Ponemon INSTITUTE

The 2025 Global Study on Closing the IT Security Gap

Sponsored by Hewlett Packard Enterprise

Independently conducted by Ponemon Institute LLC

Publication Date: February 2025

Ponemon INSTITUTE

The 2025 Global Study on Closing the IT Security Gap

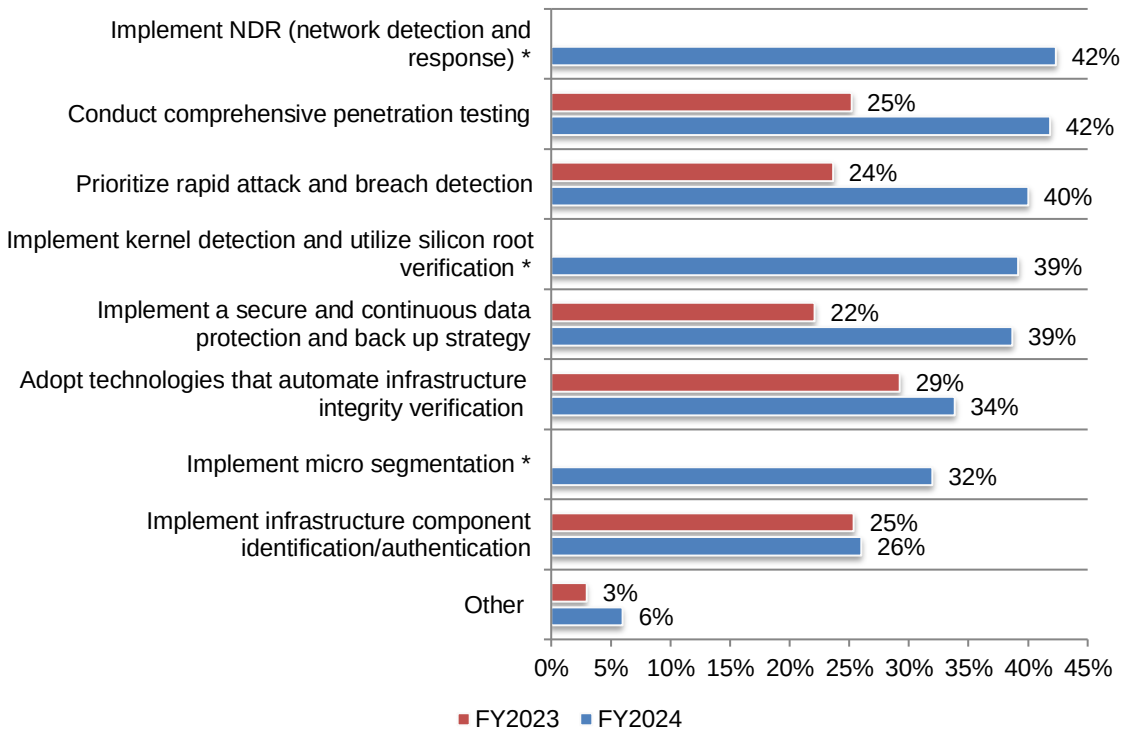
Prepared by Ponemon Institute, February 2025

Part 1. Introduction

Ransomware, network and application attacks, insider threats and denial of service attacks are just a few of the threats putting organizations on high alert. The increasing sophistication of cyber criminals—as well as these cyber criminals adopting AI—makes it more important than ever to become aggressive in closing security gaps in the IT infrastructure.

New approaches to closing the IT security gap are needed. In 2023, organizations had an average of five security breaches over a 12-month period. This increased to an average of six incidents in 2024. With the difficulty in reducing breaches and security incidents, organizations are changing their activities and use of technology. As shown in Figure 1, since 2023 the most significant changes are the use of comprehensive penetration testing (an increase of 17 percent of respondents), implementation of a secure and continuous data protection and back up strategy (an increase of 17 percent of respondents) and prioritization of rapid attack and breach detection (an increase of 16 percent of respondents). For the first time, the study asked if network detection and response (NDR) (42 percent), kernel detection/silicon root verification (39 percent) and micro segmentation (32 percent) are new technologies deployed to close the IT security gap. [1]

Figure 1. What are the most effective steps and technologies to minimize threats within the IT infrastructure?
Three responses permitted *new response in 2024



[1] NDR solutions analyze network traffic to detect suspicious activity and understand security risks and exposures. Kernel detection solutions help organizations detect and prevent kernel attacks. A kernel attack is a sophisticated cyberattack that exploits vulnerabilities in a computer's kernel or kernel drivers to gain access to the system and make changes. Micro segmentation is a security method of managing network access between workloads.

Optimizing AI technologies to close the IT security gap

AI's ability to close the cybersecurity gap depends upon close collaboration between network and security teams. Thirty-nine percent of respondents say their organizations have adopted AI to close the IT security gap. In addition to improving collaboration between network and security teams (34 percent of respondents), other AI priorities include aiding in threat investigations (32 percent of respondents) and detecting changes to the organizations' security posture (30 percent of respondents).

To have a successful AI strategy, organizations need assurances about AI accuracy, privacy safeguards and data leakage prevention. Organizations considered uncertainties about AI accuracy, difficulties in ensuring data privacy and difficulties in preventing data leakage their greatest challenges with AI (all 44 percent of respondents). Another possible deterrent to closing the IT security gap is not having the confidence that their organizations know and are able to secure **all** AI assets including infrastructure, models and data. Only 43 percent of respondents say their organizations are very or highly confident they have that visibility.

Organizations considering the use of AI for business purposes need to evaluate the possible complexity the technology will add to their operations. Fifty-three percent of the 39 percent of respondents who have adopted AI are using AI for business purposes. The security risks created when AI is used for business purposes are increased complexity because of the addition of new security tools (57 percent of respondents), potential theft or leakage of confidential and sensitive data (47 percent of respondents) and the inability to recover lost data in the event of an attack or disaster (44 percent of respondents).

Why the IT security gap continues to put organizations at risk

Not having the necessary skilled IT professionals continues to be the number one barrier to closing the IT security gap. While fewer organizations are reporting shortages in security staffing, skills and experience (30 percent vs. 39 of respondents in 2023), shortages are still affecting organizations' security posture. Additional barriers to closing the IT security gap include security solutions that can't keep up with exponentially increasing amounts of data and difficulty in complying with IT security and privacy industry standards or regulations (each 29 percent of respondents).

Too many vendors to manage and lack of collaboration between network and security teams can weaken organizations' cybersecurity posture. Fifty-six percent of respondents say managing multiple security vendors is challenging and, as a result, can diminish their organization's security posture. Forty-seven percent of respondents say it is difficult to achieve collaboration between network and security teams. Such collaboration is critical to preventing friction between IT and security teams that hinder efforts to put an effective strategy in place.

New approaches to securing the modern workplace

Secure Access Service Edge (SASE) frameworks combine networking and security capabilities into a unified, cloud-based solution, ensuring seamless access and protection for distributed workforces and enterprise assets.

Organizations are at various stages in their SASE deployment. In 2024, 23 percent of respondents say their organizations have deployed SASE, 23 percent of respondents say they will deploy in 12 months and 19 percent of respondents say their organizations will deploy SASE sometime in the future.

Reduction of costs, improved application performance and improved security posture are priorities for deploying SASE. Thirty-seven percent of respondents say their organizations deployed SASE first to reduce costs and improve application performance for users and

branches. Thirty-six percent of respondents say their organizations started their SASE journey with an SSE deployment to improve security posture and increase protection. The number one SASE deployment strategy is to engage a best-in-class SD-WAN vendor that integrates with SSE vendors (30 percent of respondents) followed by engaging a best-in-class SSE vendor that integrates with SD-WAN vendors (27 percent of respondents).

Universal Zero Trust Network Access (ZTNA) is a security framework that allows organizations to grant secure access to applications for subjects regardless of their location. Forty-eight percent of respondents say their organizations have deployed universal ZTNA in some form. According to the research, the three most important characteristics of the universal ZTNA approach are enabling least privilege access to support zero trust (35 percent of respondents), ensuring a seamless access experience for users anywhere (30 percent of respondents) and securing IoT devices and users (29 percent of respondents).

Closing IT security gaps in hybrid cloud environments.

Organizations are securing their hybrid cloud environments in multiple ways. The processes prioritized to minimize the risk in a hybrid cloud environment are the implementation of a defined cybersecurity compliance framework (46 percent of respondents) in 2024, securely shifting workloads from on-premises to the cloud (44 percent of respondents) and the modernization of IT security processes (43 percent of respondents).

Organizations are improving their ability to avoid security exploits and data breaches and secure workloads moving between on-premises and public cloud environments. Organizations appear to be making progress on several security fronts: The percentage of respondents who say challenges associated with avoiding security exploits and data decreased from 51 percent of respondents in 2023 to 43 percent of respondents in 2024. Similarly, the challenge of securing workloads moving from the edge to the cloud decreased from 43 percent in 2023 to 36 percent of respondents in 2024. The primary technology challenge continues to be enabling the free flow of data securely (46 percent of respondents).

Organizations are having greater difficulty in their ability to ensure the privacy of customer information and enable the free flow of information in the hybrid cloud environment. Since 2023, more respondents say ensuring customers' privacy and enabling the free flow of information has made it more difficult to secure the hybrid cloud environment (37 percent and 32 percent of respondents, respectively).

Separating storage and compute means they can be consumed, scaled, and priced independently. This allows businesses to pay for what they use and nothing more. Organizations in this research say their current security approach to compute and storage will change. The biggest changes organizations indicate they will face in separating storage and compute will be moving their current security approach to the cloud (28 percent of respondents), managing a combination of solutions from security and hybrid cloud infrastructure providers (25 percent of respondents) and requiring vendors to supply new security solutions (24 percent of respondents).

More organizations are making server decisions based on the security inherent within the platform (62 percent of respondents, a significant increase from 48 percent in 2023). Fifty-eight percent of respondents say their organizations require servers that leverage security certificates to identify that the system has not been compromised during delivery. Fifty-eight percent of respondents say data protection and recovery are key components of their organizations' security strategy and 58 percent of respondents say their organizations require infrastructures that leverage chip and/or certificates to determine if the system has been compromised during delivery.

Best practices of high-performing organizations

Twenty-one percent of respondents reported that their organizations are highly effective in keeping up with a constantly changing threat landscape and closing their organization's IT security gap. We refer to these organizations as "high performers" and compare their responses to the non-high performer respondents, referred to as "other".

Collaboration between network and security teams is essential to a successful security strategy. Fifty-four percent of high performers vs. 40 percent of others have achieved collaboration.

High performers are most likely to have a vendor consolidation strategy. Too many vendors to manage affect an organization's security posture. Fifty-nine percent of high performers vs. 51 percent of other respondents have a vendor consolidation strategy to improve ROI.

High performers are more likely to adopt AI. There is a significant difference in high performers' and others' adoption of AI (61 percent of respondents vs. 49 percent).

High performers place a higher value on NAC solutions and the integration of NAC functionality. Respondents were asked to rate the importance of NAC solutions and integration on a scale of 1 = not important to 10 = highly important. The importance of NAC solutions (60 percent vs. 41 percent) and integration of NAC functionality (56 percent vs. 41 percent) are rated higher by high performers.

When it comes to universal zero trust network access, high performers place notably greater importance on seamless access experience for users anywhere. High performers are more positive about seamless access and consistent enforcement at every location (34 percent of high performers vs. 26 percent of other respondents). Twenty-nine percent of high performers vs. 22 percent of the others rate consistent enforcement at every location higher than the other respondents.

High performers are more likely to make the identification and authentication of IoT devices accessing their networks critical to their organizations' security strategy. Fifty-nine percent of high performers vs. 48 percent of the others are more focused on identifying and authenticating IoT devices with access to their organizations' network.

High performers are more likely to require infrastructure that leverages chip and/or certificates to determine if the system has been compromised during delivery. Sixty-six percent of high performers vs. 49 percent of the others require infrastructure that leverages chip and/or certificates to determine if the system has been compromised during delivery.

Recommendations to close the IT security gap

To close the IT security gap organizations are making significant changes in their strategies to minimize threats within the IT infrastructure. These include implementing NDR, conducting comprehensive penetration testing, prioritizing rapid attack and breach detection and implementing a secure and continuous data protection and back up strategy. New in this year's research is organizations' adoption of AI (39 percent of respondents). Organizations' primary goals for AI are to improve collaboration between network and security teams, to aid in threat investigations and to detect changes in the organizations' security posture.

Following are actions to consider in the coming year.

- Develop an AI strategy. An effective AI deployment is dependent upon removing uncertainties about AI's accuracy, ensuring the privacy of sensitive and confidential data and assessing the risks to prevent data leakage.

- Consolidate vendors to reduce redundancies of solutions that increase costs and create inefficiencies for the IT security team. To achieve consolidation of vendors evaluate spend categories to identify vendor overlap and map vendors' capabilities to determine where cuts can be made.

- Improve cyber resiliency by taking steps to reduce the time to recover from a critical system failure caused by a cyber incident. As shown in this research, only 35 percent of respondents say recovery can be achieved in less than one hour (12 percent) or in 1 to 4 hours (23 percent). This includes making sure technologies are used efficiently and having a cybersecurity incident response plan in place to navigate a security crisis.

Part 2. Key findings

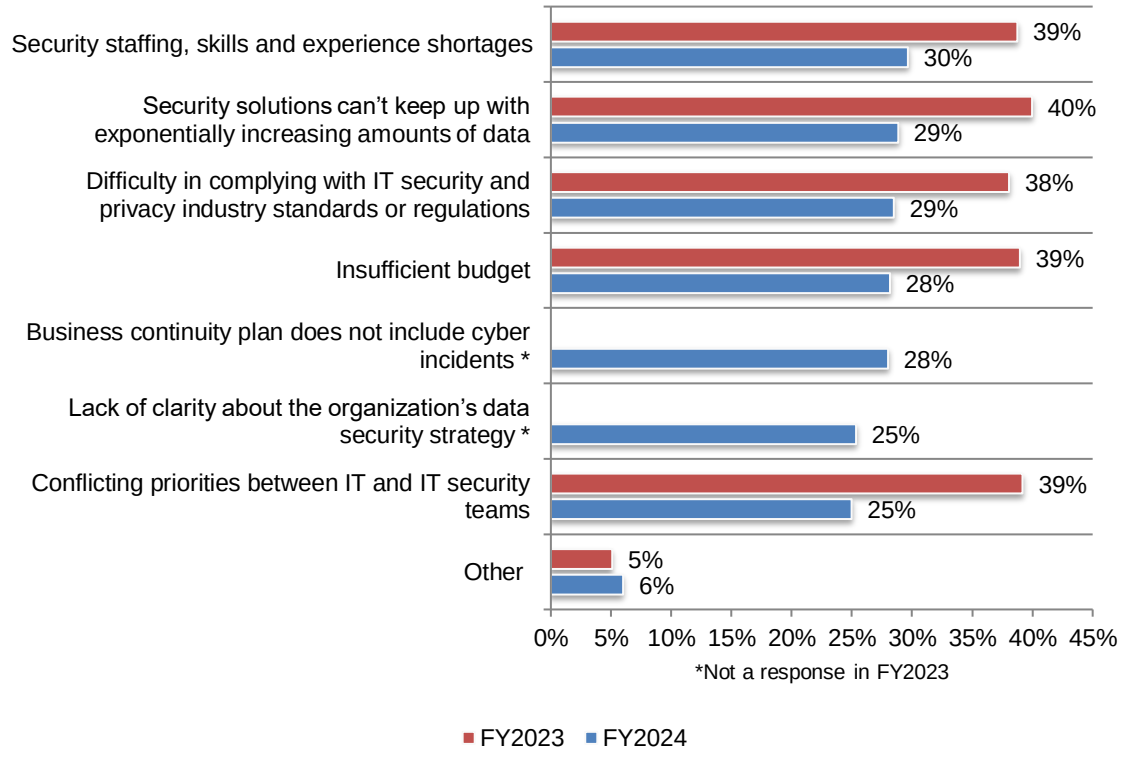
Ponemon Institute surveyed 2,120 IT and IT security practitioners in the United States (635), the United Kingdom (291), Germany (371), France (197), Australia (180) and Japan (446) in 2024 for publication in 2025. In this report, we present the 2023 and 2024 global findings. The audited findings are presented in the Appendix of this report. We have organized the findings according to the following topics.

- Barriers to closing the IT security gap
- Closing the IT security gap with artificial intelligence
- Imperatives for controlling access: zero trust, NAC, SASE and universal ZTNA
- Securing the hybrid cloud
- The separation of compute and storage
- Country differences
- Best practices in closing the IT cybersecurity gap

Barriers to closing the IT security gap

Not having the necessary skilled IT professionals continues to be the number one barrier to closing the IT security gap. As shown in Figure 2, while fewer organizations are reporting security staffing, skills and experience shortages (30 percent in 2024 vs. 39 of respondents in 2023), it is still affecting organizations' security posture. Another challenge is not having security solutions that can keep up with increasing amounts of data (29 percent in 2024 vs. 40 percent of respondents in 2023). For the first time, "business continuity plan does not include cyber incidents" (28 percent of respondents) and "lack of clarity about the organization's data security strategy" responses were added.

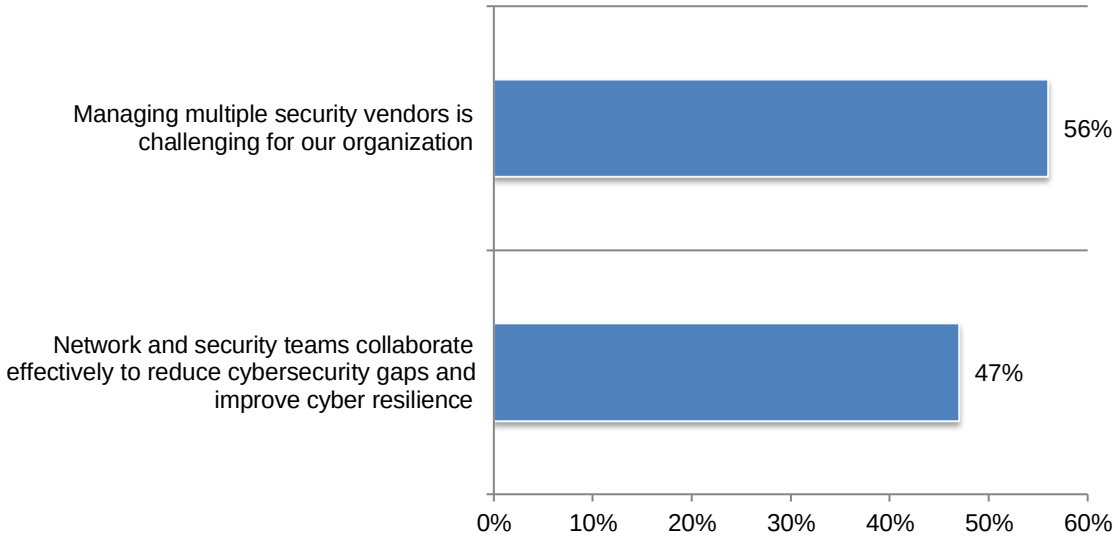
Figure 2. The operational and governance gaps in organizations' IT infrastructure
Two responses permitted



Too many vendors to manage and lack of collaboration between network and security teams can weaken organizations' cybersecurity posture. According to Figure 3, 56 percent of respondents say managing multiple security vendors is challenging and, as a result, can weaken their organization's security posture. Some of the negative consequences of having too many security vendors are redundancies of solutions used, increasing costs and the inefficiencies in managing multiple vendor contracts.

Only 47 percent of respondents say their organizations' network and security teams collaborate effectively to reduce IT security gaps. Such collaboration is critical to preventing friction between IT and security teams that hinder efforts to put an effective strategy in place. Successful collaboration starts with the CIO and CISO being in alignment about roles, responsibilities and budgets. Network and security teams working together will help close the operational and governance gaps that affect organizations' ability to defend and protect vital assets and network systems.

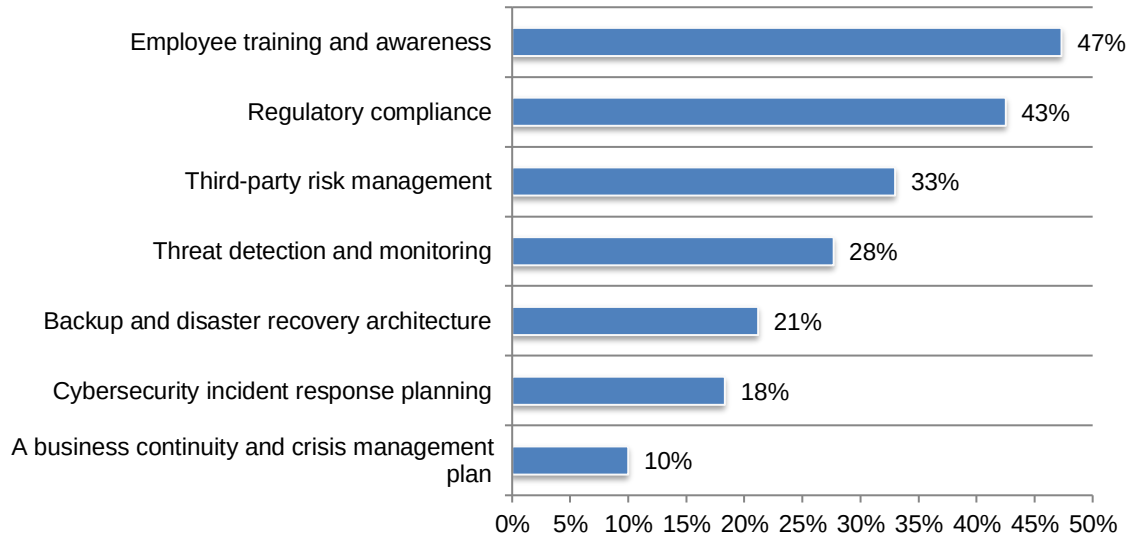
Figure 3. To shrink the security gap, reduce the number of vendors and improve collaboration between network and security teams
Strongly agree and Agree responses combined



Cyber resilience is the alignment of prevention, detection and response capabilities to manage, mitigate and move on from cyberattacks. This refers to an enterprise's capacity to maintain its core purpose and integrity in the face of cyberattacks. A cyber resilient enterprise is one that can prevent, detect, contain and recover from myriad serious threats against data, applications and IT infrastructure.

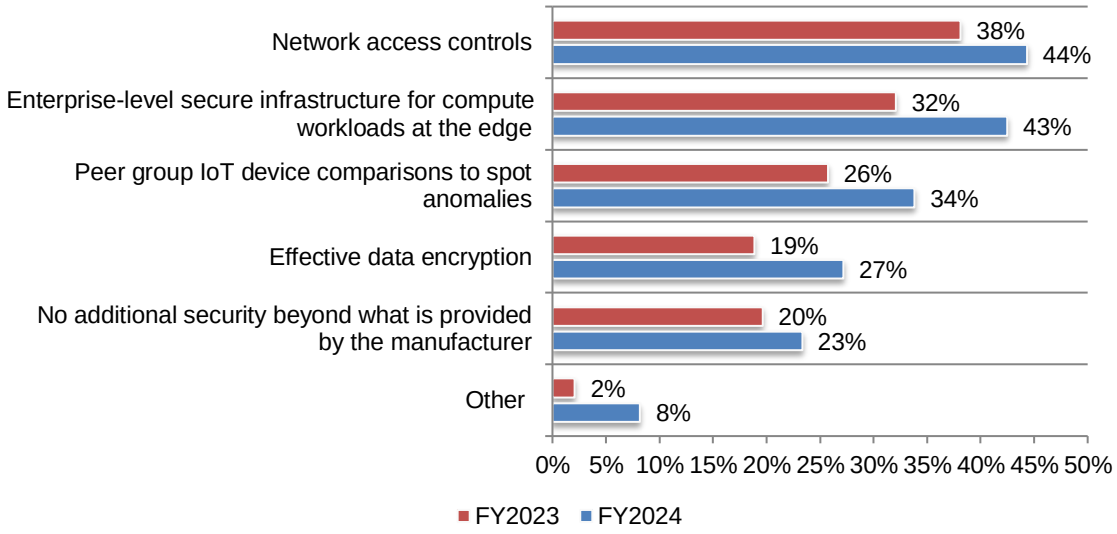
Organizations' cyber resilience is tested in how quickly they can recover from a critical system failure caused by a cyber incident. According to the research, only 35 percent of respondents say recovery can be achieved in less than one hour (12 percent) or in 1 to 4 hours (23 percent). According to Figure 4, organizations are prioritizing employee training and awareness (47 percent of respondents), regulatory compliance (43 percent of respondents) and third-party risk management (33 percent of respondents) to improve their cyber resilience

Figure 4. Priorities to improve cyber resilience
Two responses permitted



Network access controls are key to achieving a strong level of IoT security. More than half of respondents (52 percent) say identifying and authenticating IoT devices accessing the network is critical to their organizations' security strategy. As shown in Figure 5, two measures are considered most important to closing IT security gaps created by risks associated with IoT devices: network access controls (selected by 44 percent of respondents, up from 38 percent of respondents in 2023) and enterprise-level secure infrastructure for compute workloads at the edge (selected by 43 percent of respondents, up from 32 percent of respondents in 2023).

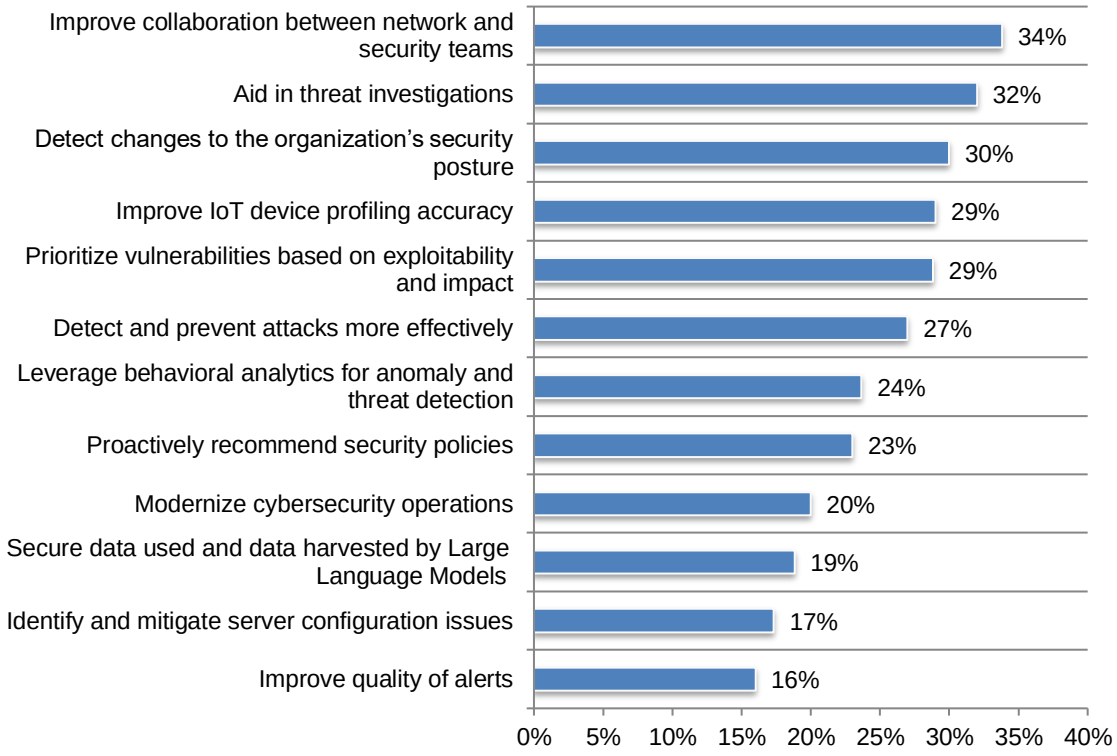
Figure 5. What is required to achieve a strong level of IoT security within your organization?
More than one response permitted



Closing the IT security gap[2] with artificial intelligence (AI)

AI's ability to close the cybersecurity gap depends upon close collaboration between network and security teams. Thirty-nine percent of respondents say their organizations have adopted AI to close the IT security gap. As shown in Figure 6, in addition to improving collaboration between network and security teams (34 percent of respondents), other AI priorities are aiding in threat investigations (32 percent of respondents) and detecting changes to the organizations' security posture (30 percent of respondents).

Figure 6. What are the priorities for using AI to close the security gap?
Three responses permitted

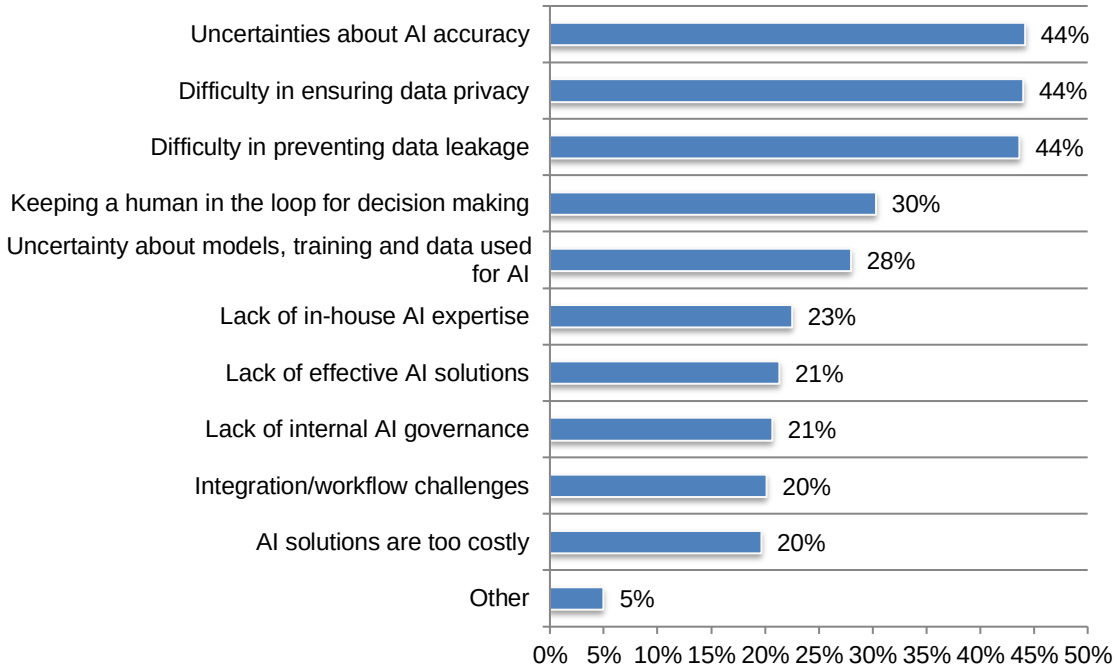


[2] In the context of this research, the IT security gap is defined as the inability of an organization's people and technologies to keep up with a constantly changing threat landscape. The IT security gap diminishes the ability of organizations to identify, detect and resolve data breaches and other security incidents.

To have a successful AI strategy, organizations need assurances about AI's accuracy, privacy safeguards and data leakage prevention. Figure 7 lists the challenges organizations need to overcome when adopting AI. These mainly are uncertainties about AI accuracy, difficulties in ensuring data privacy and difficulties in preventing data leakage (all 44 percent of respondents).

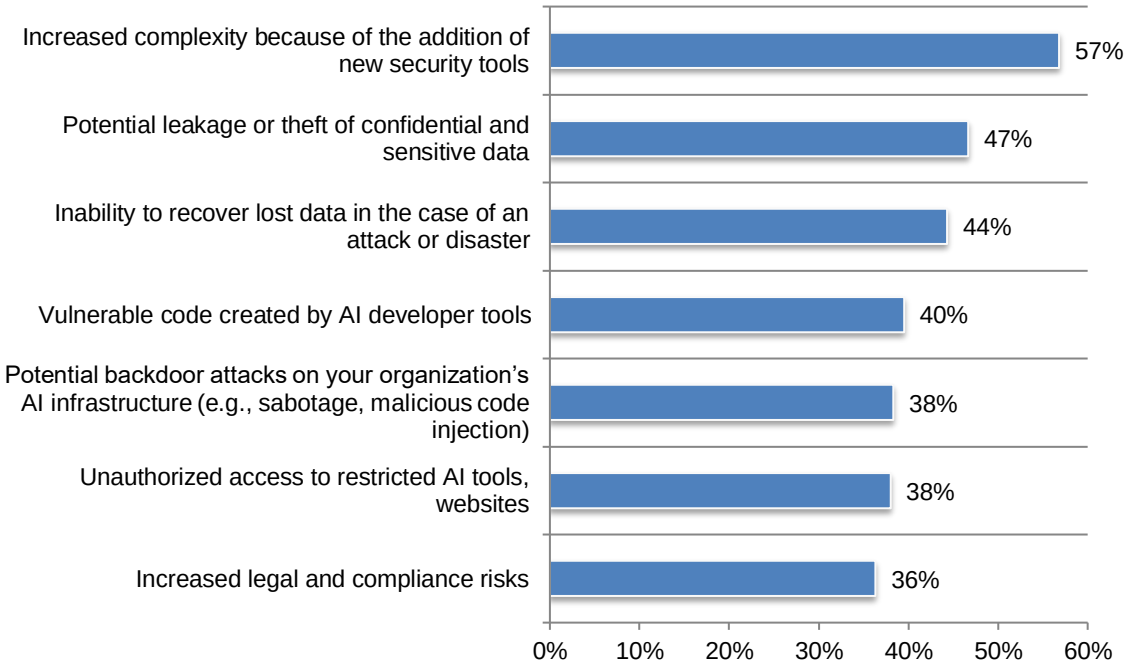
Another possible deterrent to organizations closing the IT security gap is not having the confidence that their organizations know and are able to secure **all** their AI assets including infrastructure, models and data. Only 43 percent of respondents say their organizations are very or highly confident they have that visibility.

Figure 7. What are your organization's primary challenges when adopting AI to close cybersecurity gaps?



Organizations considering the use of AI for business purposes need to evaluate the possible complexity the technology will add to their operations. Thirty-nine percent of respondents have adopted AI. Of these respondents, 53 percent are using AI for business purposes. As shown in Figure 8, the top three security risks created when AI is used for business purposes are increased complexity because of the addition of new security tools (57 percent of respondents), potential theft or leakage of confidential and sensitive data (47 percent of respondents) and the inability to recover lost data in the event of an attack or disaster (44 percent of respondents).

Figure 8. What are the security risks created by the adoption of AI for business purposes?
Three responses permitted



Imperatives for controlling access: Zero trust, NAC, SASE and universal ZTNA

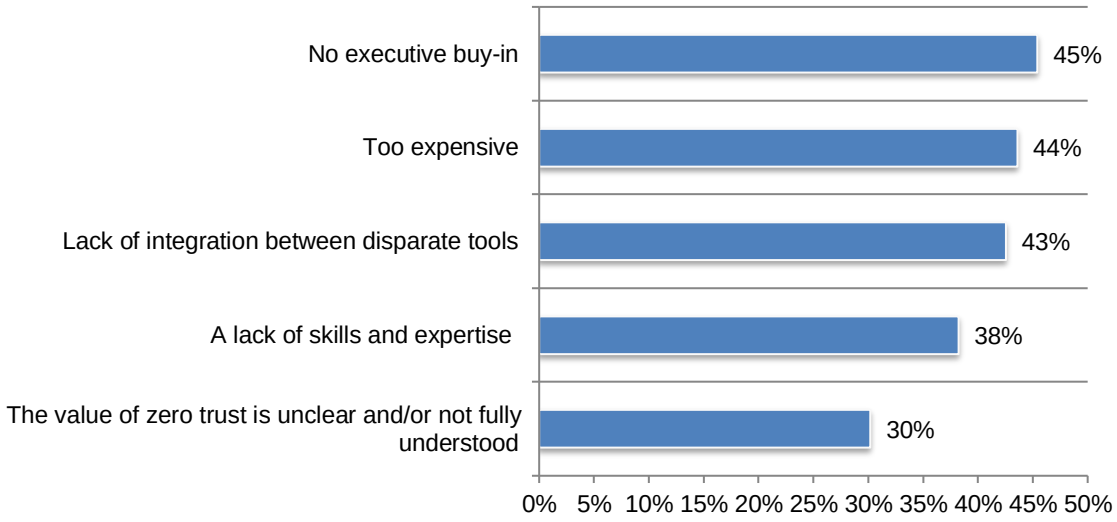
Zero trust and related strategies for controlling access to resources—network access controls (NAC), Secure Access Service Edge (SASE) and universal zero trust network access (universal ZTNA)—are increasingly being embraced as strategies to close the IT security gap. Zero-trust strategies are seen as especially effective in managing vulnerabilities and user access. As a guiding principle, zero trust assumes no implicit trust is granted to subjects based solely on their physical or network location or asset ownership.

Organizations vary in their timeline for the adoption of zero trust strategies. According to Figure 9, 28 percent of respondents say their organizations have adopted a zero-trust security model and 12 percent have adopted it because of government requirements. Twenty percent of respondents say their organization plans to adopt zero trust in the next six months (12 percent) or in a year (8 percent). Sixteen percent say their organizations do not have a zero-trust strategy.

Figure 9. What one statement best describes the adoption of your organization's approach to a zero-trust security model?
Only one choice permitted

Sixteen percent of respondents say their organizations do not have a zero-trust strategy. According to Figure 10. the top three reasons are lack of executive support (45 percent of respondents), high costs (44 percent of respondents) and the lack of integration between disparate tools (43 percent of respondents).

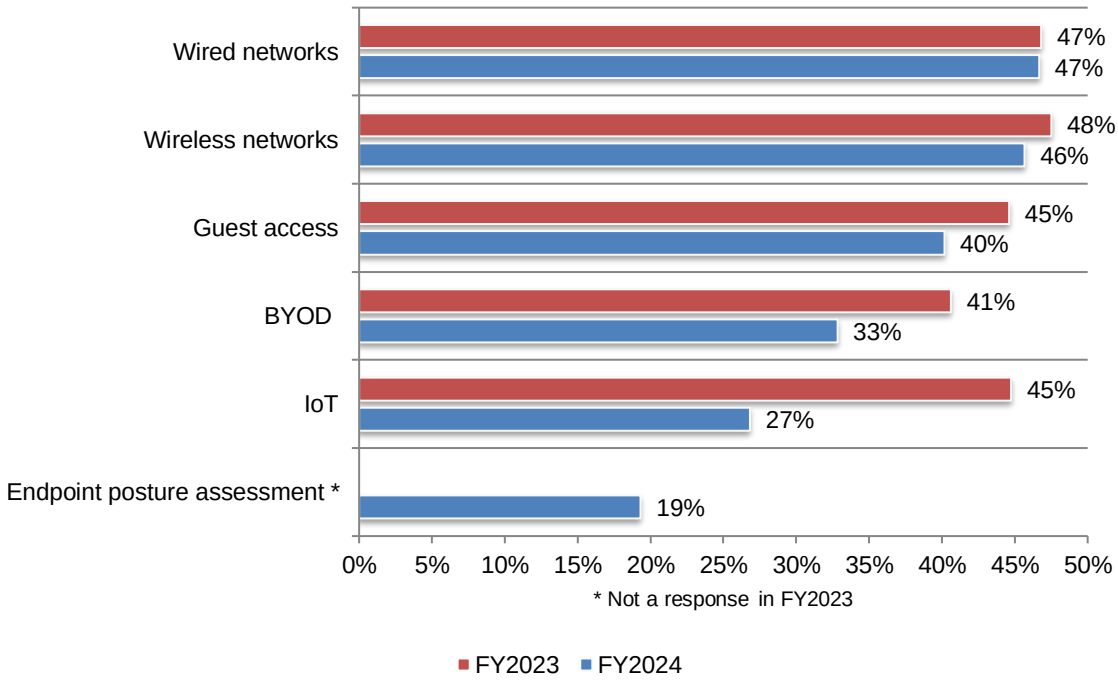
Figure 10. Why does your organization not have a zero-trust strategy?
Two responses permitted



Network access controls (NAC) restrict users and devices from reaching resources based on rules established by IT. Much like door locks and security badges keep intruders from accessing physical organizational resources like buildings and offices, NAC protects networked digital resources from unauthorized access. More than half of organizations (54 percent) in this study use NAC solutions, an increase from 32 percent in 2023.

According to Figure 11, NAC systems are primarily deployed for wired networks (47 percent of respondents) and wireless networks (46 percent of respondents). For the first time, the response "endpoint posture assessment" was added.

Figure 11. For what purposes are NAC systems deployed within your organization?



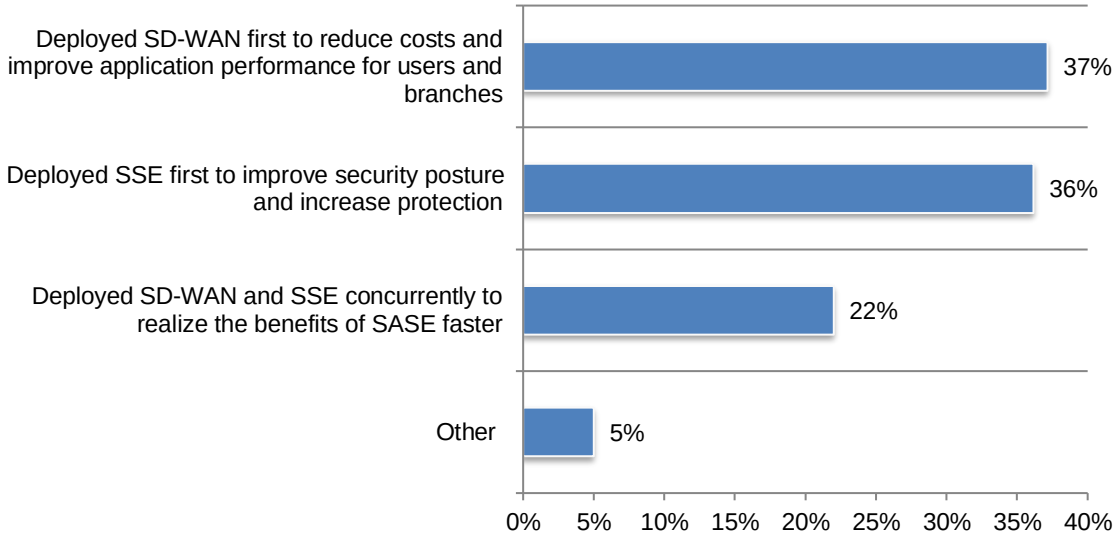
The Secure Access Service Edge (SASE) architecture refers to a cybersecurity environment that brings advanced protection right out to the farthest edge of the network: the endpoints of users. SASE brings together **Software-Defined Wide Area Network (SD-WAN) and Security Service Edge (SSE)** cloud security capabilities.

SSE comprises zero trust network access (ZTNA), cloud access security broker (CASB), secure web gateway (SWG) and other cloud-based security services that provide secure access to web, SaaS and private applications in distributed environments. In this SASE architecture definition, users are provided robust security features that are delivered directly to user devices from the cloud, enabling them to connect securely from anywhere. SASE security architecture enables users to take advantage of secure connections without having to worry about the latency that results from backhauling to the data center's firewall.

Organizations are at various stages in their SASE deployment. Twenty-three percent of respondents say their organizations have deployed SASE, 23 percent of respondents say they will deploy in 12 months and 19 percent of respondents say their organizations will deploy SASE sometime in the future.

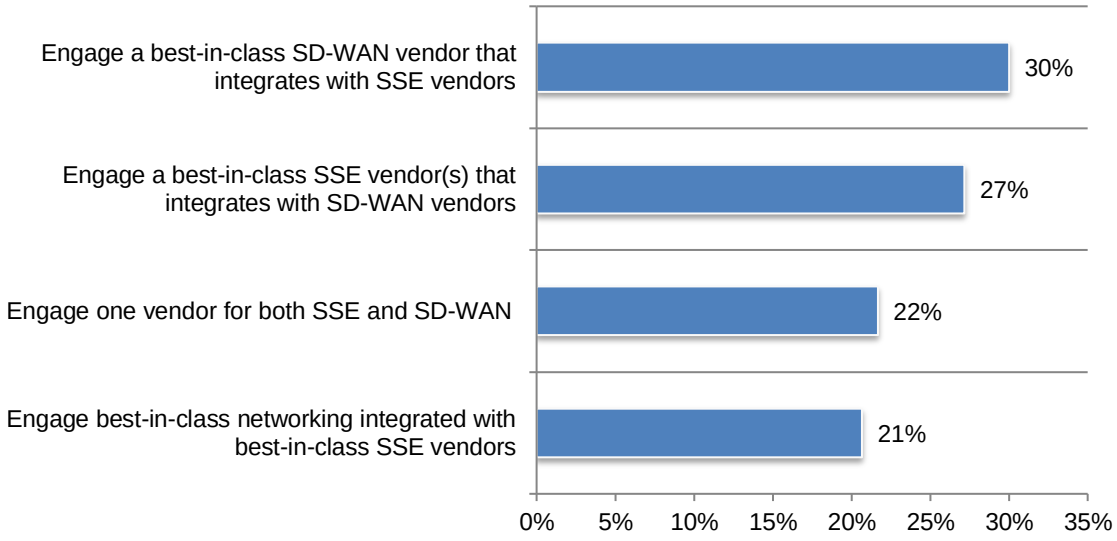
SD-WAN and SSE are deployed to reduce costs, improve application performance for users and branches and security posture. The priorities for SD-WAN and SSE deployment are listed in Figure 12. The top two choices are cost reduction and improved application performance (37 percent of respondents) and improved security posture and increased protection (36 percent of respondents).

Figure 12. What is the first step your organization took or will take in your SASE deployment?
Only one choice permitted



As shown in Figure 13, the number one SASE deployment strategy is to engage a best-in-class SD-WAN vendor that integrates with SSE vendors (30 percent of respondents) followed by engaging a best-in-class SSE vendor that integrates with SD-WAN vendors (27 percent of respondents).

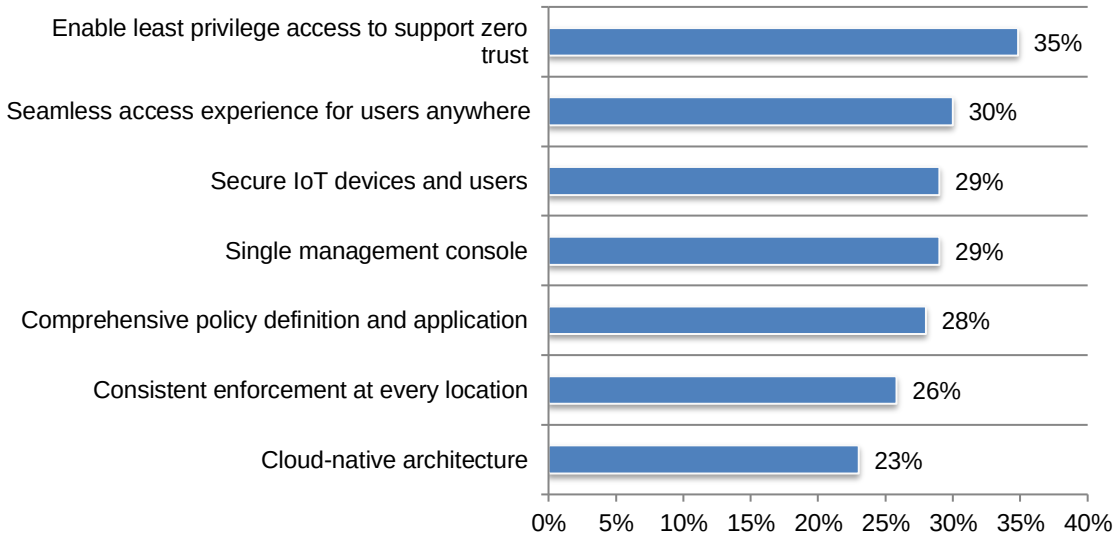
Figure 13. What best describes your organization's SASE deployment strategy?



Bringing together capabilities of NAC and SASE and universal zero trust network access allows organizations to grant users and devices secure access to applications regardless of their location. Forty-eight percent of respondents say their organizations have deployed universal ZTNA in some form.

As shown in Figure 14, the top three most important characteristics of a universal ZTNA approach are enabling least privilege access to support zero trust (35 percent of respondents), ensuring a seamless access experience for users anywhere (30 percent of respondents) and securing IoT devices along with users (29 percent of respondents).

Figure 14. What capabilities and characteristics are most important in a universal zero trust network access approach?
Two responses permitted



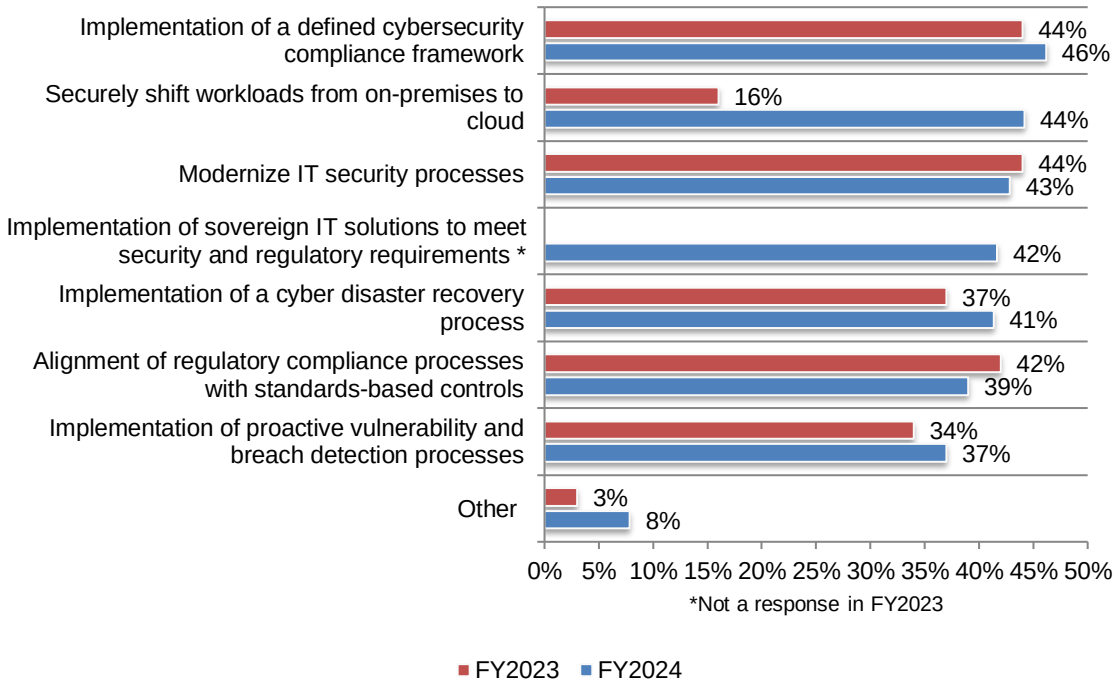
Securing the hybrid cloud

The shift to a **hybrid cloud** environment is driving connectivity to more users, devices and data than ever before. From a business perspective it means making decisions based on market demand and business opportunity, empowering consumers and fostering collaboration through innovation (mobile, cloud, IoT) and quickly and effectively releasing new applications to drive growth. From an IT security perspective, it means assessing digital exposure and overall risk to the business, protecting critical assets across the organization (network, endpoints, servers, cloud) and conforming and complying with regulations, industry standards and security best practices.

Forty-five percent of respondents say security technologies are very or highly important to a successful shift to a hybrid cloud environment. Sixty percent of respondents say their organizations' current security approach will be moved to the hybrid cloud, a slight decline from 65 percent of respondents in 2023.

Organizations are securing the hybrid cloud environment in multiple ways. As shown in Figure 15, the processes prioritized to minimize the risk in a hybrid cloud environment are the implementation of a defined cybersecurity compliance framework (46 percent of respondents), securely shifting workloads from on-premises to the cloud (a significant increase to 44 percent of respondents from 16 percent of respondents) and the modernization of IT security processes (43 percent of respondents). For the first time, the research included "implementation of sovereign IT solutions to meet security and regulatory requirements" as a possible response (42 percent of respondents).

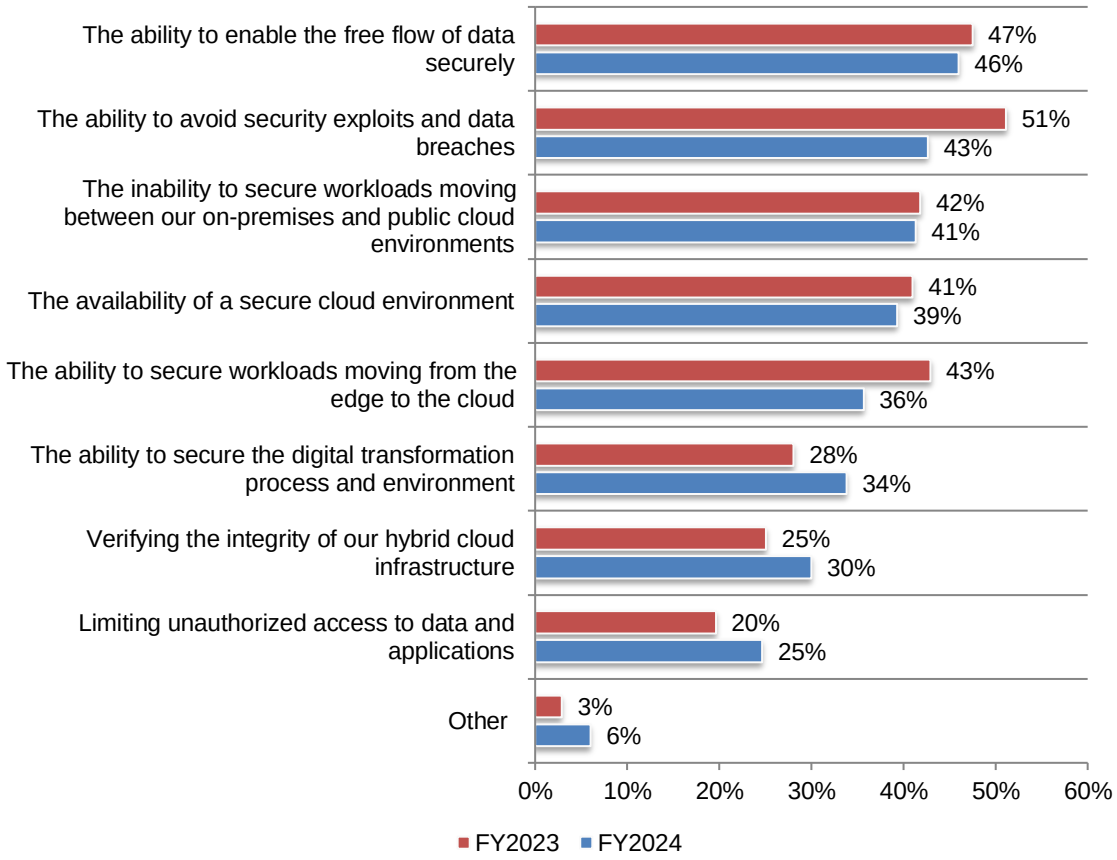
Figure 15. The processes prioritized to minimize the risk in a hybrid cloud environment
Three responses permitted



Organizations are improving their ability to avoid security exploits and data breaches. Figure 16 lists the challenges faced when securing the hybrid cloud environment. Organizations appear to be making progress on several fronts: The percentage of respondents who say challenges associated with avoiding security exploits and data breaches decreased from 51 percent of respondents in 2023 to 43 percent of respondents in 2024. Similarly, the percentage of respondents who say challenges to their ability to secure workloads moving from the edge to the cloud decreased from 43 percent in 2023 to 36 percent of respondents in 2024. The primary technology challenge continues to be enabling the free flow of data securely (46 percent of respondents).

Figure 16. The primary technology challenges when securing the hybrid cloud environment

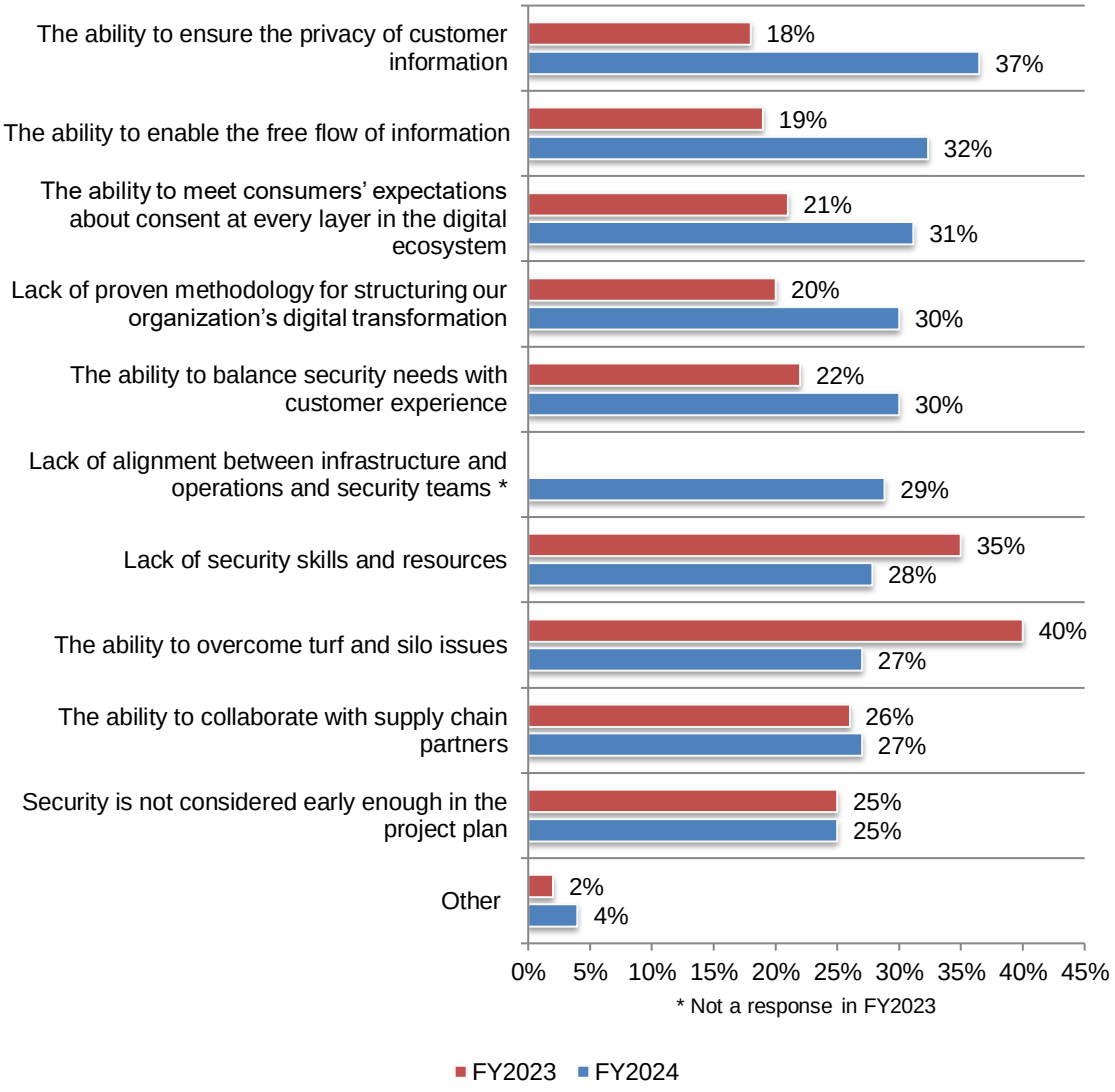
Three responses permitted



Organizations are having greater difficulty in their ability to ensure the privacy of customer information and enable the free flow of information in the hybrid cloud environment. Figure 18 lists the operational and governance challenges to securing the hybrid cloud environment.

As shown in Figure 17, since 2023, more respondents say ensuring customers' privacy and enabling the free flow of information has made it more difficult to secure the hybrid cloud environment (37 percent and 32 percent of respondents, respectively). The ability to meet consumers' expectations about consent at every layer in the digital ecosystem increased as a challenge from 21 percent to 31 percent of respondents. "Lack of alignment between infrastructure and operations and security teams" was added as a response for the first time.

Figure 17. The most significant operational and governance challenges to securing the hybrid cloud environment
Three responses permitted

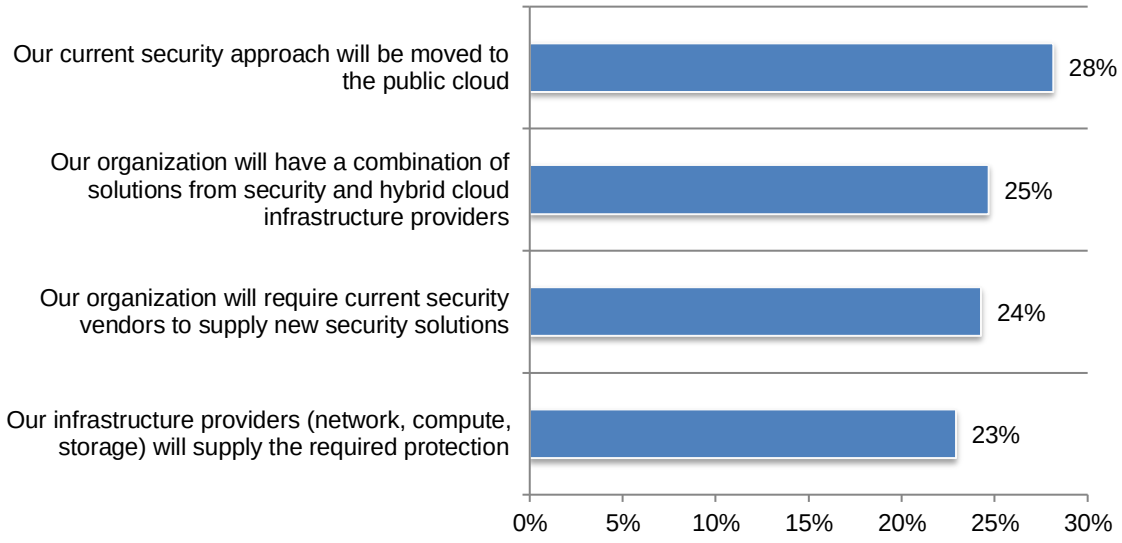


Separation of compute and storage

Separating storage and compute means they can be consumed, scaled, and priced independently. This allows businesses to pay for what they use and nothing more. Organizations in this research say their current security approach to compute and storage will change.

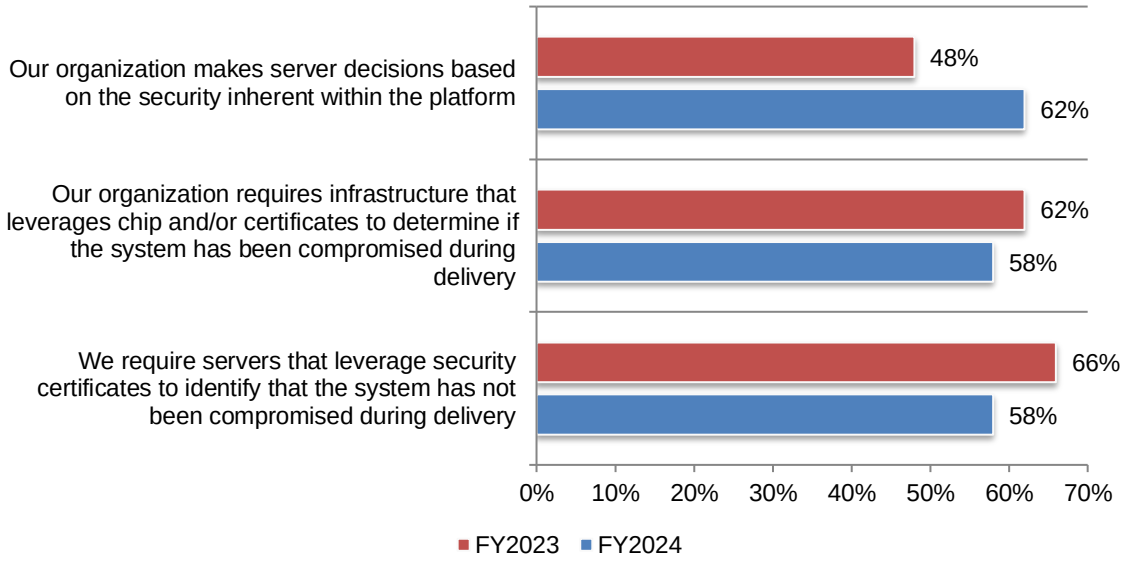
According to Figure 18, the biggest change as compute and storage moves from the datacenter to the edge will be moving their organizations' current security approach to the cloud (28 percent of respondents) followed by a combination of solutions from security and hybrid cloud infrastructure providers (25 percent of respondents).

Figure 18. How will your organization's current security approach change as compute and storage moves from the datacenter to the edge?



More organizations are making server decisions based on the security inherent within the platform. This is a significant increase from 48 percent of respondents in 2023 to 62 percent of respondents in 2024. As shown in Figure 19, 58 percent of respondents say their organizations require servers that leverage security certificates to identify that the system has not been compromised during delivery. Fifty-eight percent of respondents say data protection and recovery are key components of their organizations' security strategy and 58 percent of respondents say their organizations require infrastructures that leverages chip and/or certificates to determine if the system has been compromised during delivery.

Figure 19. Organizations' requirements for secure computing
Strongly agree and Agree responses combined

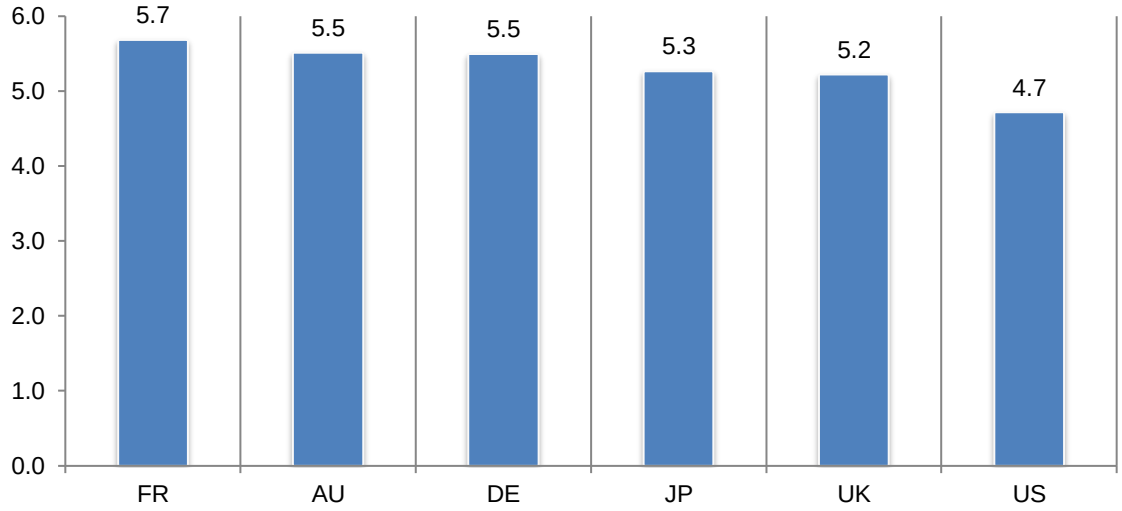


Country differences

In this section, we present some of the most interesting differences among the countries represented in this research. The countries and number of respondents include the United States (635), the United Kingdom (291), Germany (371), France (197), Australia (180) and Japan (446).

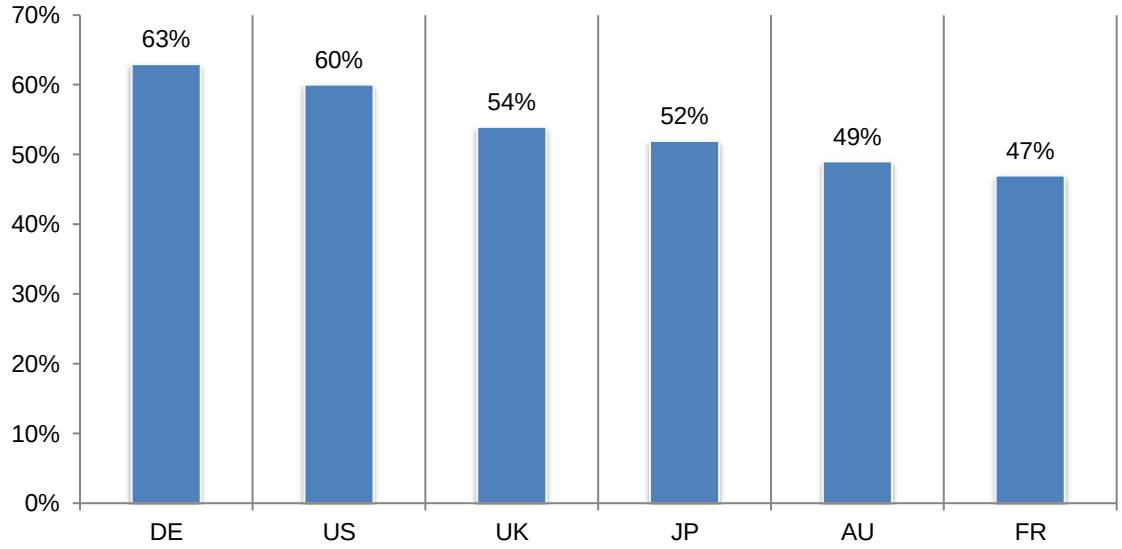
France had slightly more security breaches than other countries. As shown in Figure 20, France had an average of 5.7 breaches and the US had the lowest number (4.7 breaches).

Figure 20. How many security breaches did your organization experience in the past 12 months that resulted in data loss or downtime?
Extrapolated average presented



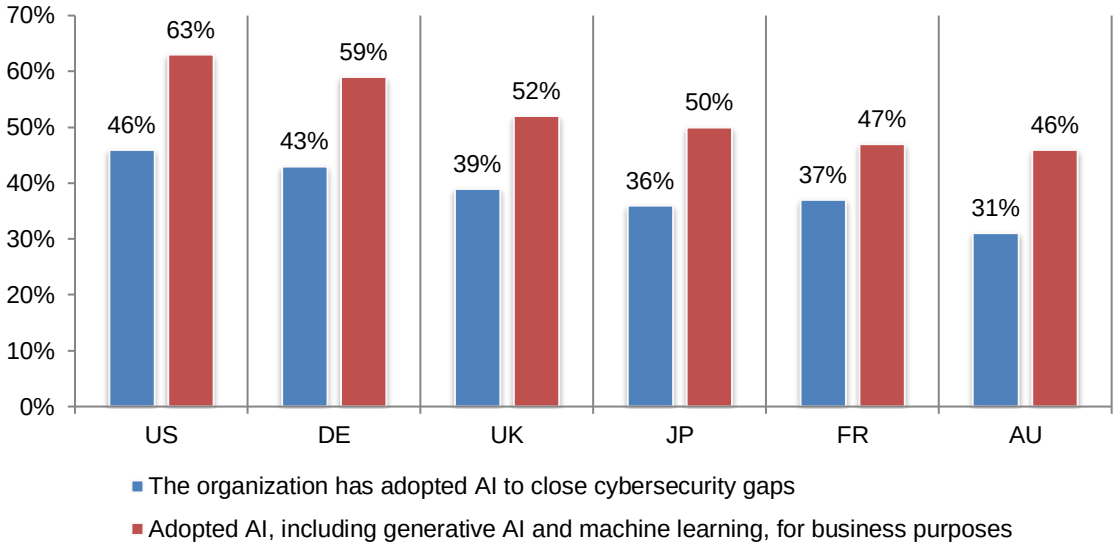
German and US organizations are more likely to have a vendor consolidation strategy (63 percent and 60 percent of respondents, as shown in Figure 21). Australia and France are least likely to have such a strategy (49 percent and 47 percent of respondents, respectively).

Figure 21. Does your organization have a vendor consolidation strategy to improve ROI without creating cybersecurity gaps?
Yes responses presented



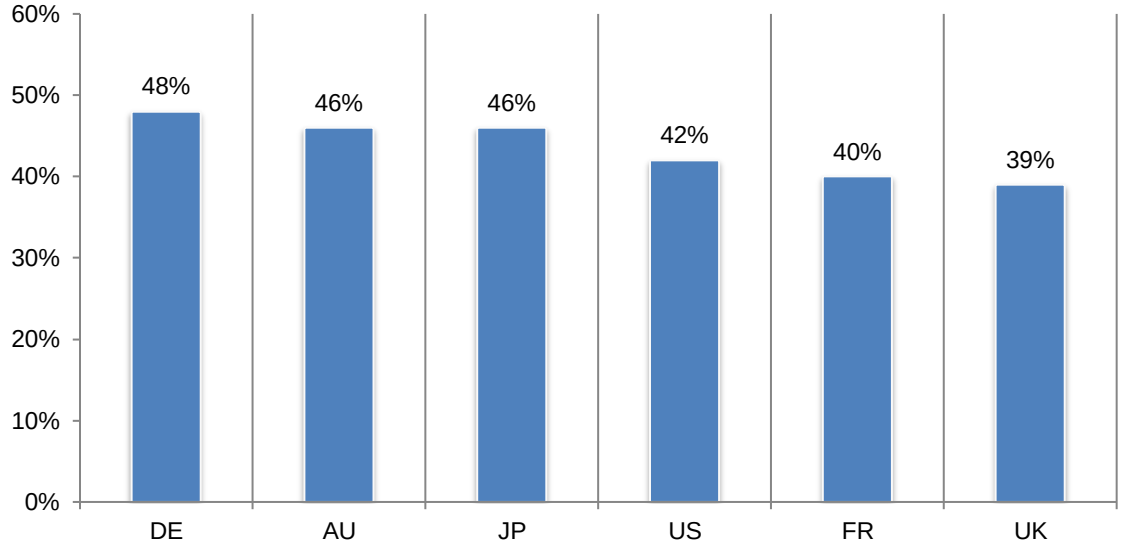
US organizations are most likely to have adopted AI both to close the cybersecurity gap and for business purposes. Figure 22 shows the differences in adoption of AI and if AI was adopted how many organizations are using it for business purposes. Forty-six percent of US organizations have adopted AI and of these, 63 percent of respondents say they are using it for business purposes. Forty-three percent of German respondents say their organizations have adopted AI to close cybersecurity gaps. Of these respondents, 59 percent say their organization have adopted AI for business purposes.

Figure 22. Has your organization adopted AI to close cybersecurity gaps and for business purposes?
Yes responses presented



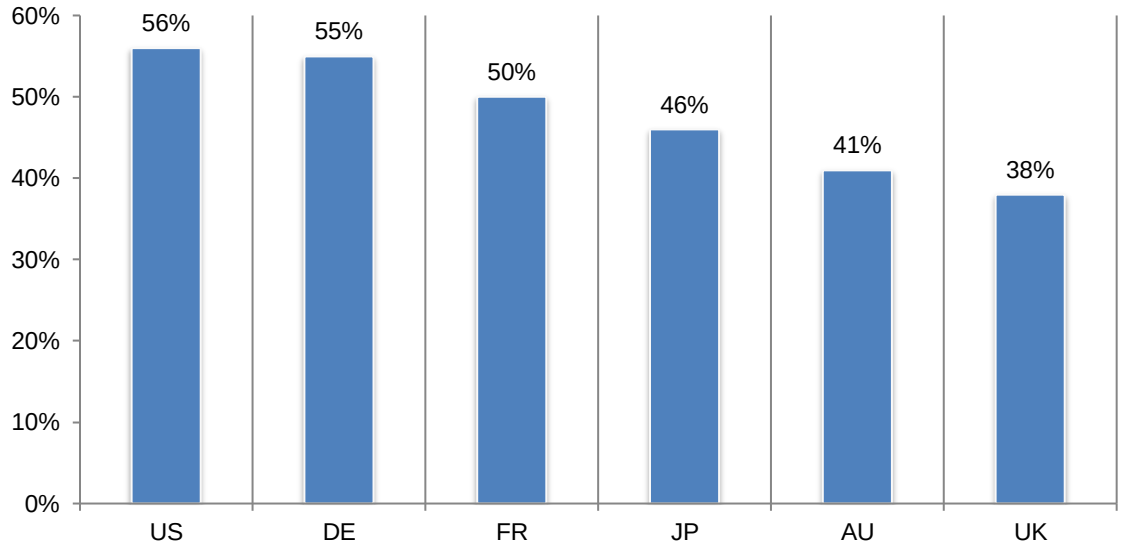
Respondents were asked to rate their level of confidence in knowing and securing all AI assets withing their organizations on a scale from 1 = no confidence to 10 = highly confident. Figure 23 presents the highly confident responses. As shown in Figure 23, German organizations have the most confidence in knowing and securing all AI assets with their organization, including infrastructure, models and data. Forty-six percent of respondents in Australia and Japan are highly confident.

Figure 23. How confident are you that you know and secure all AI assets within your organization, including infrastructure, models and data
On a scale from 1 = no confidence to 10 = highly confident, 7+ responses presented



As shown in Figure 24, US and German organizations are most likely to have deployed universal zero trust network access. Australia (41 percent of respondents) and the UK (38 percent of respondents) have the lowest deployment of universal zero trust network access.

Figure 24. Has your organization deployed universal zero trust network access approach?
Yes responses presented

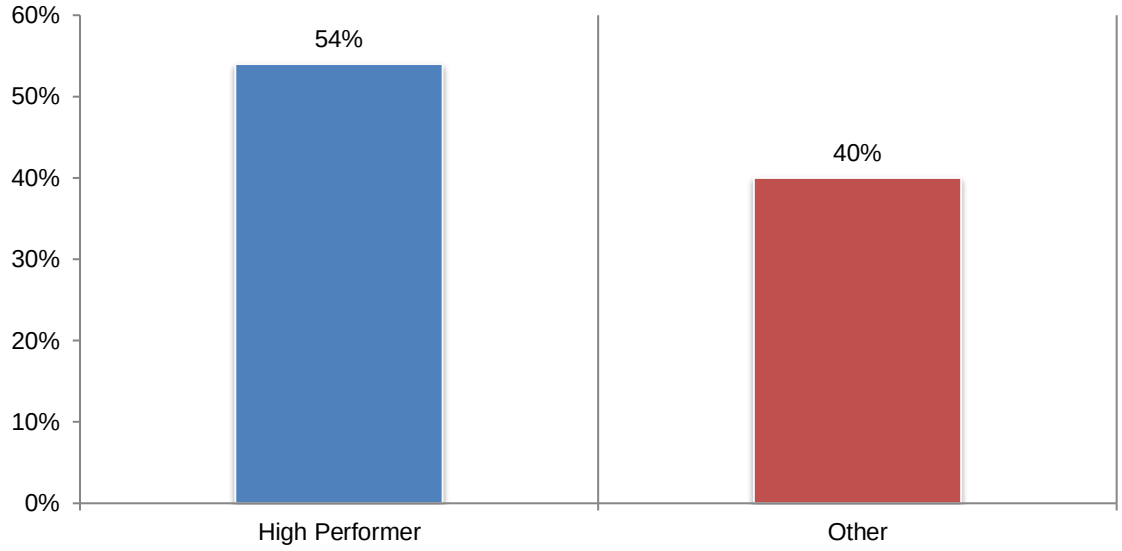


Best practices of high-performing organizations

Twenty-one percent of respondents reported that their organizations are highly effective in keeping up with a constantly changing threat landscape and closing its organization's IT security gap. We refer to these organizations as "high performers" and compare their responses to the non-high performer respondents. In the figures below, we refer to these non-high performer respondents as "other".

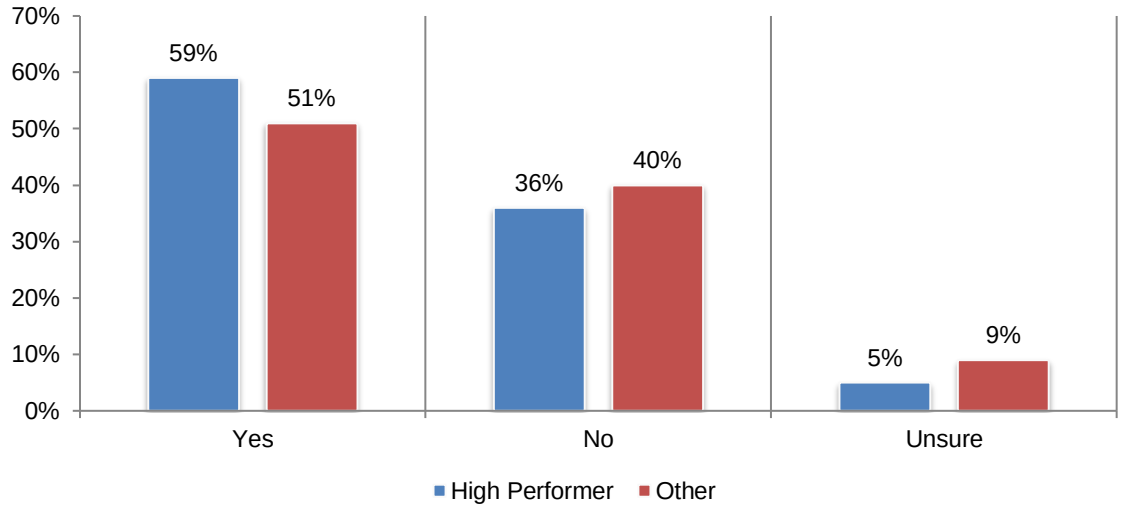
Collaboration between network and security teams is essential to closing the IT security gap. According to Figure 25, 54 percent of high performers vs. 40 percent of others believe they have achieved collaboration.

Figure 25. Network and security teams collaborate effectively to reduce cybersecurity gaps and improve cyber resilience
Strongly agree and Agree responses combined



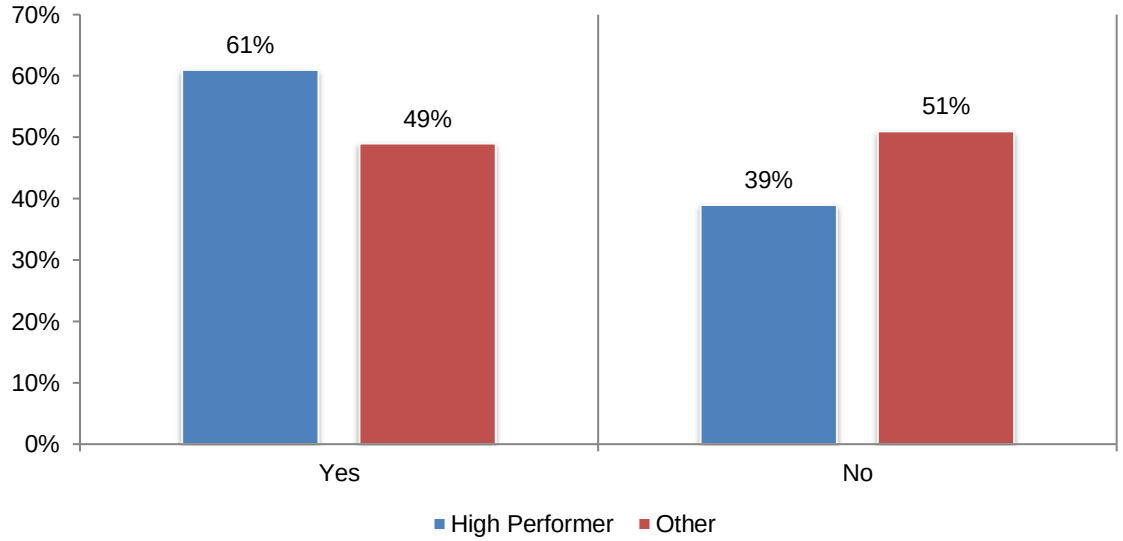
High performers are most likely to have a vendor consolidation strategy. Too many vendors to manage affect an organization's security posture. As shown in Figure 26, 59 percent of high performers vs. 51 percent of other respondents have a vendor consolidation strategy to improve ROI.

Figure 26. Does your organization have a vendor consolidation strategy to improve the ROI without creating cybersecurity gaps?



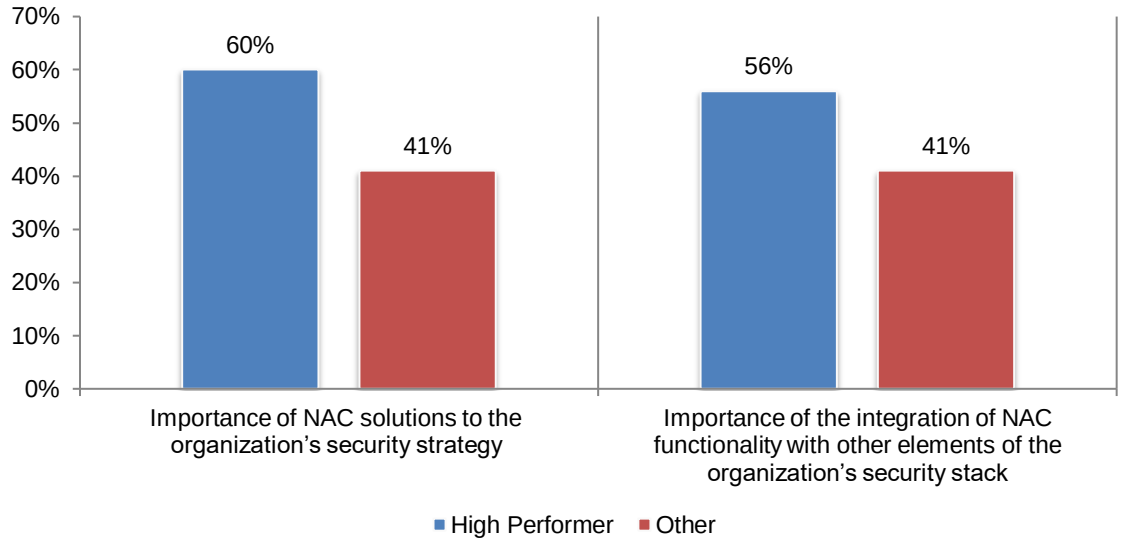
High performers are more likely to adopt AI. Forty-three percent of high performers vs. 35 percent of other respondents have adopted AI to close cybersecurity gaps in their organization. According to Figure 27, there is a significant difference in high performers and others in the adoption of AI for business purposes (61 percent of respondents vs. 49 percent).

Figure 27. Has your organization adopted AI, including generative AI and machine learning for business purposes?



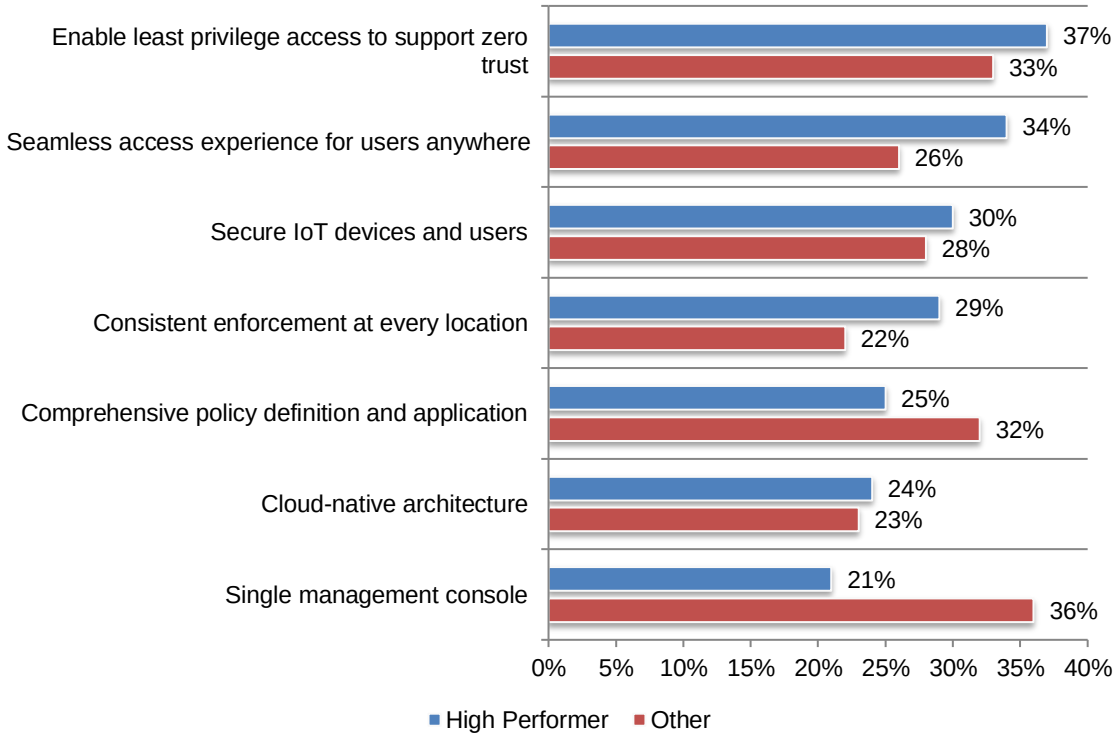
High performers place a higher value on NAC solutions and the integration of NAC functionality. Respondents were asked to rate the importance of NAC solutions and integration on a scale of 1 = not important to 10 = highly important. As shown in Figure 28, the importance of NAC solutions (60 percent vs. 41 percent) and integration of NAC functionality (56 percent vs. 41 percent) are rated higher by high performers.

Figure 28. The importance of NAC solutions and integration of NAC functionality
On a scale of 1 = not important to 10 = highly Important, 7+ responses presented



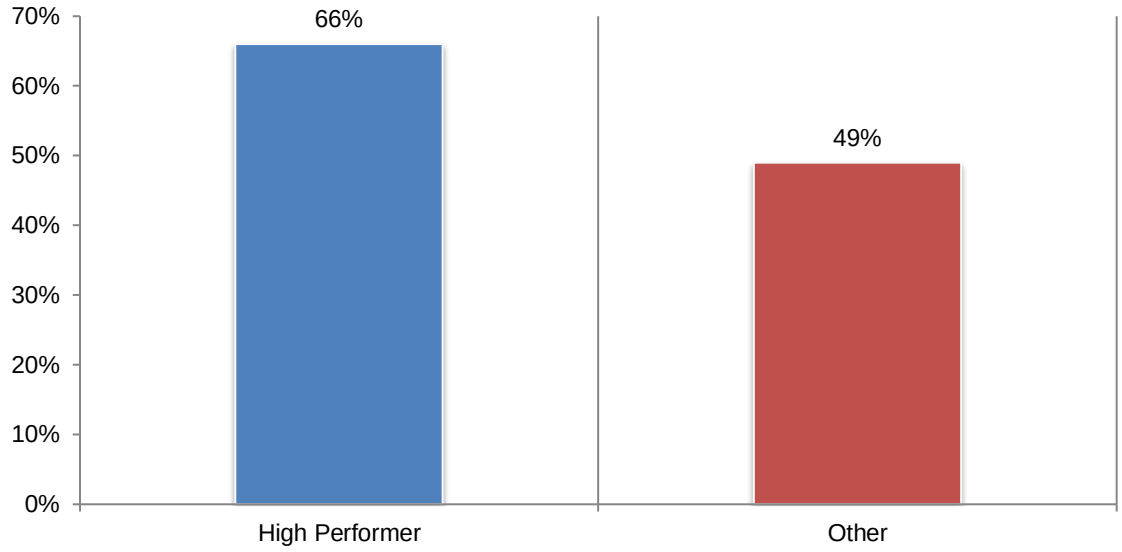
When it comes to universal zero trust network access, high performers place notably greater importance on seamless access experience for users anywhere. Fifty-three percent of high performers vs. 43 percent of other respondents have deployed universal zero trust network access. Figure 29 presents the capabilities that are most important in a universal zero trust network access approach. High performers are more positive about seamless access (34 percent vs. 26 percent) and consistent enforcement at every location (29 percent vs. 22 percent).

Figure 29. What capabilities and characteristics are most important in a universal zero trust network access approach?
More than one response permitted



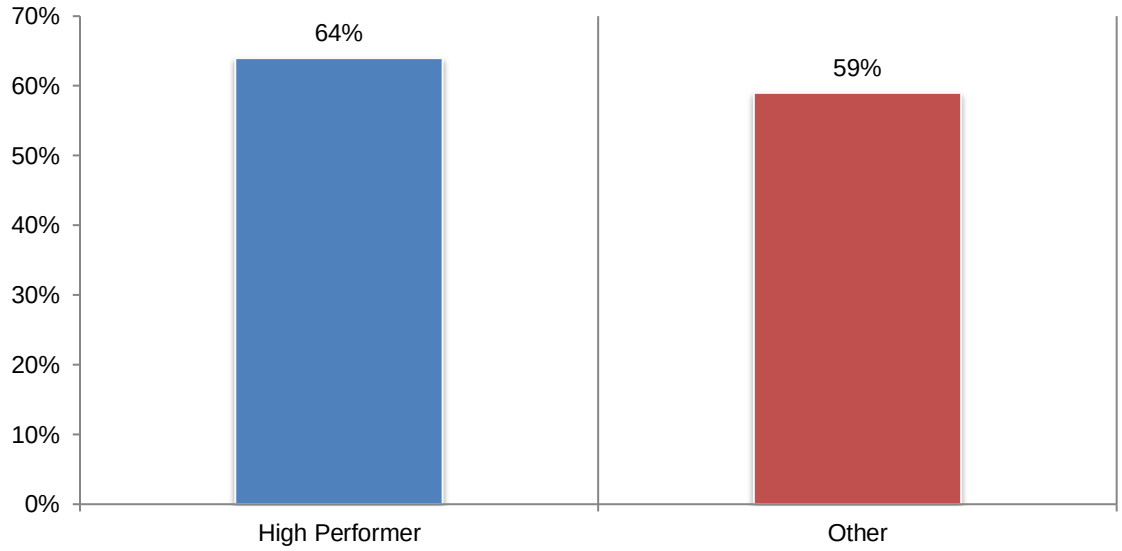
As shown in Figure 30, high performers are far more likely to require infrastructure that leverages chip and/or certificates to determine if the system has been compromised during delivery (66 percent of high performers vs. 49 percent of other).

Figure 30. Perceptions about compute and storage
Strongly agree and Agree responses combined



According to Figure 31, high performers are more likely to move their current security approach to the hybrid cloud (64 percent of high performers vs. 59 percent of others).

Figure 31. Our current security approach will be moved to the hybrid cloud
Strongly agree and Agree responses combined



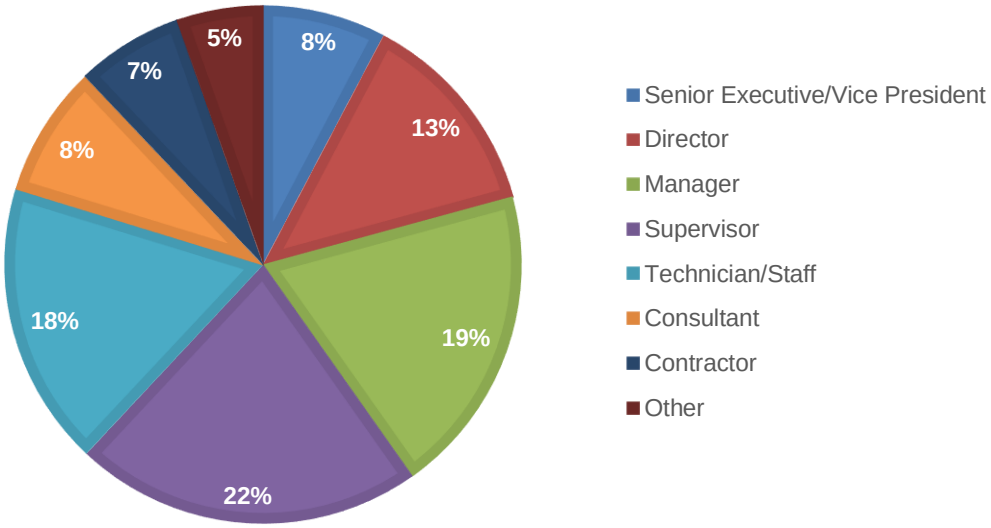
Part 3. Methods

The sampling frame is composed of 58,768 IT and IT security practitioners in the United States, the United Kingdom, Germany, Australia, Japan and France. As shown in Table 1, 2,392 respondents completed the survey. Screening removed 272 surveys. The final sample was 2,120 surveys (or a 3.6 percent response rate).

Table 1. Sample response	Freq	Pct%
Total sampling frame	58,768	100.0%
Total returns	2,392	4.1%
Rejected or screened surveys	272	0.5%
Final sample	2,120	3.6%

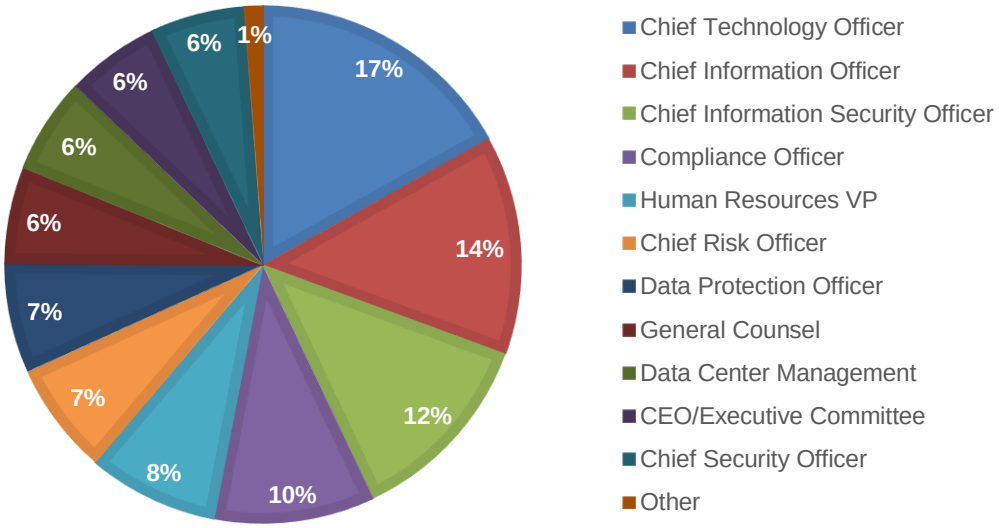
Pie Chart 1 reports the current position or organizational level of the respondents. Sixty-two percent of respondents reported their current position as supervisory or above. The largest category at 22 percent of respondents is supervisor.

Pie Chart 1. Distribution of respondents according to position level



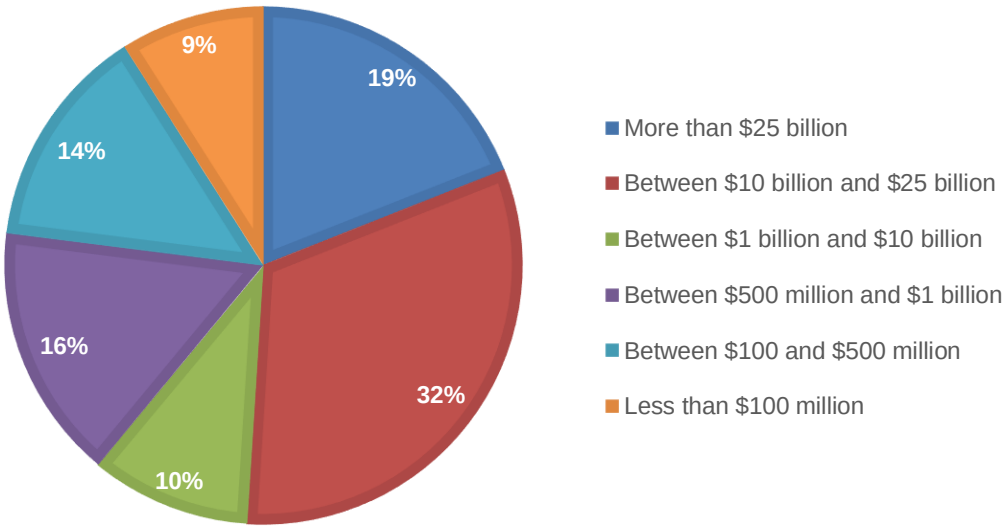
Pie Chart 2 identifies the primary person to whom the respondent or their IT security leader reports. Seventeen percent of respondents identified the chief technology officer as the person to whom they report. Another 14 percent indicated they report directly to the chief information officer and 12 percent of respondents report to the chief information security officer.

Pie Chart 2. Distribution of respondents according to reporting channel



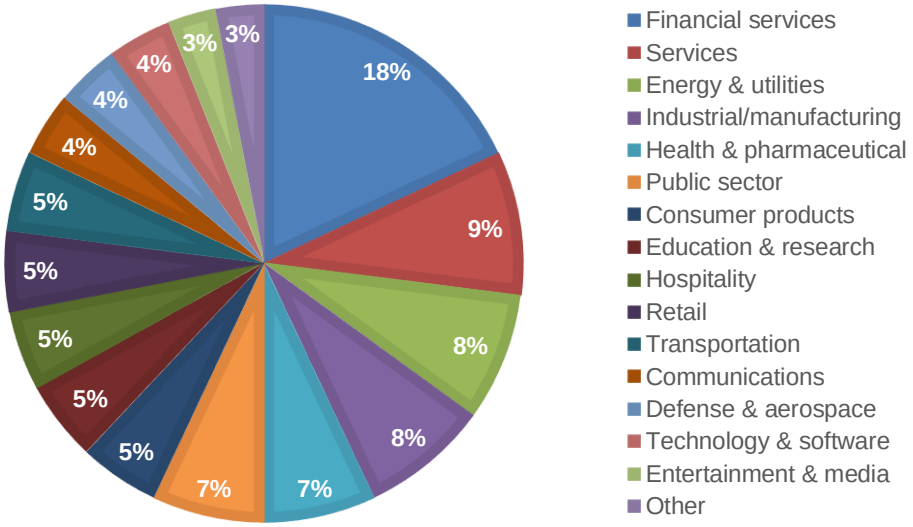
Pie Chart 3 reports the worldwide revenue of the respondents' organizations. More than half (61 percent) of respondents reported their organization's annual worldwide revenue to be greater than $1 billion.

Pie Chart 3. Distribution of respondents according to worldwide revenue
US dollars



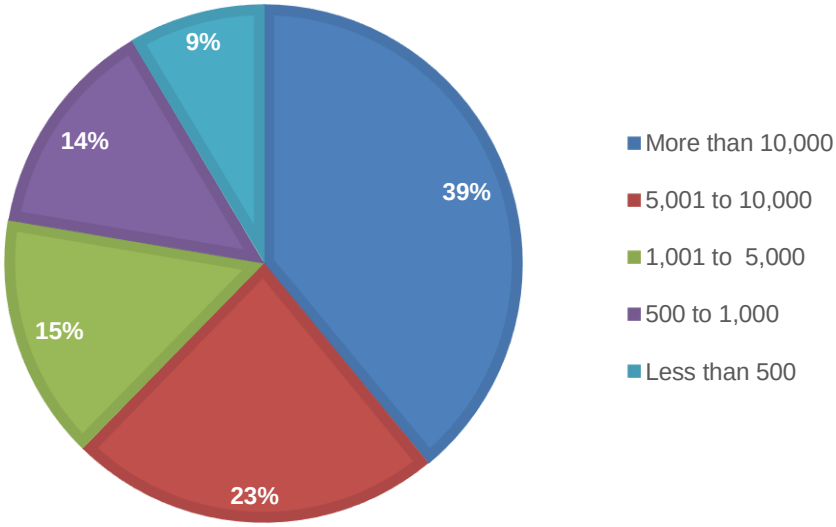
Pie Chart 4 reports the primary industry classification of respondents' organizations. This chart identifies financial services (18 percent of respondents) as the largest segment, which includes banking, insurance, brokerage, investment management and payment processing. Other large verticals include services (9 percent of respondents), energy and utilities (8 percent of respondents), industrial/manufacturing (8 percent of respondents), health and pharmaceuticals (7 percent of respondents), and public sector (7 percent of respondents).

Pie chart 4. Distribution of respondents according to primary industry classification



According to Pie Chart 5, 62 percent of respondents are from organizations with a global headcount of more than 5,000 employees.

Pie Chart 5. Distribution of respondents according to the number of employees within the organization



Part 4. Caveats

There are inherent limitations to survey research that need to be carefully considered before drawing inferences from findings. The following items are specific limitations that are germane to most web-based surveys.

Non-response bias: The current findings are based on a sample of survey returns. We sent surveys to a representative sample of individuals, resulting in a large number of usable surveys. Despite non-response tests, it is always possible that individuals who did not participate are substantially different in terms of underlying beliefs from those who completed the instrument.

Sampling frame bias: The accuracy is based on contact information and the degree to which the list is representative of individuals who are IT or IT security practitioners in various organizations in North America, the United Kingdom, Germany, Australia, Japan and France. We also acknowledge that the results may be biased by external events such as media coverage. We also acknowledge bias caused by compensating subjects to complete this research within a specified time period.

Self-reported results: The quality of survey research is based on the integrity of confidential responses received from subjects. While certain checks and balances can be incorporated into the survey process, there is always the possibility that a subject did not provide accurate responses.

Appendix: Detailed Survey Results

The following tables provide the frequency or percentage frequency of responses to all survey questions contained in this study.

Survey response	FY2024	FY2023
Sampling frame	58,768	56,555
Total returns	2,392	2,344
Rejected surveys	272	260
Final sample	2120	2,084
Response rate	3.6%	3.7%

Part 1. Screening		
S1. What best describes your involvement in IT security investments within your organization?	FY2024	FY2023
None (stop)	0%	0%
Responsible for overall solution/purchase	44%	44%
Responsible for administration/management	50%	48%
Involved in evaluating solutions	49%	52%
Total	143%	145%
S2. What best describes your role within your organization's IT or IT security department?	FY2024	FY2023
Security leadership (CSO/CISO)	47%	49%
IT management	47%	49%
IT operations	50%	53%
Security practitioner	51%	
Security architect	51%	
Networking practitioner	45%	
Network architect	43%	
Data administration	34%	30%
Compliance administration	26%	20%
Applications development	21%	21%
Data Protection Office	5%	4%
None of the above (stop)	0%	
Total	420%	356%

S3. How knowledgeable are you about your organization's IT security strategy and tactics?	FY2024	FY2023
Very knowledgeable	36%	37%
Knowledgeable	33%	39%
Somewhat knowledgeable	31%	24%
Slightly knowledgeable (stop)	0%	0%
No knowledge (stop)	0%	0%
Total	100%	100%

Part 2. Attributions about the IT security gap		
Q1. How many security breaches did your organization experience in the past 12 months that resulted in data loss or downtime?	FY2024	FY2023
1 or 2	16%	16%
3 or 4	15%	17%
5 or 6	21%	23%
7 or 8	23%	22%
9 or 10	18%	15%
More than 10	7%	7%
Total	100%	100%
Extrapolated average	5.32	5.18

Q2. How effective is your organization's ability to keep up with a constantly changing threat landscape and close its organization's IT security gap on a scale of 1 = not effective to 10 = highly effective?	FY2024	FY2023
1 or 2	21%	17%
3 or 4	18%	17%
5 or 6	18%	22%
7 or 8	22%	24%
9 or 10	21%	20%
Total	100%	100%

Q3. What are the primary **operational and governance gaps** in your organization's IT infrastructure? Please select **two** choices	FY2024	FY2023
Security staffing, skills and experience shortages	30%	39%
Conflicting priorities between IT and IT security teams	25%	39%
Security solutions can't keep up with exponentially increasing amounts of data	29%	40%
Difficulty in complying with IT security and privacy industry standards or regulations	29%	38%
Insufficient budget	28%	39%
Lack of clarity about the organization's data security strategy	25%	
Business continuity plan does not include cyber incidents	28%	
Other	6%	5%
Total	200%	200%

Q4. Who makes security solution architecture/product decisions within your organization? Please select **one choice** only.	FY2024	FY2023
The network team	29%	31%
The security team	29%	26%
Individual teams leading IT transformation projects	22%	28%
Both the network and security team	20%	15%
Total	100%	100%

Q5. Network and security teams collaborate effectively to reduce cybersecurity gaps and improve cyber resilience.	FY2024
Strongly agree	20%
Agree	27%
Unsure	17%
Disagree	20%
Strongly disagree	16%
Total	100%

Q6. Managing multiple security vendors is challenging for our organization**.**	FY2024
Strongly agree	27%
Agree	29%
Unsure	15%
Disagree	17%
Strongly disagree	12%
Total	100%

Q7. Does your organization have a vendor consolidation strategy in place to improve the return on security investments without creating cybersecurity gaps?	FY2024
Yes	54%
No	39%
Unsure	7%
Total	100%

Q8. What are the most effective steps to take to minimize threats within your organization's IT infrastructure? Please select the **top three** most effective steps.	FY2024	FY2023
Implement infrastructure component identification/authentication	26%	25%
Implement kernel detection and utilize silicon root verification	39%	
Implement NDR (network detection and response**)**	42%	
Adopt technologies that automate infrastructure integrity verification	34%	29%
Implement a secure and continuous data protection and back up strategy	39%	22%
Prioritize rapid attack and breach detection	40%	24%
Conduct comprehensive penetration testing	42%	25%
Implement micro segmentation	32%	
Other	6%	3%
Total	300%	300%

Part 3. AI and security

Q9a. Has your organization adopted AI to close cybersecurity gaps in your organization?	FY2024
Yes	39%
No	61%
Total	100%

Q9b. If your organization has adopted AI to close cybersecurity gaps, how familiar are you with its AI security strategy**?**	FY2024
Very familiar	29%
Familiar	29%
Somewhat familiar	23%
Not familiar (please skip to Q12a)	19%
Total	100%

Q10. What are your priorities for using AI to close cybersecurity gaps? Please select your **top three choices**.	FY2024
Improve IoT device profiling accuracy	29%
Detect changes to the organization's security posture	30%
Improve quality of alerts	16%
Aid in threat investigations	32%
Modernize cybersecurity operations	20%
Detect and prevent attacks more effectively	27%
Proactively recommend security policies	23%
Leverage behavioral analytics for anomaly and threat detection	24%
Prioritize vulnerabilities based on exploitability and impact	29%
Identify and mitigate server configuration issues	17%
Improve collaboration between network and security teams	34%
Secure data used and data harvested by Large Language Models (LLMs)	19%
Total	300%

Q11. What are your primary challenges when adopting AI to close cybersecurity gaps? Please select the **top three choices**.	FY2024
Uncertainties about AI accuracy	44%
Difficulty in ensuring data privacy	44%
Difficulty in preventing data leakage	44%
Keeping a human in the loop for decision making	30%
Uncertainty about models, training and data used for AI	28%
Lack of in-house AI expertise	23%
Integration/workflow challenges	20%
Lack of internal AI governance	21%
Lack of effective AI solutions	21%
AI solutions are too costly	20%
Other (please specify)	5%
Total	300%

Q12a. Has your organization adopted AI, including generative AI and machine learning, for **business purposes**?	FY2024
Yes	53%
No	47%
Total	100%

Q12b. If yes, how familiar are you with the security risks created by the adoption of AI for business purposes?	FY2024
Very familiar	31%
Familiar	25%
Somewhat familiar	19%
Not familiar (please skip to Q15)	25%
Total	100%

Q13. What are the security risks created by the adoption of AI for business purposes? Please select the top two choices.	FY2024
Potential backdoor attacks on your organization's AI infrastructure (e.g., sabotage, malicious code injection)	38%
Potential leakage or theft of confidential and sensitive data	47%
Vulnerable code created by AI developer tools	40%
Increased legal and compliance risks	36%
Unauthorized access to restricted AI tools, websites	38%
Increased complexity because of the addition of new security tools	57%
Inability to recover lost data in the case of an attack or disaster	44%
Total	300%

Q14. How confident are you that you know and secure ALL AI assets within your organization, including infrastructure, models and data on a scale from 1 = no confidence to 10 = highly confident?	FY2024
1 or 2	13%
3 or 4	21%
5 or 6	23%
7 or 8	22%
9 or 10	21%
Total	100%
Extrapolated average	5.87

Part 4. Zero Trust security strategies

Q15. What **one** statement best describes the state of your organization's approach to a zero-trust security model? Please select one choice only.	FY2024
Our zero-trust strategy has been adopted	28%
Our zero-trust strategy has been adopted because government policies require it	12%
Our organization plans to adopt zero trust in the next six months	12%
Our organization plans to adopt zero trust in a year	8%
Adoption of zero trust is a goal that will take time	17%
Our organization does not have a zero-trust strategy (please skip to Q17)	16%
I am not familiar with my organization's zero-trust strategy (please skip to Q17)	8%
Total	100%

Q16. If your organization has not implemented a zero-trust framework, why? Please select the top **two** choices.	FY2024
A lack of skills and expertise	38%
The value of zero trust is unclear and/or not fully understood	30%
No executive buy-in	45%
Too expensive	44%
Lack of integration between disparate tools	43%
Total	200%

Part 5. Securing connectivity at the edge

Q17. Has your organization deployed, or does it plan to deploy, SASE, which includes SD-WAN and SSE?	FY2024
Yes, it has been deployed	23%
Yes, it will be deployed within 12 months	23%
Yes, but no deployment has been scheduled	19%
Don't know if deployment is planned (please skip to Q20)	20%
No plans to deploy (please skip to Q20)	15%
Total	100%

Q18. What best describes your SASE deployment strategy? Please select **one** choice only.	FY2024
Engage one vendor for both SSE and SD-WAN	22%
Engage a best-in-class SD-WAN vendor that integrates with SSE vendors	30%
Engage a best-in-class SSE vendor(s) that integrates with SD-WAN vendors	27%
Engage best-in-class networking integrated with best-in-class SSE vendors	21%
Total	100%

Q19. What is the first step your organization took or will take in your SASE deployment? Please select **one** choice only.	FY2024
Deployed SD-WAN first to reduce costs and improve application performance for users and branches	37%
Deployed SSE first to improve security posture and increase protection	36%
Deployed SD-WAN and SSE concurrently to realize the benefits of SASE faster	22%
Other (please specify)	5%
Total	100%

Q20. How confident are you that you know ALL the users and devices connected to your network ALL the time on a scale of 1 = no confidence to 10= highly confident?	FY2024	FY2023
1 or 2	14%	25%
3 or 4	25%	29%
5 or 6	22%	19%
7 or 8	23%	16%
9 or 10	16%	11%
Total	100%	100%
Extrapolated average	5.50	4.71

Q21. Does your organization use NAC solutions?	FY2024	FY2023
Yes	54%	32%
No	46%	68%
Total	100%	100%

Q22. For what purposes are NAC systems deployed within your organization? Please check all that apply.	FY2024	FY2023
Wired networks	47%	47%
Wireless networks	46%	48%
Guest access	40%	45%
BYOD	33%	41%
IoT	27%	45%
Endpoint posture assessment	19%	
Total	212%	343%

Q23. How important are NAC solutions to your organization's security strategy on a scale of 1 = not important to 10 = highly Important?	FY2024	FY2023
1 or 2	15%	11%
3 or 4	17%	10%
5 or 6	18%	19%
7 or 8	24%	29%
9 or 10	26%	31%
Total	100%	100%

Q24. How important is the integration of NAC functionality with other elements of your organization's security stack on a scale from 1 = not at all important to 10 = highly important?	FY2024	FY2023
1 or 2	15%	10%
3 or 4	18%	14%
5 or 6	20%	18%
7 or 8	22%	32%
9 or 10	25%	26%
Total	100%	100%

Q25. Do you know what universal zero trust network access is?	FY2024
Yes	54%
No	46%
Total	100%

Q26. Has your organization deployed universal zero trust network access?	FY2024
Yes	48%
No	52%
Total	100%

Q27. What capabilities and characteristics are most important in a universal zero trust network access approach? Please select the **top two** choices.	FY2024
Seamless access experience for users anywhere	30%
Comprehensive policy definition and application	28%
Secure IoT devices and users	29%
Single management console	29%
Enable least privilege access to support zero trust	35%
Consistent enforcement at every location	26%
Cloud-native architecture	23%
Total	200%

Q28. What is required to achieve a strong level of IoT security within your organization? Please check all that apply.	FY2024	FY2023
Network access controls	44%	38%
Effective data encryption	27%	19%
Enterprise-level secure infrastructure for compute workloads at the edge	43%	32%
Peer group IoT device comparisons to spot anomalies	34%	26%
No additional security beyond what is provided by the manufacturer	23%	20%
Other (please specify)	8%	2%
Total	179%	137%

Please rate each one of the following statements using the agreement scale provided below each item.		
Q29. Identifying and authenticating IoT devices accessing our network is critical to our organization's security strategy.	FY2024	FY2023
Strongly agree	28%	30%
Agree	24%	37%
Unsure	22%	16%
Disagree	13%	10%
Strongly disagree	13%	7%
Total	100%	100%

Part 6. Hybrid cloud security

Q30. Is your security team involved in ensuring security is designed into your organization's hybrid environments?	FY2024	FY2023
Yes, fully involved	23%	34%
Yes, partially involved	34%	31%
Yes, minimally involved	24%	18%
No involvement (please skip to Q35)	19%	17%
Total	100%	100%

Q31. How important are security technologies to a successful shift to a hybrid cloud environment from 1 = not important to 10 = highly important.	FY2024	FY2023
1 or 2	13%	10%
3 or 4	21%	12%
5 or 6	21%	20%
7 or 8	20%	32%
9 or 10	25%	26%
Total	100%	100%

Q32. What do you see as the top three primary **technology challenges** when securing your hybrid cloud environment? Please select your **top three** choices only.	FY2024	FY2023
The availability of a secure cloud environment	39%	41%
The inability to secure workloads moving between our on-premises and public cloud environments	41%	42%
The ability to secure workloads moving from the edge to the cloud	36%	43%
The ability to avoid security exploits and data breaches	43%	51%
The ability to enable the free flow of data securely	46%	47%
The ability to secure the digital transformation process and environment	34%	28%
Verifying the integrity of our hybrid cloud infrastructure	30%	25%
Limiting unauthorized access to data and applications	25%	20%
Other	6%	3%
Total	300%	300%

Q33. What do you see as the most significant **operational and governance challenges** to achieving a secure hybrid cloud environment in your organization today? Please select your **top three** choices only.	FY2024	FY2023
Security is not considered early enough in the project plan	25%	25%
The ability to enable the free flow of information	32%	19%
The ability to collaborate with supply chain partners	27%	26%
The ability to ensure the privacy of customer information	37%	18%
The ability to meet consumers' expectations about consent at every layer in the digital ecosystem	31%	21%
The ability to balance security needs with customer experience	30%	22%
The ability to overcome turf and silo issues	27%	40%
Lack of security skills and resources	28%	35%
Lack of alignment between infrastructure and operations and security teams	29%	
Lack of proven methodology for structuring our organization's digital transformation	30%	20%
Other	4%	2%
Total	300%	300%

Q34. Which processes are prioritized to minimize the risk in a hybrid cloud environment? Please select the **top three** choices only.	FY2024	FY2023
Alignment of regulatory compliance processes with standards-based controls	39%	42%
Implementation of a cyber disaster recovery process	41%	37%
Modernize IT security processes	43%	44%
Implementation of a defined cybersecurity compliance framework	46%	44%
Implementation of proactive vulnerability and breach detection processes	37%	34%
Securely shift workloads from on-premises to cloud	44%	16%
Implementation of sovereign IT solutions to meet security and regulatory requirements	42%	
Other	8%	3%
Total	300%	300%

Part 7. Compute and storage		
Q35. As compute and storage moves from the datacenter to the edge, how will your organization's current security approach change?	FY2024	FY2023
Our organization will require current security vendors to supply new security solutions	24%	35%
Our infrastructure providers (network, compute, storage) will supply the required protection	23%	35%
Our organization will have a combination of solutions from security and hybrid cloud infrastructure providers	25%	36%
Our current security approach will be moved to the public cloud	28%	31%
Total	100%	136%

Q36. Please rate the following statements using the agreement scale below each item		
Q36a. Our organization makes server decisions based on the security inherent within the platform.	FY2024	FY2023
Strongly agree	32%	20%
Agree	30%	28%
Unsure	16%	19%
Disagree	13%	20%
Strongly disagree	9%	13%
Total	100%	100%

Q36b. We require servers that leverage security certificates to identify that the system has not been compromised during delivery.	FY2024	FY2023
Strongly agree	27%	40%
Agree	31%	26%
Unsure	17%	17%
Disagree	15%	11%
Strongly disagree	10%	6%
Total	100%	100%

Q36c. Data protection and recovery are key components of our organization's security and resiliency strategy.	FY2024	FY2023
Strongly agree	27%	29%
Agree	31%	27%
Unsure	19%	15%
Disagree	15%	16%
Strongly disagree	9%	13%
Total	100%	100%

Q36d. Our organization requires infrastructure that leverages chip and/or certificates to determine if the system has been compromised during delivery	FY2024	FY2023
Strongly agree	29%	38%
Agree	29%	24%
Unsure	18%	20%
Disagree	15%	11%
Strongly disagree	9%	7%
Total	100%	100%

Q36e. Our current security approach will be moved to the hybrid cloud.	FY2024	FY2023
Strongly agree	29%	39%
Agree	31%	26%
Unsure	17%	16%
Disagree	15%	12%
Strongly disagree	8%	7%
Total	100%	100%

Part 8. Cyber resilience	
Q37. How quickly can your organization recover from a critical system failure caused by a cyber incident?	FY2024
Less than 1 hour	12%
1 to 4 hours	23%
4 to 24 hours	39%
More than 24 hours	26%
Total	100%

Q38. What are your organization's two highest priorities to improve its cyber resiliency? Please select **two** choices only.	FY2024
A business continuity and crisis management plan	10%
Backup and disaster recovery architecture	21%
Cybersecurity incident response planning	18%
Threat detection and monitoring	28%
Third-party risk management	33%
Regulatory compliance	43%
Employee training and awareness	47%
Total	200%

Part 9. Your role and organization		
D1. What organizational level best describes your current position?	FY2024	FY2023
Senior Executive/Vice President	8%	7%
Director	13%	17%
Manager	19%	20%
Supervisor	22%	16%
Technician/Staff	18%	29%
Consultant	8%	9%
Contractor	7%	1%
Other	5%	1%
Total	100%	100%

D2. Check the **Primary Person** you or your leader reports to within the organization.	FY2024	FY2023
CEO/Executive Committee	6%	5%
General Counsel	6%	3%
Chief Information Officer (CIO)	14%	43%
Chief Technology Officer (CTO)	17%	11%
Chief Information Security Officer (CISO)	12%	14%
Compliance Officer	10%	7%
Human Resources VP	8%	3%
Chief Security Officer (CSO)	6%	2%
Data Center Management	6%	5%
Chief Risk Officer (CRO)	7%	6%
Data Protection Officer (DPO)	7%	1%
Other	1%	0%
Total	100%	100%

D3. What range best defines the worldwide revenue of your organization?	FY2024	FY2023
Less than $100 million	9%	9%
Between $100 and $500 million	14%	23%
Between $500 million and $1 billion	16%	23%
Between $1 billion and $10 billion	10%	29%
Between $10 billion and $25 billion	32%	10%
More than $25 billion	19%	6%
Total	100%	100%

D4. What best describes your organization's primary industry classification?	FY2024	FY2023
Agriculture & food services	2%	1%
Communications	4%	2%
Consumer products	5%	6%
Defense & aerospace	4%	1%
Education & research	5%	3%
Energy & utilities	8%	6%
Entertainment & media	3%	2%
Financial services	18%	17%
Health & pharmaceutical	7%	11%
Hospitality	5%	5%
Industrial/manufacturing	8%	8%
Public sector	7%	10%
Retail	5%	8%
Services	9%	7%
Technology & software	4%	8%
Transportation	5%	3%
Other	1%	2%
Total	100%	100%
D5. How many employees are in your organization?	FY2024	FY2023
Less than 500	9%	14%
500 to 1,000	14%	19%
1,001 to 5,000	15%	24%
5,001 to 10,000	23%	26%
More than 10,000	39%	17%
Total	100%	100%

Ponemon Institute

Advancing Responsible Information Management

Ponemon Institute is dedicated to independent research and education that advances responsible information and privacy management practices within business and government. Our mission is to conduct high quality, empirical studies on critical issues affecting the management and security of sensitive information about people and organizations.

We uphold strict data confidentiality, privacy and ethical research standards. We do not collect any personally identifiable information from individuals (or company identifiable information in our business research). Furthermore, we have strict quality standards to ensure that subjects are not asked extraneous, irrelevant or improper questions.