The 2022 Study on Closing the IT Security Gap: Global

Sponsored by Hewlett Packard Enterprise

Independently conducted by Ponemon Institute LLC

Publication Date: January 2022

Ponemon Institute© Research Report

The 2022 Study on Closing the IT Security Gap: Global

Prepared by Ponemon Institute, January 2022

Part 1. Introduction

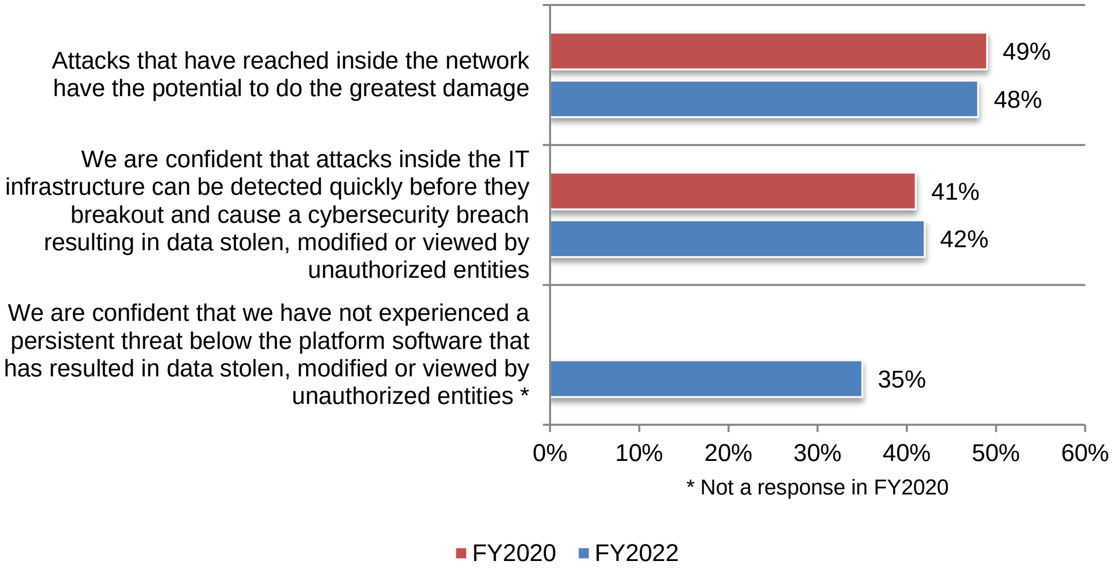
As the threat landscape becomes more sinister, the ability to close the IT security gap is more critical than ever. Sponsored by HPE, the study has been tracking organizations' efforts to close gaps in their IT security infrastructure that allow attackers to penetrate their defenses since 2018[1].

The IT security gap is defined as the inability of an organization's people, processes and technologies to keep up with a constantly changing threat landscape. It diminishes the ability of organizations to identify, detect, contain 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) and the California Consumer Privacy Act (CCPA). Only 30 percent of respondents say their organizations are highly effective in keeping up with a constantly changing threat landscape and close the IT security gap.

Ponemon Institute surveyed 1,848 IT and IT security practitioners in North America, the United Kingdom, Germany, Australia and Japan. This report presents the global findings and compares them to the 2020 global findings[2]. All respondents are knowledgeable about their organizations' IT security and strategy and are involved in decisions related to the investment in technologies.

Few respondents are confident that their organizations can prevent a persistent threat below the platform that would result in data stolen, modified or viewed by unauthorized entities. As shown in Figure 1, only 35 percent of respondents have such confidence. Similar to the last study, 48 percent of respondents believe attacks that have reached inside the network have the potential to do the greatest damage. Forty-two percent of respondents say that attacks inside the IT infrastructure can be detected quickly before they breakout and cause a cybersecurity breach resulting in data stolen, modified or viewed by unauthorized entities.

Figure 1. Perceptions about the threat of attacks on the inside
Strongly agree and Agree responses combined



[1] *Closing the IT Security Gap with Automation & AI in the Era of IoT: Global,* September 2018, conducted by Ponemon Institute and sponsored by HPE.

[2] The research findings for the last report were collected in 2019 and published in 2020. The findings for this year's study were collected in 2021 and published in 2022.

Best practices from organizations that are effective in closing the IT security gap

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

Following are the nine best practices of high performing organizations.

High performers are more likely to have visibility and control into users' activities and devices. Only 33 percent of high performers believe their security teams **lack visibility and control** into all activity of every user and device. In contrast, 80 percent of those in the other category say their teams lack visibility and control. High performers are also more likely to get value from their security investments (59 percent vs. 42 percent of respondents). However, both groups agree that the IT infrastructure has gaps that allow attackers to penetrate its defenses (60 percent of high performers and 61 percent of respondents in the other category).

High performers are more likely to agree that attacks that have reached inside the network have the potential to do the greatest damage. Fifty-six percent of high performers recognize the potential damage from attacks that have reached inside the network vs. 45 percent of respondents in the other category. Forty-seven percent of high performers are confident that their organizations have not experienced a persistent threat below the platform software that has resulted in data stolen, modified or viewed by unauthorized entities vs. 30 percent in the other category.

High performing organizations are more likely to implement a Zero Trust Model. Sixty-four percent of high performing organizations have a Zero Trust Model because government policies required it (25 percent), have a Zero Trust Model for other reasons (24 percent of respondents) or selected elements from the Zero-Trust framework to improve security (15 percent). Thirty-six percent of organizations in the other category are not interested in a Zero Trust approach (25 percent of respondents) or have chosen not to implement (11 percent of respondents).

High performers say as compute and storage moves from the data center to the edge it requires a combination of traditional security solutions and secure infrastructure (61 percent). The other respondents are more likely to say a new type of security will be required (59 percent).

IoT security is more of a concern for high performers. Eighty-five percent of respondents say identifying and authenticating IoT devices accessing our network is critical to their organization's security strategy. Only slightly more than half (55 percent) of other respondents agree with this. In addition, high performers are more likely to say legacy IoT technologies are difficult to secure (80 percent vs. 69 percent of respondents in the other category. Forty percent of high performer respondents say their IoT devices are appropriately secured with a proper security strategy in place vs. 15 percent of respondents in the other sample.

High performing organizations say security technologies are very important for their digital transformation strategy. Seventy-seven percent of high performing organizations say it is important (35 percent of respondents) or highly important (42 percent of respondents) to have security technologies to support digital transformation. In contrast, 53 percent of the other respondents say it is important or highly important.

High performers take a different approach to server security and backup and recovery. Eighty-eight percent of high performer respondents say backup and recovery is a key component of their security strategy and 68 percent of high performers say their organizations make server decisions based on the security inherent within the platform.

High performing organizations are more aware of the benefits of automation. The most important benefits are the ability to find attacks before they do damage or gain persistence (78 percent of high performers), reduction in the number of false positives that analysts must investigate (74 percent of high performers) and automation is critical when implementing an effective Zero Trust Security Model (71 percent of respondents).

High performing organizations are more likely to see the important connection between privacy and security. Ninety-four percent of respondents in high performing organizations say it is not possible to have privacy without a strong security posture. Eighty-seven percent of high performers believe a strong cybersecurity posture reduces the privacy risk to employees, business partners and customers. High performers are less likely to believe human error is a risk to privacy.

Part 2. Key findings

In this section of the report, we provide an analysis of the research findings and comparisons to the findings reported in 2020. The complete audited findings are presented in the Appendix of this report.

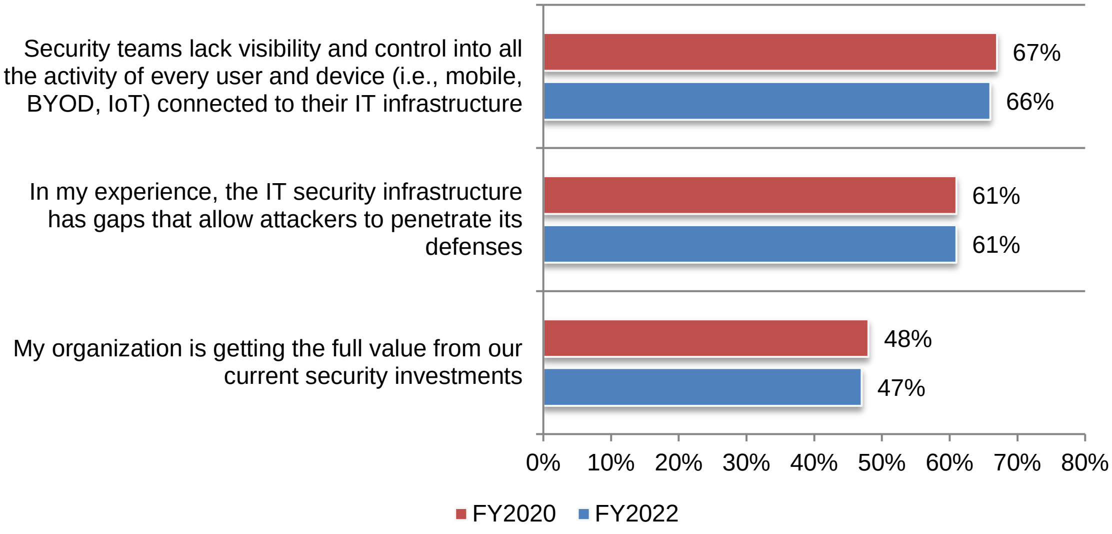
We have organized the findings according to the following topics:

- Trends in the state of the IT security gap
- A strong cybersecurity posture supports digital transformation
- Strategies to close the IT security gap
- The role of AI and automation in closing the IT security gap
- Best practices in closing the IT security gap

Trends in the state of the IT security gap

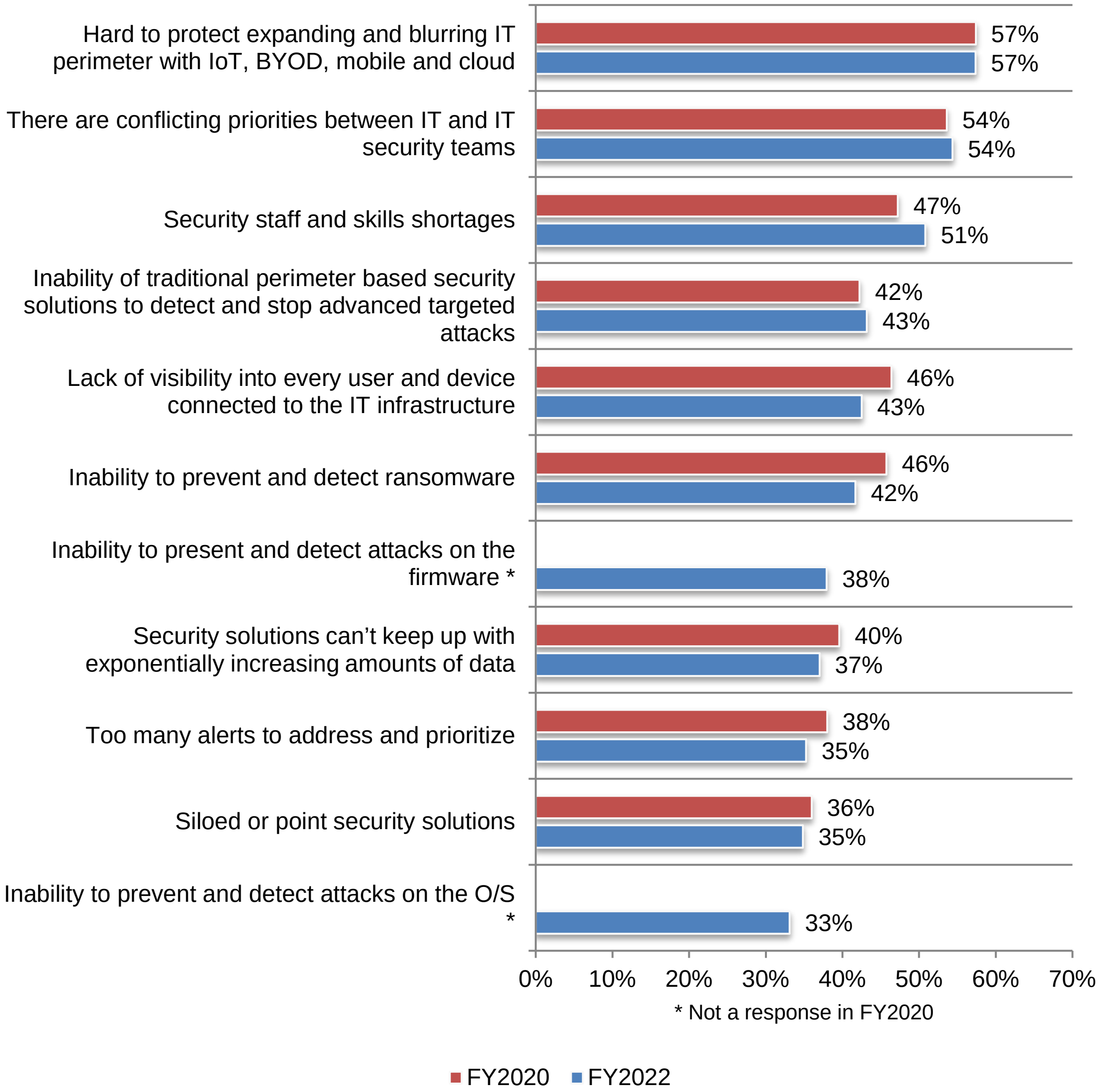
Since 2020, not much progress has been made in closing the IT security gap that allows attackers to penetrate organizations' defenses. As shown in Figure 2, the primary reason for the gap is the lack of visibility and control into all the activity of every user and device connected to their IT infrastructure (66 percent of respondents). Another reason for the IT security gap is that only 47 percent of respondents get full value from their current security investments.

Figure 2. Reasons the IT security gap exists
Strongly agree and agree responses combined



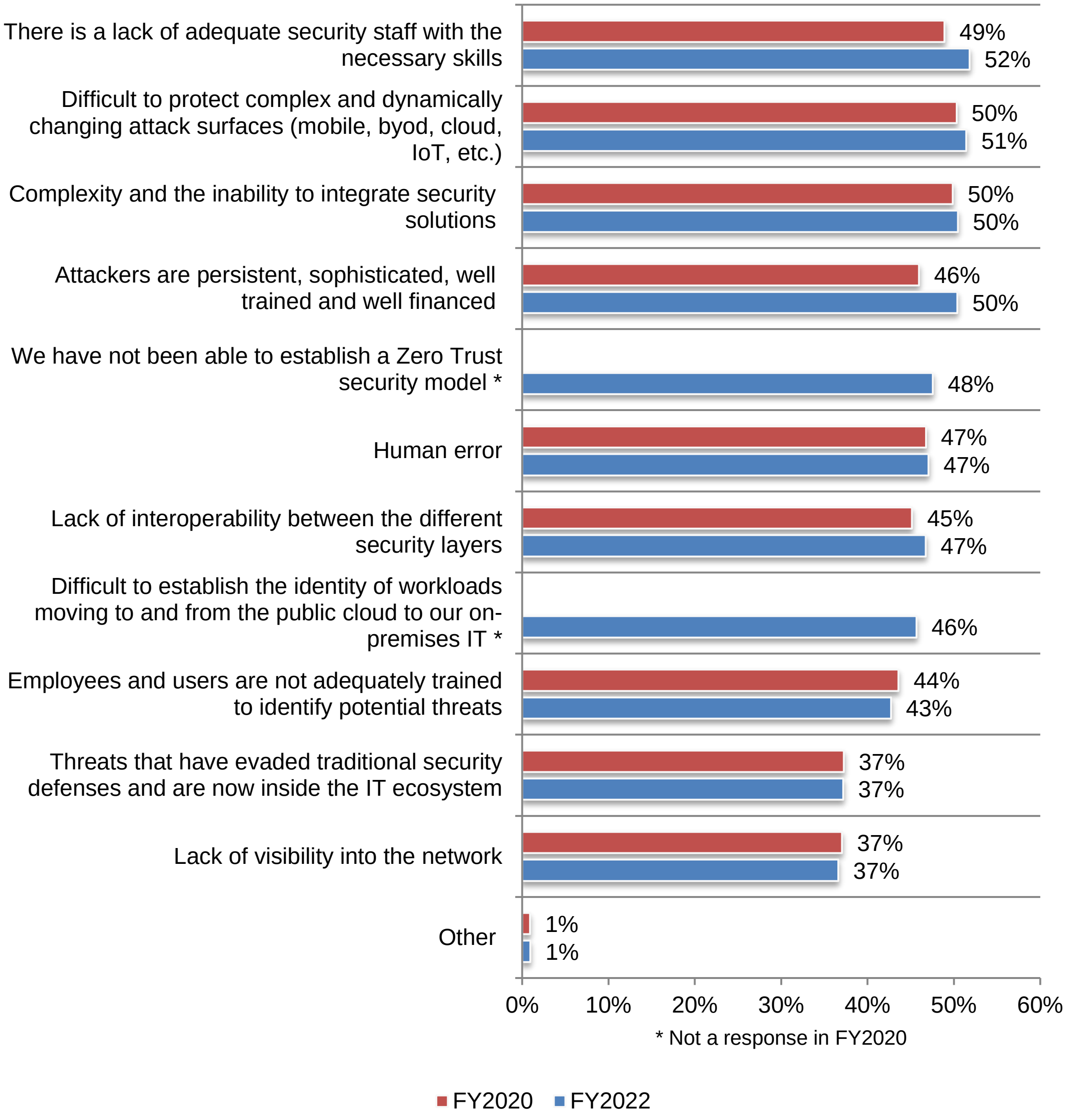
Organizations continue to find it difficult to protect the expanding and blurring IT perimeter with IoT, BYOD, mobile and cloud. According to Figure 3**,** 57 percent of respondents say the IT security gap exists because it is hard to protect the expanding and blurring IT perimeter with IoT, BYOD, mobile and cloud. Fifty-four percent of respondents say there are conflicting priorities between IT and IT security teams. New in this year's research is that 38 percent of respondents say the gap is the result of the inability to prevent and detect attacks on the firmware and 33 percent of respondents say it is the failure to prevent and detect attacks on the O/S.

Figure 3. Why there are gaps in the IT security infrastructure
More than one response permitted



Staffing issues and complexity continue to prevent the closing of the security gap and stopping data breaches. According to Figure 4, more than half (52 percent) of respondents say there is inadequate security staff with the necessary skills to prevent data breaches. This is followed by the difficulty in protecting complex and dynamically changing attack surfaces (51 percent of respondents). In this year's research, 48 percent of respondents have not been able to establish a Zero Trust Model and 46 percent of respondents say it is difficult to establish the identity of workloads moving to and from the public cloud to their on-premises IT.

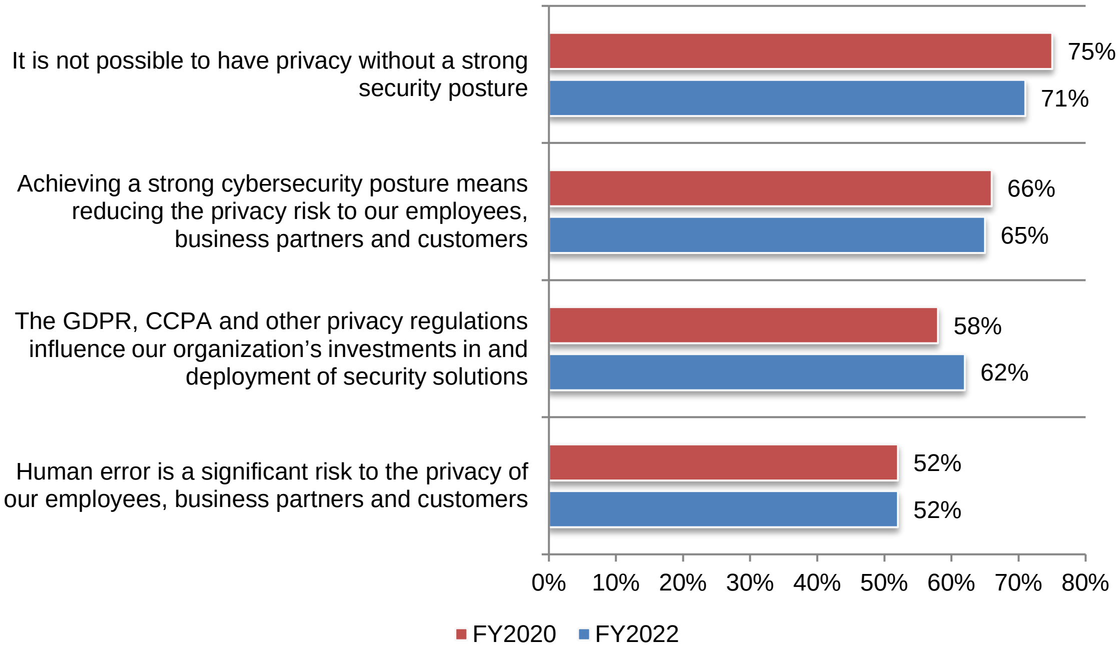
Figure 4. Why breaches are still happening
More than one response permitted



A strong cybersecurity posture supports organizations' privacy initiatives. Most organizations represented in this research (65 percent of respondents) understand the connection between having a strong cybersecurity posture and reducing the privacy risk to employees, business partners and customer, as shown in Figure 5.

Sixty-two percent of respondents say the GDPR and CCPA and other privacy regulations influence their organization's investments in and deployment of security solutions. Further, a strong cybersecurity posture makes it possible to have an effective privacy program (71 percent of respondents). However, it is difficult to minimize the privacy risks to individuals because of human error (52 percent of respondents).

Figure 5. Perceptions about the connection between privacy and cybersecurity posture
Strongly agree and Agree responses combined

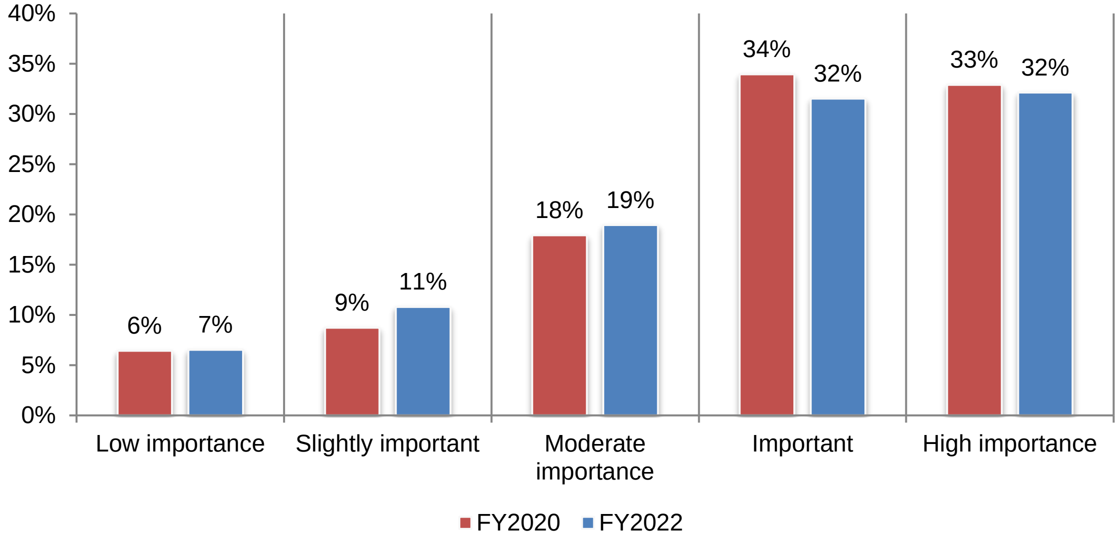


A strong cybersecurity posture supports digital transformation

Digital transformation is increasing connectivity to more users, devices and data than ever before. From an IT security perspective, it means assessing digital exposure and overall risk to the business, protecting critical assets throughout the organization (network, endpoints, servers and cloud) and conforming and complying with regulations, industry standards and security best practices.

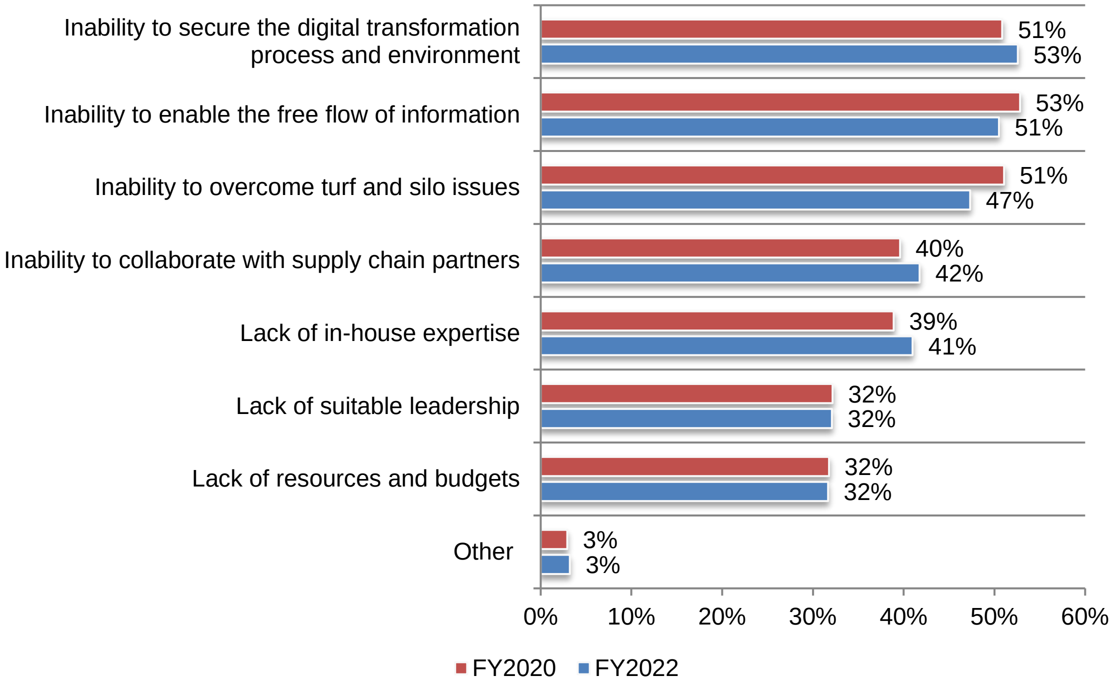
Security technologies are necessary to minimize risks during the digital transformation process. Seventy-five percent of respondents say they are involved in their organizations' digital transformation process. Of these respondents, as shown in Figure 6, 64 percent of respondents say security technologies are important and highly important (32 percent + 32 percent). This is similar to 67 percent of respondents in the 2020 study.

Figure 6. The importance of security technologies to a successful digital transformation strategy



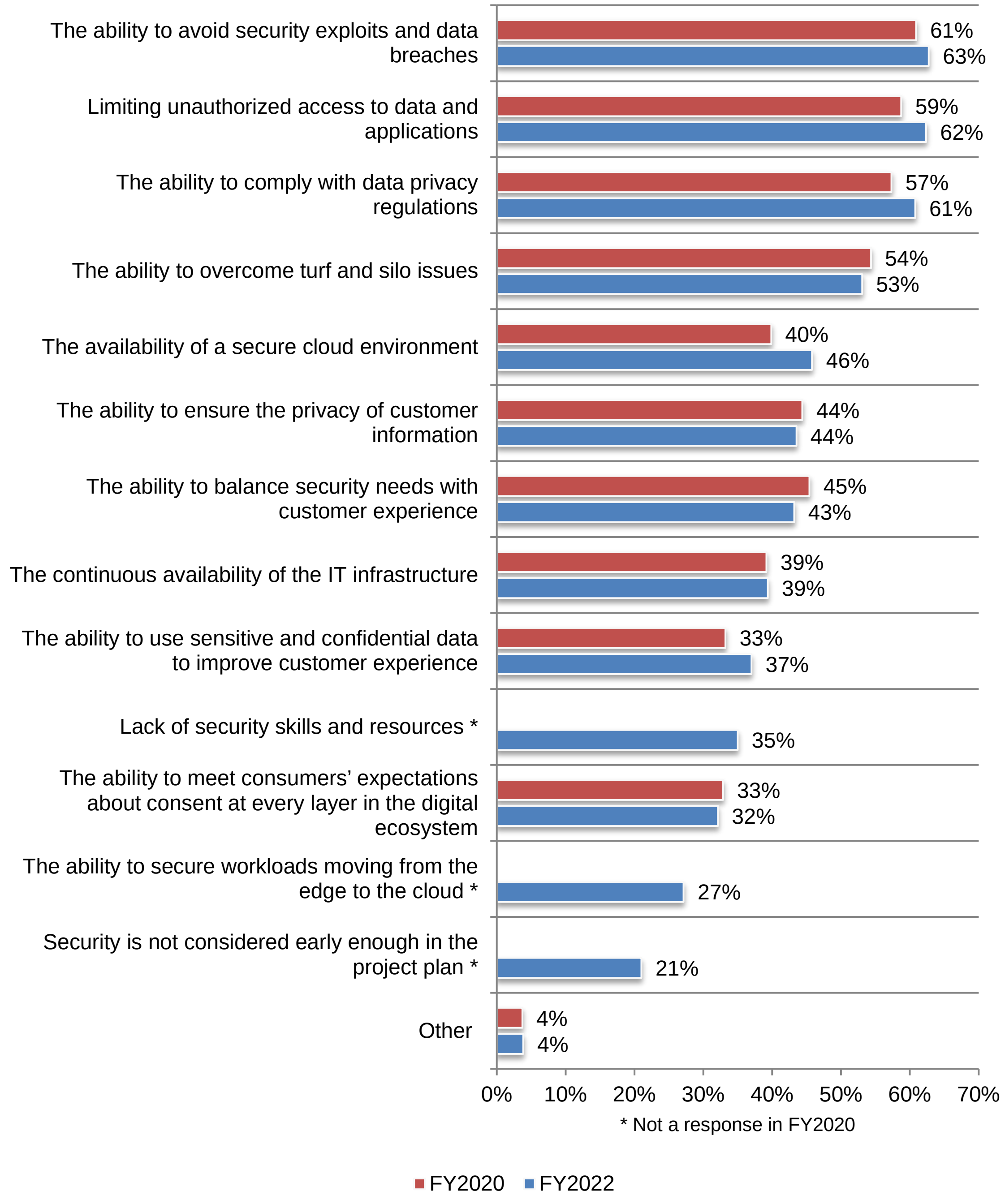
Most respondents are concerned about the ability to secure the digital transformation process and environment. Figure 7 lists the most significant barriers to having a successful digital transformation process. The inability to secure the digital transformation process and environment and the inability to enable the free flow of information are the most significant barriers, according to 53 percent and 51 percent of respondents, respectively.

Figure 7. The most significant barriers to having a successful digital transformation process
More than one response permitted



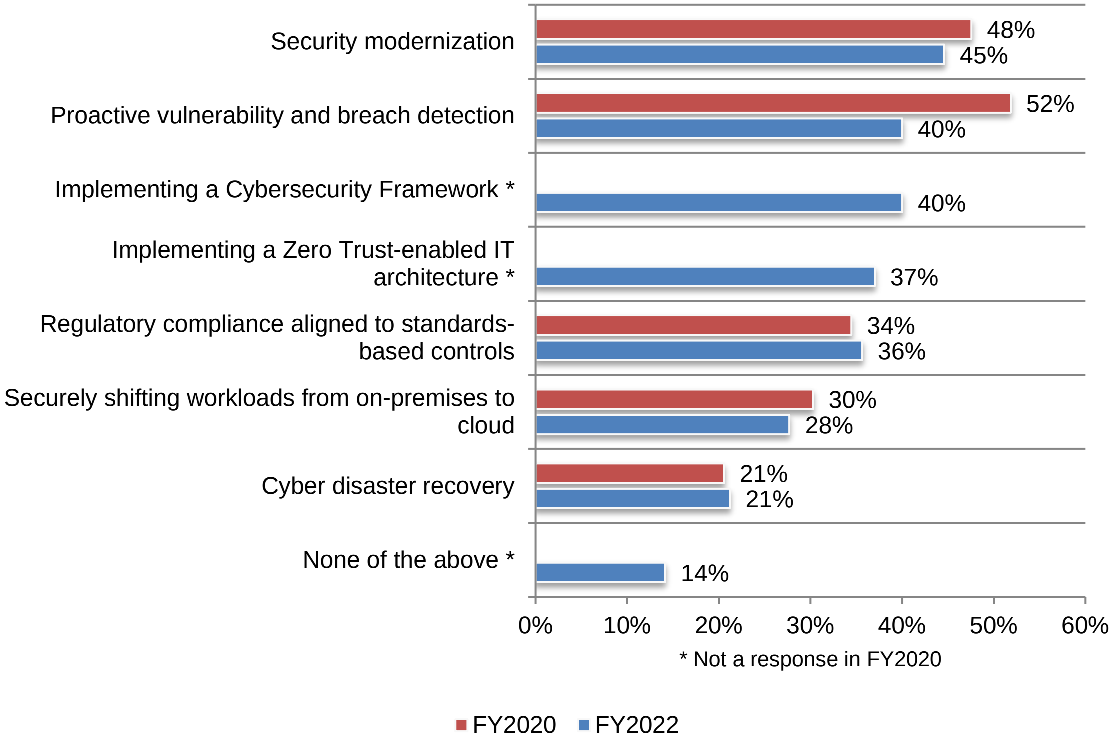
Organizations must ensure a secure digital transformation process to close the IT security gap. As discussed previously, the lack of visibility into end-users' activities is the number one barrier to closing the IT security gap. As a result, 63 percent of respondents say their organizations are challenged to avoid security exploits and data breaches followed by limiting unauthorized access to data and applications (62 percent of respondents).

Figure 8. The most significant challenges to achieving a secure digital transformation process in their organizations
More than one response permitted



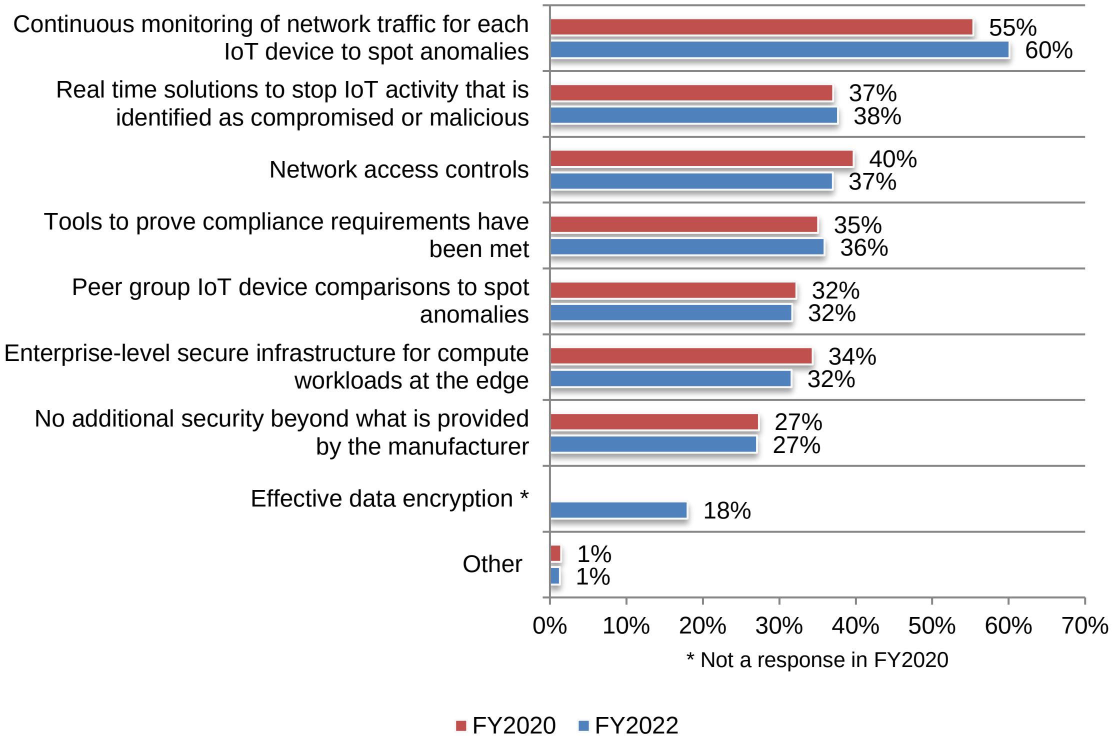
Proactive vulnerability and breach detection has declined as a priority in minimizing the risk of digital transformation. As shown in Figure 9, only 40 percent of respondents say their organizations prioritize proactive vulnerability and breach detection, a decline from 52 percent of respondents in 2020. Security modernization continues to be the top priority (45 percent of respondents). In this year's research, organizations made implementing a cybersecurity framework (40 percent of respondents) and implementing a Zero Trust-enabled IT architecture (37 percent of respondents) a priority.

Figure 9. Processes prioritized to minimize the risk of digital transformation
More than one response permitted



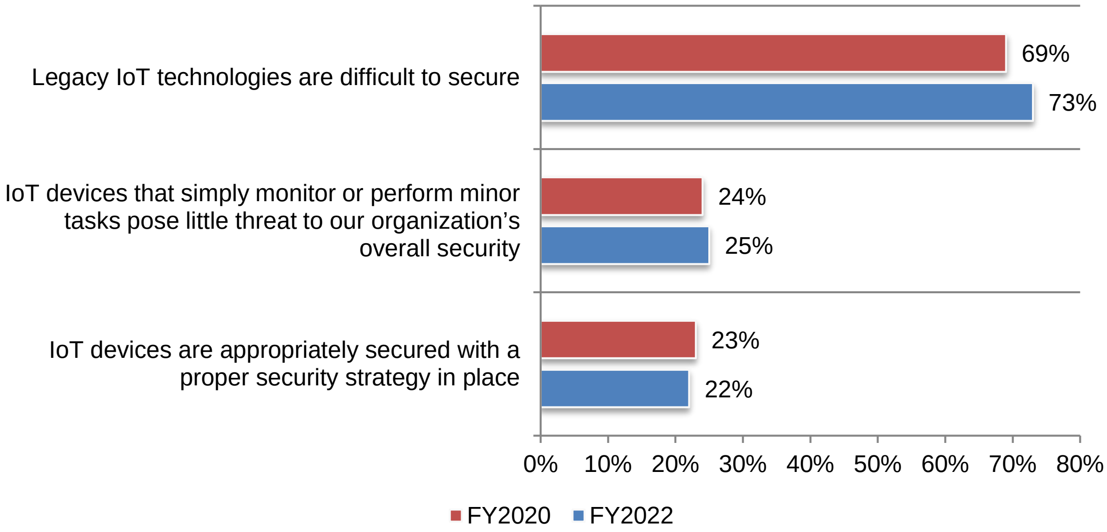
Continuous monitoring of IoT devices to spot anomalies has become more critical. Only 9 percent of respondents say their organizations have a high ability to secure IoT devices and apps. To secure their IoT devices, 60 percent of respondents believe their organizations need to conduct continuous monitoring of network traffic for each IoT device to spot anomalies. This is followed by real time solutions to stop IoT activity that is identified as compromised or malicious (38 percent of respondents).

Figure 10. What is required to achieve a high level of IoT security?
More than one response permitted



Organizations are not making progress in securing legacy technologies. As shown in Figure 11, 73 percent of respondents say legacy IoT technologies are difficult to secure. As in last year's research, most respondents **do not** believe that IoT devices that simply monitor or perform minor tasks pose little threat to their organization's overall security posture. Only 22 percent of respondents believe IoT devices are appropriately secured with a proper security strategy in place.

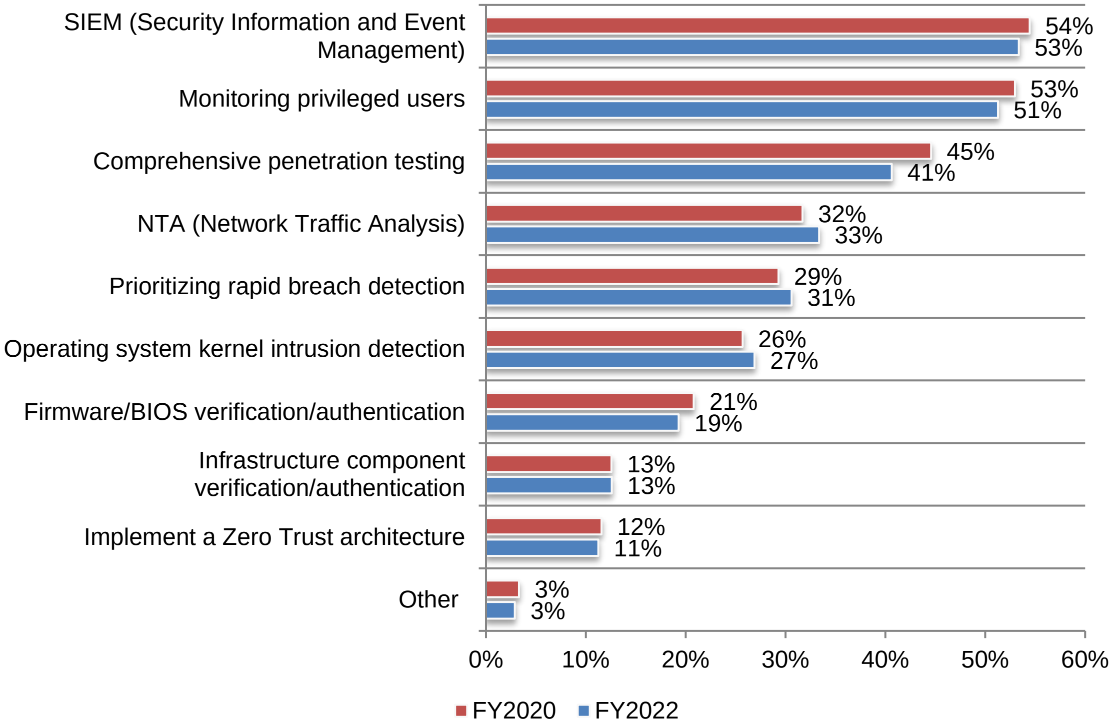
Figure 11. Perceptions about IoT security risks
Strongly agree and Agree responses combined



Strategies to close the IT security gap

SIEM and monitoring privileged users are most often used to minimize hidden threats. Figure 12 presents a list of steps that could be taken to minimize stealthy and hidden threats within the IT infrastructure. Fifty-three percent of respondents say their organizations use SIEM and 51 percent of respondents say they are monitoring privileged users.

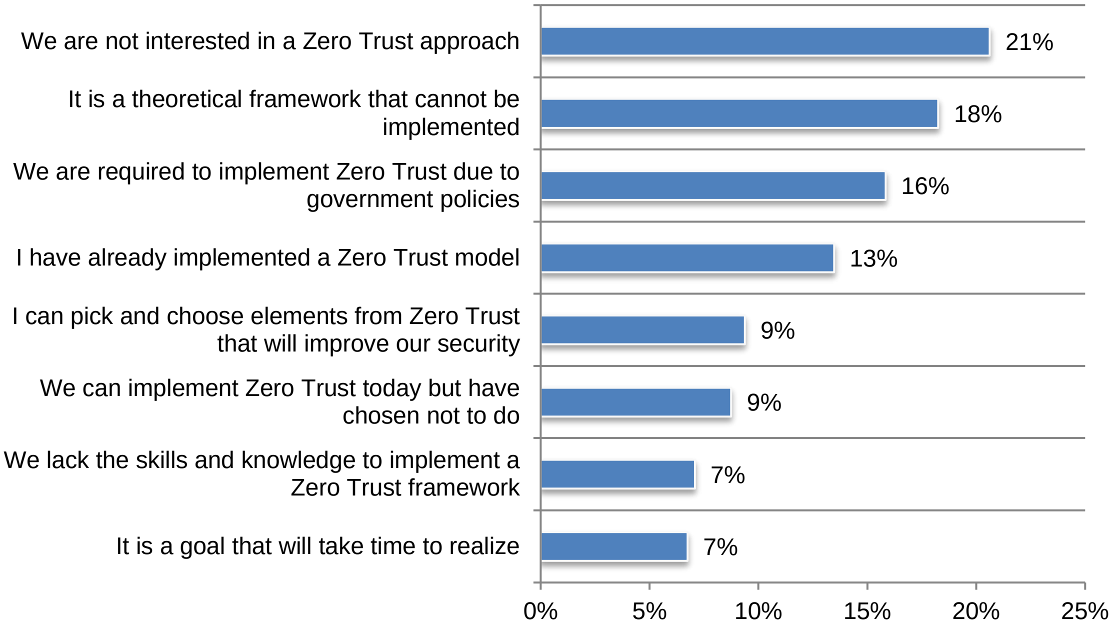
Figure 12. What steps should be taken to minimize stealthy, hidden threats within the IT infrastructure?
More than one response permitted



Organizations are slow to adopt a Zero-Trust Security Model. Zero Trust is a security concept centered on the belief that organizations should not automatically trust anything inside or outside its perimeters and instead must verify anything and everything trying to connect to their systems before granting access.

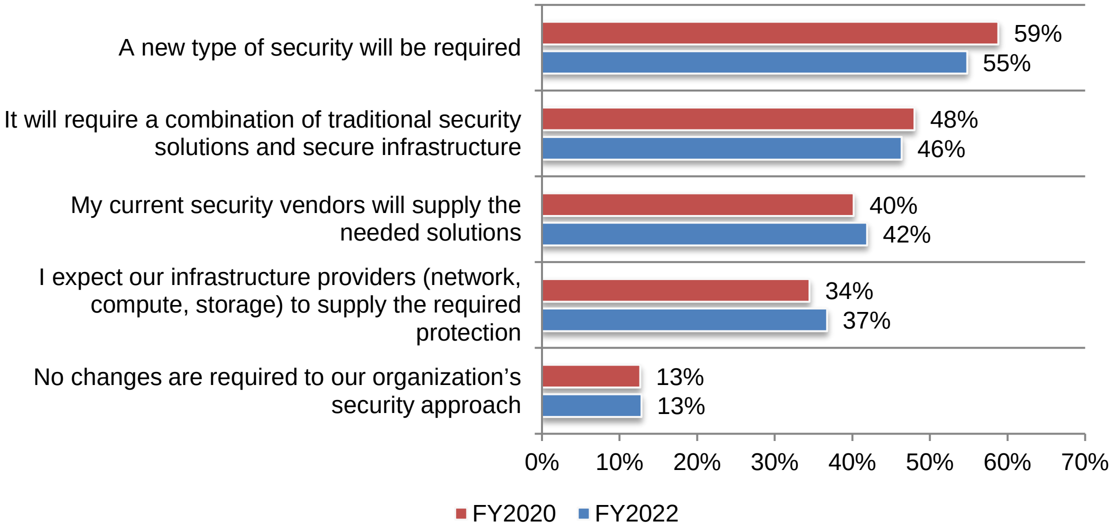
According to Figure 13, 38 percent of respondents have implemented a Zero-Trust Model because of government policies (16 percent), have already implemented a Zero-Trust Model (13 percent) and 9 percent of respondents say their organizations have selected elements from Zero Trust that will improve security. Another 39 percent of respondents say their organizations are not interested in a Zero Trust approach (21 percent) or it is a theoretical framework that cannot be implemented (18 percent).

Figure 13. What one statement best describes your organization's approach to a Zero Trust Security Model?



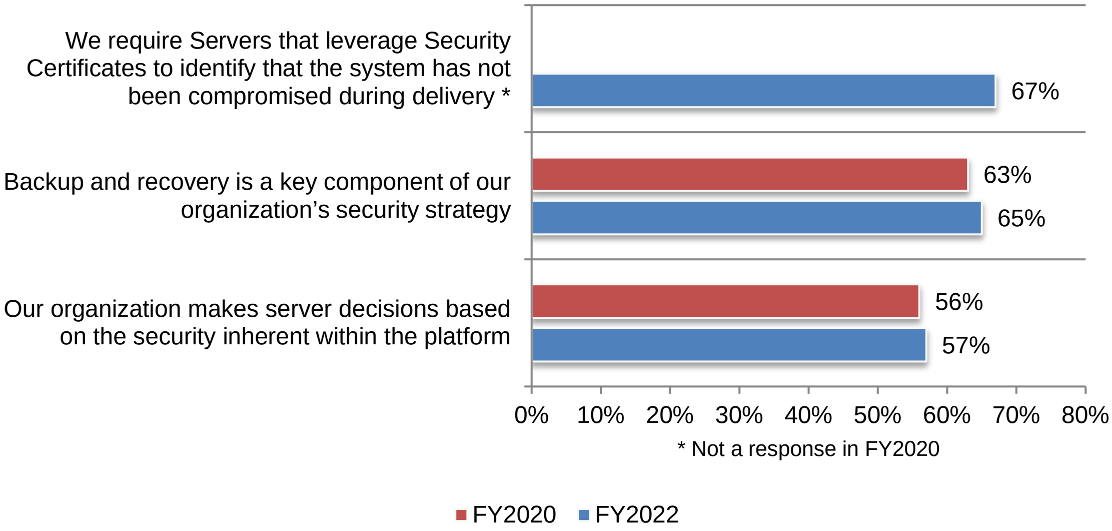
New security solutions are needed when compute and storage moves from the data center to the edge. According to Figure 14, 55 percent of respondents believe new security solutions are needed when compute and storage move from the data center to the edge. Forty-six percent of respondents say it requires a combination of traditional security solutions and secure infrastructure. Only 13 percent of respondents say no changes to their organizations' security approach are needed.

Figure 14. How will your organization implement the required security when compute and storage move from the data center to the edge?
More than one response permitted



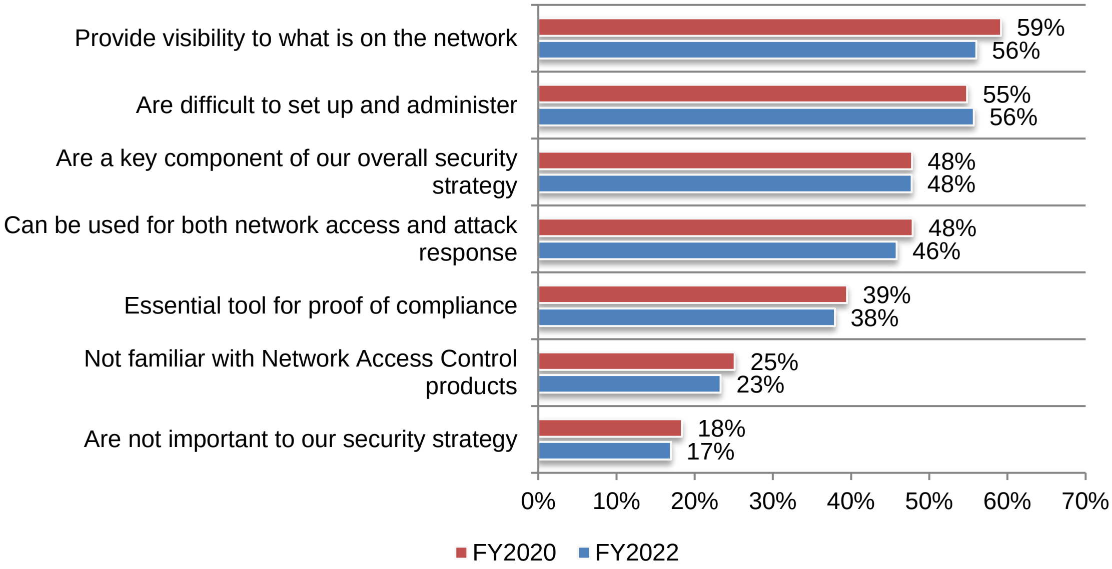
Organizations are requiring servers that leverage security certificates to identify that the system has not been compromised during delivery, as shown in Figure 15. Sixty-five percent of respondents say backup and recovery is a key component of their organizations' security strategy. Fifty-seven percent of respondents say the security inherent within the platform influences decisions about servers.

Figure 15. Perceptions about backup and recovery
Strongly agree and Agree responses combined



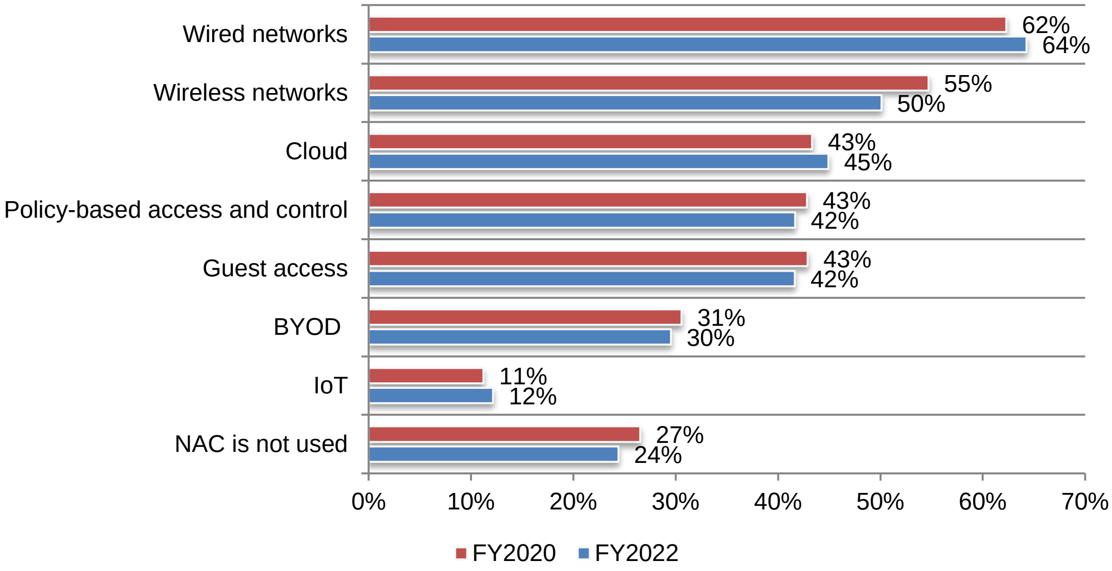
Network Access Control (NAC) improves visibility to what is on the network. Seventy-six percent of respondents say their organizations use NAC products. As discussed throughout the report, a lack of visibility impedes the ability to close the IT security gap. According to Figure 16, 56 percent of respondents say their organizations' NAC products improve visibility to what is on the network and 48 percent of respondents say they are a key component of their overall security strategy. However, 56 percent of respondents say they are difficult to set up and administer.

Figure 16. What statements best describe your opinion about NAC products deployed by your organization?
More than one response permitted



The top two purposes for their NAC systems are wired networks (64 percent of respondents) and wireless networks (50 percent of respondents).

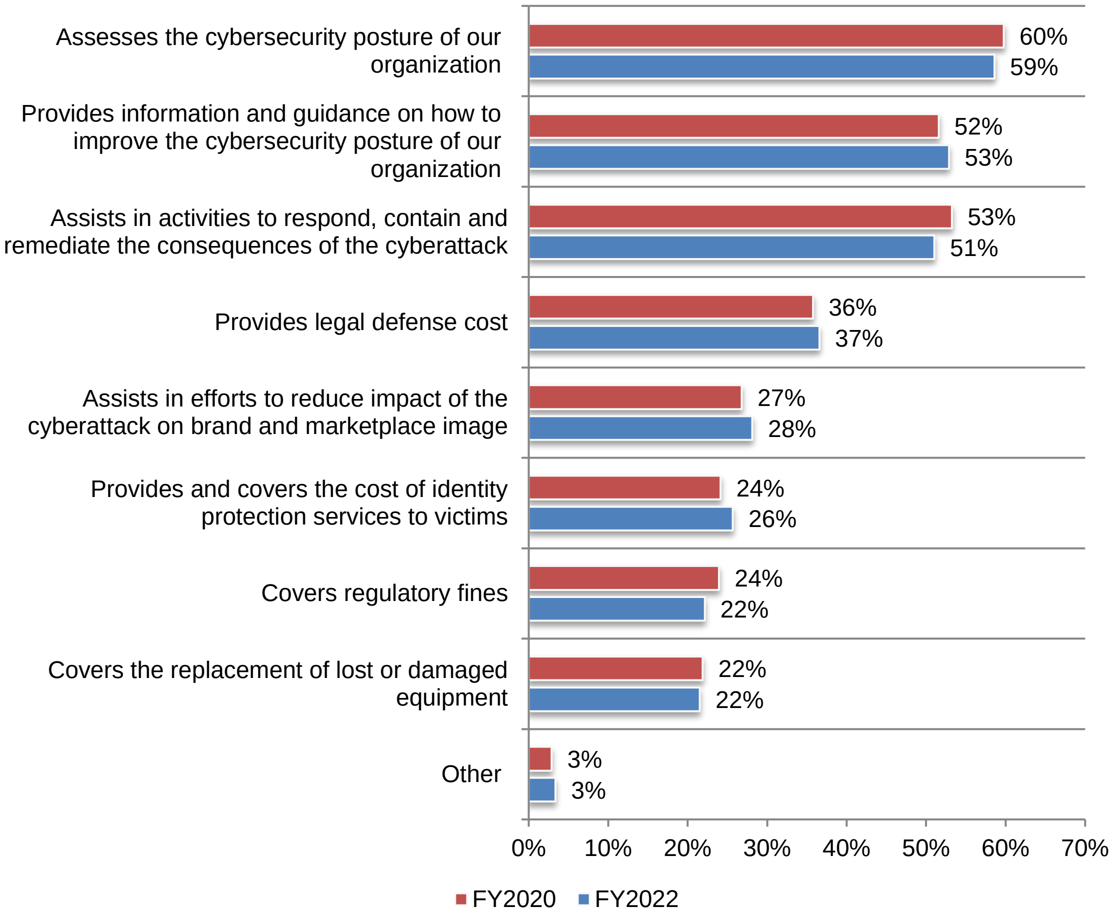
Figure 17. For what purposes are NAC systems deployed within your organization?
More than one response permitted



Cyber insurance is considered to improve an organization's cybersecurity posture. Eighty-one percent of respondents say their organization has a cyber insurance policy currently or will purchase a policy in the next six or 12 months. Seventy-one percent of respondents say cyber insurance is important or very important to their organizations' overall cybersecurity posture.

According to Figure 18, respondents believe the primary benefit of cyber insurance is to improve their organizations' cybersecurity posture. Specifically, it assesses the organization's cybersecurity posture, provides information and guidance on how to improve it and assists in activities to respond, contain and remediate the consequences of a cyberattack (59 percent, 53 percent and 51 percent of respondents, respectively).

Figure 18. Why is cyber insurance important?
Three responses permitted

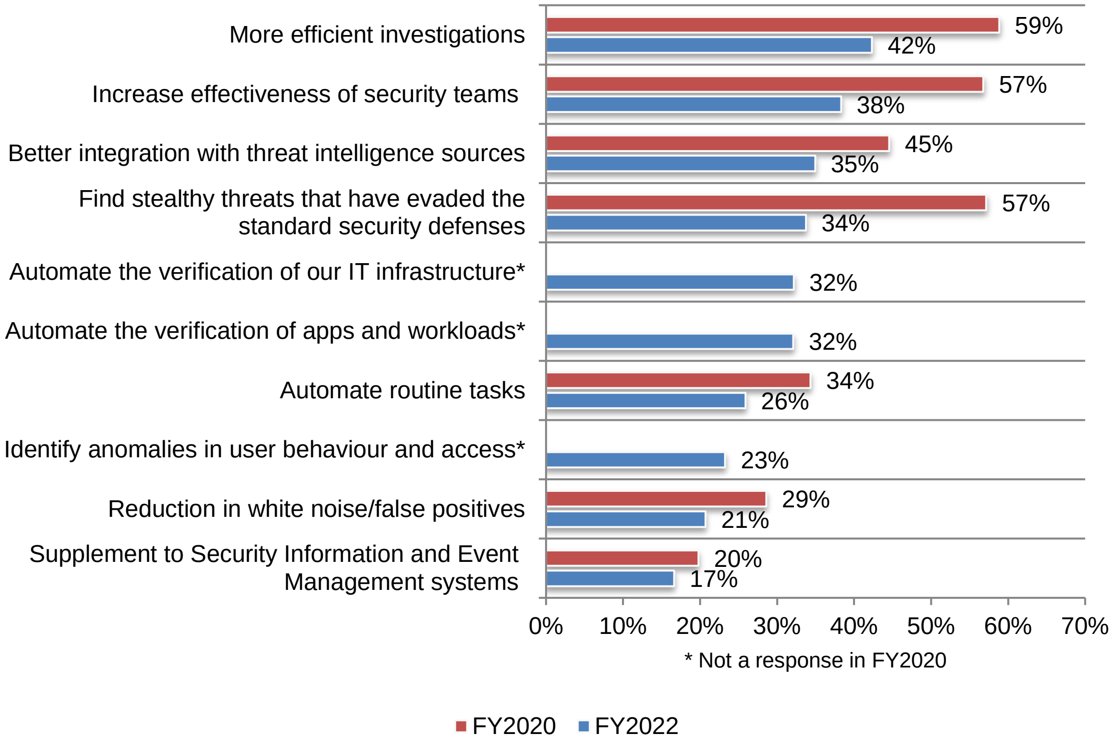


The role of artificial intelligence (AI) and automation in closing the IT security gap

AI finds stealthy threats and makes security teams more effective and efficient. Fifty-two percent of respondents say AI technologies (machine learning and behavioral analytics) are essential to detecting attacks on the inside before they do damage.

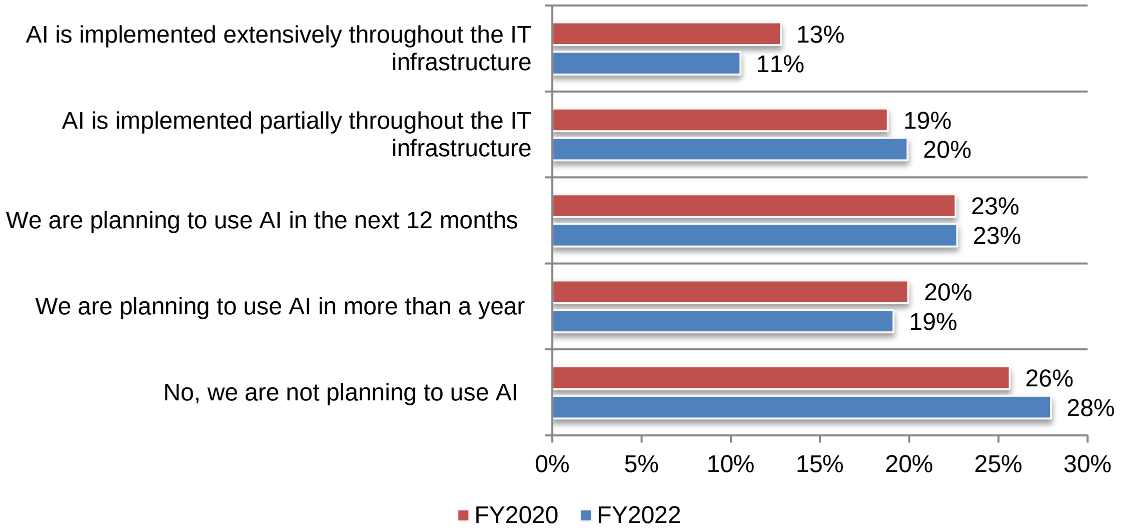
As shown in Figure 19, the top three benefits of AI are more efficient investigations (42 percent of respondents), more effective security teams (38 percent of respondents) and better integration with threat intelligence sources (35 percent of respondents). In this year's research, approximately one-third of respondents say AI and advanced analytics automate the verification of their IT infrastructure, apps and workloads.

Figure 19. What are the top three key security benefits of using AI and advanced analytics?
Three responses permitted



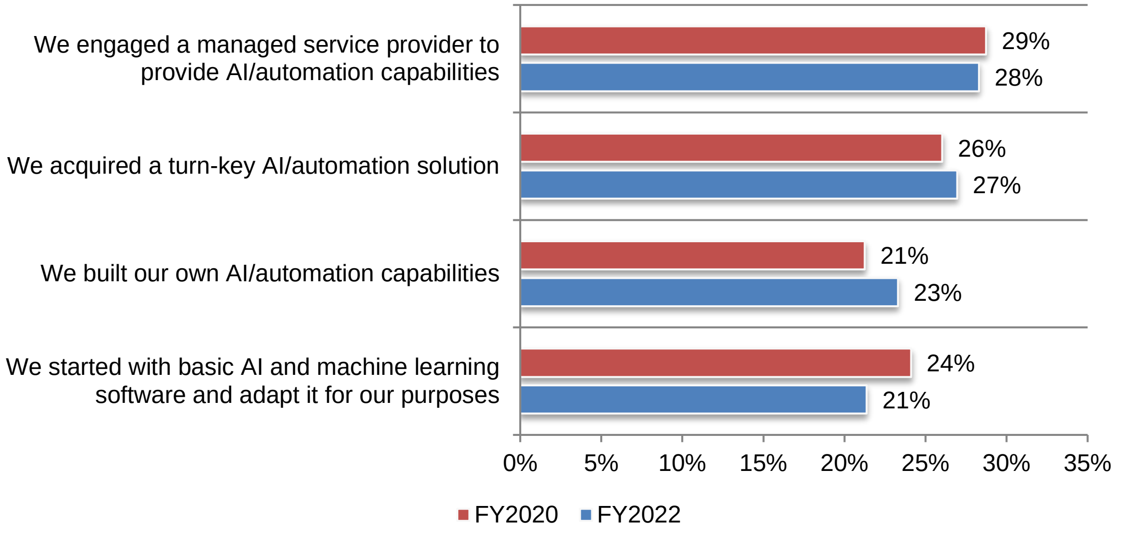
The use of AI has not grown since the last research. As shown in Figure 20, 31 percent of respondents say AI is implemented extensively (11 percent) or partially (20 percent). In last year's research, 32 percent of respondents said AI is implemented extensively (13 percent) or partially (20 percent).

Figure 20. What best describes the use of AI for security purposes within your organization?



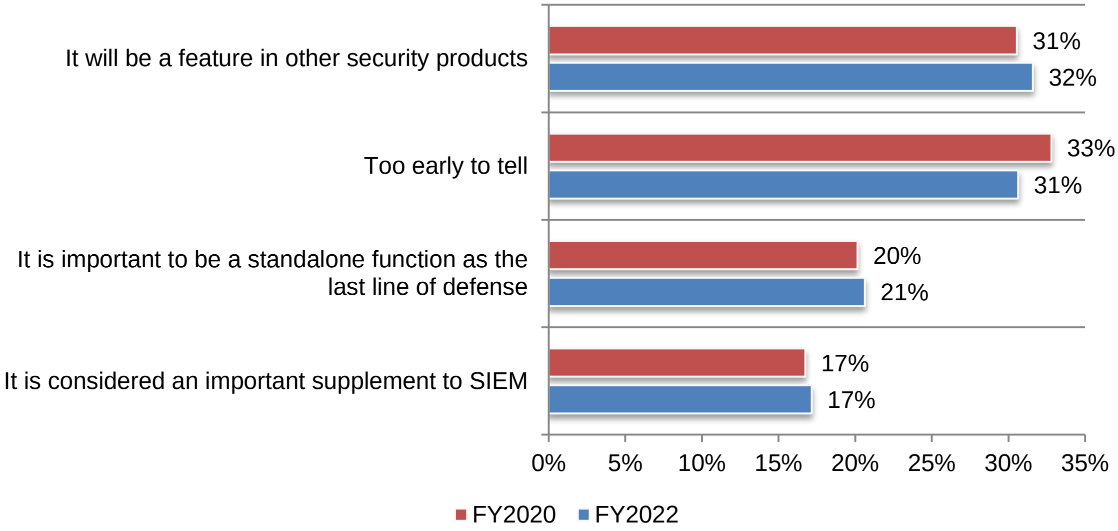
Of those respondents who say AI is implemented extensively (11 percent) or partially (20 percent), most engaged a managed service provider to provide AI/automation capabilities (28 percent of respondents) as shown in Figure 21. This is followed by the acquisition of a turn-key AI/automation solution (27 percent of respondents).

Figure 21. What best describes how machine learning is deployed for attack detection?



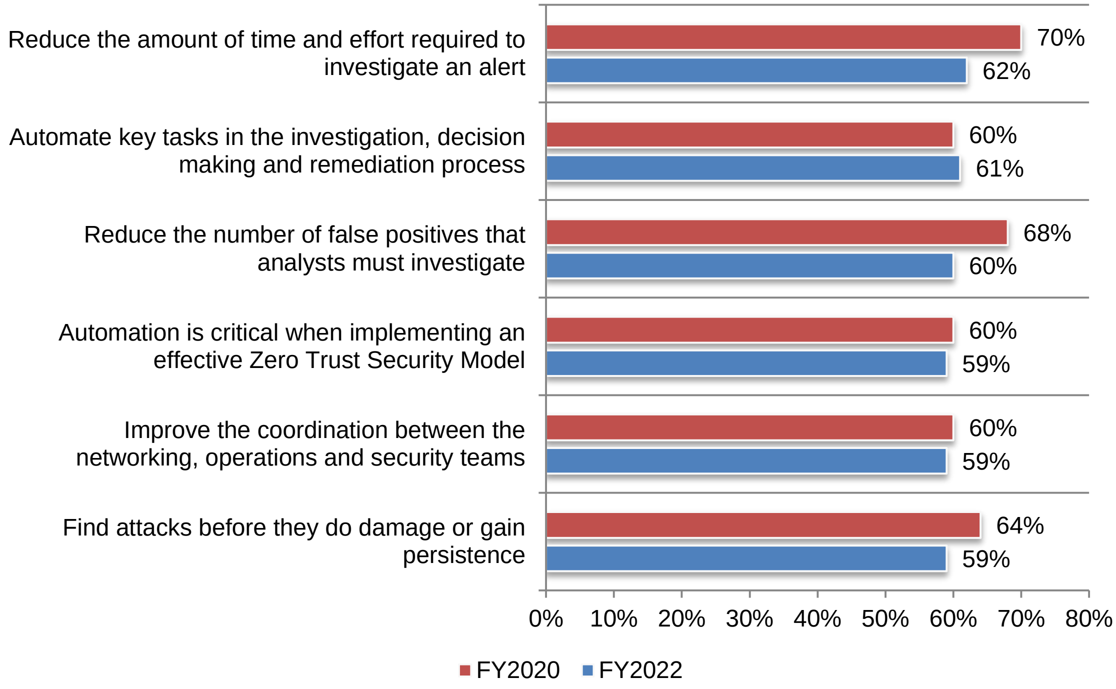
Most respondents are positive about the deployment of AI/machine learning. As shown in Figure 22, 32 percent of respondents say it should be a feature in other security products, 21 percent say it should be a standalone function as the last line of defense and 17 percent of respondents say it should be an important supplement to SIEM. Less than one-third (31 percent) of respondents say it is too early to tell how the market considers AI/machine learning attack detection.

Figure 22. What best describes how the market considers AI/machine learning attack detection?



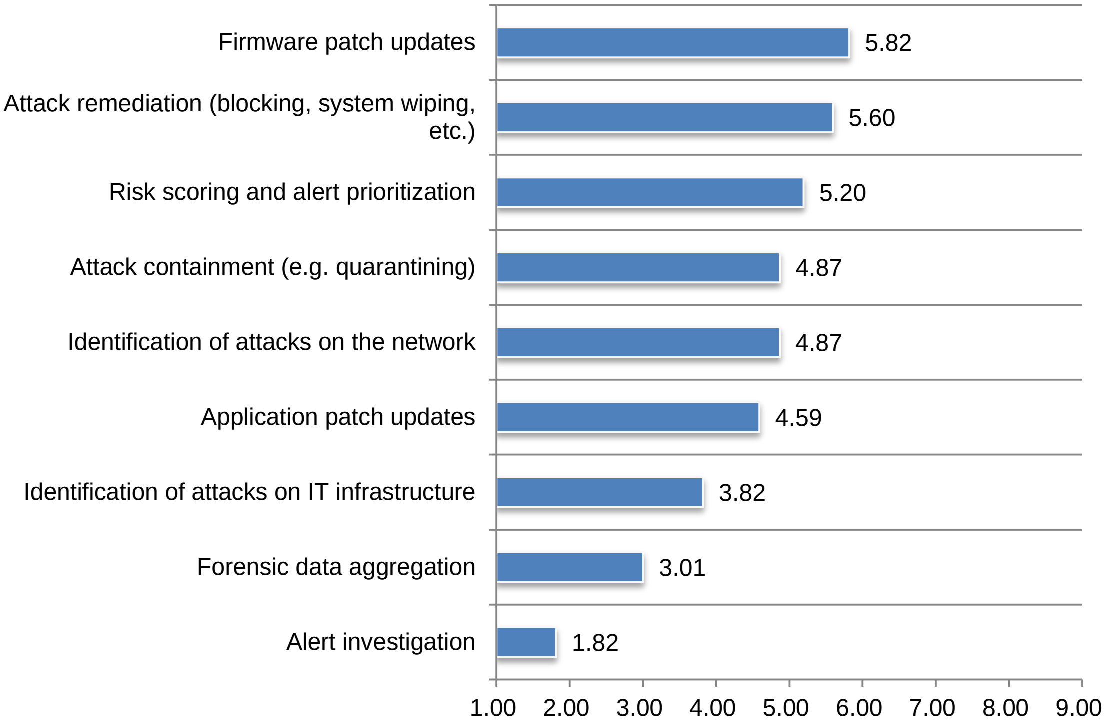
According to Figure 23, for a variety of reasons, most organizations believe automation is important for creating a more efficient and effective security posture. The most important features are the ability to reduce the amount of time and effort required to investigate an alert (62 percent of respondents), automation of key tasks in the investigation process (61 percent of respondents) and a reduction in the number of false positives that analysts must investigate (60 percent of respondents).

Figure 23. The importance of the benefits of automation in achieving a more efficient and effective security posture
High importance and Important responses combined



Respondents were asked to rate the processes most likely to be automated on a scale of 1 = least likely to 9 = most likely. Figure 24 presents the respondents' average ranking of these processes. Firmware patch updates, attack remediation, risk scoring and alert prioritization, attack containment and identification of attacks on the network are the most likely to be automated.

Figure 24. Which processes are most likely to be automated by your organization?
Ranked from 1 = least likely to 9 = most likely



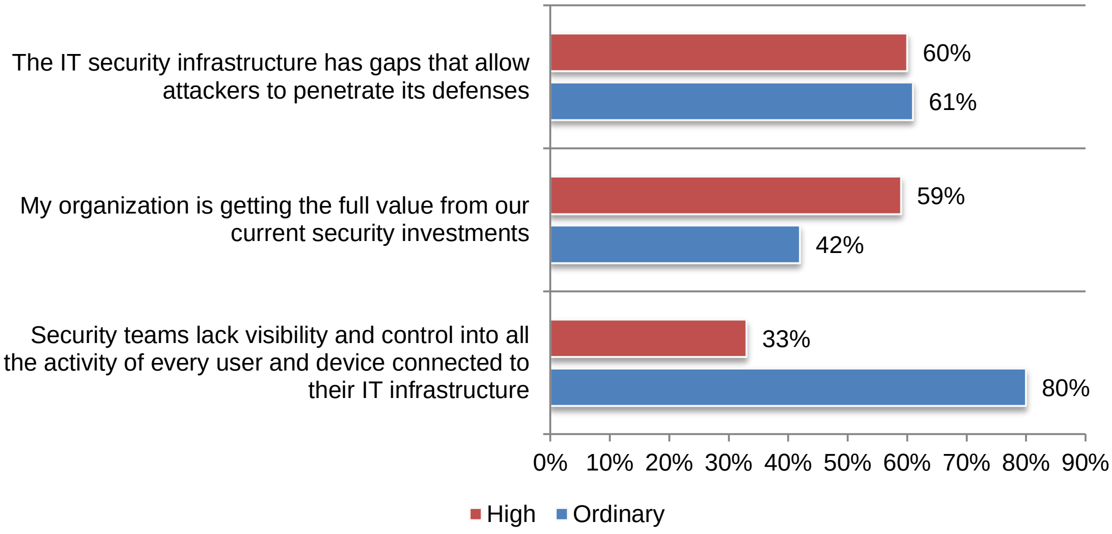
Best practices in closing the IT security gap

Thirty percent of respondents self-reported their organizations are highly effective in keeping up with a constantly changing threat landscape and close its organization's IT security gap (9+ responses on a scale of 1 = not effective to 10 = 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 70 percent of respondents in the other organizations represented in this research.

High performers are more confident that their security team has visibility and control into users' activities. As shown in Figure 25, only 33 percent of high performers believe their security teams **lack visibility and control** into all activity of every user and device connected to their IT infrastructure. In contrast, 80 percent of those in the other category have difficulty closing their IT security gap because of the lack of visibility and control.

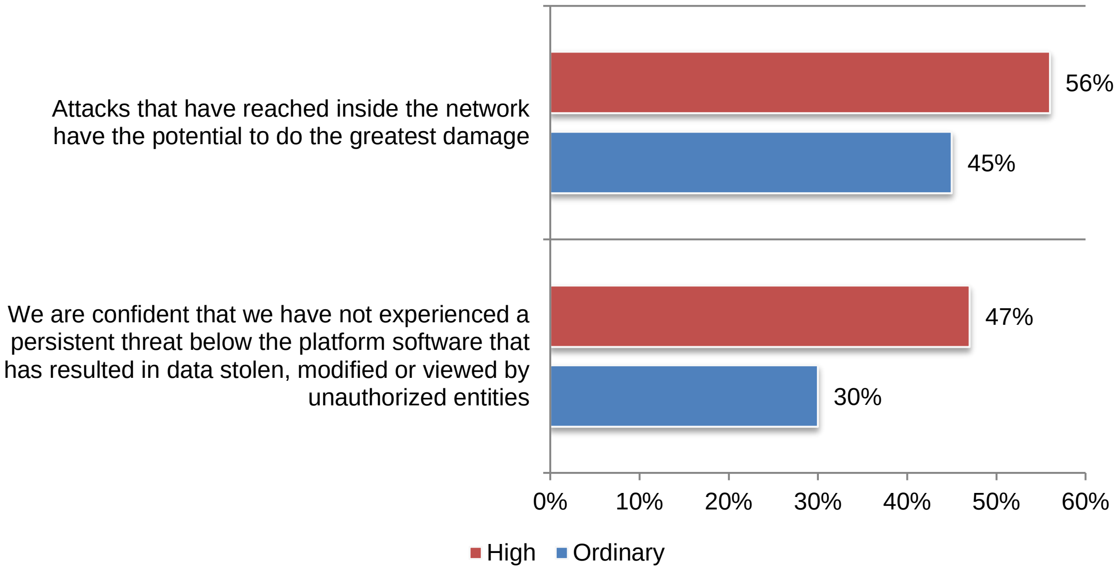
High performers are also more likely to get value from their security investments (59 percent vs. 42 percent of respondents). Sixty percent of high performers say the IT infrastructure has gaps that allow attackers to penetrate its defenses vs. 61 percent of those respondents in the other category.

Figure 25. Difference in perceptions about the IT security gap
Strongly agree and Agree responses combined



High performers are more likely to agree that attacks that have reached inside the network have the potential to do the greatest damage. As shown in Figure 26, 56 percent of high performers recognize the threat of attacks that have reached inside the network vs. 45 percent of respondents in the other category. Forty-seven percent of high performers are confident that their organization has not experienced a persistent threat below the platform software that has resulted in data stolen, modified or viewed by unauthorized entities vs. 30 percent in the other sample.

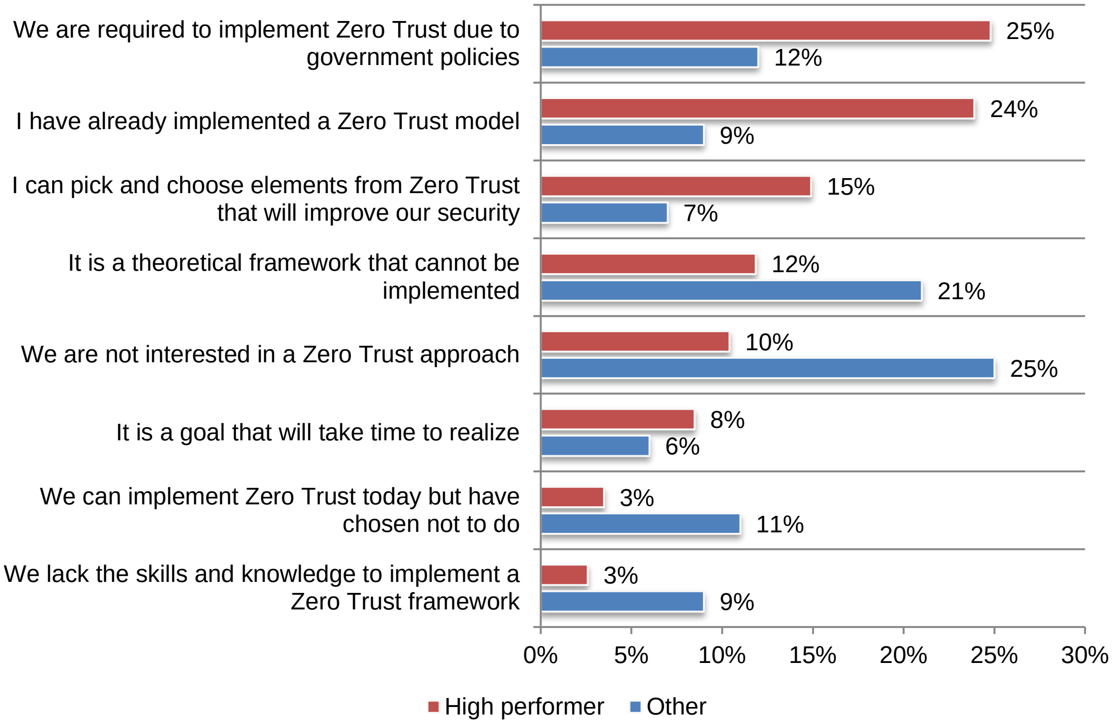
Figure 26. Perceptions about cyberattacks
Strongly agree and Agree responses combined



As discussed previously, Zero Trust is a security concept centered on the belief that organizations should not automatically trust anything inside or outside its perimeters and instead must verify anything and everything trying to connect to their systems before granting access.

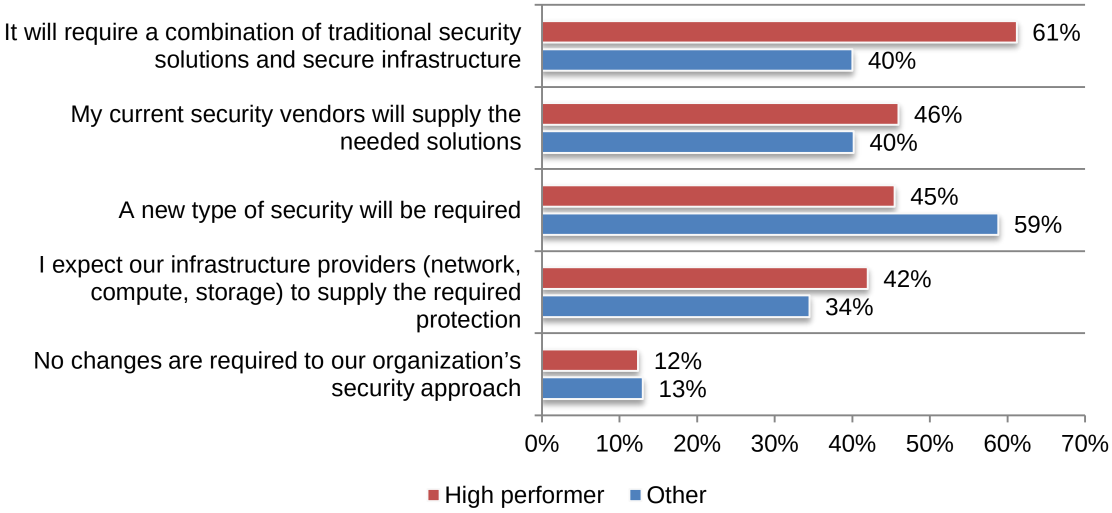
High performing organizations are more likely to implement a Zero Trust Model. According to Figure 27, 64 percent of high performing respondents have implemented a Zero Trust Model because government policies required it (25 percent), have already implemented Zero Trust (24 percent of respondents) or have selected elements from the Zero Trust framework to improve security (15 percent). Thirty-six percent of organizations in the other category are not interested in a Zero Trust approach (25 percent of respondents) or have chosen not to implement (11 percent of respondents).

Figure 27. Organizations' approach to a Zero Trust security Model



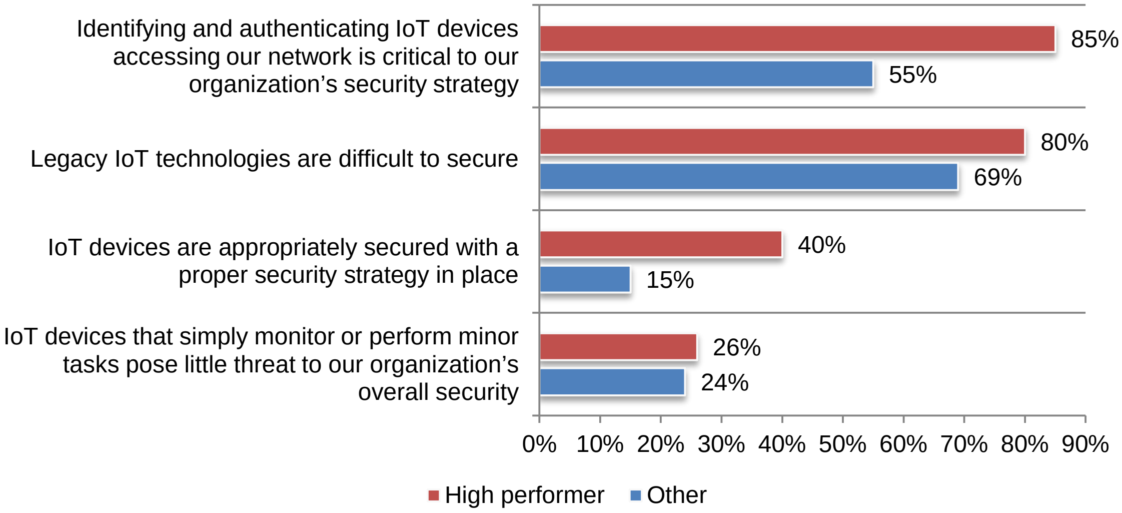
High performers are far more likely to say the move from the data center to the edge requires a combination of traditional security solutions and secure infrastructure. As shown in Figure 28, while 61 percent of high performer respondents say as compute and storage moves from the data center to the edge, a combination of traditional security solutions and secure infrastructure will be required. The respondents in the other category are more likely to say a new type of security will be required (59 percent of respondents).

Figure 28. As compute and storage moves from the data center to the edge, how will your organization implement the required security?
More than one choice permitted



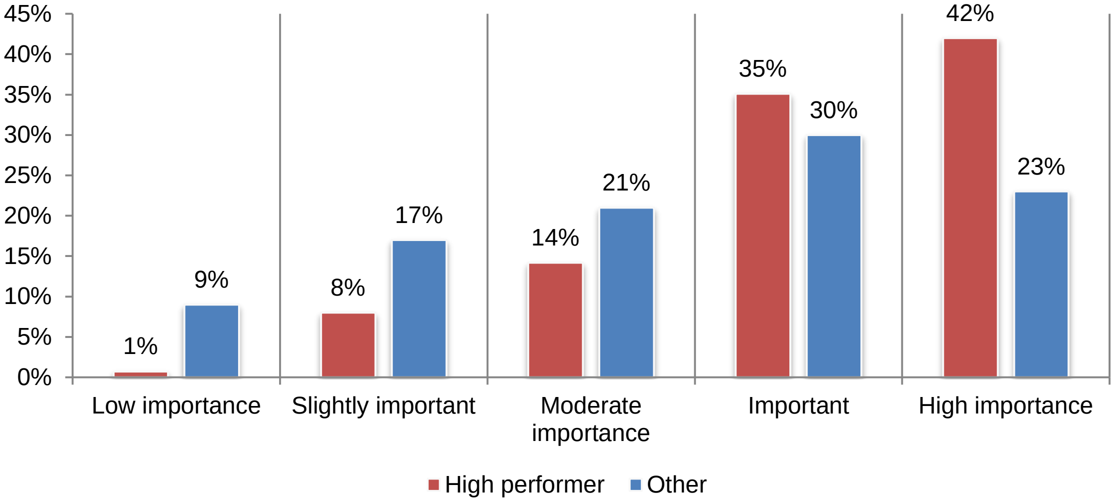
IoT security is more of a concern for high performers. As shown in Figure 29, 85 percent of respondents say identifying and authenticating IoT devices accessing their network is critical to their organization's security strategy. Only slightly more than half (55 percent) of other respondents agree with this. In addition, high performers are more likely to say legacy IoT technologies are difficult to secure (80 percent vs. 69 percent of respondents in the other sample). Forty percent of high performer respondents say their IoT devices are appropriately secured with a proper security strategy in place vs.15 percent of respondents in the other sample.

Figure 29. Perceptions about IoT security
Strongly agree and Agree responses combined



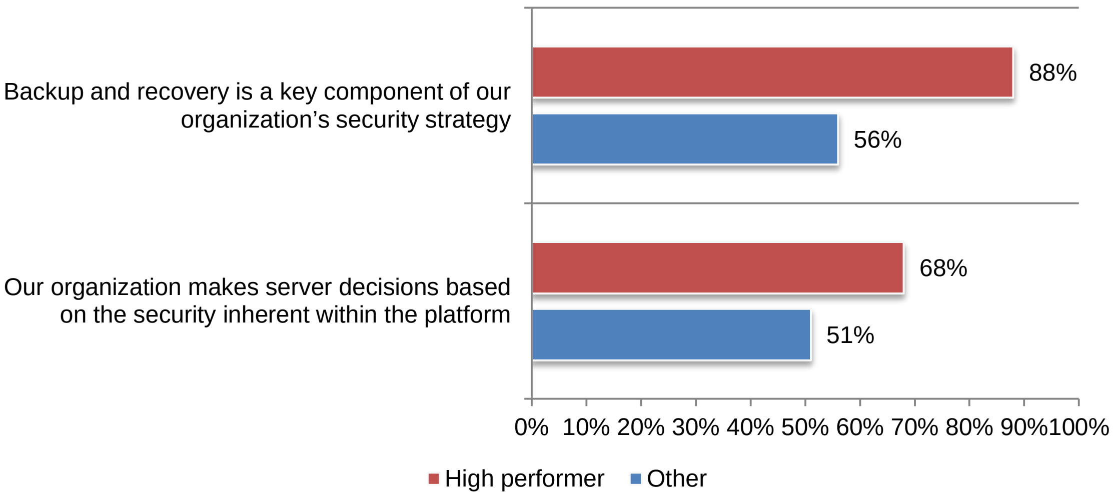
High performing organizations say security technologies are very important for their digital transformation strategy. According to Figure 30, 77 percent of high performing organizations say it is important (35 percent of respondents) or highly important (42 percent of respondents) to have security technologies to support digital transformation. In contrast, 53 percent of respondents in the other category say it is important or very important.

Figure 30. The importance of security technologies to a successful digital transformation strategy
Scale is 1 = low importance to 5 = high importance



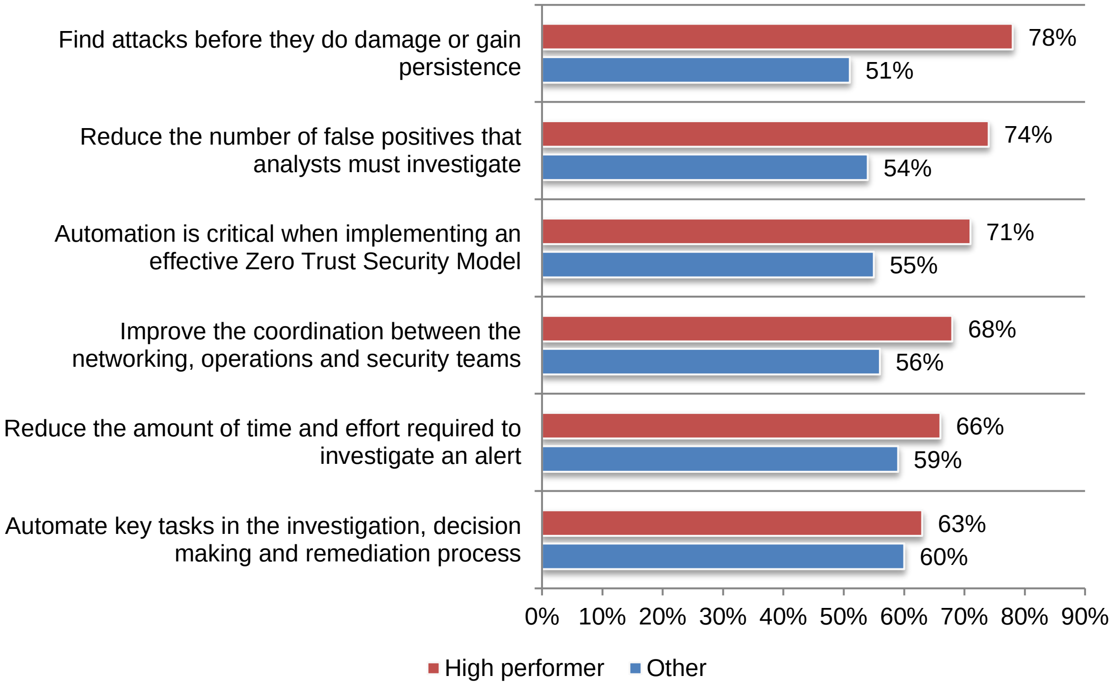
High performers take a different approach to server security and backup and recovery. As shown in Figure 31, 88 percent of high performer respondents say backup and recovery is a key component of their security strategy and 68 percent of high performers say their organizations make server decisions based on the security inherent within the platform.

Figure 31. Perceptions about server security and backup and recovery
Strongly agree and Agree responses combined



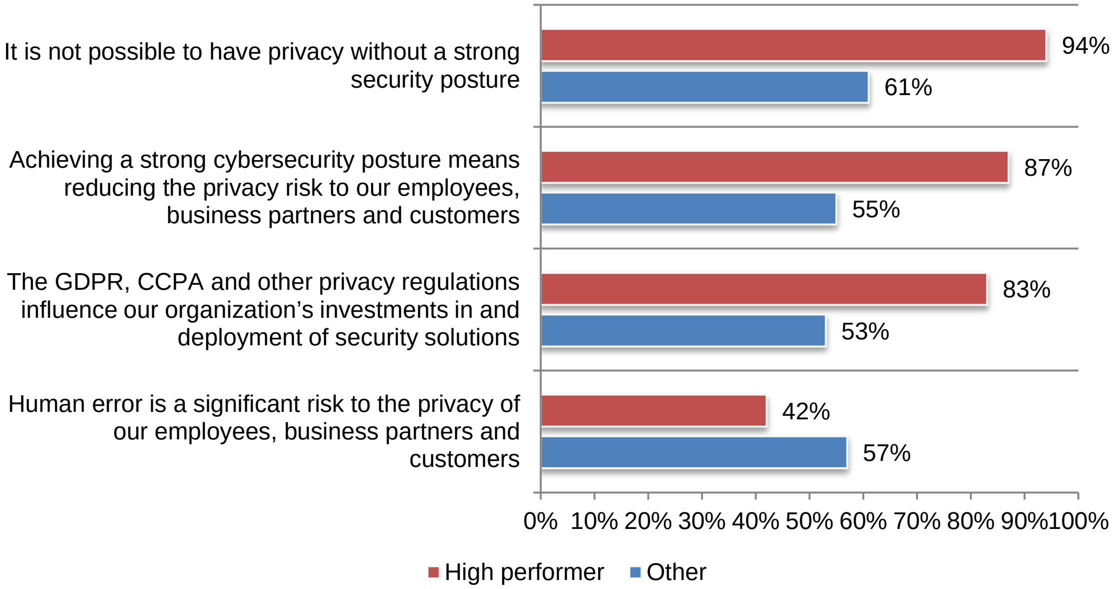
High performing organizations are more aware of the benefits of automation. As shown in Figure 32, the most important benefits of automation are the ability to find attacks before they do damage or gain persistence (78 percent of high performers), reduction in the number of false positives that analysts must investigate (74 percent of high performers) and automation is critical when implementing an effective Zero Trust Security Model (71 percent of respondents).

Figure 32. The importance of the following benefits of automation to achieving a more efficient and effective security posture
Important and High importance responses combined



High performing organizations are more likely to see the important connection between privacy and security. According to Figure 33, 94 percent of respondents in high performing organizations are more likely to believe it is not possible to have privacy without a strong security posture, 87 percent of high performers believe a strong cybersecurity posture means reducing the privacy risk to employees, business partners and customers. Eighty-three percent of high performers say regulations affect investment in security. High performers are less likely to believe human error is a risk to privacy.

Figure 33. Perceptions about the connection between privacy and security
Strongly agree and Agree responses combined



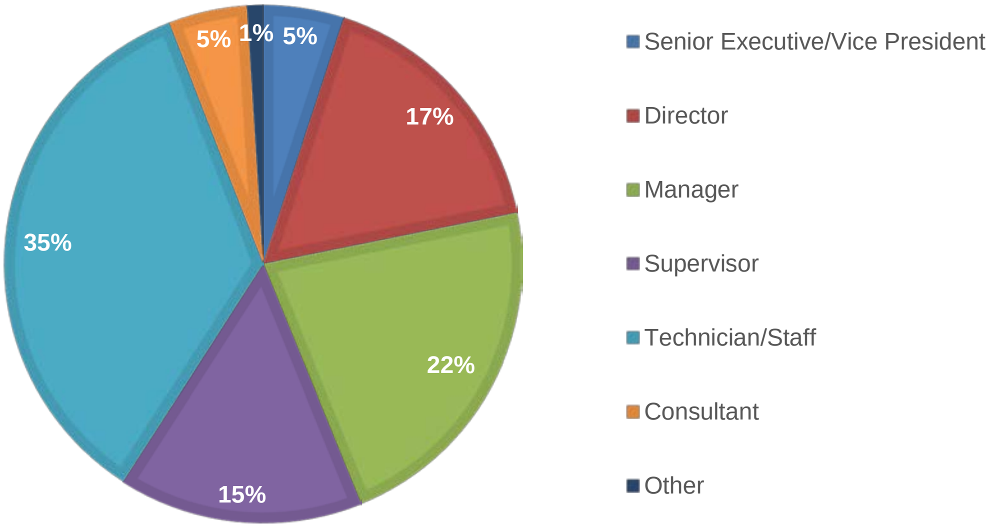
Part 3. Methods

The sampling frame is composed of 52,595 IT and IT security practitioners in North America, the United Kingdom, Germany, Australia and Japan. As shown in Table 1, 2,070 respondents completed the survey. Screening removed 222 surveys. The final sample was 1,848 surveys (or a 3.2 percent response rate).

Table 1. Sample response	Freq	Pct%
Total sampling frame	52,595	100.0%
Total returns	2,070	3.9%
Rejected or screened surveys	222	0.4%
Final sample	1,848	3.2%

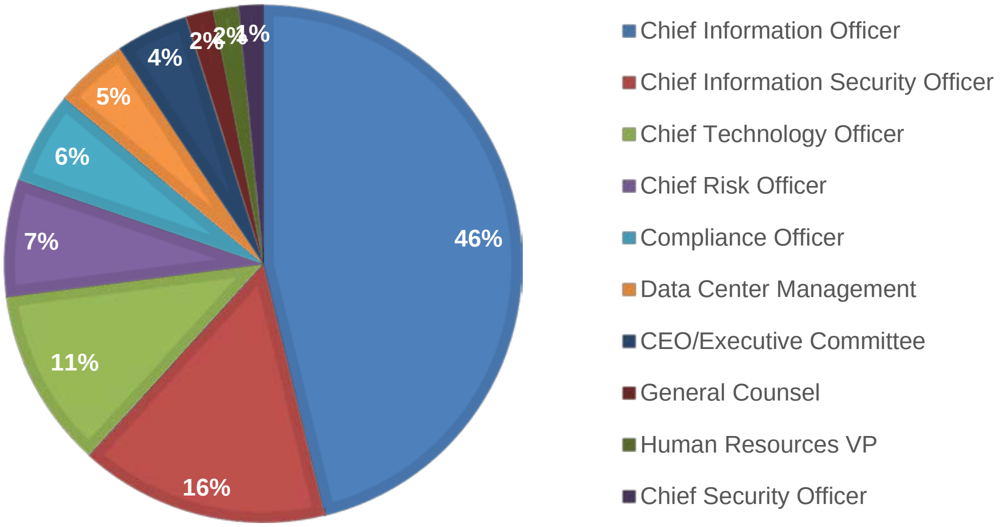
Pie Chart 1 reports the current position or organizational level of the respondents. Fifty-nine percent of respondents reported their current position as supervisory or above and 35 percent of respondents reported their position as technician/staff.

Pie Chart 1. Distribution of respondents according to position level



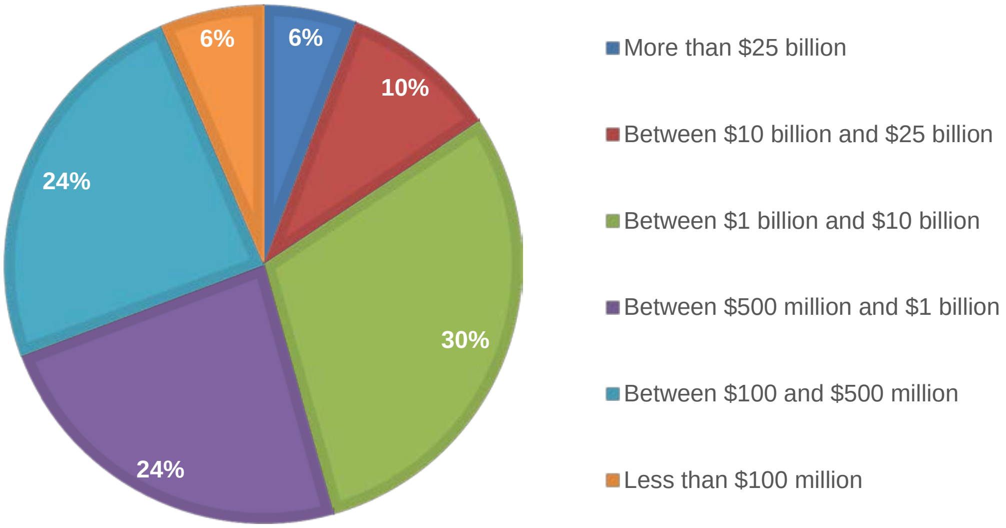
Pie Chart 2 identifies the primary person to whom the respondent or their IT security leader reports. Forty-six percent of respondents identified the chief information officer as the person to whom they report. Another 16 percent indicated they report directly to the chief information security officer and 11 percent of respondents report to the chief technology officer.

Pie Chart 2. Distribution of respondents according to reporting channel



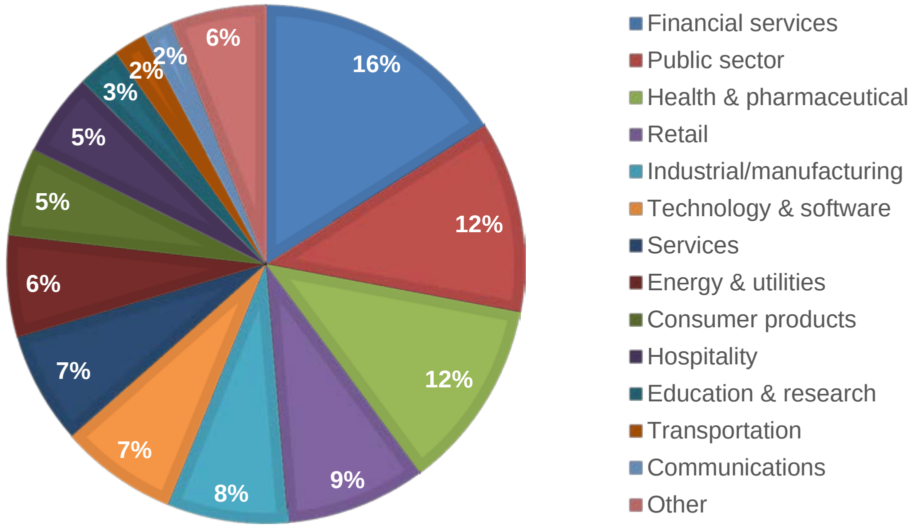
Pie Chart 3 reports the worldwide revenue of the respondents' organizations. Seventy percent of respondents reported their organization's annual worldwide revenue to be greater than $500 million.

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



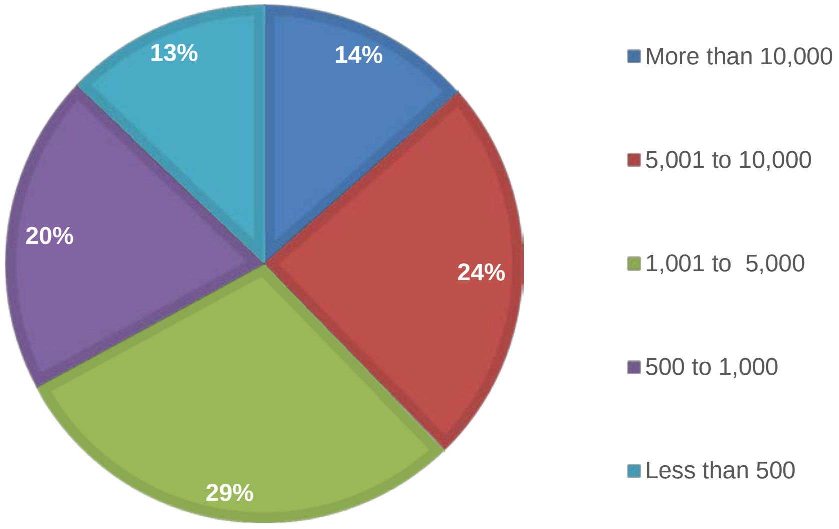
Pie Chart 4 reports the primary industry classification of respondents' organizations. This chart identifies financial services (16 percent of respondents) as the largest segment, which includes banking, insurance, brokerage, investment management and payment processing. Other large verticals include public sector (12 percent of respondents), health and pharmaceutical (12 percent of respondents), retail (9 percent of respondents), and industrial/manufacturing (8 percent of respondents).

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



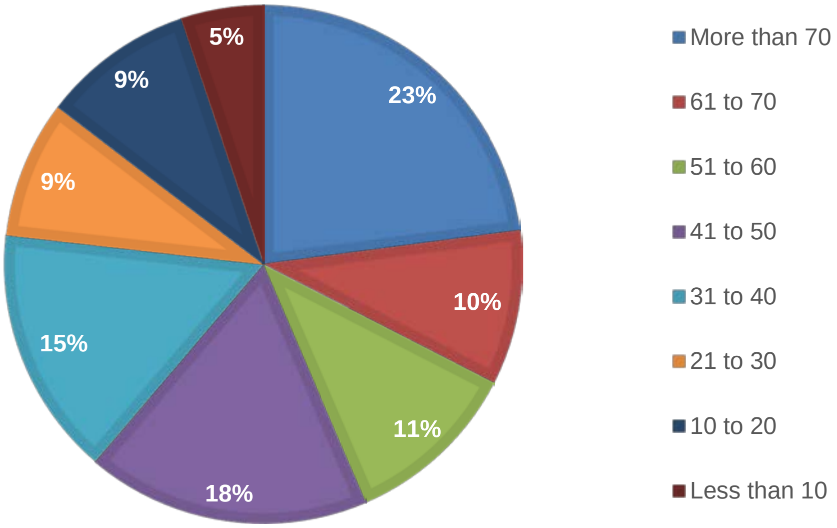
According to Pie Chart 5, 67 percent of respondents are from organizations with a global headcount of more than 1,000 employees.

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



Pie Chart 6 reports the number of security solutions in use within the respondents' organizations. More than half (62 percent) of respondents reported that their organizations are currently using more than 40 security solutions.

Pie Chart 6. Distribution of respondents according to the number security solutions



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 returned responses. 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 and Japan. 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 November 2021.

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

Part 1. Screening

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

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

S3. How knowledgeable are you about your organization's IT security strategy and tactics?	FY2022	FY2020
Very knowledgeable	33%	35%
Knowledgeable	48%	48%
Somewhat knowledgeable	20%	17%
Slightly knowledgeable (stop)	0%	0%
No knowledge (stop)	0%	0%
Total	100%	100%

Part 2. Attributions about the IT security gap

Q1. 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?	FY2022	FY2020
1 or 2	9%	8%
3 or 4	12%	12%
5 or 6	27%	28%
7 or 8	22%	25%
9 or 10	30%	28%
Total	100%	100%
Extrapolated value	6.54	6.58

Q2. Please rate each one of the following statements using the agreement scale provided below each item.		
Q2a. 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.	FY2022	FY2020
Strongly agree	32%	34%
Agree	34%	33%
Unsure	15%	15%
Disagree	12%	11%
Strongly disagree	8%	7%
Total	100%	100%

Q2b. My organization is getting the full value from our current security investments.	FY2022	FY2020
Strongly agree	20%	21%
Agree	27%	27%
Unsure	26%	25%
Disagree	17%	17%
Strongly disagree	9%	10%
Total	100%	100%

Q2c. In my experience, the IT security infrastructure has gaps that allow attackers to penetrate its defenses.	FY2022	FY2020
Strongly agree	32%	31%
Agree	29%	30%
Unsure	20%	21%
Disagree	10%	10%
Strongly disagree	9%	8%
Total	100%	100%

Q3. What are the primary gaps in your organization’s IT security infrastructure? Please select all that apply.	FY2022	FY2020
Security staff and skills shortages	51%	47%
Too many alerts to address and prioritize	35%	38%
There are conflicting priorities between IT and IT security teams	54%	54%
Inability to prevent and detect ransomware	42%	46%
Inability to prevent and detect attacks on the O/S	33%	
Inability to present and detect attacks on the Firmware	38%	
Security solutions can’t keep up with exponentially increasing amounts of data	37%	40%
Hard to protect expanding and blurring IT perimeter with IoT, BYOD, mobile and cloud	57%	57%
Siloed or point security solutions	35%	36%
Inability of traditional perimeter based security solutions to detect and stop advanced targeted attacks	43%	42%
Lack of visibility into every user and device connected to the IT infrastructure	43%	46%
Other (please specify)	0%	0%
Total	469%	407%

Q4. Despite all the cybersecurity investments made by companies, why are breaches still happening? Please select op three choices.	FY2022	FY2020
It is difficult to protect complex and dynamically changing attack surfaces (mobile, byod, cloud, IoT, etc.)	51%	50%
It is difficult to establish the identity of workloads moving to and from the public cloud to our on-premises IT	46%	
There is a lack of adequate security staff with the necessary skills	52%	49%
Attackers are persistent, sophisticated, well trained and well financed	50%	46%
Complexity and the inability to integrate security solutions	50%	50%
Lack of visibility into the network	37%	37%
Lack of interoperability between the different security layers	47%	45%
We have not been able to establish a zero-trust security Model	48%	
Employees and users are not adequately trained to identify potential threats	43%	44%
Threats that have evaded traditional security defenses and are now inside the IT ecosystem	37%	37%
Human error	47%	47%
Other (please specify)	1%	1%
Total	509%	406%

Part 3. Attacks on the inside

Q5. Please rate each one of the following statements using the agreement scale provided below each item.

Q5a. Attacks that have reached inside the network have the potential to do the greatest damage.	FY2022	FY2020
Strongly agree	26%	24%
Agree	22%	25%
Unsure	21%	21%
Disagree	19%	18%
Strongly disagree	12%	12%
Total	100%	100%

Q5b. We are confident that attacks inside the IT infrastructure can be detected quickly before they breakout and cause a cybersecurity breach resulting in data stolen, modified or viewed by unauthorized entities.	FY2022	FY2020
Strongly agree	20%	18%
Agree	22%	23%
Unsure	22%	22%
Disagree	23%	24%
Strongly disagree	13%	15%
Total	100%	100%

Q5c. We are confident that we have not experienced a persistent threat below the platform software that has resulted in data stolen, modified or viewed by unauthorized entities.	FY2022	FY2020
Strongly agree	15%	
Agree	20%	
Unsure	12%	
Disagree	31%	
Strongly disagree	21%	
Total	100%	

Q6. Which of the following do you believe pose the greatest inside threat to your IT infrastructure? Please rank each threat from 1 = lowest threat to 5 = highest threat.	FY2022	FY2020
Attacks against our IT hardware supply chain	2.94	
Attacks initiated in our software supply chain	3.26	
Compromised legitimate users	4.68	4.34
Malicious insiders	1.75	1.82
Negligent users	3.32	3.37
Compromised IoT devices	2.64	2.67
Advanced targeted attacks that have bypassed traditional perimeter defenses	2.51	2.43
Average	3.01	2.93

Part 4. Attack mitigation and visibility

Q7. What steps should be taken to minimize stealthy, or hidden threats within the IT infrastructure? Please check all that apply.	FY2022	FY2020
Implement a Zero Trust architecture	11%	12%
Infrastructure component verification/authentication	13%	13%
Operating system kernel intrusion detection	27%	26%
Firmware/BIOS verification/authentication	19%	21%
SIEM (Security Information and Event Management)	53%	54%
NTA (Network Traffic Analysis)	33%	32%
Monitoring privileged users	51%	53%
Prioritizing rapid breach detection	31%	29%
Comprehensive penetration testing	41%	45%
Other (please specify)	3%	3%
Total	282%	286%

Q8. What one statement best describes your organization's approach to a Zero Trust security Model?	FY2022	FY2020
We are required to implement Zero Trust due to government policies	16%	
I have already implemented a Zero Trust Model	13%	22%
I can pick and choose elements from Zero Trust that will improve our security	9%	12%
We lack the skills and knowledge to implement a Zero Trust framework	7%	
We can implement Zero Trust today but have chosen not to do	9%	13%
It is a goal that will take time to realize	7%	
It is a theoretical framework that cannot be implemented	18%	24%
We are not interested in a Zero Trust approach	21%	29%
Total	100%	100%

Q9. As compute and storage moves from the datacenter to the edge, how will your organization implement the required security? Please select all that apply.	FY2022	FY2020
My current security vendors will supply the needed solutions	42%	40%
I expect our infrastructure providers (network, compute, storage) to supply the required protection	37%	34%
It will require a combination of traditional security solutions and secure infrastructure	46%	48%
A new type of security will be required	55%	59%
No changes are required to our organization's security approach	13%	13%
Total	193%	192%

Part 5.Is AI-enabled automation – hype or reality?

Q10. AI and ML technologies (machine learning, behavioral analytics) are essential to detecting attacks on the inside before they do damage.	FY2022	FY2020
Strongly agree	25%	25%
Agree	27%	27%
Unsure	27%	26%
Disagree	16%	16%
Strongly disagree	5%	6%
Total	100%	100%

Q11. What are the top three key security benefits of using AI and advanced analytics? Please select your top three choices.	FY2022	FY2020
Automate routine tasks	26%	34%
Reduction in white noise/false positives	21%	29%
Identify anomalies in user behaviour and access	23%	
Find stealthy threats that have evaded the standard security defenses	34%	57%
Automate the verification of our IT infrastructure	32%	
Automate the verification of apps and workloads	32%	
Increase effectiveness of security teams	38%	57%
Better integration with threat intelligence sources	35%	45%
More efficient investigations	42%	59%
Supplement to Security Information and Event Management systems (SIEM)	17%	20%
Total	300%	300%

Q11a. What **one** statement best describes the use of AI for security purposes within your organization?	FY2022	FY2020
AI is implemented extensively throughout the IT infrastructure	11%	13%
AI is implemented partially throughout the IT infrastructure	20%	19%
We are planning to use AI in the next 12 months	23%	23%
We are planning to use AI in more than a year	19%	20%
No, we are not planning to use AI	28%	26%
Total	100%	100%

Q11b. What one statement best describes how AI/ML is deployed for attack detection?	FY2022	FY2020
We built our own AI/automation capabilities	23%	21%
We started with basic AI and machine learning software and adapt it for our purposes	21%	24%
We engaged a managed service provider to provide AI/automation capabilities	28%	29%
We acquired a turn-key AI/automation solution	27%	26%
Total	100%	100%

Q12. What best describes how the market considers ML-based attack detection solutions?	FY2022	FY2020
It is important to be a standalone function as the last line of defense	21%	20%
It is considered an important supplement to SIEM	17%	17%
It will be a feature in other security products	32%	31%
Too early to tell	31%	33%
Total	100%	100%

Part 6. Automation

Q13. Using the following 5-point scale, please rate the importance of the following benefits of automation to achieving a more efficient and effective security posture from 1 = low importance to 5 = high importance.		
Q13a. Reduce the number of false positives that analysts must investigate	FY2022	FY2020
1=low importance	4%	3%
2= slightly important	11%	9%
3= moderate importance	25%	20%
4= important	33%	37%
5= high importance	27%	31%
Total	100%	100%
Extrapolated value	3.94	3.81

Q13b. Reduce the amount of time and effort required to investigate an alert	FY2022	FY2020
1=low importance	5%	1%
2= slightly important	8%	5%
3= moderate importance	26%	25%
4= important	36%	41%
5= high importance	26%	29%
Total	100%	100%
Extrapolated value	3.95	3.92

Q13c. Find attacks before they do damage or gain persistence	FY2022	FY2020
1=low importance	5%	4%
2= slightly important	9%	10%
3= moderate importance	27%	23%
4= important	32%	38%
5= high importance	27%	26%
Total	100%	100%
Extrapolated value	3.76	3.72

Q13d. Improve the coordination between the networking, operations and security teams	FY2022	FY2020
1=low importance	5%	6%
2= slightly important	10%	9%
3= moderate importance	25%	25%
4= important	30%	29%
5= high importance	29%	31%
Total	100%	100%
Extrapolated value	375%	3.71

Q13e. Automate key tasks in the investigation, decision making and remediation process	FY2022	FY2020
1=low importance	6%	6%
2= slightly important	13%	13%
3= moderate importance	19%	21%
4= important	30%	30%
5= high importance	31%	30%
Total	100%	100%
Extrapolated value	3.65	3.65

Q13f. Automation is critical when implementing an effective Zero Trust Security Model	FY2022	FY2020
1=low importance	6%	6%
2= slightly important	13%	13%
3= moderate importance	21%	21%
4= important	29%	30%
5= high importance	30%	30%
Total	100%	100%
Extrapolated value	376%	3.65

Q14. Which of the following nine processes will most likely be automated by your organization? Please rank each process from 1 = least likely to 9 = most likely. *	FY2022	FY2020
Identification of attacks on IT infrastructure	3.82	
Identification of attacks on the network	4.87	
Risk scoring and alert prioritization	5.20	5.11
Forensic data aggregation	3.01	3.08
Alert investigation	1.82	1.57
Attack containment (e.g. quarantining)	4.87	4.91
Attack remediation (blocking, system wiping, etc.)	5.60	5.28
Firmware patch updates	5.82	5.66
Application patch updates	4.59	
Average	4.40	3.88

Part 7. Network Access Control (NAC)

Q15. What is your level of confidence that you know ALL the users and devices connected to your network ALL the time?	FY2022	FY2020
Very confident	5%	5%
Confident	13%	14%
Somewhat confident	14%	16%
Not confident	32%	32%
No confidence	36%	34%
Total	100%	100%

Q16. What statements best describe your opinion about NAC products deployed by your organization? Please check all that apply.	FY2022	FY2020
Are not important to our security strategy	17%	18%
Provide visibility to what is on the network	56%	59%
Are difficult to set up and administer	56%	55%
Are a key component of our overall security strategy	48%	48%
Can be used for both network access and attack response	46%	48%
Not familiar with Network Access Control products	23%	25%
Essential tool for proof of compliance	38%	39%
Total	284%	293%

Q17. For what purposes are NAC systems deployed within your organization? Please check all that apply.	FY2022	FY2020
Wired networks	64%	62%
Wireless networks	50%	55%
Guest access	42%	43%
BYOD	30%	31%
IoT	12%	11%
Cloud	45%	43%
Policy-based access and control	42%	43%
NAC is not used	24%	27%
Total	309%	317%

Part 8. Internet of things (IoT)

Q18. Using the following 5-point scale, please rate your organization's ability to secure IoT devices and apps from 1 = low ability to 5 = high ability.	FY2022	FY2020
1=low ability	17%	17%
2= slight ability	28%	29%
3= moderate ability	25%	24%
4= adequate ability	21%	23%
5= high ability	9%	8%
Total	100%	100%
Extrapolated value	2.75	0%

Q19. What is required to achieve a strong level of IoT security within your organization? Please check all that apply.	FY2022	FY2020
Network access controls	37%	40%
Effective data encryption	18%	
Enterprise-level secure infrastructure for compute workloads at the edge	32%	34%
Continuous monitoring of network traffic for each IoT device to spot anomalies	60%	55%
Peer group IoT device comparisons to spot anomalies	32%	32%
Real time solutions to stop IoT activity that is identified as compromised or malicious	38%	37%
Tools to prove compliance requirements have been met	36%	35%
No additional security beyond what is provided by the manufacturer	27%	27%
Other (please specify)	1%	1%
Total	310%	263%

Q20. Please rate each one of the following statements using the agreement scale provided below each item.		
Q20a. IoT devices are appropriately secured with a proper security strategy in place.	FY2022	FY2020
Strongly agree	11%	11%
Agree	11%	12%
Unsure	16%	16%
Disagree	37%	34%
Strongly disagree	25%	27%
Total	100%	100%

Q20b. Legacy IoT technologies are difficult to secure.	FY2022	FY2020
Strongly agree	31%	30%
Agree	42%	39%
Unsure	17%	19%
Disagree	9%	11%
Strongly disagree	1%	1%
Total	100%	100%

Q20c. IoT devices that simply monitor or perform minor tasks pose little threat to our organization’s overall security.	FY2022	FY2020
Strongly agree	12%	11%
Agree	13%	13%
Unsure	18%	18%
Disagree	26%	27%
Strongly disagree	31%	31%
Total	100%	100%

Q20d. Identifying and authenticating IoT devices accessing our network is critical to our organization’s security strategy.	FY2022	FY2020
Strongly agree	31%	32%
Agree	33%	34%
Unsure	15%	14%
Disagree	9%	9%
Strongly disagree	12%	12%
Total	100%	100%

Q21. Who within your organization is most responsible for ensuring the security of IoT devices and apps?	FY2022	FY2020
Chief information officer (CIO)	32%	31%
Chief technology officer (CTO)	5%	5%
Chief information security officer (CISO)	20%	18%
Chief security officer (CSO)	3%	3%
Line of business leadership	10%	12%
End-users of IoT devices	11%	13%
Data Protection Officer (DPO)	0%	1%
No one function has overall responsibility	17%	16%
Other (please specify)	1%	1%
Total	100%	100%

Part 9. Cyber insurance

Q22. Does your organization have a cyber insurance policy?	FY2022	FY2020
Yes, we currently have a policy	41%	39%
We will purchase a policy in the next six months	23%	22%
We will purchase a policy in the next 12 months	17%	18%
We have no plans to purchase a policy Skip to Q25	19%	21%
Total	100%	100%

Q23. Using the following 5-point scale, please rate the importance of cyber insurance as part of your organization's overall cybersecurity strategy from 1 = low importance to 5 = high importance.	FY2022	FY2020
1=low importance	7%	8%
2= slightly important	12%	11%
3= moderate importance	10%	11%
4= important	39%	42%
5= high importance	32%	29%
Total	100%	100%
Extrapolated value	3.64	3.72

Q24. If important, why is it important to your cyber insurance strategy (4+ responses). Please select your top three choices.	FY2022	FY2020
Provides legal defense cost	37%	36%
Covers regulatory fines	22%	24%
Assists in efforts to reduce impact of the cyberattack on brand and marketplace image	28%	27%
Provides and covers the cost of identity protection services to victims	26%	24%
Assesses the cybersecurity posture of our organization	59%	60%
Provides information and guidance on how to improve the cybersecurity posture of our organization	53%	52%
Covers the replacement of lost or damaged equipment	22%	22%
Assists in activities to respond, contain and remediate the consequences of the cyberattack	51%	53%
Other (please specify)	3%	3%
Total	300%	300%

Part 10. Digital transformation

Q25. Do you have any involvement in managing digital transformation activities within your organization?	FY2022	FY2020
Yes, fully involved	25%	27%
Yes, partially involved	29%	30%
Yes, minimally involved	20%	19%
No involvement Skip to Q30a.	25%	25%
Total	100%	100%

Q26. Using the following 5-point scale, please rate the importance of security technologies to a successful transformation strategy from 1 = low importance to 5 = high importance.	FY2022	FY2020
1=low importance	7%	6%
2= slightly important	11%	9%
3= moderate importance	19%	18%
4= important	32%	34%
5= high importance	32%	33%
Total	100%	100%
Extrapolated value	3.75	3.78

Q27. What are the most significant barriers to having a **successful digital transformation process**? Please choose only your top three choices.	FY2022	FY2020
Inability to enable the free flow of information	51%	53%
Inability to secure the digital transformation process and environment	53%	51%
Inability to collaborate with supply chain partners	42%	40%
Inability to overcome turf and silo issues	47%	51%
Lack of suitable leadership	32%	32%
Lack of in-house expertise	41%	39%
Lack of resources and budgets	32%	32%
Other (please specify)	3%	3%
Total	300%	300%

Q28. What do you see as the most significant **challenges** to achieving a **secure digital transformation process** in your organization today? Please choose only your top **three** choices.	FY2022	FY2020
Security is not considered early enough in the project plan	21%	
The availability of a secure cloud environment	46%	40%
The ability to secure workloads moving from the edge to the cloud	27%	
The ability to ensure the privacy of customer information	44%	44%
The ability to meet consumers' expectations about consent at every layer in the digital ecosystem	32%	33%
The ability to balance security needs with customer experience	43%	45%
The ability to comply with data privacy regulations	61%	57%
The ability to avoid security exploits and data breaches	63%	61%
The ability to use sensitive and confidential data to improve customer experience	37%	33%
The ability to overcome turf and silo issues	53%	54%
The continuous availability of the IT infrastructure	39%	39%
Lack of Security skills and resources	35%	
Limiting unauthorized access to data and applications	62%	59%
Other (please specify)	4%	4%
Total	532%	470%

Q29. Which processes are prioritized to minimize the risk of digital transformation? Please select all that apply.	FY2022	FY2020
Regulatory compliance aligned to standards-based controls	36%	34%
Cyber disaster recovery	21%	21%
Security modernization	45%	48%
Implementing a Zero Trust-enabled IT architecture	37%	
Implementing a Cybersecurity Framework	40%	
Proactive vulnerability and breach detection	40%	52%
Securely shifting workloads from on-premises to cloud	28%	30%
None of the above	14%	
Total	260%	187%

Part 11. Compute and storage

Q30a. Our organization makes server decisions based on the security inherent within the platform.	FY2022	FY2020
Strongly agree	28%	29%
Agree	29%	27%
Unsure	22%	21%
Disagree	14%	16%
Strongly disagree	8%	7%
Total	100%	100%

Q30b. Backup and recovery is a key component of our organization’s security strategy.	FY2022	FY2020
Strongly agree	35%	35%
Agree	30%	28%
Unsure	18%	20%
Disagree	11%	12%
Strongly disagree	5%	5%
Total	100%	100%

Q30c. We require Servers that leverage Security Certificates to identify that the system has not been compromised during delivery.	FY2022
Strongly agree	40%
Agree	27%
Unsure	18%
Disagree	10%
Strongly disagree	4%
Total	100%

Q31. Does your organization’s storage supplier provide backup and recovery solutions?	FY2022	FY2020
Yes	32%	35%
No	68%	65%
Total	100%	100%

Part 12. Privacy

Q32a. Achieving a strong cybersecurity posture means reducing the privacy risk to our employees, business partners and customers.	FY2022	FY2020
Strongly agree	30%	33%
Agree	35%	33%
Unsure	18%	17%
Disagree	12%	11%
Strongly disagree	6%	6%
Total	100%	100%

Q32b. 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.	FY2022	FY2020
Strongly agree	33%	30%
Agree	29%	28%
Unsure	18%	22%
Disagree	14%	14%
Strongly disagree	6%	6%
Total	100%	100%

Q32c. Human error is a significant risk to the privacy of our employees, business partners and customers.	Total	Total
Strongly agree	25%	25%
Agree	27%	27%
Unsure	21%	25%
Disagree	18%	16%
Strongly disagree	8%	8%
Total	100%	100%

Q32d. It is not possible to have privacy without a strong security posture.	FY2022	FY2020
Strongly agree	38%	39%
Agree	33%	36%
Unsure	14%	13%
Disagree	8%	7%
Strongly disagree	6%	5%
Total	100%	100%

Part 13. Your role and organization

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

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

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

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

D5. How many employees are in your organization?	FY2022	FY2020
Less than 500	13%	13%
500 to 1,000	20%	21%
1,001 to 5,000	29%	29%
5,001 to 10,000	24%	23%
More than 10,000	13%	14%
Total	99%	100%

D6. How many security solutions does your organization use?	Total	Total
Less than 10	5%	5%
10 to 20	9%	9%
21 to 30	9%	8%
31 to 40	16%	17%
41 to 50	18%	15%
51 to 60	11%	8%
61 to 70	10%	9%
More than 70	23%	28%
Total	100%	100%

Q34d. It is not possible to have privacy without a strong security posture.	FY2020
Strongly agree	39%
Agree	35%
Unsure	13%
Disagree	7%
Strongly disagree	6%
Total	100%

Part 13. Your role and organization

D1. What organizational level best describes your current position?	FY2020	FY2018
Senior Executive/Vice President	8%	5%
Director	17%	17%
Manager	22%	23%
Supervisor	14%	14%
Technician/Staff	33%	35%
Consultant	4%	4%
Contractor	0%	
Other	2%	1%
Total	100%	100%

D2. Check the **Primary Person** you or your leader reports to within the organization.	FY2020	FY2018
CEO/Executive Committee	4%	4%
General Counsel	1%	1%
Chief Information Officer (CIO)	44%	43%
Chief Technology Officer (CTO)	11%	6%
Chief Information Security Officer (CISO)	19%	18%
Compliance Officer	6%	4%
Human Resources VP	1%	
Chief Security Officer (CSO)	2%	2%
Data Center Management	4%	4%
Chief Risk Officer (CRO)	7%	6%
Data Protection Officer (DPO)	1%	
Other	0%	0%
Line of business (LOB) management	0%	12%
Total	100%	100%

D3. What range best defines the worldwide revenue of your organization?	FY2020	FY2018
Less than $100 million	8%	5%
Between $100 and $500 million	22%	19%
Between $500 million and $1 billion	25%	29%
Between $1 billion and $10 billion	27%	30%
Between $10 billion and $25 billion	10%	10%
More than $25 billion	8%	6%
Total	100%	100%

D4. What best describes your organization’s primary industry classification?	FY2020	FY2018
Agriculture & food services	1%	1%
Communications	2%	2%
Consumer products	6%	5%
Defense & aerospace	0%	0%
Education & research	3%	2%
Energy & utilities	6%	6%
Entertainment & media	1%	1%
Financial services	18%	18%
Health & pharmaceutical	13%	12%
Hospitality	4%	4%
Industrial/manufacturing	9%	9%
Public sector	9%	10%
Retail	9%	9%
Services	9%	10%
Technology & software	7%	8%
Transportation	2%	2%
Other	2%	
Total	100%	100%

D5. How many employees are in your organization?	FY2020	FY2018
Less than 500	12%	11%
500 to 1,000	21%	21%
1,001 to 5,000	28%	29%
5,001 to 10,000	24%	23%
More than 10,001	16%	16%
Total	100%	100%

D6. How many security solutions does your organization use?	FY2020
Less than 10	5%
10 to 20	9%
21 to 30	13%
31 to 40	16%
41 to 50	15%
51 to 60	8%
61 to 70	10%
More than 70	24%
Total	100%
Extrapolated value	46.8

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.