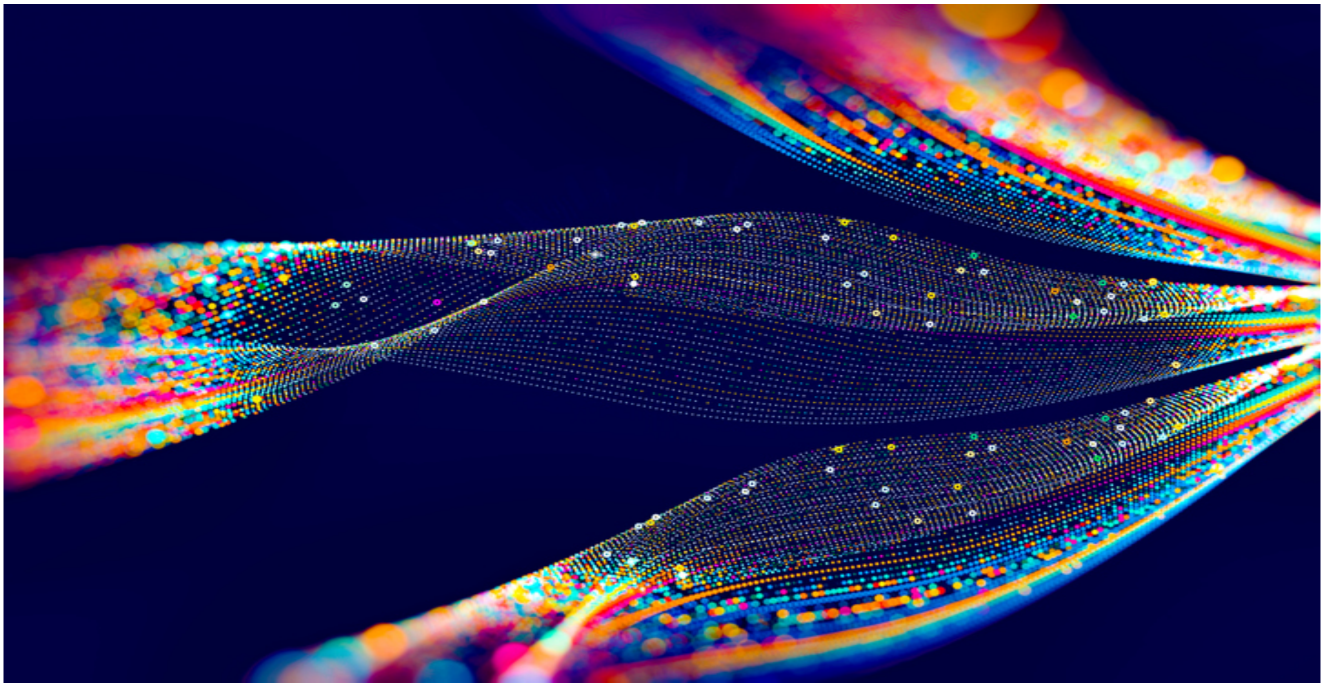


The 2023 Global Study on Closing the IT Security Gap: Addressing Cybersecurity Gaps from Edge to Cloud

Sponsored by

Hewlett Packard Enterprise

Independently conducted by Ponemon Institute LLC

Publication Date: March 2023

The 2023 Global Study on Closing the IT Security Gap: Addressing Cybersecurity Gaps from Edge to Cloud[1]

Prepared by Ponemon Institute, March 2023

Table of Contents	Page
Part 1. Executive summary	3 to 5
Part 2. Key findings	6 to 28
Is the IT security gap shrinking?	6 to 9
The role of zero trust and SASE in closing the IT security gap	10 to 12
Solutions to achieving network visibility and security connectivity at the edge	13 to 17
The importance of securing the hybrid cloud environment	18 to 21
Best practices in closing the IT security gap: an analysis of high performing organizations	22 to 28
Part 3. Methods	29 to 32
Part 4. Caveats	32
Appendix: Audited findings	33 to 48

[1] 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 identity, detect and resolve data breaches and other security incidents. The consequences of the gap can include financial losses, diminishment in reputation and the inability to comply with privacy regulations such as the EU's General Data Protection Regulation (GDPR).

Part 1. Executive summary

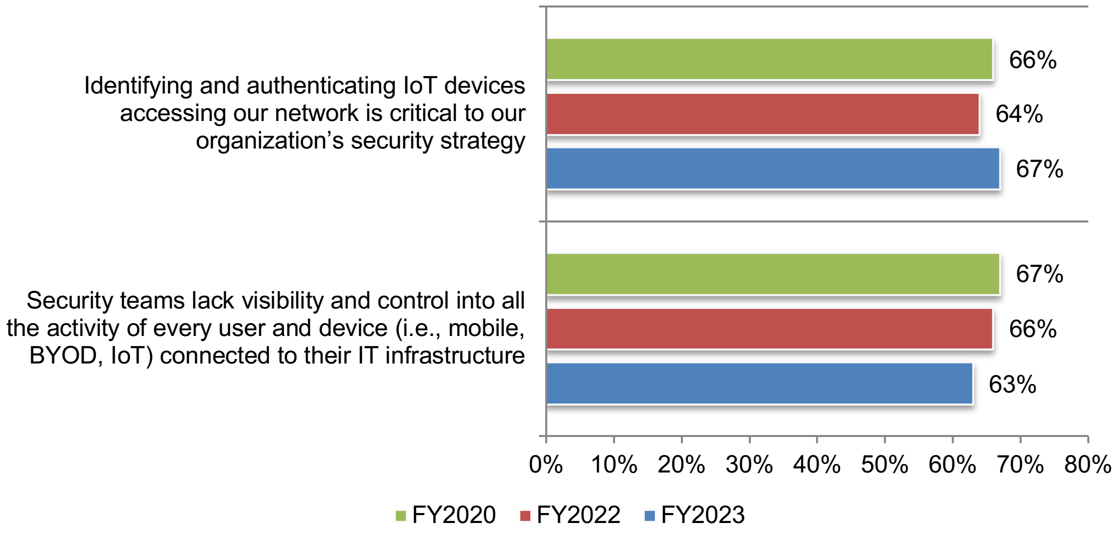
2023 marks the beginning of a new age of data-driven transformation. Security and IT teams must scale to keep pace with the needs of business to ensure the protection of any data, anywhere. Modern hybrid cloud landscapes present complex environments and daunting security challenges for security and IT teams who are responsible for the protection of data and apps and workloads operating across a heterogenous landscape of data centers, hybrid clouds and edge computing devices. As the volume of data generated by IoT devices and systems grows exponentially, the ability to close the IT security gap is proving to be elusive and frustrating.

The 2023 Global Study on Closing the IT Security Gap: Addressing Cybersecurity Gaps from Edge to Cloud, now in its third year[2], is sponsored by Hewlett Packard Enterprises (HPE) to look deeply into the critical actions needed to close security gaps and protect valuable data. In this year's research, Ponemon Institute surveyed 2,084 IT and IT security practitioners in North America, the United Kingdom, Germany, Australia, Japan, and for the first time, France. All participants in this research are knowledgeable about their organizations' IT security and strategy and are involved in decisions related to the investment in technologies.

Security and IT teams face the challenge of trying to manage operational risk without preventing their organizations from growing and being innovative. In this year's study, only 44 percent of respondents say they are very effective or highly effective in keeping up with a constantly changing threat landscape. However, as shown in this research there are strategies security and IT teams can implement to defend against threats in complex edge-to-cloud environments.

The IT security gap is not shrinking because of the lack of visibility and control into user and device activities. According to Figure 1, as the proliferation of IoT devices continues, respondents say identifying and authenticating IoT devices accessing their network is critical to their organizations' security strategy (67 percent of respondents). However, 63 percent of respondents say their security teams lack visibility and control into all the activity of every user device connected to their IT infrastructure.

Figure 1. Visibility into the activities of every user and device, especially IoT devices, is critical to closing the IT security gap
Strongly agree and Agree responses combined



[2] 2022 study hyperlink: Ponemon Institute 2022 Global Study on Closing the IT Security gaps
2020 study hyperlink: Closing the IT Security Gaps - 2020 Ponemon Institute Study | HPE__

How high performing teams are closing the IT security gap

Twenty percent of respondents self-reported their organizations are highly effective in keeping up with a constantly changing threat landscape and close their organizations' IT security gap (9+ responses on a scale of 1 = not effective to highly effective). We refer to these organizations as "high performers". In this section, we analyze what these organizations are doing differently to achieve a more effective cybersecurity posture and close the IT security gap as compared to the 80 percent of respondents in the other organizations represented in this research.

As evidence of their effectiveness, high performing organizations had fewer security breaches in the past 12 months that resulted in data loss or downtime. Almost half of respondents (46 percent) in other respondents say their organizations had at least 7 and more than 10 incidents in just the past 12 months. In contrast, only 35 percent of high performers say their organizations had between 7 and more than 10 security incidents.

High performing organizations have a larger IT security function. Fifty-four percent of high performing organizations say their organizations have a minimum of 21 to more than 50 employees in their IT security function. Only 44 percent of respondents of other organizations had the same range of employees in IT security.

High performers are more likely to control the deployment of zero trust within a Network as a Service (NaaS) deployment. Of those familiar with their organization's zero-trust strategy, more high performers (36 percent of respondents) than others (28 percent of respondents) say their organization is responsible for implementing zero trust within a NaaS. Only 20 percent of high performers say it is the responsibility of the NaaS provider and 10 percent say a third-party managed service provider is responsible.

High performers centralize decisions about investments in security solutions and architectures. Sixty percent of high performers say it is either the network team (30 percent) or security team (30 percent) who are the primary decision makers about security solutions and architectures. Only 15 percent say both functions are responsible.

More high performers have deployed or plan to deploy the SASE architecture. Forty-nine percent of high performers have deployed (32 percent) or plan to deploy (17 percent) the SASE architecture. In contrast only 39 percent of respondents in the other organizations have deployed (24 percent) or plan to deploy (15 percent) the SASE architecture.

More high performers have achieved visibility of all users and devices. High performers are slightly more confident (38 percent of respondents) than other respondents (30 percent of respondents) that their organizations know all the users and devices connected to their networks all the time.

Far more high performers are positive about the use of Network Access Control (NAC) solutions and their importance to proving compliance. These respondents are more likely to use these solutions for IoT security. Fifty-one percent of high performers say NAC solutions are an essential tool for proof of compliance vs. 42 percent of respondents in other organizations. Fifty-five percent of high performers vs. 38 percent of other respondents say NAC solutions are best delivered by the cloud.

High performers recognize the importance of the integration of NAC functionality with the security stack. Respondents were asked to rate the importance of the integration of NAC functionality with other elements of the security stack on a scale from 1 = not important to 10 = highly important. Sixty-two percent of high performers vs. 54 percent of other respondents say such integration is important.

High performers are more likely to believe continuous monitoring of network traffic and real-time solutions will reduce IoT risks. Sixty-two percent of high performers vs. 52 percent of other respondents say continuous monitoring of network traffic for each IoT device to spot anomalies is required. Forty-seven percent of high performers vs. 38 percent of other respondents say real-time solutions to stop compromised or malicious IoT activity is required.

High performers are more likely to require current security vendors to supply new security solutions as compute and storage moves from the data center to the edge. Forty percent of high performers vs. 30 percent of other respondents say their organizations will require current security vendors to supply new security solutions. Respondents in other organizations say their infrastructure providers will be required to supply protection (45 percent vs. 34 percent in high performing organizations).

High performers are more likely to require servers that leverage security certificates and infrastructures that leverage chips and/or certificates. The research reveals significant differences regarding compute and storage requirements. Specifically, high performers require servers that leverage security certificates to identify that the system has not been compromised during delivery (67 percent vs. 60 percent in other organizations). High performers are more likely to require infrastructure that leverages chip and/or certificates to determine if the system has been compromised during delivery (64 percent vs. 56 percent in other organizations). High performers also are more likely to believe data protection and recovery are key components of their organizations' security and resiliency strategy (58 percent vs. 50 percent in other organizations).

Conclusion: Recommendations to close the IT security gap

According to the research, the most effective steps to minimize stealthy or hidden threats within the IT infrastructure are the adoption of technologies that automate infrastructure integrity verification and implement network segmentation. The research also reveals there is a growing adoption of zero trust and Secure Access Service Edge (SASE) architectures to manage vulnerabilities and user access. Important activities to achieving a stronger level of IoT security, according to the research, is the continuous monitoring of network traffic for each IoT device to spot anomalies and real-time solutions to stop compromised or malicious IoT activity.

Other actions to be considered in the coming year include the following:

- Require servers that leverage security certificates and infrastructures that leverage chips and/or certificates.

- Invest in having a fully staffed and well-trained IT security function. Such expertise is critical to ensuring data protection and recovery are key components of an organization's security and resiliency strategy. A lack of skills and expertise is also the primary deterrent to adopting a zero-trust framework.

- Consider centralizing decisions about investments in security solutions and architectures as high performers in this research tend to do. A concern of respondents is the inability of IT and IT security teams to agree on the activities that should be prioritized to close the IT security gap. This concern is exacerbated by the siloed or point security solutions in organizations.

- Deploy Network Access Control (NAC) solutions to improve IoT and BYOD security. These solutions support network visibility and access management through policy enforcement for devices on users of computer networks. NAC solutions can improve visibility and verify the security of all apps and workloads.

Part 2. Key findings

In this section of the report, we provide a detailed analysis of the of the research findings. Whenever possible, we compare this year's results to previous studies. The complete audited findings are presented in the Appendix of this report.

We have organized the findings according to the following topics:

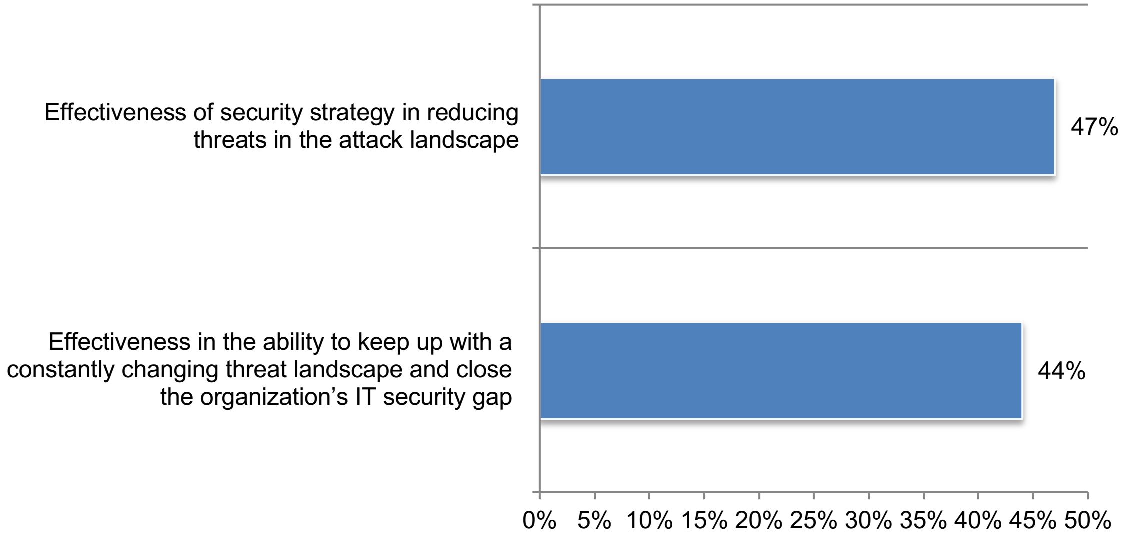
2.1 Is the IT security gap shrinking?
2.2 The role of zero trust and SASE in closing the IT security gap
2.3 Solutions to achieving network visibility
2.4 The importance of securing the hybrid cloud environment
2.5 Best practices in closing the IT security gap

2.1 Is the IT security gap shrinking?

The difficulty in reducing threats in the attack landscape is why the IT security gap is not shrinking. Seventy-eight percent of respondents had at least one security breach in just the past 12 months and 44 percent of respondents say their organizations had between 7 and more than 10.

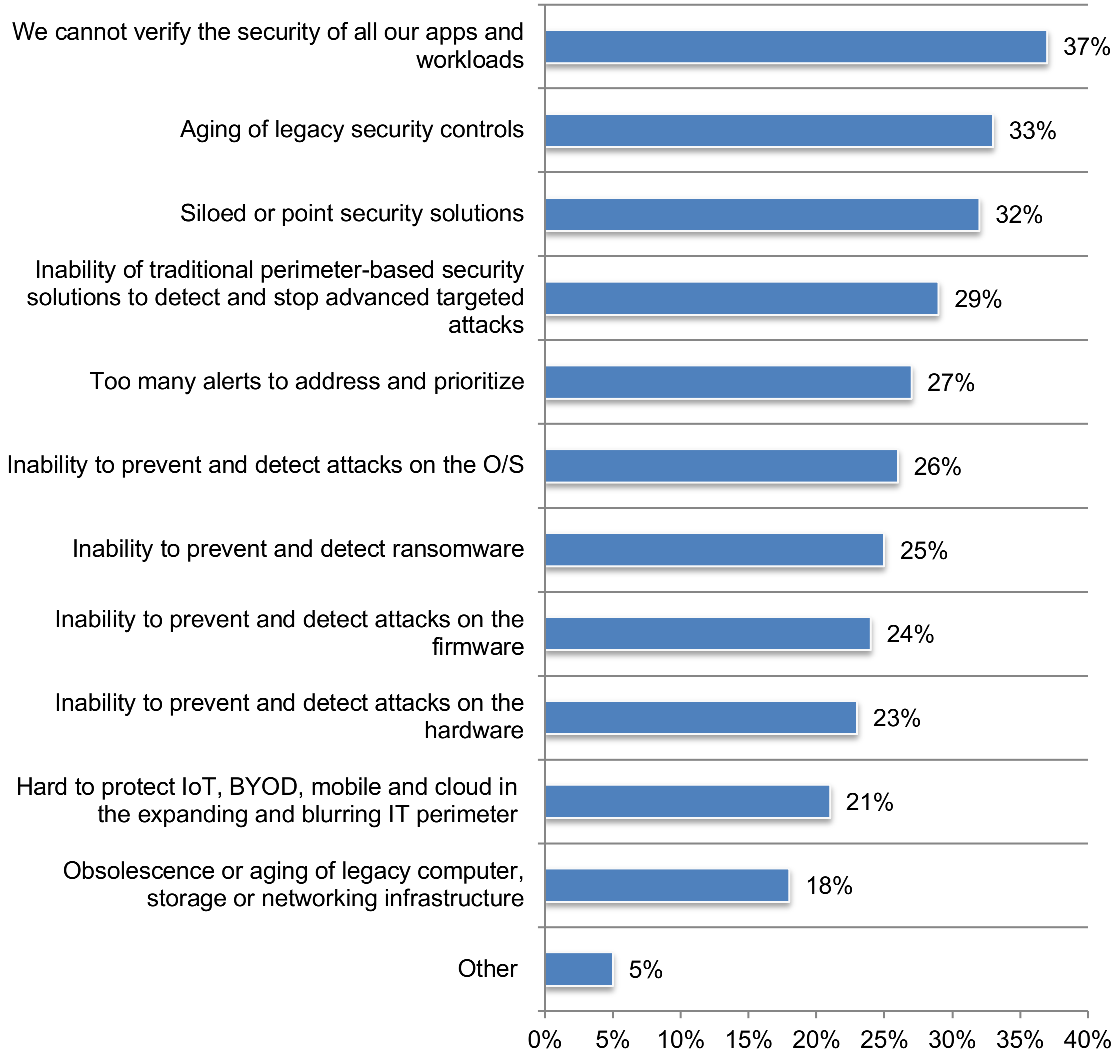
Respondents were asked to rate the effectiveness of their security strategies on a scale of 1 = not effective to 10 = highly effective. Figure 2 presents the 7+ responses (very high and highly effective). As shown, less than half (44 percent of respondents) rate their organizations' ability to keep up with a constantly changing threat landscape and close the IT security gap as very or highly effective (7+ responses). Similarly, only 47 percent of respondents rate their organization as very or highly effective in reducing threats in the attack landscape.

Figure 2. Effectiveness in reducing threats
On a scale of 1 = not effective to 10 = highly effective, 7+ responses presented



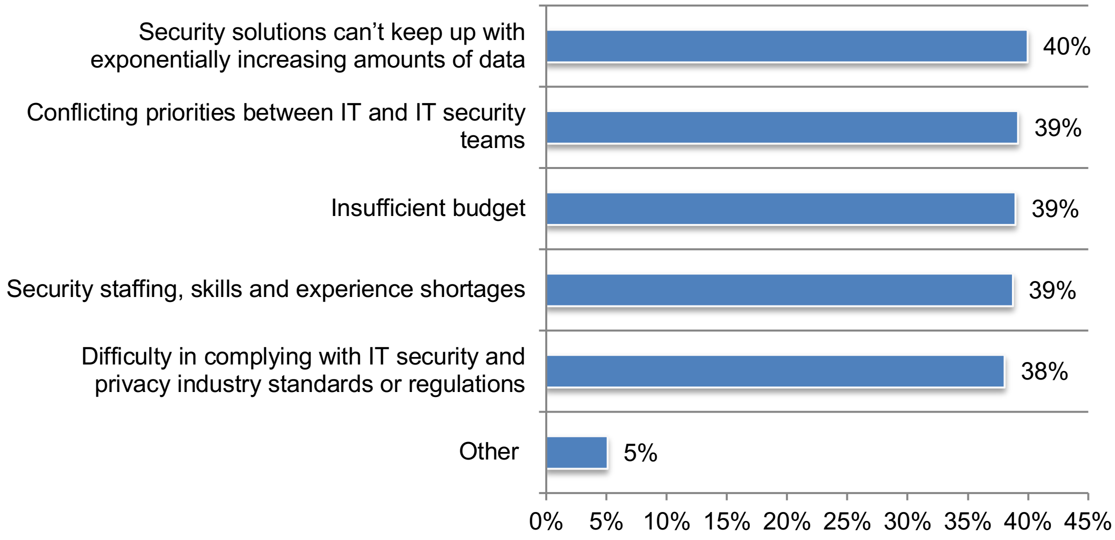
Organizations lack the visibility to verify the security of all apps and workloads. Figure 3 presents a list of security gaps organizations must overcome to have a stronger security posture. The top three are the inability to verify the security of all apps and workloads (37 percent of respondents), the aging of legacy security controls (33 percent of respondents) and siloed or point security solutions (32 percent of respondents).

Figure 3. The primary security gaps in your organization's IT infrastructure
Three responses permitted



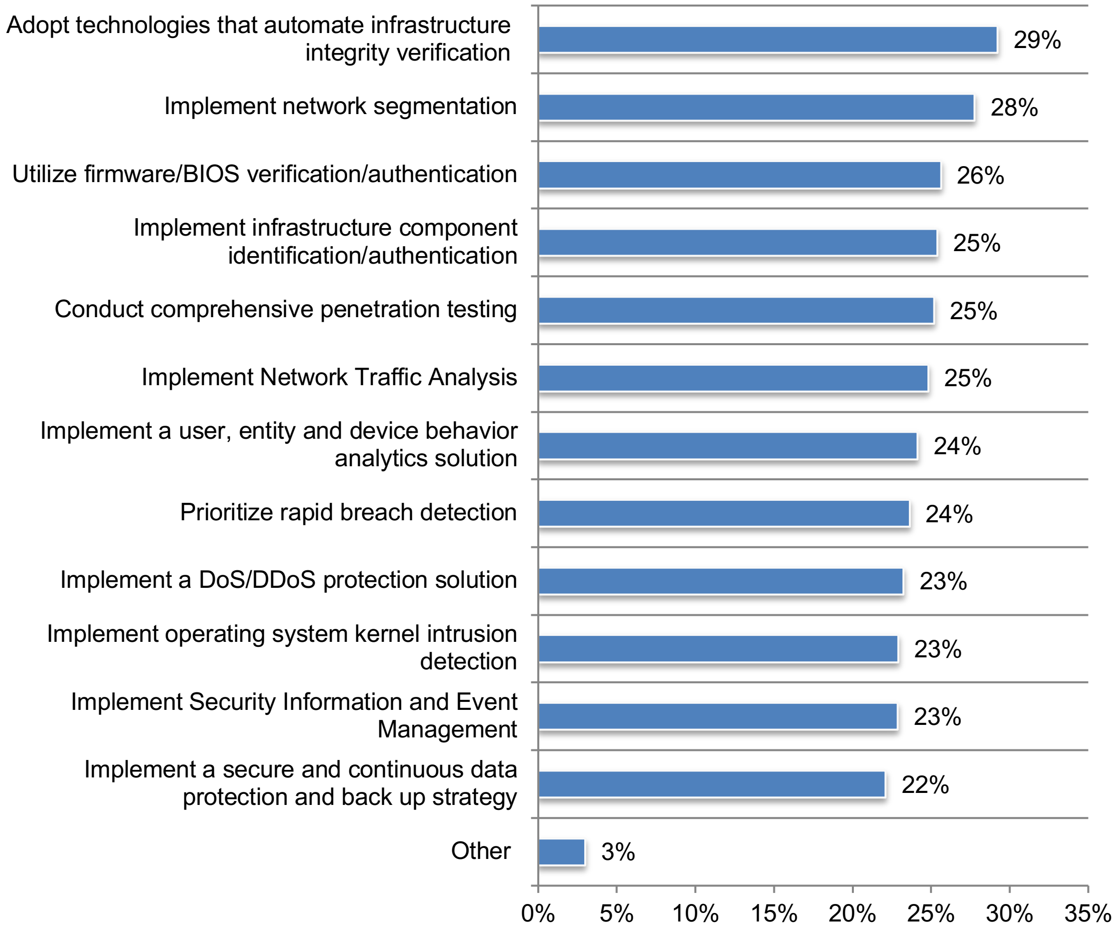
Organizations are overwhelmed dealing with the explosion of data. Figure 4 presents organizations' operational and governance gaps. The number one challenge is not having the security solutions that can keep up with exponentially increasing amounts of data (40 percent of respondents). This is followed by the inability of IT and IT security teams to agree on the activities that should be prioritized to close the IT security gap. These problems are exacerbated by the siloed or point security solutions in organizations.

Figure 4. What are the primary operational and governance gaps in your organization's IT infrastructure?
Two responses permitted



Adoption of authentication technologies is considered most effective in reducing stealthy or hidden threats. Figure 5 provides a long list of steps organizations can take to minimize stealthy or hidden threats. As shown, the number one is the adoption of technologies that automate infrastructure integrity verification followed by network segmentation, firmware/BIOS verification/authentication and identification/authentication for the infrastructure.

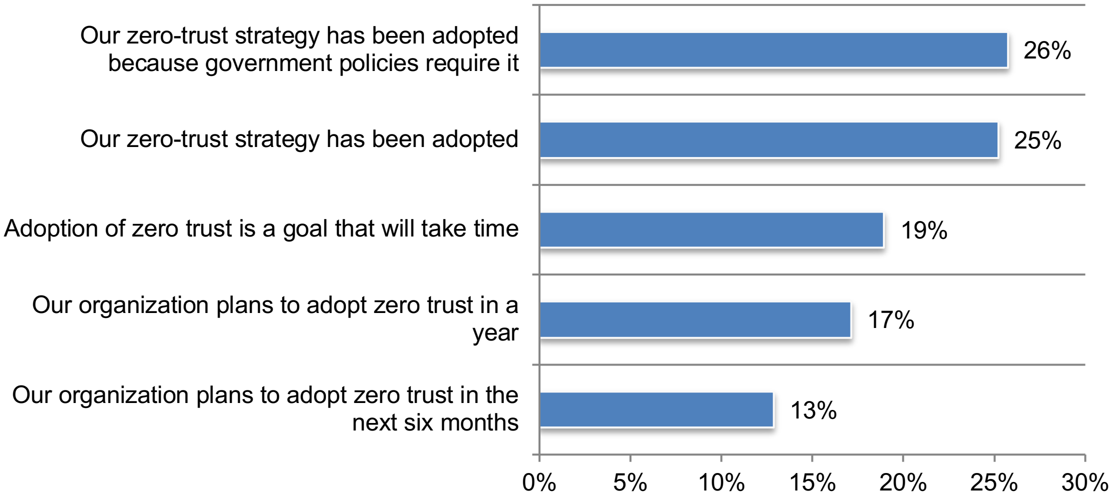
Figure 5. What are the most effective steps to take to minimize stealthy, or hidden threats within your organization's IT infrastructure?
Three responses permitted



2.2 The role of zero trust and SASE in closing the IT security gap

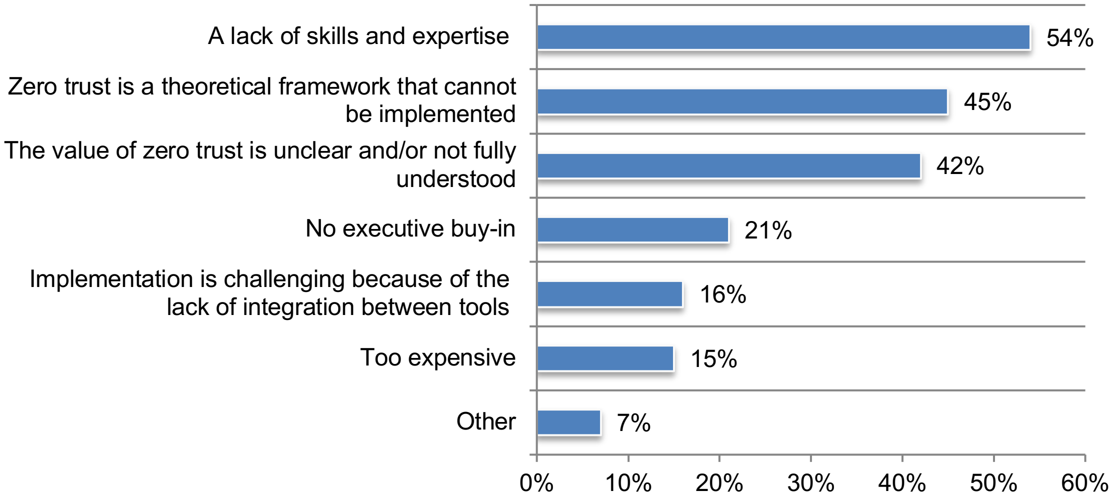
Zero trust and Secure Access Service Edge (SASE) architecture are increasingly being embraced as strategies to close the IT security gap. Zero trust is seen as especially effective in managing vulnerabilities and user access. It assumes no implicit trust is granted to assets or user accounts based solely on their physical or network location or asset ownership. As shown in Figure 6, 51 percent of respondents have adopted a zero-trust strategy. Twenty-six percent of respondents say adoption occurred because government policies require it.

Figure 6. What one statement best describes the state of your organization's approach to a zero-trust security model?



A lack of skills and expertise is the primary deterrent to adopting a zero-trust framework. Twenty-one percent of respondents say their organizations have not adopted a zero-trust framework. Fifty-four percent of these respondents say their organizations do not have the necessary skills and expertise. Respondents are also not sold on the value of zero trust. Forty-five percent of respondents say it is not a practical but a theoretical framework that cannot be implemented and 42 percent of respondents do not fully understand its value.

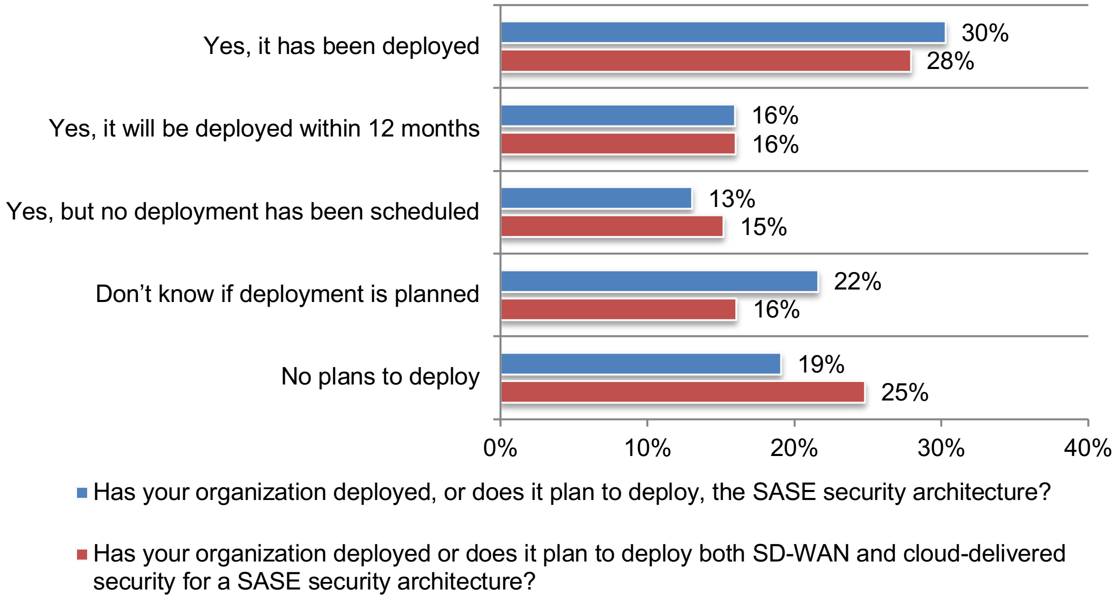
Figure 7. If your organization has not implemented a zero-trust framework, why?
Two responses permitted



SASE architecture brings advanced protection to the farthest edge of the network: the endpoints of users. Users are provided robust security features directly to their devices from the cloud, enabling them to connect securely from everywhere. 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.

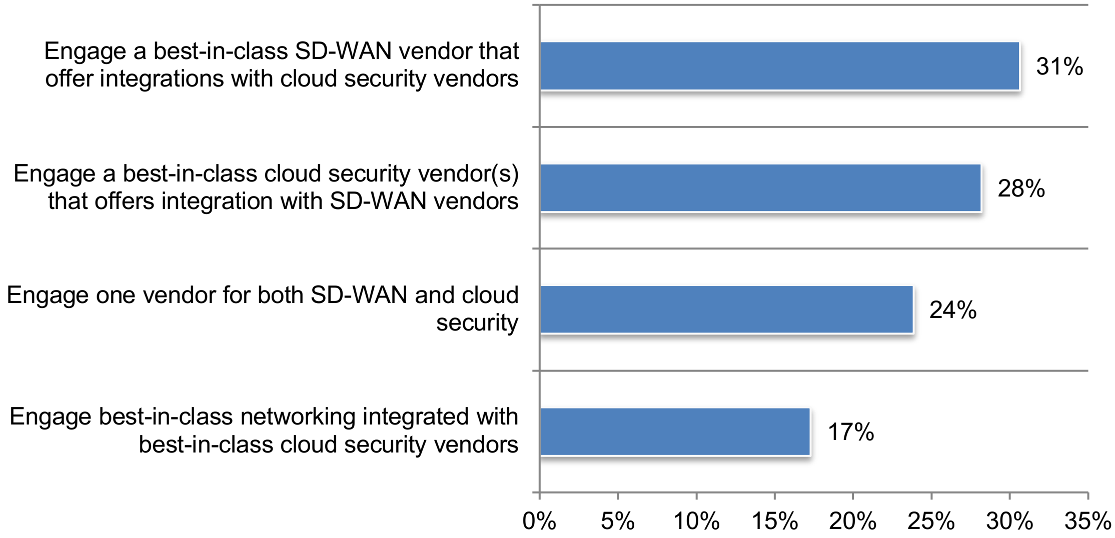
According to Figure 8, almost half (46 percent of respondents) say their organizations have deployed (30 percent) or will deploy in one year the SASE security architecture (16 percent). Concurrently, 44 percent of respondents say they have deployed (28 percent) or plan to deploy (16 percent) both SD-WAN and cloud-delivered security for a SASE security architecture.

Figure 8. Has your organization deployed, or does it plan to deploy, the SASE security architecture, both SD-WAN and cloud-delivered security for a SASE security architecture?



Best-in-class is how vendors are selected. Respondents were asked to select the **one** preferred characteristic of vendors who would deploy SD-WAN and cloud-based security for a SASE architecture. According to Figure 9, 31 percent of respondents say their organizations would engage a best-in-class SD-WAN vendor that offers integrations with cloud security vendors and 28 percent of respondents say it would be a best-in-class security vendor that offers integration with SD-WAN vendors.

Figure 9. How would vendors be selected?
Only one choice permitted

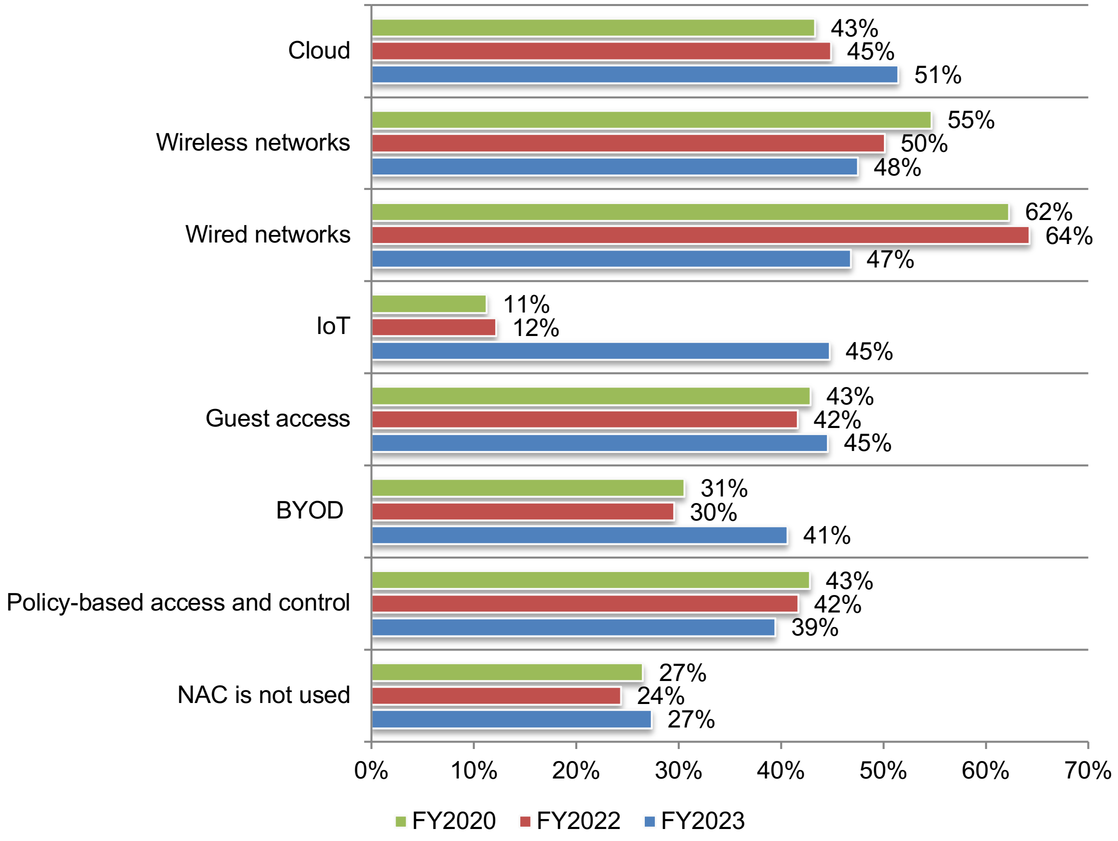


2.3 Solutions to achieving network visibility and security connectivity at the edge

Increasingly, Network Access Control (NAC) solutions are being used to improve IoT and BYOD security. These solutions support network visibility and access management through policy enforcement for devices on users of computer networks. Thirty-two percent of respondents say their organizations have deployed NAC.

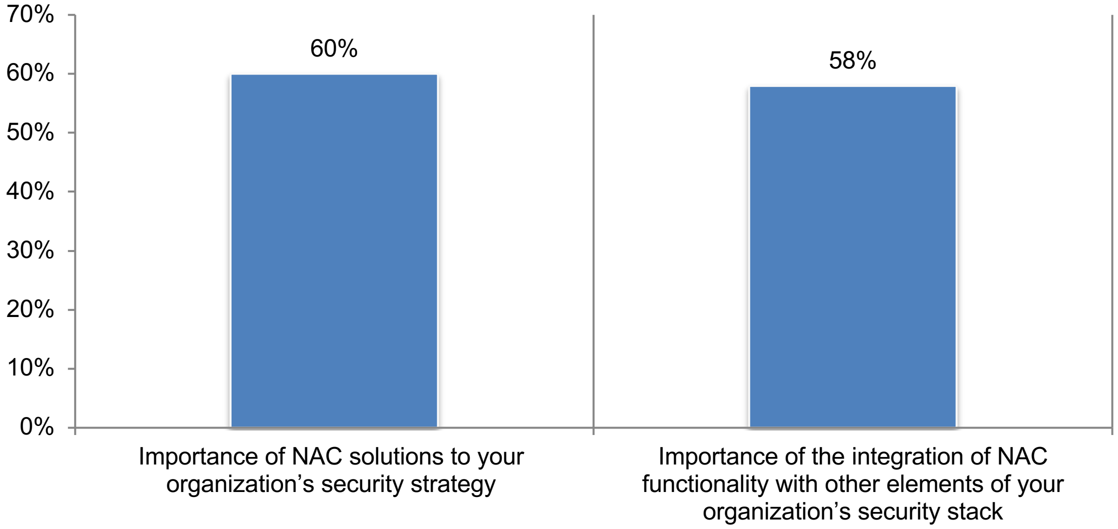
Figure 10 lists the purposes NAC is used. As shown, NAC in support of IoT has increased significantly from 12 percent of respondents to 45 percent of respondents in this year's research and BYOD has increased from 30 percent of respondents to 41 percent of respondents. The use of NAC for wired networks has decreased from 64 percent of respondents in 2021 to 47 percent of respondents in 2023.

Figure 10. For what purposes are NAC solutions deployed within your organization?
More than one response permitted



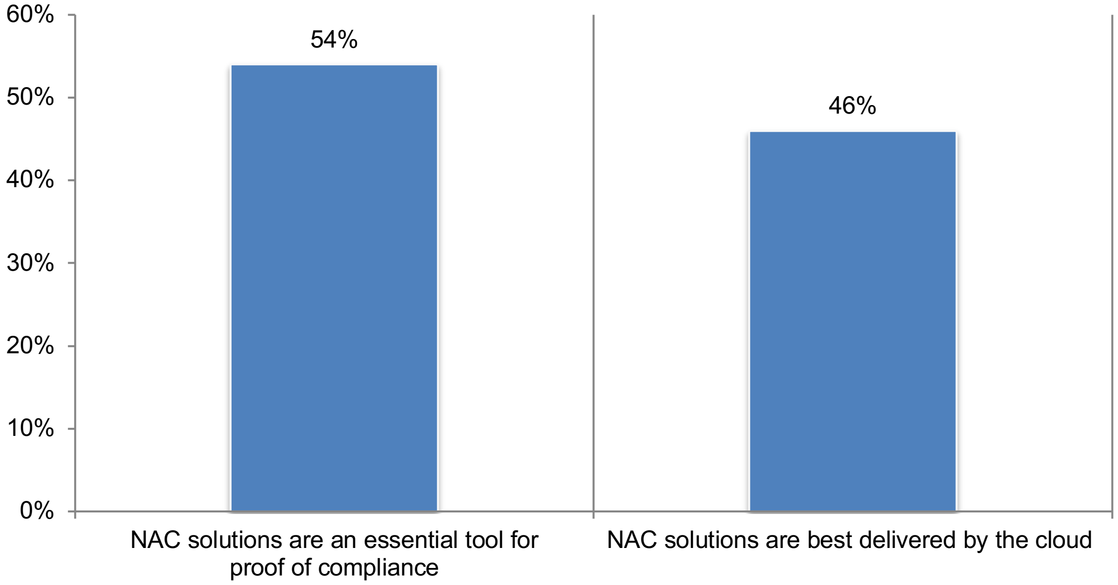
NAC solutions are very important to organizations' security strategies. Organizations that have adopted NAC solutions believe they can make a positive difference in their security strategies. Respondents were asked to rate the importance of NAC and the integration of NAC functionality with other elements of the security stack on a scale of 1 = not important to 10 = highly important. Figure 11 presents the very and highly important responses (7+ on the 10-point scale). As shown, 60 percent say NAC solutions are important and 58 percent of respondents say the integration of NAC functionality with other elements of their security stack is very or highly important.

Figure 11. The importance of NAC and its integration with other elements of your organization's security stack
On a scale of 1 = not important to 10 = highly Important, 7+ responses presented



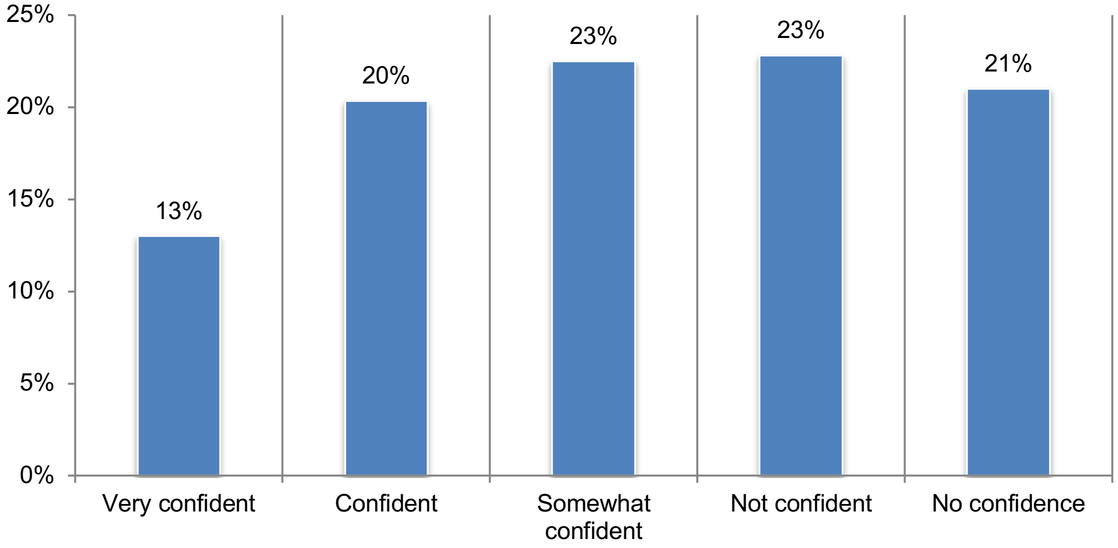
Fifty-four percent of respondents say NAC solutions are an essential tool for proof of compliance. Less than half (46 percent of respondents) say these solutions are best delivered by the cloud, as shown in Figure 12.

Figure 12. Perceptions about NAC solutions
Strongly agree and Agree responses combined



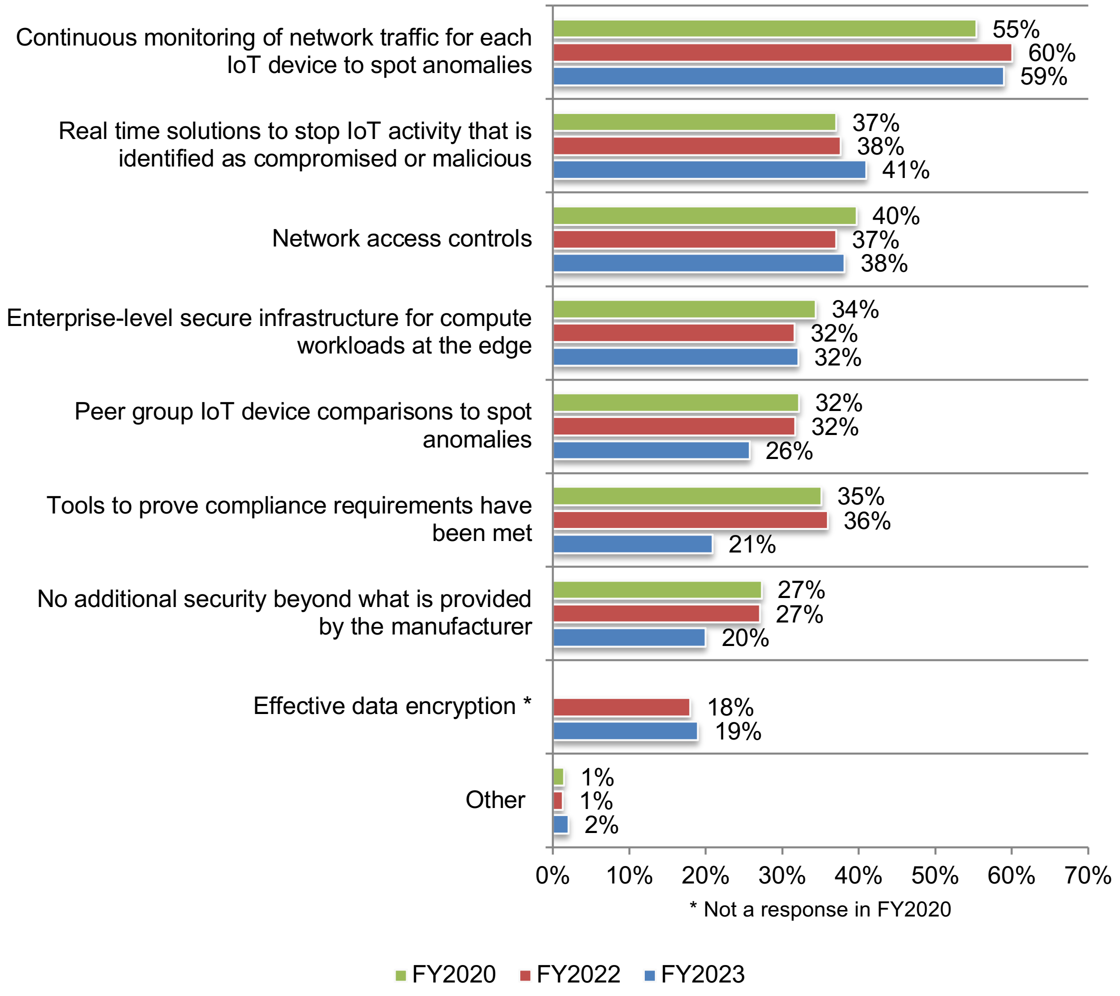
Perceptions are mixed about the ability of their NAC solutions and practices to keep pace with change. According to Figure 13, 56 percent of respondents say they are very confident (13 percent), confident (20 percent) or somewhat confident (23 percent) that NAC solutions and practices will keep pace with changes. However, 44 percent of respondents are not confident (23 percent) or have no confidence (21 percent) in their NAC solutions and practices to adapt to changes in the organization that might increase threats and risks.

Figure 13. How confident are you that your NAC solutions and practices will keep pace with changes in your organization?



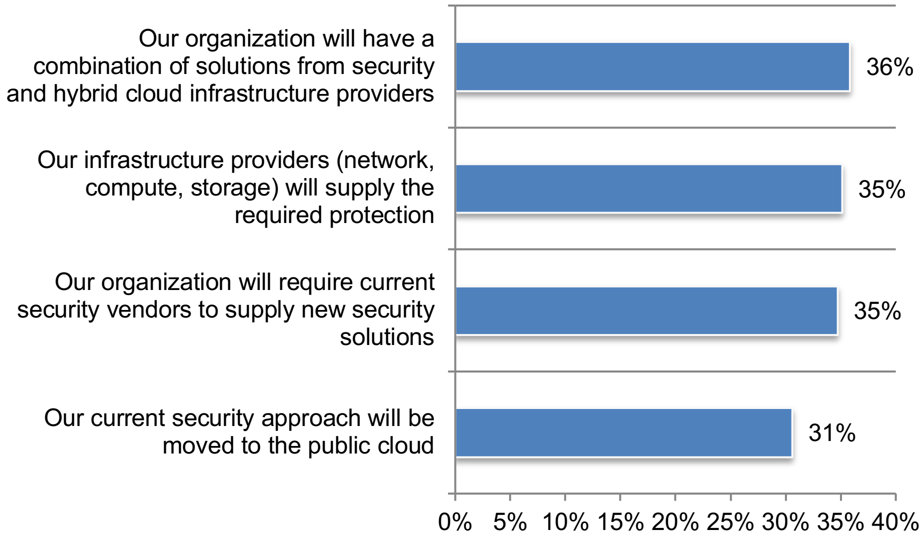
Only 40 percent of respondents are very confident in their organizations' ability to secure IoT devices' workloads and apps at the edge. According to Figure 14, continuous monitoring of network traffic for each IoT device to spot anomalies would increase their confidence in achieving a strong level of IoT security (59 percent of respondents). This is followed by having real time solutions to stop compromised or malicious IoT activity (41 percent of respondents) and network access controls (38 percent of respondents).

Figure 14. What is required to achieve a strong level of IoT security within your organizations
More than one response permitted



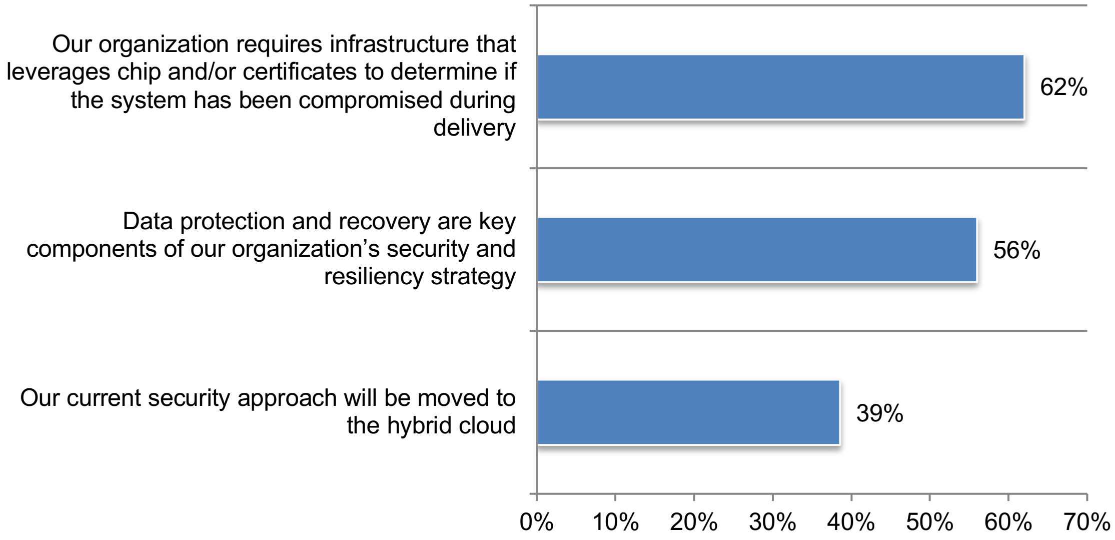
Security strategies are expected to change as edge computing and storage increases. According to Figure 15, respondents report that their organizations will have a combination of solutions from security and hybrid cloud infrastructure providers (36 percent of respondents), infrastructure providers will supply the required protection (35 percent of respondents) and current security vendors will be required to supply new security solutions (35 percent of respondents).

Figure 15. As compute and storage moves from the datacenter to the edge, how will your organization's current security approach change?
More than one response permitted



Compute and storage changes organizations' approach to data protection. According to Figure 16, 62 percent of respondents say their organizations require infrastructure that leverages chip and/or certificates to determine if the system has been compromised during delivery and 56 percent of respondents say data protection and recovery are key components of their security and resiliency strategy.

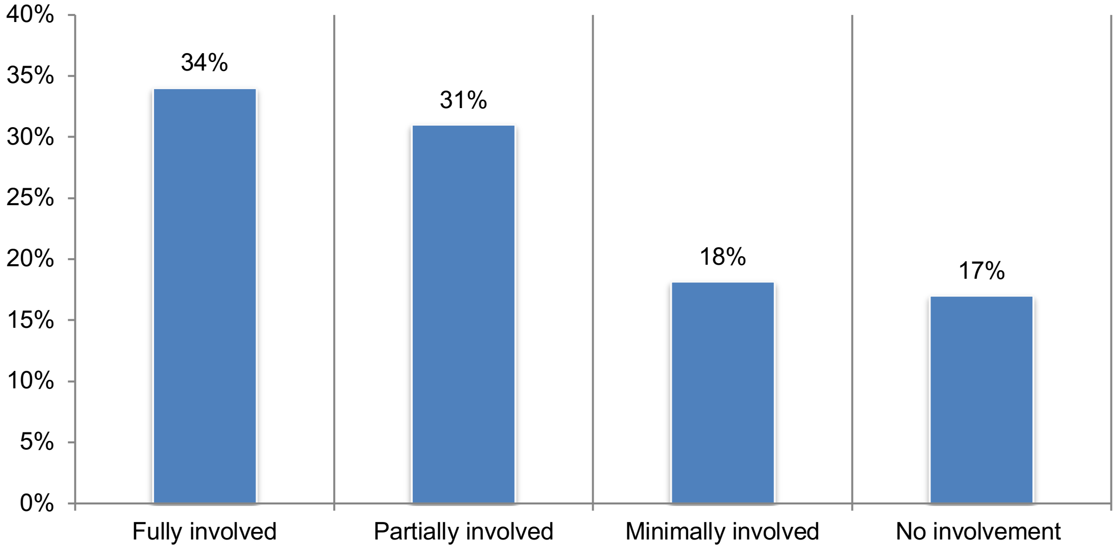
Figure 16. Perceptions about security approaches to compute and storage
Strongly agree and Agree responses combined



2.4 The importance of securing the hybrid cloud environment

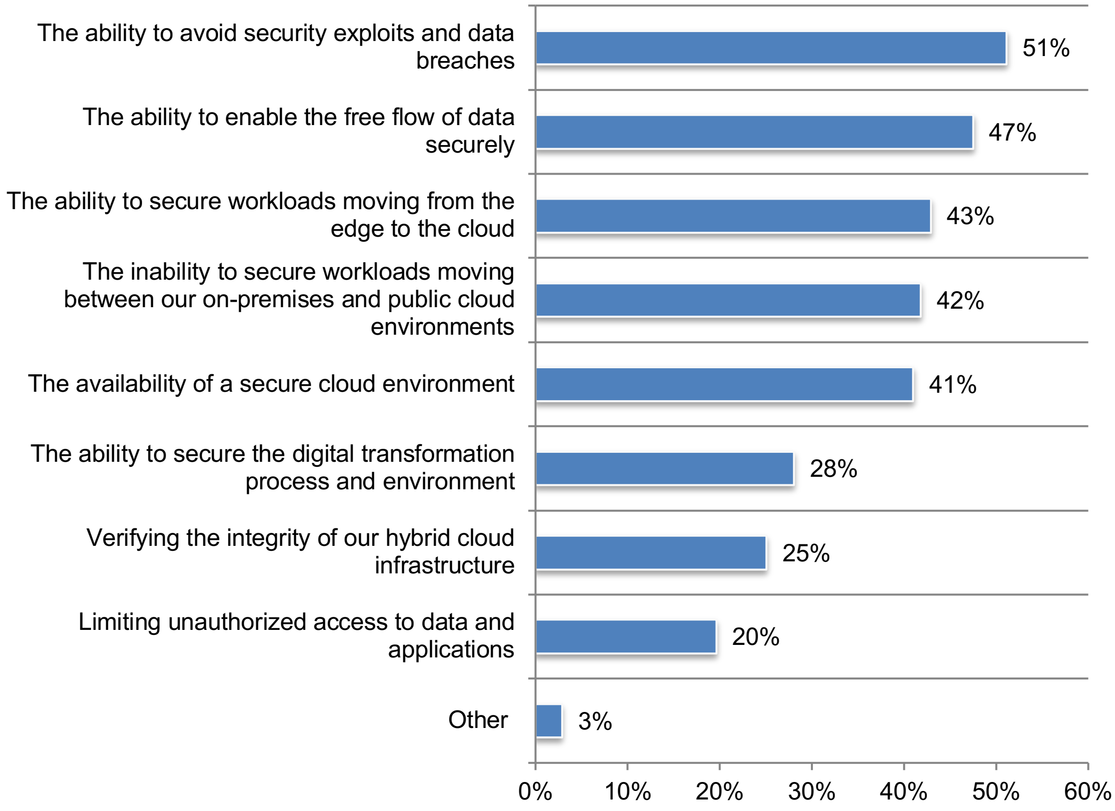
Security teams are involved in ensuring the security of the hybrid cloud environment. According to Figure 17, 65 percent of respondents say their security teams are fully involved (34 percent) or partially involved (31 percent). Typically, these teams assess digital exposure and overall risk to the business, protect critical assets across the organization (network, endpoints, servers and cloud) and ensure conformance and compliance with regulations, industry standards and security best practices.

Figure 17. Is your security team involved in ensuring security is designed into your organization's hybrid environments?



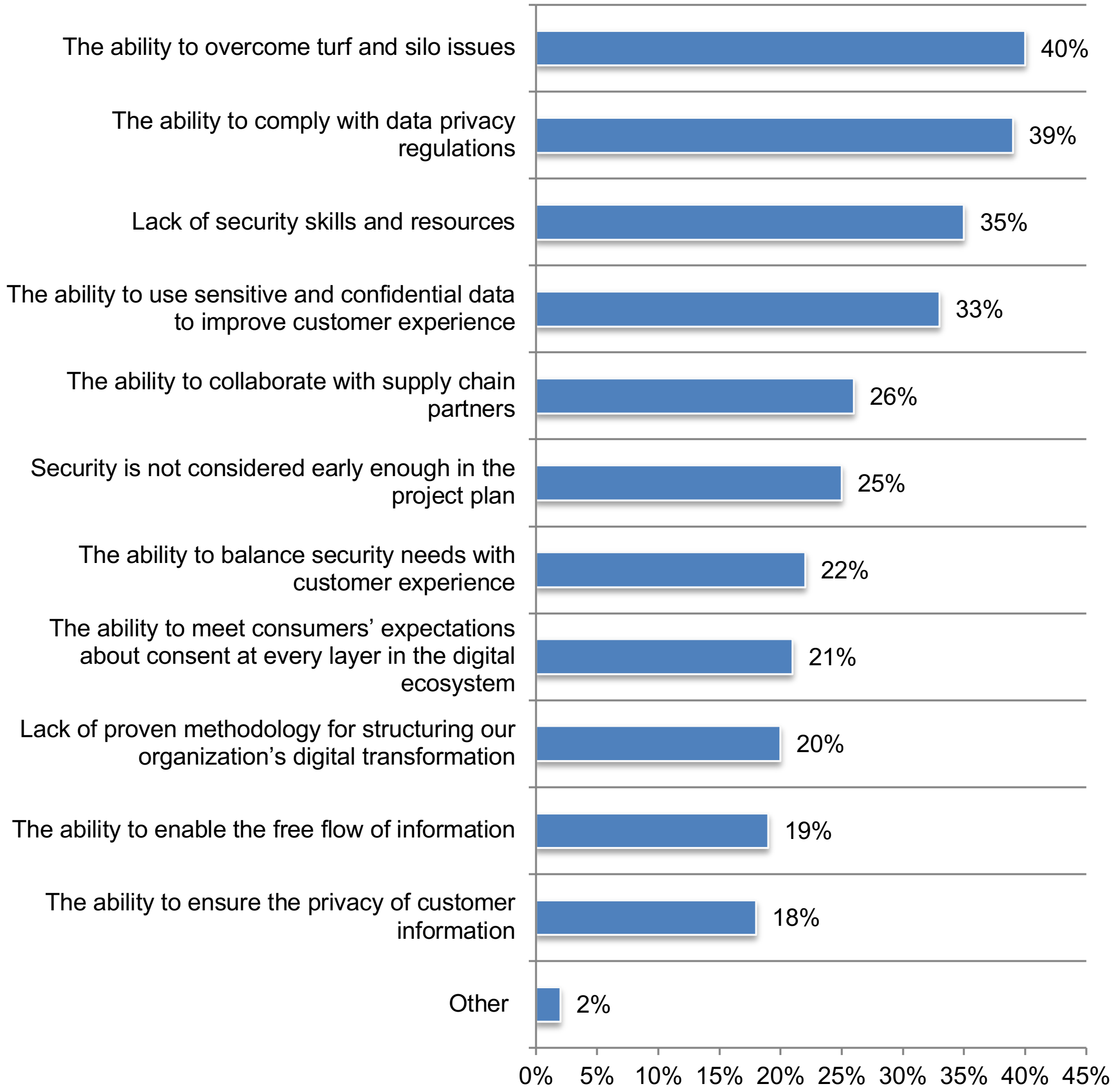
Fifty-eight percent of respondents say a successful shift to a hybrid cloud environment is dependent upon security technologies. Figure 18 presents a list of the challenges organizations face when securing the cloud environment. Most difficult is the ability to avoid security exploits and data breaches (51 percent of respondents), the ability to enable the free flow of data securely (47 percent of respondents) and the ability to secure workloads moving from the edge to the cloud (43 percent of respondents).

Figure 18. The top three primary technology challenges when securing your hybrid cloud environment
Three responses permitted



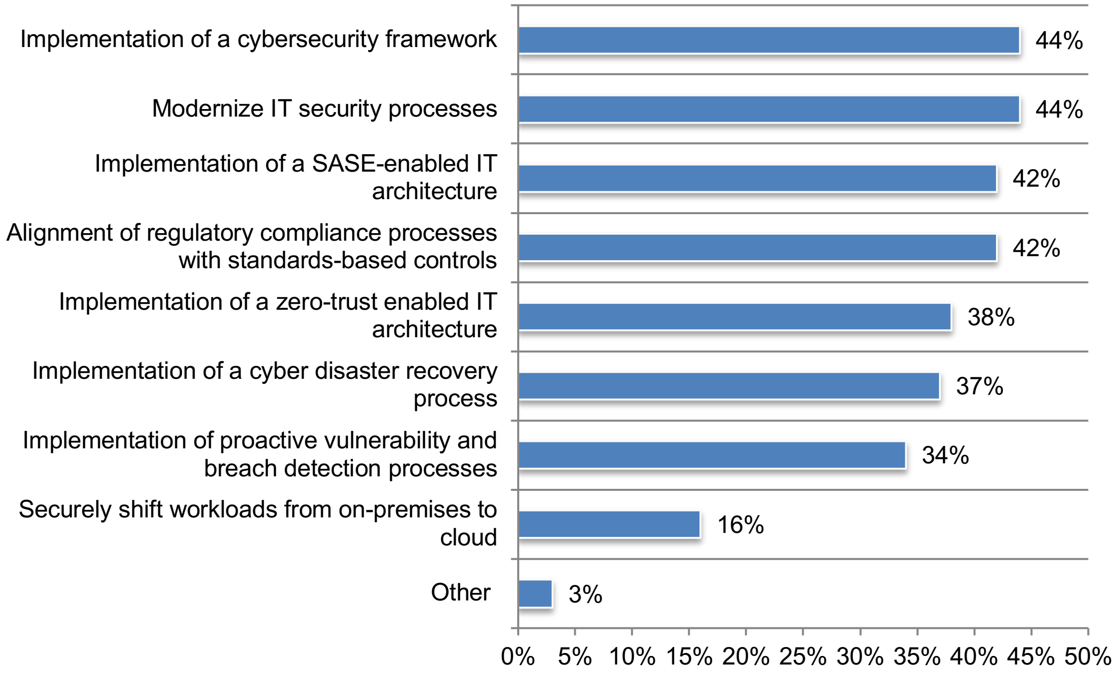
Once again, turf and silo issues affect security. Figure 19 presents operational and governance challenges to securing the hybrid cloud environment. Forty percent of respondents say the top challenge is the ability to overcome turf and silo issues, 39 percent of respondents say it is the ability to comply with data privacy regulations and 35 percent of respondents say it is a lack of security skills and resources.

Figure 19. The most significant operational and governance challenges to achieving a secure hybrid cloud environment in organizations
Three responses permitted



To minimize risk in a hybrid cloud environment, 44 percent of respondents say it is the implementation of a cybersecurity framework and the modernization of IT security processes that should be a priority. A SASE-enabled IT architecture (42 percent of respondents) and a zero-trust enabled architecture also should be at the top of the list.

Figure 20. Which processes are prioritized to minimize the risk in a hybrid cloud environment?
Three responses permitted



2.5 Best practices in closing the IT security gap

Twenty percent of respondents self-reported their organizations are highly effective in keeping up with a constantly changing threat landscape and close their organizations' IT security gap (9+ responses on a scale of 1 = not effective to highly effective). We refer to these organizations as "high performers". In this section, we analyze what these organizations are doing to achieve a more effective cybersecurity posture and close the IT security gap as compared to the 80 percent of respondents in the other organizations represented in this research.

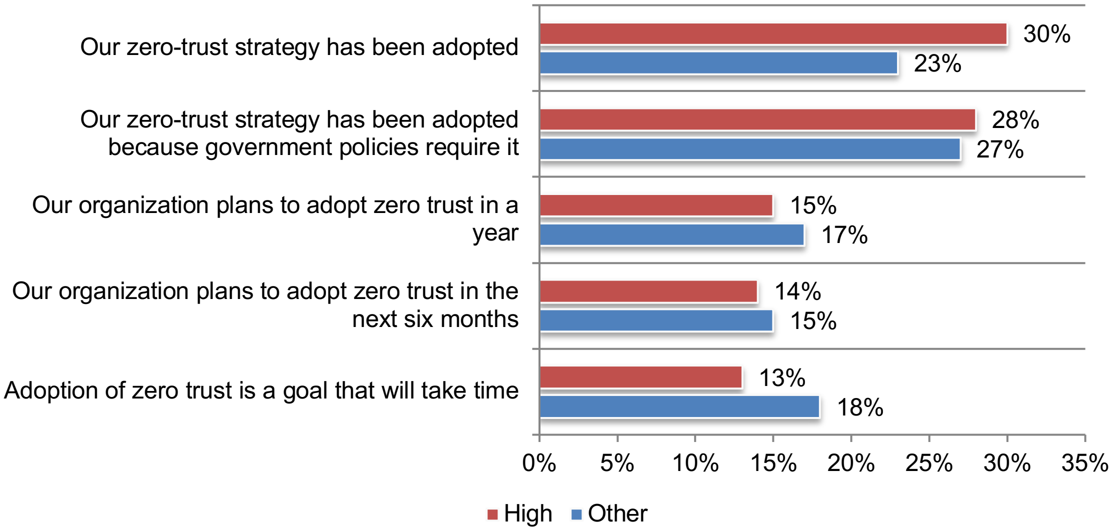
As evidence of their high effectiveness, high performing organizations had fewer security breaches in the past 12 months that resulted in data loss or downtime. Almost half of respondents (46 percent) in other organizations say their organizations had at least 7 and more than 10 incidents in just the past 12 months. In contrast, only 35 percent of high performing organizations had between 7 and more than 10 security incidents.

High performing organizations have a larger IT security function. Fifty-four percent of high performing organizations say their organizations have a minimum of 21 to more than 50 employees in their IT security function. Only 44 percent of respondents in other organizations had the same range of employees in IT security.

Most respondents are familiar with their organizations' approach to a zero-trust security model. Sixty-six percent of high performers are very familiar (23 percent) familiar (28 percent) or somewhat familiar (15 percent) with their organizations zero-trust strategy. Sixty-one percent of respondents in the other group say they are very familiar (20 percent), familiar (25 percent) or somewhat familiar (16 percent).

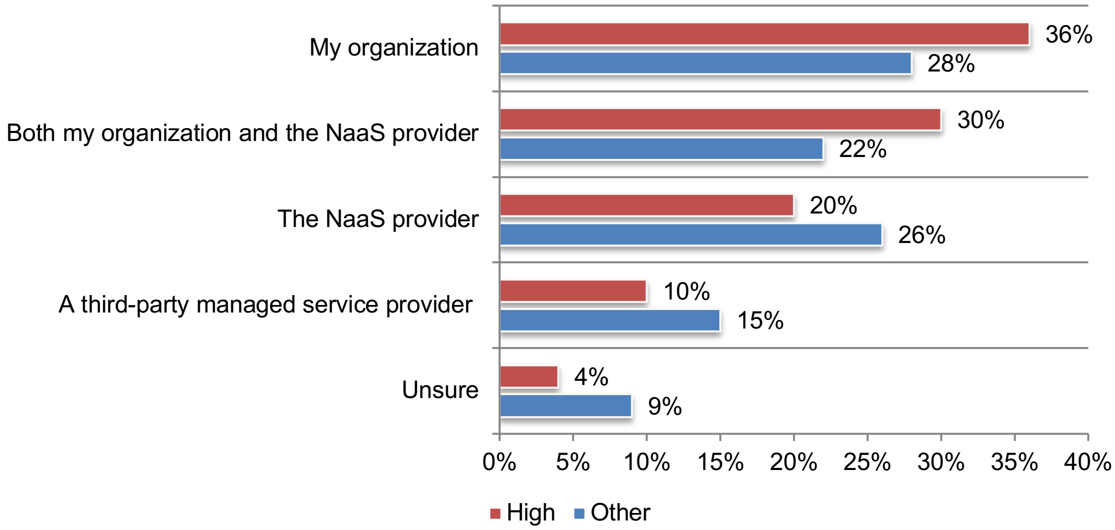
Government policies can drive zero trust adoption. As shown in Figure 21, 28 percent of respondents in high performing organizations and 27 percent of respondents in other organizations say adoption was based on government requirements.

Figure 21. What one statement best describes the state of your organization's approach to a zero-trust security model?



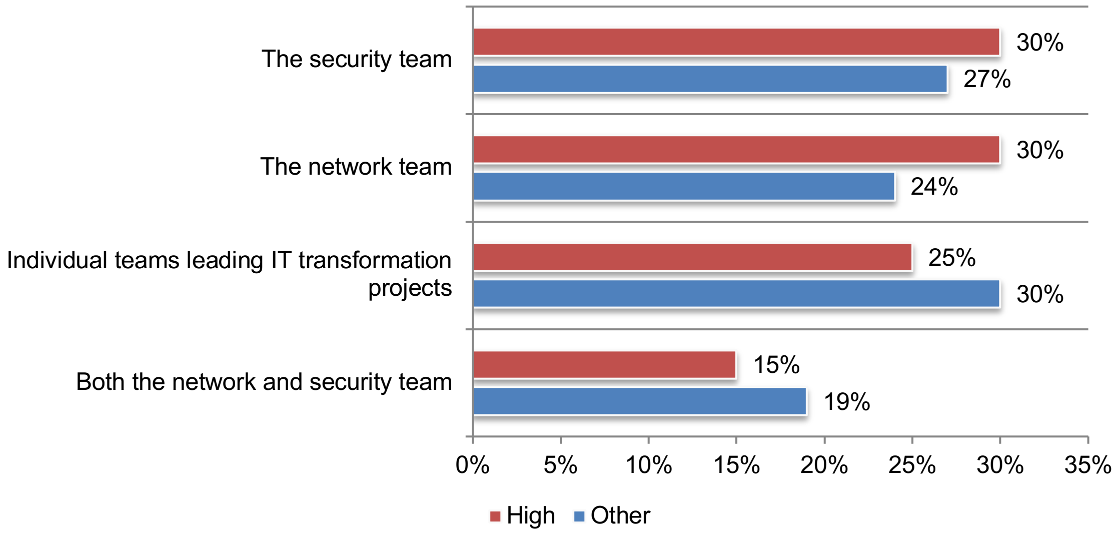
High performers control the deployment of zero trust within a Network as a Service (NaaS) deployment. Of those familiar with their organization's zero-trust strategy, more high performers (36 percent of respondents) than other respondents (28 percent of respondents) say their organizations are responsible for implementing zero trust security, as shown in Figure 22. Only 20 percent of high performers say it is the responsibility of the NaaS provider and 10 percent say a third-party managed service provider is responsible.

Figure 22. Within a Network as a Service (NaaS) deployment, whom would you expect to be responsible for implementing zero trust security?



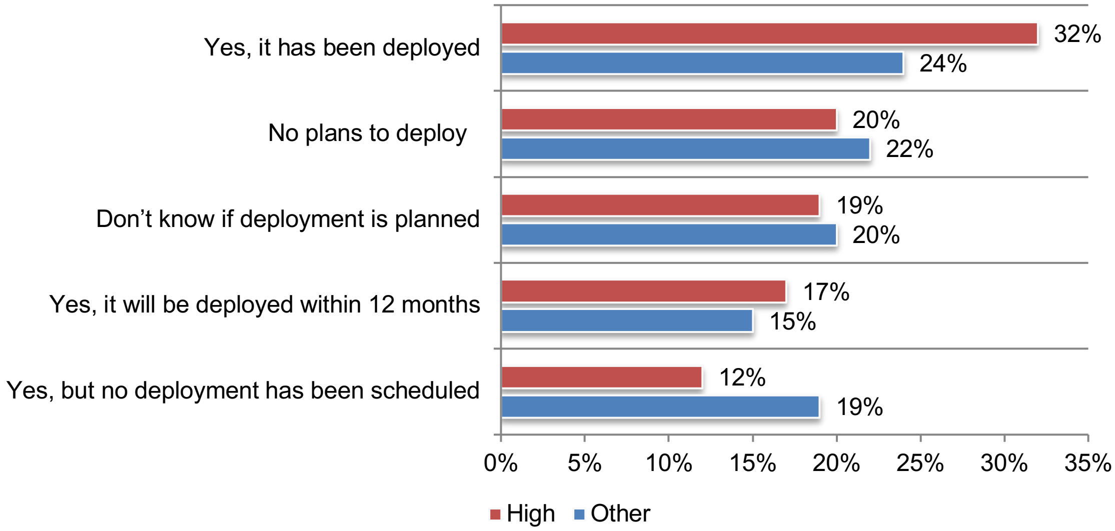
High performers centralize decisions about investments in security solutions and architectures. Figure 23 reports the primary responsibility for deciding on how resources are allocated for security solutions and products. Sixty percent of high performers say it is either the security team (30 percent) or network team (30 percent) are the decision makers. Only 15 percent say both functions are responsible.

Figure 23. Who makes security solution architecture/product decisions within your organization?



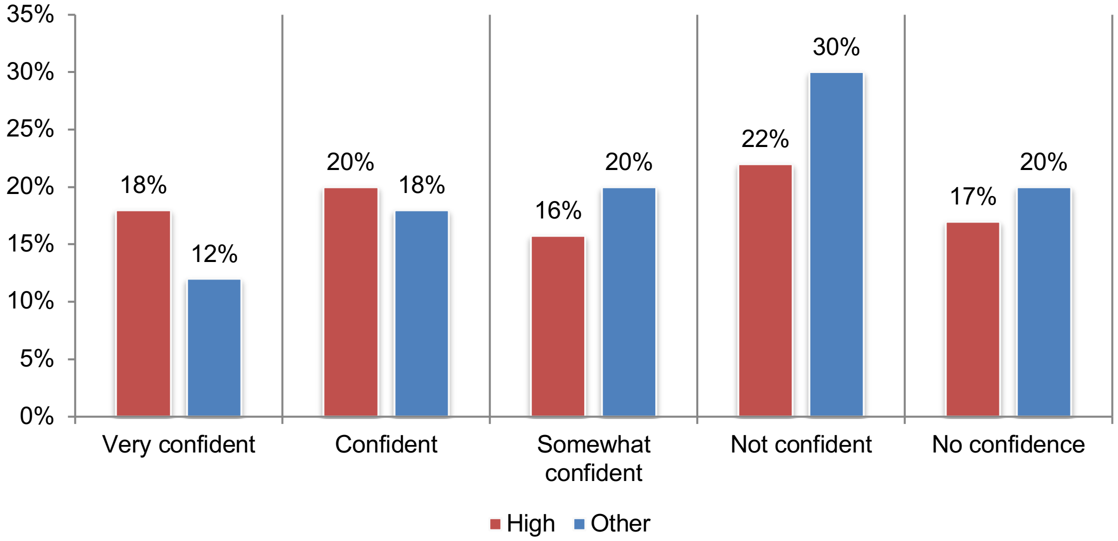
More high performers have deployed or plan to deploy the SASE architecture. According to Figure 24, 49 percent of high performers have deployed (32 percent) or plan to deploy (17 percent) the SASE architecture. In contrast only 39 percent of respondents in the other organizations have deployed (24 percent) or plan to deploy (15 percent) the SASE architecture.

Figure 24. Has your organization deployed, or does it plan to deploy, the SASE architecture?



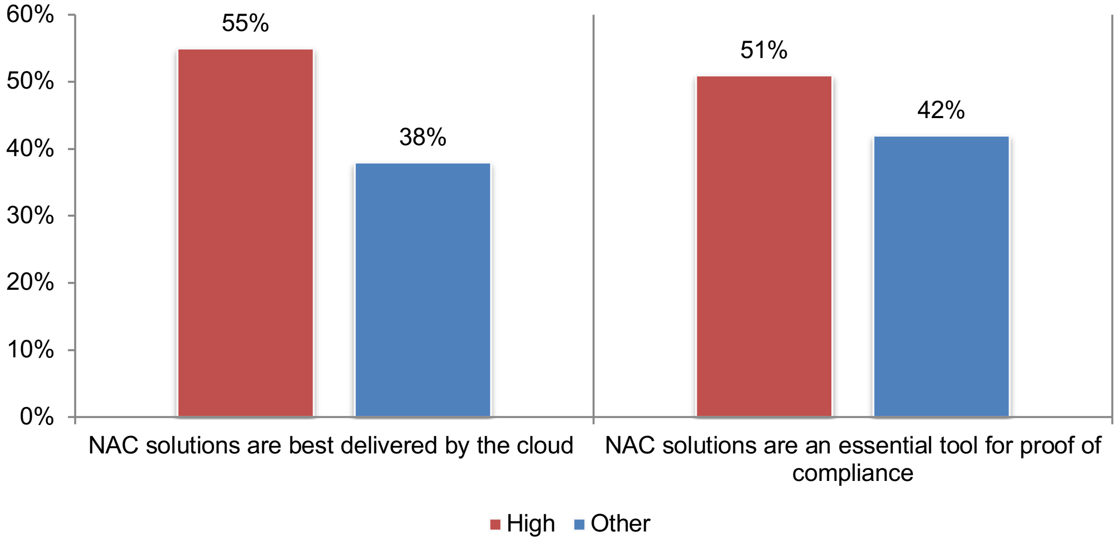
More high performers have achieved visibility of all users and devices. According to Figure 25, high performers are slightly more confident (38 percent of respondents) than other respondents (30 percent of respondents) that their organizations know all the users and devices connected to their networks all the time.

Figure 25. How confident are you that you know ALL the users and devices connected to your network ALL the time?



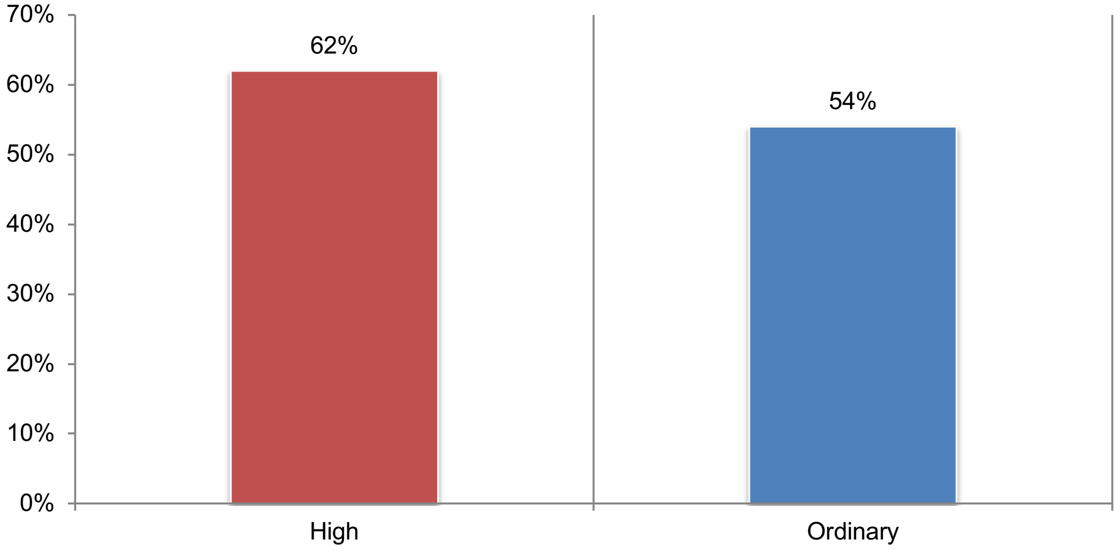
Far more high performers are positive about the use of NAC solutions and their importance to proving compliance. According to Figure 26, 51 percent of high performers say NAC solutions are an essential tool for proof of compliance vs. 42 percent of respondents in the other organizations. Fifty-five percent of high performers vs. 38 percent of other respondents say NAC solutions are best delivered by the cloud.

Figure 26. Perceptions about NAC solutions
Strongly agree and Agree responses combined



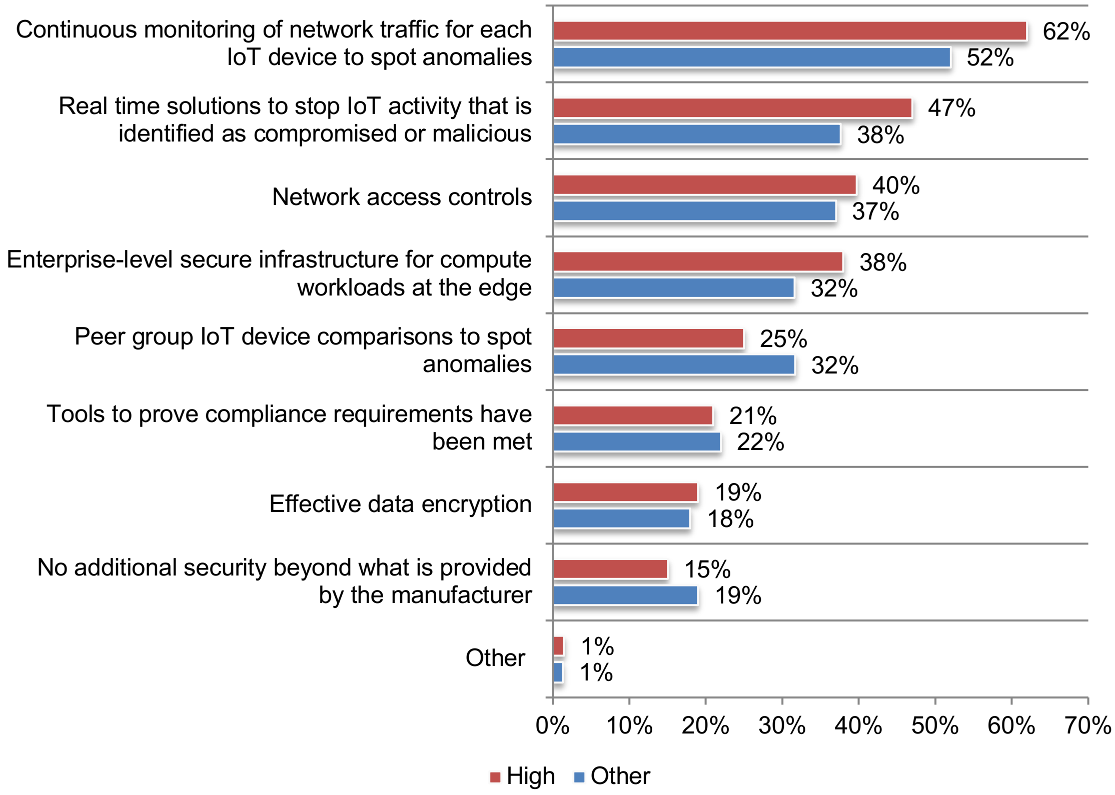
High performers recognize the importance of the integration of NAC functionality with the security stack. Respondents were asked to rate the importance of the integration of NAC functionality with other elements of the security stack on a scale from 1 = not important to 10 = highly important. Figure 27 shows the very and highly important responses (7+ responses). Sixty two percent of high performers vs. 54 percent of other respondents say such integration is important.

Figure 27. 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, 7+ responses presented



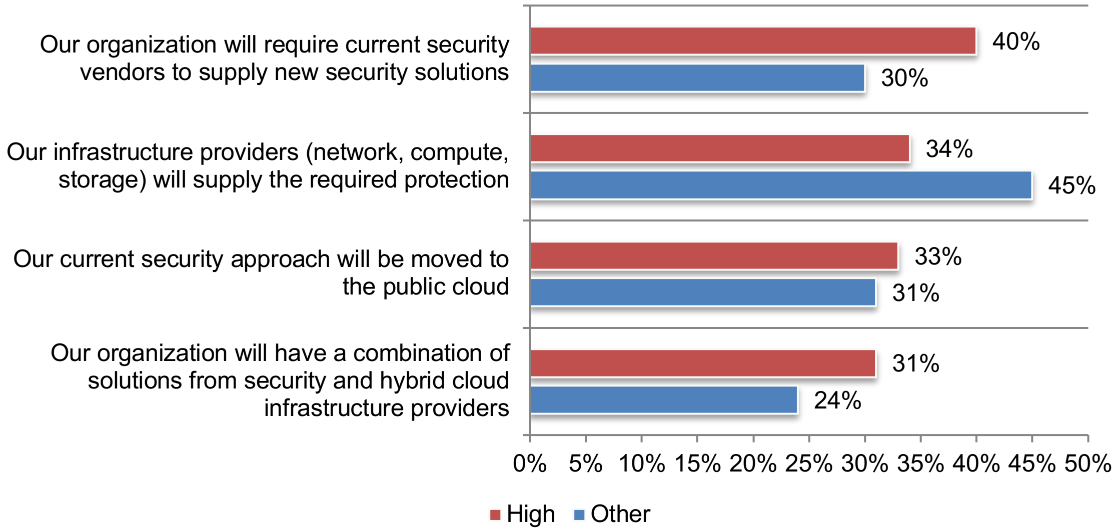
High performers are more likely to believe continuous monitoring of network traffic and real-time solutions will reduce IoT risks. Figure 28 presents a list of steps organizations can take to achieve a high level of IoT security. Sixty-two percent of high performers vs. 52 percent of other respondents say continuous monitoring of network traffic for each IoT device to spot anomalies is required. Forty-seven percent of high performers vs. 38 percent of other respondents say real-time solutions to stop compromised or malicious IoT activity is required.

Figure 28. What is required to achieve a strong level of IoT security within your organization?
More than one response presented



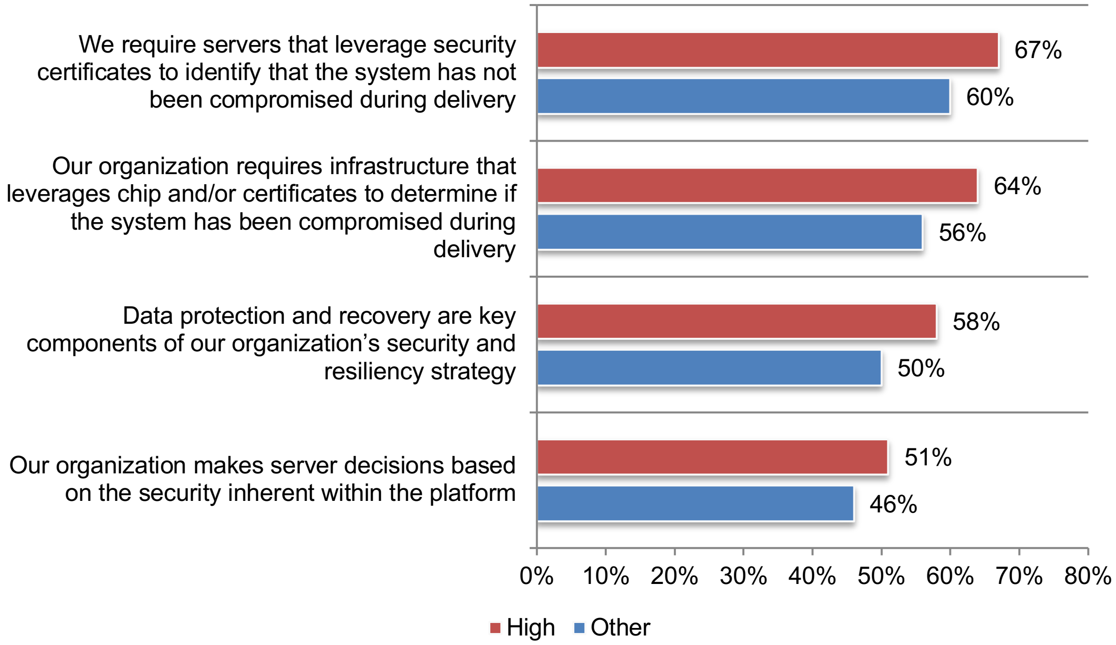
High performers are more likely to require current security vendors to supply new security solutions as compute and storage moves from the data center to the edge. As shown in Figure 29, 40 percent of high performers vs. 30 percent of other respondents say their organizations will require current security vendors to supply new security solutions. Respondents in other organizations are more likely to require their infrastructure providers to supply the required protection (45 percent vs. 34 percent in the high performing organizations).

Figure 29. As compute and storage moves from the data center to the edge, how will your organization's current strategy approach change?
More than one response permitted



High performers are more likely to require servers that leverage security certificates and infrastructures that leverage chips and/or certificates. Figure 30 shows significant differences between high performers and other respondents about compute and storage. Specifically, high performers require servers that leverage security certificates to confirm that the system has not been compromised during delivery (67 percent vs. 60 percent in other organizations). High performers also require infrastructure that leverages chip and/or certificates to determine if the system has been compromised during delivery (64 percent vs. 56 percent of respondents in other organizations). High performers also are more likely to believe data protection and recovery are key components of their organization's security and resiliency strategy (58 percent vs. 50 percent in other organizations).

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



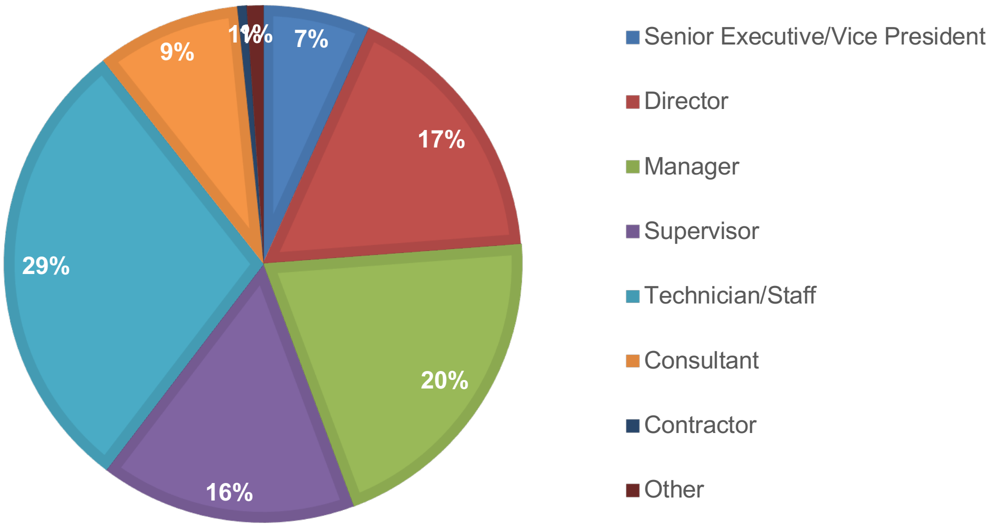
Part 3. Methods

The sampling frame is composed of 56,555 IT and IT security practitioners in North America, the United Kingdom, Germany, Australia, Japan and France. As shown in Table 1, 2,344 respondents completed the survey. Screening removed 260 surveys. The final sample was 2,084 surveys (or a 3.7 percent response rate).

Table 1. Sample response	Freq	Pct%
Total sampling frame	56,555	100.0%
Total returns	2,344	4.1%
Rejected or screened surveys	260	0.5%
Final sample	2,084	3.7%

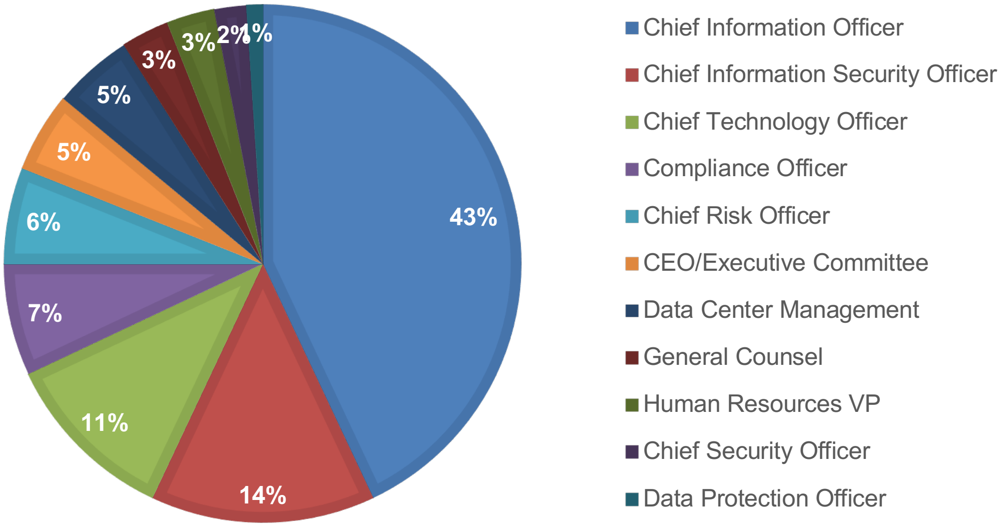
Pie Chart 1 reports the current position or organizational level of the respondents. Sixty percent of respondents reported their current position as supervisory or above and 29 percent of respondents reported their position as technician/staff.

Pie Chart 1. Distribution of respondents according to position level



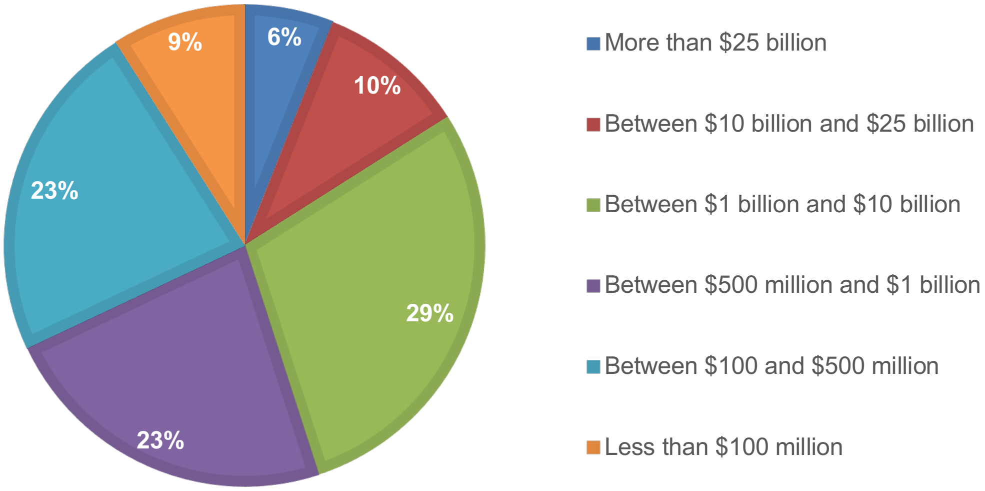
Pie Chart 2 identifies the primary person to whom the respondent or their IT security leader reports. Forty-three percent of respondents identified the chief information officer as the person to whom they report. Another 14 percent indicated they report directly to the chief information security officer and 11 percent of respondents report to the chief technology officer.

Pie Chart 2. Distribution of respondents according to reporting channel



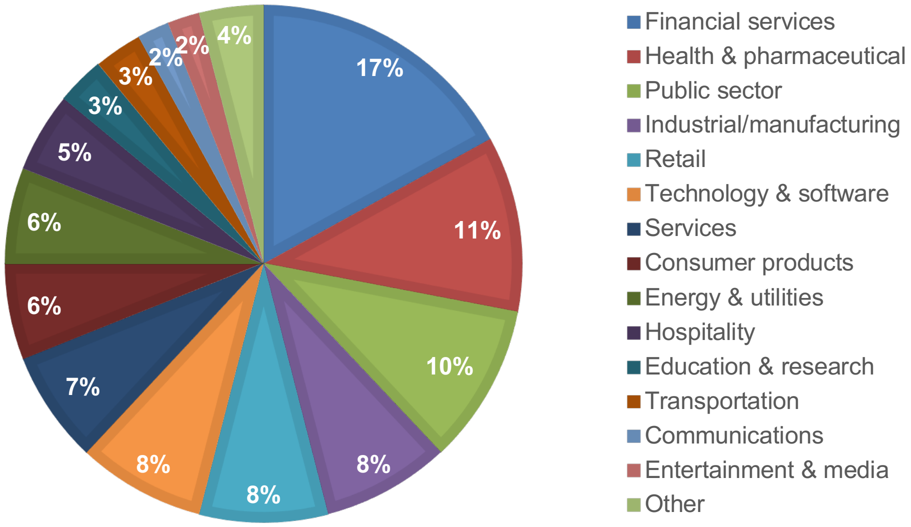
Pie Chart 3 reports the worldwide revenue of the respondents' organizations. More than half (54 percent) of respondents reported their organization's annual worldwide revenue to be greater than $1 billion.

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



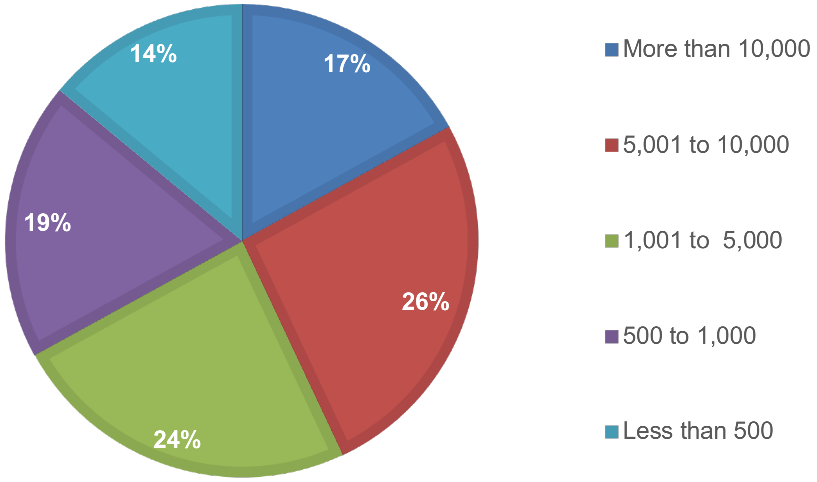
Pie Chart 4 reports the primary industry classification of respondents' organizations. This chart identifies financial services (17 percent of respondents) as the largest segment, which includes banking, insurance, brokerage, investment management and payment processing. Other large verticals include health and pharmaceutical (11 percent of respondents), public sector (10 percent of respondents), industrial/manufacturing (8 percent of respondents), retail (8 percent of respondents), and technology and software (8 percent of respondents).

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



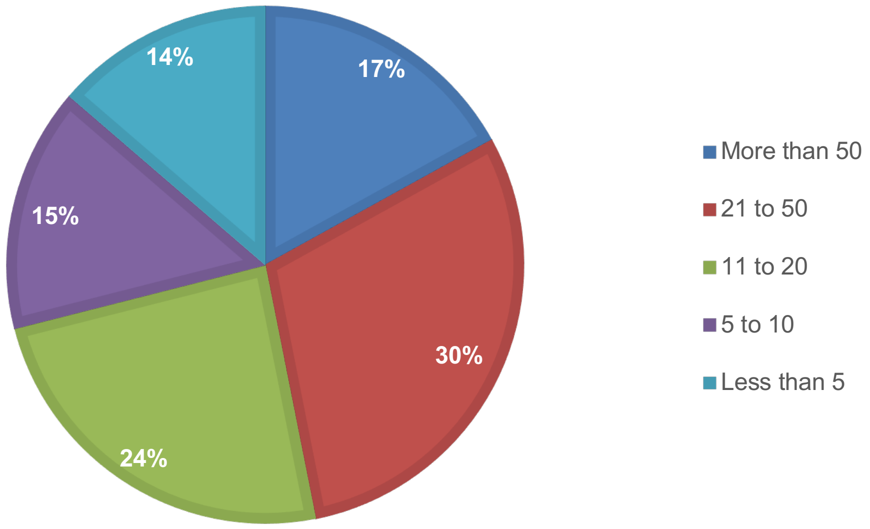
According to Pie Chart 5, 67 percent of respondents are from organizations with a global headcount of more than 1,000 employees.

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



Pie Chart 6 reports the number of employees that work in the IT security function. More than half (71 percent) of respondents reported that their organizations currently have more than 11 employees within the IT security function.

Pie Chart 6. Distribution of respondents according to the number of employees that work in IT security



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. All survey responses were captured in January 2023.

Survey response	FY2023	FY2022	FY2020
Sampling frame	56,555	52,595	52,045
Total returns	2,344	2,070	2,008
Rejected surveys	260	222	211
Final sample	2,084	1,848	1,796
Response rate	3.7%	3.2%	3.2%

Part 1. Screening

S1. What best describes your involvement in IT security investments within your organization?	FY2023	FY2022	FY2020
None (stop)	0%	0%	0%
Responsible for overall solution/purchase	44%	46%	46%
Responsible for administration/management	48%	57%	57%
Involved in evaluating solutions	52%	62%	68%
Total	145%	165%	171%

S2. What best describes your role within your organization's IT or IT security department?	FY2023	FY2022	FY2020
Security leadership (CSO/CISO)	49%	43%	40%
IT management	49%	53%	51%
IT operations	53%	48%	49%
Security management	58%	51%	53%
Security monitoring and response	71%	70%	68%
Data administration	30%	27%	27%
Compliance administration	20%	17%	17%
Applications development	21%	21%	22%
Data Protection Office	4%	3%	2%
I'm not involved in my organization's IT or IT security function	0%	0%	0%
Total	356%	333%	329%

S3. How knowledgeable are you about your organization's IT security strategy and tactics?	FY2023	FY2022	FY2020
Very knowledgeable	37%	33%	35%
Knowledgeable	39%	48%	48%
Somewhat knowledgeable	24%	20%	17%
Slightly knowledgeable (stop)	0%	0%	0%
No knowledge (stop)	0%	0%	0%
Total	100%	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?	FY2023
1 or 2	16%
3 or 4	17%
5 or 6	23%
7 or 8	22%
9 or 10	15%
More than 10	7%
Total	100%

Q2. How effective is your organization's ability to keep up with a constantly changing threat landscape and close the organization's IT security gap on a scale of 1 = not effective to 10 = highly effective?	FY2023	FY2022	FY2020
1 or 2	17%	9%	8%
3 or 4	17%	12%	12%
5 or 6	22%	27%	28%
7 or 8	24%	22%	25%
9 or 10	20%	30%	28%
Total	100%	100%	100%
Extrapolated value	5.76	6.54	6.58

Q3. How effective is your organization's security strategy in reducing threats in the attack landscape on a scale of 1 = not effective to 10 = highly effective?	FY2023
1 or 2	12%
3 or 4	19%
5 or 6	22%
7 or 8	23%
9 or 10	24%
Total	100%

Q4. Please rate each one of the following statements using the agreement scale provided below each item.

Q4a. Security teams lack visibility and control into all the activity of every user and device (i.e., mobile, BYOD, IoT) connected to their IT infrastructure.	FY2023	FY2022	FY2020
Strongly agree	35%	32%	34%
Agree	28%	34%	33%
Unsure	18%	15%	15%
Disagree	11%	12%	11%
Strongly disagree	8%	8%	7%
Total	100%	100%	100%

Q4b. My organization is getting the full value from our current security investments.	FY2023	FY2022	FY2020
Strongly agree	21%	20%	21%
Agree	26%	27%	27%
Unsure	20%	26%	25%
Disagree	19%	17%	17%
Strongly disagree	14%	9%	10%
Total	100%	100%	100%

Q5. What are the primary **security gaps** in your organization's IT infrastructure? Please select your top **three** choices	FY2023
Too many alerts to address and prioritize	27%
Inability to prevent and detect ransomware	25%
Inability to prevent and detect attacks on the hardware	23%
Inability to prevent and detect attacks on the O/S	26%
Inability to prevent and detect attacks on the firmware	24%
Hard to protect IoT, BYOD, mobile and cloud in the expanding and blurring IT perimeter	21%
Siloed or point security solutions	32%
Inability of traditional perimeter-based security solutions to detect and stop advanced targeted attacks	29%
Aging of legacy security controls	33%
Obsolescence or aging of legacy computer, storage or networking infrastructure	18%
We cannot verify the security of all our apps and workloads	37%
Other (please specify)	5%
Total	300%

Q6. What are the primary **operational and governance gaps** in your organization's IT infrastructure? Please select **two** choices only	FY2023
Security staffing, skills and experience shortages	39%
Conflicting priorities between IT and IT security teams	39%
Security solutions can't keep up with exponentially increasing amounts of data	40%
Difficulty in complying with IT security and privacy industry standards or regulations	38%
Insufficient budget	39%
Other	5%
Total	200%

Q7. Who makes security solution architecture/product decisions within your organization? Please select **one choice** only.	FY2023
The network team	31%
The security team	26%
Individual teams leading IT transformation projects	28%
Both the network and security team	15%
Total	100%

Q8. What are your organization's top three priorities when using automation to close the security gap? Please select the top **three** priorities.	FY2023
Reduce the number of false positives that analysts must investigate	38%
Reduce the amount of time and effort required to investigate an alert	41%
Reduce human intervention and as a result possibly human errors	31%
Detect attacks before they do damage or gain persistence	34%
Improve the coordination between the networking operations and security teams	35%
Automate key tasks in identity-based access control	39%
Continuously scan and monitor for changes	32%
Resolve threats/threat remediation (blocking, system wiping, etc.)	24%
Apply software patch updates (firmware, applications)	23%
Other	3%
Total	300%

Part 3. Attack mitigation and visibility

Q9. What are the most effective steps to take to minimize stealthy, or hidden threats within your organization's IT infrastructure? Please select the **top three** most effective steps.	FY2023
Implement infrastructure component identification/authentication	25%
Implement operating system kernel intrusion detection	23%
Utilize firmware/BIOS verification/authentication	26%
Implement SIEM (Security Information and Event Management)	23%
Implement NTA (Network Traffic Analysis)	25%
Adopt technologies that automate infrastructure integrity verification	29%
Implement a a secure and continuous data protection and back up strategy	22%
Prioritize rapid breach detection	24%
Conduct comprehensive penetration testing	25%
Implement network segmentation	28%
Implement a user, entity and device behavior analytics solution	24%
Implement a DoS/DDoS protection solution	23%
Other	3%
Total	300%

Q10. How familiar are you with your organization's zero-trust strategy?	FY2023
Very familiar	23%
Familiar	24%
Somewhat familiar	16%
Not familiar (please skip to Q14)	16%
Our organization does not have a zero-trust strategy (please skip to Q13)	21%
Total	100%

Q11. What **one** statement best describes the state of your organization's approach to a zero-trust security model? Please select **one** choice only.	FY2023
Our zero-trust strategy has been adopted	25%
Our zero-trust strategy has been adopted because government policies require it	26%
Our organization plans to adopt zero trust in the next six months	13%
Our organization plans to adopt zero trust in a year	17%
Adoption of zero trust is a goal that will take time	19%
Total	100%

Q12. Within a Network as a Service (NaaS) deployment, whom would you expect to be responsible for implementing zero trust security?	FY2023
My organization	32%
The NaaS provider	25%
Both my organization and the NaaS provider	20%
A third-party managed service provider (MSP)	15%
Unsure	8%
Total	100%

Q13. If your organization has not implemented a zero-trust framework, why? Please select the top **two** choices.	FY2023
A lack of skills and expertise	54%
Zero trust is a theoretical framework that cannot be implemented	45%
The value of zero trust is unclear and/or not fully understood	42%
No executive buy-in	21%
Too expensive	15%
Implementation is challenging because of the lack of integration between tools	16%
Other	7%
Total	200%

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. In this SASE architecture definition, users are provided robust security features directly to their 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.

Q14. How familiar are you with the Secure Access Service Edge (SASE) security architecture?	FY2023
Very familiar	33%
Familiar	33%
Somewhat familiar	21%
Not familiar (please skip to Q18)	13%
Total	100%

Q15. Has your organization deployed, or does it plan to deploy, the SASE security architecture?	FY2023
Yes, it has been deployed	30%
Yes, it will be deployed within 12 months	16%
Yes, but no deployment has been scheduled	13%
Don't know if deployment is planned	22%
No plans to deploy (please skip to Q18)	19%
Total	100%

Q16. Has your organization deployed or does it plan to deploy both SD-WAN and cloud-delivered security for a SASE security architecture?	FY2023
Yes, it has been deployed	28%
Yes, it will be deployed within 12 months	16%
Yes, but no deployment has been scheduled	15%
Don't know if deployment is planned (please skip to Q18)	16%
No plans to deploy (please skip to Q18)	25%
Total	100%

Q17. If yes, how would vendors be selected? Please select one choice only.	FY2023
Engage one vendor for both SD-WAN and cloud security	24%
Engage best-in-class networking integrated with best-in-class cloud security vendors	17%
Engage a best-in-class SD-WAN vendor that offer integrations with cloud security vendors	31%
Engage a best-in-class cloud security vendor(s) that offers integration with SD-WAN vendors	28%
Total	100%

Part 4. Network Access Control (NAC)

Q18. 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 5 = highly confident?	FY2023	FY2022	FY2020
Very confident	11%	5%	5%
Confident	16%	13%	14%
Somewhat confident	19%	14%	16%
Not confident	29%	32%	32%
No confidence	25%	36%	34%
Total	100%	100%	100%

Network Access Control (NAC) solutions support network visibility and access management through policy enforcement on devices and users of computer networks.

Q19. Does your organization use NAC solutions?	FY2023
Yes	32%
No (please skip to Q25)	68%
Total	100%

Q20. For what purposes are NAC systems deployed within your organization? Please check all that apply.	FY2023	FY2022	FY2020
Wired networks	47%	64%	62%
Wireless networks	48%	50%	55%
Guest access	45%	42%	43%
BYOD	41%	30%	31%
IoT	45%	12%	11%
Cloud	51%	45%	43%
Policy-based access and control	39%	42%	43%
NAC is not used	27%	24%	27%
Total	343%	309%	317%

Q21. How important are NAC solutions to your organization's security strategy on a scale of 1 = not important to 10 = highly Important?	FY2023
1 or 2	11%
3 or 4	10%
5 or 6	19%
7 or 8	29%
9 or 10	31%
Total	100%

Q22. Please rate the following statements using the agreement scale below.	
Q22a. NAC solutions are best delivered by the cloud	FY2023
Strongly agree	21%
Agree	25%
Unsure	18%
Disagree	23%
Strongly disagree	13%
Total	100%

Q22b. NAC solutions are an essential tool for proof of compliance	FY2023
Strongly agree	22%
Agree	32%
Unsure	18%
Disagree	15%
Strongly disagree	13%
Total	100%

Q23. 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?	FY2023
1 or 2	10%
3 or 4	14%
5 or 6	18%
7 or 8	32%
9 or 10	26%
Total	100%

Q24. How confident are you that that your NAC solutions and practices are flexible to keep pace with changes in your organization on a scale of 1 = no confidence to 5 = Highly confident?	FY2023
Very confident	13%
Confident	20%
Somewhat confident	23%
Not confident	23%
No confidence	21%
Total	100%

Part 5. Securing connectivity at the edge

Q25. How confident are you that your organization can secure IoT devices workloads and apps at the edge from 1 = no confidence to 10 = highly confident.	FY2023
1 or 2	14%
3 or 4	20%
5 or 6	26%
7 or 8	23%
9 or 10	17%
Total	100%

Q26. What is required to achieve a strong level of IoT security within your organization? Please check all that apply.	FY2023	FY2022	FY2020
Network access controls	38%	37%	40%
Effective data encryption	19%	18%	
Enterprise-level secure infrastructure for compute workloads at the edge	32%	32%	34%
Continuous monitoring of network traffic for each IoT device to spot anomalies	59%	60%	55%
Peer group IoT device comparisons to spot anomalies	26%	32%	32%
Real time solutions to stop IoT activity that is identified as compromised or malicious	41%	38%	37%
Tools to prove compliance requirements have been met	21%	36%	35%
No additional security beyond what is provided by the manufacturer	20%	27%	27%
Other (please specify)	2%	1%	1%
Total	258%	310%	263%

Q27. Please rate each one of the following statements using the agreement scale provided below each item.			
Q27a. Identifying and authenticating IoT devices accessing our network is critical to our organization's security strategy.	FY2023	FY2022	FY2020
Strongly agree	30%	31%	32%
Agree	37%	33%	34%
Unsure	16%	15%	14%
Disagree	10%	9%	9%
Strongly disagree	7%	12%	12%
Total	100%	100%	100%

Q28. Who within your organization is most responsible for ensuring the security of IoT devices and apps?	FY2023	FY2022	FY2020
Chief information officer (CIO)	20%	32%	31%
Chief technology officer (CTO)	20%	5%	5%
Chief information security officer (CISO)	20%	20%	18%
Chief security officer (CSO)	15%	3%	3%
Line of business leadership	8%	10%	12%
End-users of IoT devices	8%	11%	13%
Data Protection Officer (DPO)	4%	0%	1%
No one function has overall responsibility	3%	17%	16%
Other (please specify)	2%	1%	1%
Total	100%	100%	100%

Part 6. Hybrid cloud security

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.

Q29. Is your security team involved in ensuring security is designed into your organization's hybrid environments?	FY2023
Yes, fully involved	34%
Yes, partially involved	31%
Yes, minimally involved	18%
No involvement (please skip to Q35)	17%
Total	100%

Q30. How important are security technologies to a successful shift to a hybrid cloud environment from 1 = not important to 10 = highly important.	FY2023
1 or 2	10%
3 or 4	12%
5 or 6	20%
7 or 8	32%
9 or 10	26%
Total	100%

Q31. What do you see as the top three primary **technology challenges** when securing your hybrid cloud environment? Please select your **top three** choices only.	FY2023
The availability of a secure cloud environment	41%
The inability to secure workloads moving between our on-premises and public cloud environments	42%
The ability to secure workloads moving from the edge to the cloud	43%
The ability to avoid security exploits and data breaches	51%
The ability to enable the free flow of data securely	47%
The ability to secure the digital transformation process and environment	28%
Verifying the integrity of our hybrid cloud infrastructure	25%
Limiting unauthorized access to data and applications	20%
Other	3%
Total	300%

Q32. 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.	FY2023
Security is not considered early enough in the project plan	25%
The ability to enable the free flow of information	19%
The ability to collaborate with supply chain partners	26%
The ability to ensure the privacy of customer information	18%
The ability to meet consumers’ expectations about consent at every layer in the digital ecosystem	21%
The ability to balance security needs with customer experience	22%
The ability to comply with data privacy regulations	39%
The ability to use sensitive and confidential data to improve customer experience	33%
The ability to overcome turf and silo issues	40%
Lack of security skills and resources	35%
Lack of proven methodology for structuring our organization’s digital transformation	20%
Other	2%
Total	300%

Q33. Which processes are prioritized to minimize the risk in a hybrid cloud environment? Please select the **top three** choices only.	FY2023
Alignment of regulatory compliance processes with standards-based controls	42%
Implementation of a cyber disaster recovery process	37%
Modernize IT security processes	44%
Implementation of a zero-trust enabled IT architecture	38%
Implementation of a SASE-enabled IT architecture	42%
Implementation of a cybersecurity framework	44%
Implementation of proactive vulnerability and breach detection processes	34%
Securely shift workloads from on-premises to cloud	16%
Other	3%
Total	300%

Part 7. Compute and storage

Q34. As compute and storage moves from the datacenter to the edge, how will your organization's current security approach change?	FY2023
Our organization will require current security vendors to supply new security solutions	35%
Our infrastructure providers (network, compute, storage) will supply the required protection	35%
Our organization will have a combination of solutions from security and hybrid cloud infrastructure providers	36%
Our current security approach will be moved to the public cloud	31%
Total	136%

Q35. Please rate the following statements using the agreement scale below each item			
Q35a. Our organization makes server decisions based on the security inherent within the platform.	FY2023	FY2022	FY2020
Strongly agree	20%	28%	29%
Agree	28%	29%	27%
Unsure	19%	22%	21%
Disagree	20%	14%	16%
Strongly disagree	13%	8%	7%
Total	100%	100%	100%

Q35b. We require servers that leverage security certificates to identify that the system has not been compromised during delivery.	FY2023	FY2022
Strongly agree	40%	40%
Agree	26%	27%
Unsure	17%	18%
Disagree	11%	10%
Strongly disagree	6%	4%
Total	100%	100%

Q35c. Data protection and recovery are key components of our organization's security and resiliency strategy.	FY2023
Strongly agree	29%
Agree	27%
Unsure	15%
Disagree	16%
Strongly disagree	13%
Total	100%

Q35d. Our organization requires infrastructure that leverages chip and/or certificates to determine if the system has been compromised during delivery	FY2023
Strongly agree	38%
Agree	24%
Unsure	20%
Disagree	11%
Strongly disagree	7%
Total	100%

Q35e. Our current security approach will be moved to the hybrid cloud.	FY2023
Strongly agree	39%
Agree	26%
Unsure	16%
Disagree	12%
Strongly disagree	7%
Total	100%

Part 7. Privacy, governance and compliance

Q36. Please rate the following statements using the agreement scale provided below.			
Q36a. Achieving a strong cybersecurity posture means reducing the privacy risk to our employees, business partners and customers.	FY2023	FY2022	FY2020
Strongly agree	28%	30%	33%
Agree	29%	35%	33%
Unsure	19%	18%	17%
Disagree	12%	12%	11%
Strongly disagree	12%	6%	6%
Total	100%	100%	100%

Q36b. The General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA) and other privacy regulations influence our organization's investments in and deployment of security solutions.	FY2023	FY2022	FY2020
Strongly agree	29%	33%	30%
Agree	28%	29%	28%
Unsure	17%	18%	22%
Disagree	17%	14%	14%
Strongly disagree	9%	6%	6%
Total	100%	100%	100%

Q36c. It is not possible to have privacy without a strong security posture.	FY2023	FY2022	FY2020
Strongly agree	34%	38%	39%
Agree	29%	33%	36%
Unsure	19%	14%	13%
Disagree	12%	8%	7%
Strongly disagree	6%	6%	5%
Total	100%	100%	100%

Q36d. Executive orders and regulations impact investments and deployments of security solutions.	FY2023	FY2022	FY2020
Strongly agree	38%	38%	39%
Agree	30%	33%	36%
Unsure	18%	14%	13%
Disagree	10%	8%	7%
Strongly disagree	4%	6%	5%
Total	100%	100%	100%

Q36e. Investments are based on the ability of suppliers to ensure products and solutions are manufactured in secure facilities with compliance to high security standards.	FY2023	FY2022	FY2020
Strongly agree	36%	38%	39%
Agree	36%	33%	36%
Unsure	14%	14%	13%
Disagree	8%	8%	7%
Strongly disagree	6%	6%	5%
Total	100%	100%	100%

Part 8. Your role and organization

D1. What organizational level best describes your current position?	FY2023	FY2022	FY2020
Senior Executive/Vice President	7%	5%	5%
Director	17%	17%	18%
Manager	20%	22%	22%
Supervisor	16%	15%	16%
Technician/Staff	29%	35%	34%
Consultant	9%	5%	4%
Contractor	1%	0%	0%
Other	1%	1%	1%
Total	100%	100%	100%

D2. Check the **Primary Person** you or your leader reports to within the organization.	FY2023	FY2022	FY2020
CEO/Executive Committee	5%	4%	4%
General Counsel	3%	2%	2%
Chief Information Officer (CIO)	43%	46%	45%
Chief Technology Officer (CTO)	11%	11%	10%
Chief Information Security Officer (CISO)	14%	16%	18%
Compliance Officer	7%	6%	6%
Human Resources VP	3%	2%	2%
Chief Security Officer (CSO)	2%	1%	2%
Data Center Management	5%	5%	4%
Chief Risk Officer (CRO)	6%	7%	7%
Data Protection Officer (DPO)	1%	0%	0%
Other	0%	0%	0%
Total	100%	100%	100%

D3. What range best defines the worldwide revenue of your organization?	FY2023	FY2022	FY2020
Less than $100 million	9%	6%	5%
Between $100 and $500 million	23%	24%	24%
Between $500 million and $1 billion	23%	24%	25%
Between $1 billion and $10 billion	29%	30%	28%
Between $10 billion and $25 billion	10%	10%	11%
More than $25 billion	6%	6%	6%
Total	100%	100%	100%

D4. What best describes your organization’s primary industry classification?	FY2023	FY2022	FY2020
Agriculture & food services	1%	1%	1%
Communications	2%	2%	2%
Consumer products	6%	6%	5%
Defense & aerospace	1%	1%	1%
Education & research	3%	3%	3%
Energy & utilities	6%	6%	6%
Entertainment & media	2%	1%	1%
Financial services	17%	16%	17%
Health & pharmaceutical	11%	12%	12%
Hospitality	5%	5%	4%
Industrial/manufacturing	8%	8%	8%
Public sector	10%	12%	11%
Retail	8%	9%	9%
Services	7%	7%	8%
Technology & software	8%	7%	7%
Transportation	3%	2%	2%
Other	2%	3%	2%
Total	100%	100%	100%

D5. How many employees are in your organization?	FY2023	FY2022	FY2020
Less than 500	14%	12%	13%
500 to 1,000	19%	21%	21%
1,001 to 5,000	24%	28%	29%
5,001 to 10,000	26%	23%	23%
More than 10,000	17%	16%	14%
Total	100%	100%	100%

D6. How many employees work in your IT security function?	FY2023
Less than 5	14%
5 to 10	15%
11 to 20	24%
21 to 50	30%
More than 50	17%
Total	100%

Please contact research@ponemon.org or call us at 800.887.3118 if you have any questions.

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.