for more than 15.2% of participants.

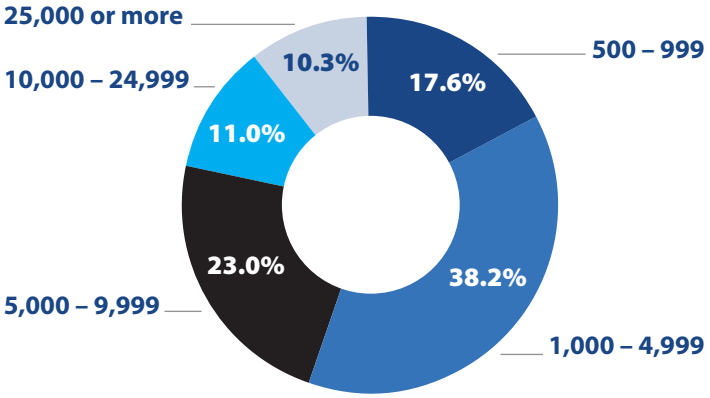

Figure 44: Survey participants by organization employee count.

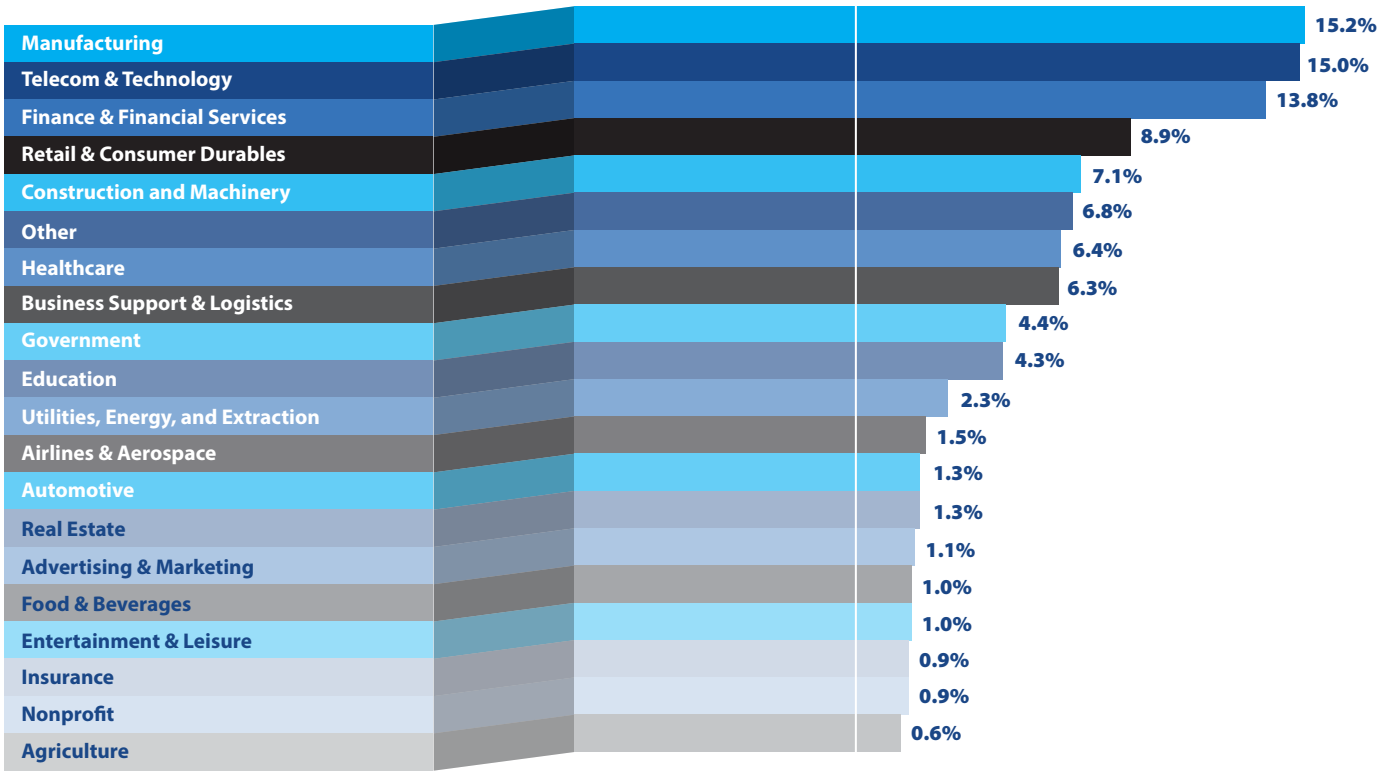

Figure 45: Survey participants by industry.

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 and December 2025. 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 its survey data is of the highest caliber by following these industry best practices:

- Ensuring that the right people are being surveyed by (politely) exiting respondents from the survey who don't meet the respondent filter criteria of the survey (e.g., job role, job seniority, company size, industry)
- Ensuring that disqualified respondents (who do not meet respondent filter criteria) cannot restart the survey (from the same IP address) in an attempt to obtain the survey incentive
- Constructing survey questions in a way that eliminates survey bias and minimizes the potential for survey fatigue
- Only accepting completed surveys after the respondent has provided answers to all of the 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

Google Cloud Security | cloud.google.com/security

Make Google part of your security team with unmatched threat visibility, a unified security platform, and Mandiant frontline expertise — supercharged by AI. Google is ushering in a new era of AI-powered security. Google's unique full-stack AI capabilities, powerful automation, and world-class experts help when you need it. Agentic AI makes everyone more productive and bends the curve on decades-old security challenges to protect organizations like never before. Organizations can further reduce digital risk and secure their AI transformation with Google.

ISC2 | www.isc2.org

ISC2 is the world's leading member organization for cybersecurity professionals, driven by our vision of a safe and secure cyber world. Our more than 265,000 certified members, and associates, are a force for good, safeguarding the way we live. Our award-winning certifications – including cybersecurity's premier certification, the CISSP® – enable professionals to demonstrate their knowledge, skills and abilities at every stage of their careers. ISC2 strengthens the influence, diversity and vitality of the cybersecurity profession through advocacy, expertise and workforce empowerment that accelerates cyber safety and security in an interconnected world.

Rubrik | www.rubrik.com

Rubrik is the Security and AI Operations Company. The company's data security platform secures and recovers data from cyber threats and operational disruptions. Rubrik has been recognized as a Leader in the Gartner Magic Quadrant for Enterprise Backup and Recovery Software Solutions for two consecutive years and is trusted by over 6,600+ customers across the globe. Rubrik Security Cloud delivers complete cyber resilience by securing, monitoring, and recovering data, identities, and workloads across clouds. Rubrik Agent Cloud accelerates trusted AI agent deployments at scale by monitoring and auditing agentic actions, enforcing real-time guardrails, fine-tuning for accuracy and undoing agentic mistakes.

SentinelOne | www.sentinelone.com

SentinelOne (NYSE:S) is the world's most advanced, autonomous AI-powered cybersecurity platform. Built on the first unified Data Lake, SentinelOne empowers the world to run securely by creating intelligent, data-driven systems that think for themselves, stay ahead of complexity and risk, and evolve on their own. The SentinelOne Singularity™ Platform enables global enterprises to automatically prevent, detect, and respond to cyber-attacks with machine speed and pinpoint accuracy. Leading organizations—including Fortune 10, Fortune 500, and Global 2000 companies, as well as prominent governments—all trust SentinelOne to Secure Tomorrow™.

Appendix 3: Research Sponsors

Gold Sponsors

ColorTokens | www.colortokens.com

ColorTokens is a leading provider of enterprise microsegmentation and breach-containment solutions, dedicated to making organizations "breach ready." By preventing the lateral spread of ransomware and advanced malware, ColorTokens protects complex network infrastructures through its innovative Xshield™ platform. The platform visualizes traffic between workloads, OT/IoT/IoMT devices, and users, enforcing granular micro-perimeters for effective breach response. Recognized as a Leader in both The Forrester Wave™: Microsegmentation Solutions and the GigaOm Radar for Microsegmentation, industry-leading organizations in healthcare, manufacturing, finance, and critical infrastructure depend on ColorTokens to ensure the continuity of their operations and protect their critical systems from compromise.

HackerOne | www.hackerone.com

HackerOne is a global leader in Continuous Threat Exposure Management, helping organizations identify and eliminate vulnerabilities before they can be exploited. Its platform combines AI-powered capabilities with the expertise of the world's largest community of security researchers to continuously test across the software development life cycle. From bug bounty programs to AI red teaming, HackerOne enables organizations to discover, validate, prioritize, and remediate risks in real time. Trusted by leading enterprises and government agencies, HackerOne delivers measurable security outcomes, reducing risk, strengthening resilience, and helping teams build trust in an increasingly complex threat landscape.

Veracode | www.veracode.com

Veracode, a global leader in Application Risk Management for the AI era, empowers organizations to secure software from code creation to cloud deployment. Trusted by thousands of development and security teams, Veracode delivers actionable insights, real-time vulnerability remediation, and scalable risk reduction. Its award-winning platform offers comprehensive solutions, including Veracode Fix, Static and Dynamic Analysis, Software Composition Analysis, Container Security, Application Security Posture Management, Malicious Package Detection, and Penetration Testing. Powered by trillions of code scans and an AI-assisted remediation engine, Veracode ensures secure software development across the entire lifecycle.

XBOW | www.xbow.com

XBOW is an autonomous offensive security platform that operationalizes penetration testing as a continuous, AI-driven system. Leveraging multi-agent AI to emulate attacker workflows, XBOW autonomously discovers, exploits, and validates vulnerabilities across applications, providing reproducible proof of exploitability. XBOW enables enterprises to prioritize real risk, compress time-to-remediation, and scale offensive security coverage. Adopted by companies from startups to Fortune 500 firms and global enterprises, XBOW is a mission-critical layer in today's security stacks. Visit our website to start your pentest today.

Appendix 3: Research Sponsors

Silver Sponsors

Cynet | www.cynet.com

Cynet's unified, AI-powered cybersecurity platform delivers a comprehensive suite of security capabilities in a single, simple solution backed by 24×7 SOC security experts. As a global cybersecurity company, Cynet is purpose-built to enhance protection for small-to-medium enterprises and empower partners to maximize margins while delivering world-class security.

Keeper Security | www.keepersecurity.com

Keeper Security is transforming cybersecurity for millions of individuals and thousands of organizations globally. Built with end-to-end encryption, Keeper's intuitive cybersecurity platform is trusted by Fortune 100 companies to protect every user, on every device, in every location. Our patented zero-trust and zero-knowledge privileged access management solution unifies enterprise password, secrets and connections management with zero-trust network access and remote browser isolation. By combining these critical identity and access management components into a single cloud-based solution, Keeper delivers unparalleled visibility, security and control while ensuring compliance and audit requirements are met.

Mitiga | www.mitiga.io

Mitiga takes cyber resilience from idea to reality by providing a safety net for cyber defenders operating across today's expanding cloud and AI attack surface. Mitiga's Zero-Impact cloud detection & response (CDR) platform ensures cyberattacks cause no impact, giving security teams real-time visibility, control, and breach prevention when it matters most. Mitiga tracks activity as it happens across SaaS, identities, AI infrastructure, and cloud services, identifying anomalous behavior and decoding attacks into clear timelines so teams can stop active threats. In a world where attackers no longer break in but log in, Mitiga empowers organizations to stay in control.

Wallarm | www.wallarm.com

AI security is API security. Every interaction with AI is mediated through APIs, and the explosive growth of AI drives development, adoption, and usage of APIs. This is why APIs have become the number one attack surface. At the same time, AI adoption isn't slowing down. Organizational leaders need to drive AI adoption seamlessly and securely. Confident AI transformation starts with secure APIs. Wallarm protects every connection, at runtime and at scale. We secure every business transaction by protecting the applications, APIs, and AI systems in real time, in production. That means CISOs and CIOs can move fast, reduce risk, and scale securely

Media Sponsor

Security Buzz | https://securitybuzz.com/

Security Buzz is a leading cybersecurity news website. A subsidiary of CyberEdge Group, our mission is to deliver accurate, timely, and actionable information to help IT professionals and the general public navigate the complex world of cybersecurity. By offering a mix of breaking news, expert insights, and practical resources, we aim to empower our readers to make informed decisions and enhance their cyber defense strategies.

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.

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, CISO Magazine,* and *Security Buzz.*

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
- Artificial Intelligence (AI)
- Cloud Security
- Data Security
- Deception Technology
- DevSecOps
- DoS/DDoS Protection
- Endpoint Security (EDR & EPP)
- ICS/OT Security
- Identity Security
- 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@cyberedgegroup.com, or connect to our website at www.cyberedgegroup.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: 2026 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 www.cyberedgegroup.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@cyberedgegroup.com.

Copyright © 2026, CyberEdge Group, LLC. All rights reserved. The CyberEdge Group name and logo are the property of CyberEdge Group, LLC. All other company names, trademarks, and service marks are the property of their respective owners. Version 1.0