Ponemon INSTITUTE

Security Innovation: Secure Systems Start with Foundational Hardware

Sponsored by Intel

Independently conducted by Ponemon Institute LLC

Publication Date: April 2022

Ponemon Institute© Research Report

Security Innovation: Secure Systems Start with Foundational Hardware

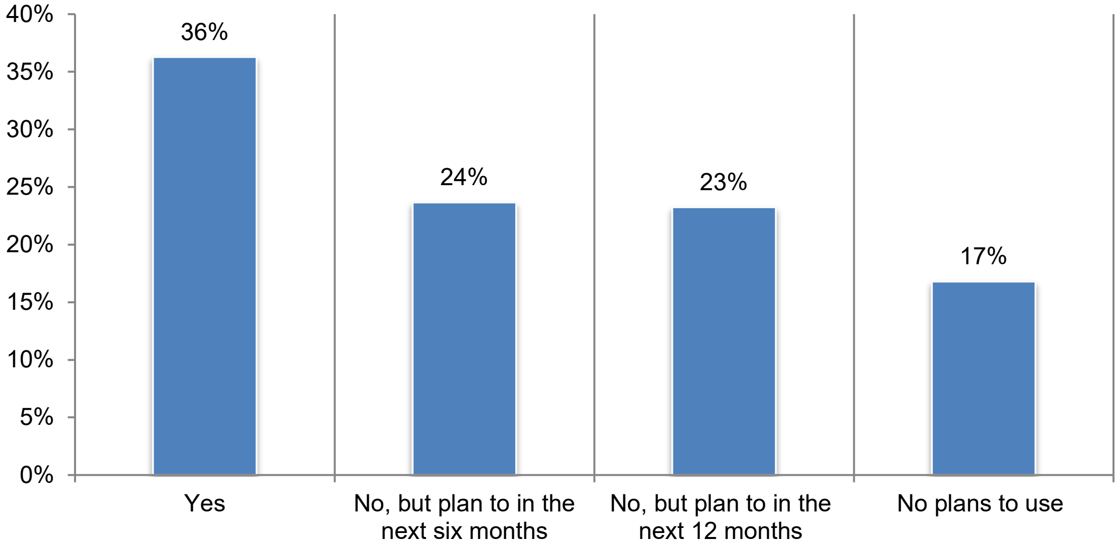
Prepared by Ponemon Institute, April 2022

Part 1. Introduction

A constantly changing threat landscape requires organizations to be agile and innovative in their cybersecurity practices. The purpose of this research is to understand how hardware-enabled security solutions can support an organization's security posture and enable innovation in the creation and deployment of cybersecurity solutions. Additionally, this study examines what types of technologies organizations prioritize when exploring security innovation. Sponsored by Intel and conducted by Ponemon Institute, 1,406 IT and IT security practitioners in the United States, LATAM and EMEA who are influential in IT security decision-making regarding investment in technologies and activities were surveyed.

As shown in Figure 1, while only 36 percent of these respondents say their organizations have adopted hardware-assisted security solutions, 47 percent of respondents say their organizations will adopt these security solutions in the next six months (24 percent) or in the next 12 months (23 percent). In the context of this research, hardware-enabled security capabilities include control-flow enforcement technology, hardware telemetry to inform malicious signals, cryptographic encryption and acceleration, virtualized machines, offload engines to enable greater cryptographic security and/or endpoint authentication and a trusted platform module (TPM) chip.

Figure 1. Does your organization's current cybersecurity solutions/protocols use hardware-assisted security solutions?



Following are findings regarding the adoption and benefits of foundational hardware. While almost half of organizations surveyed are considering adopting these solutions, currently 36 percent of respondents say their organizations have adopted hardware-assisted security solutions. The following findings are based on these 36 percent of respondents.

- Eighty-five percent of these respondents say hardware and/or firmware-based security in their organizations is a high or a very high priority.
- Sixty-four percent of these respondents say their organizations are taking steps to advance security at the hardware level, especially within the cloud infrastructure, data centers, security operations centers (SOC) and edge computing devices and are proactively taking steps to ensure the integrity of data with improved hardware or firmware-level security solutions (65 percent of respondents).

- Sixty-four percent of these respondents say hardware is part of their organizations' endpoint (PC/IoT) security strategy. Fifty-three percent of respondents say their organizations deploy tools or policies to ensure hardware supply chain assurance and transparency. Thirty-eight percent of respondents say their organizations take advantage of hardware-enabled accelerators to offset the cost of authenticating endpoints before enabling access.

- Eighty-one percent of these respondents say it is important or highly important for the technology provider to offer hardware-based security solutions and evidence that the components are operating in a known and trusted state. Only 39 percent of respondents say their anti-virus software vendor offers hardware-assisted telemetry to detect malware behavior signals below the operating system.

- Hardware or firmware security solutions make vulnerability management more effective, according to 69 percent of these respondents. Fifty-eight percent of respondents say their organizations have good or significant visibility into their hardware and firmware operating in a known good state.

- To plan and deploy security and functional updates for basic input output systems (BIOS) and firmware, 31 percent of respondents use automated industry software/tools. Manual methods are primarily used such as manual checks against the manufacturer's BIOS release and system configuration (30 percent of respondents) or manual matching of vulnerabilities against the configuration database (23 percent of respondents).

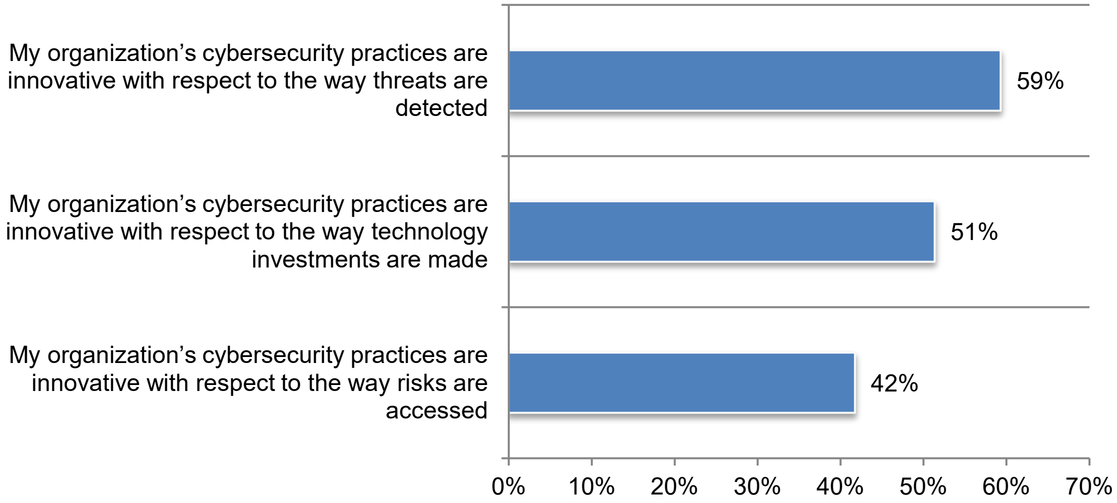
Part 2. Key findings

The report is organized according to the following themes.

- Keeping up with the pace of cybersecurity innovation is a priority for organizations
- Organizations see the promise in Zero Trust and hardware-based security solutions
- Visibility remains essential in activating timely security updates

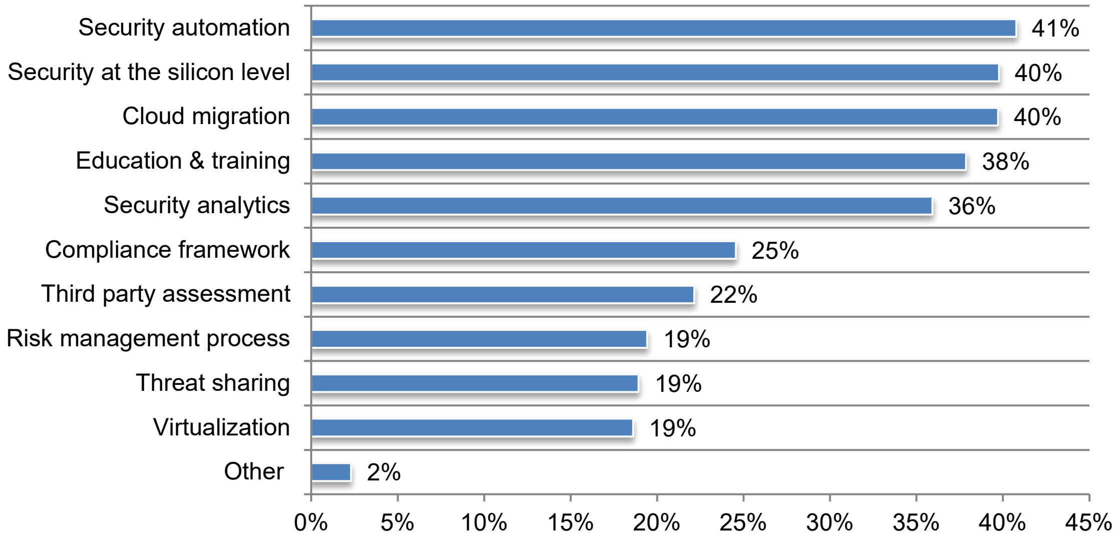
How innovative are organizations' cybersecurity practices? According to Figure 2, most organizations (59 percent of respondents) believe their cybersecurity practices are most innovative in the detection of threats followed by how technology investments are made (51 percent of respondents). However, only 42 percent of respondents say their organization's cybersecurity practices are innovative with respect to the way risks are assessed.

Figure 2. Perceptions about cybersecurity innovation
Strongly agree and Agree responses combined



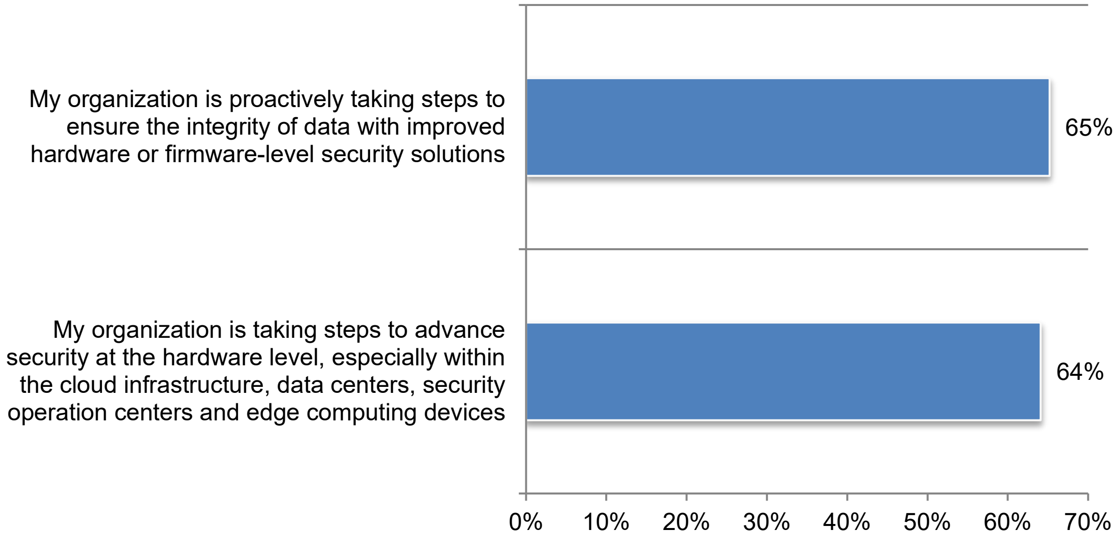
As shown in Figure 3, the top areas of security innovation within organizations today are security automation (41 percent of respondents), security at the silicon level (40 percent of respondents), cloud migration (40 percent of respondents) and education and training (38 percent of respondents).

Figure 3. The top areas of security innovation within organizations today
Three responses permitted



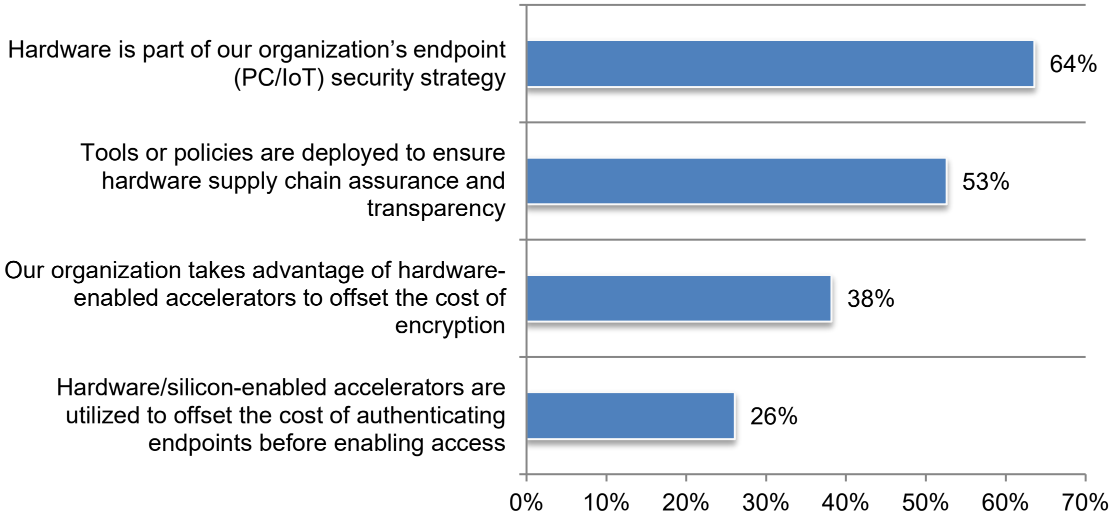
Factors to consider when deploying hardware and firmware security solutions. Of the 36 percent of respondents in organizations using hardware-assisted security, 85 percent say hardware and/or firmware-based security in their organizations is a high or very high priority. According to Figure 4, as a result, 64 percent of respondents say their organization is taking steps to advance security at the hardware level, especially within cloud infrastructure, data centers, security operation centers (SOC) and edge computing devices and is proactively taking steps to ensure the integrity of data with improved hardware or firmware-level security solutions (65 percent of respondents).

Figure 4. Perceptions about the deployment of hardware and firmware security solutions
Strongly agree and Agree responses combined



According to Figure 5, 64 percent of these respondents (36 percent) say hardware is part of their organization’s endpoint (PC/IoT) security strategy. Fifty-three percent of respondents say their organizations deploy tools or policies to ensure hardware supply chain assurance and transparency. Thirty-eight percent of respondents say their organizations take advantage of hardware-enabled accelerators to offset the cost of encryption and 26 percent of respondents say their organizations deploy hardware/silicon-enabled accelerators to offset the cost of authenticating endpoints before enabling access.

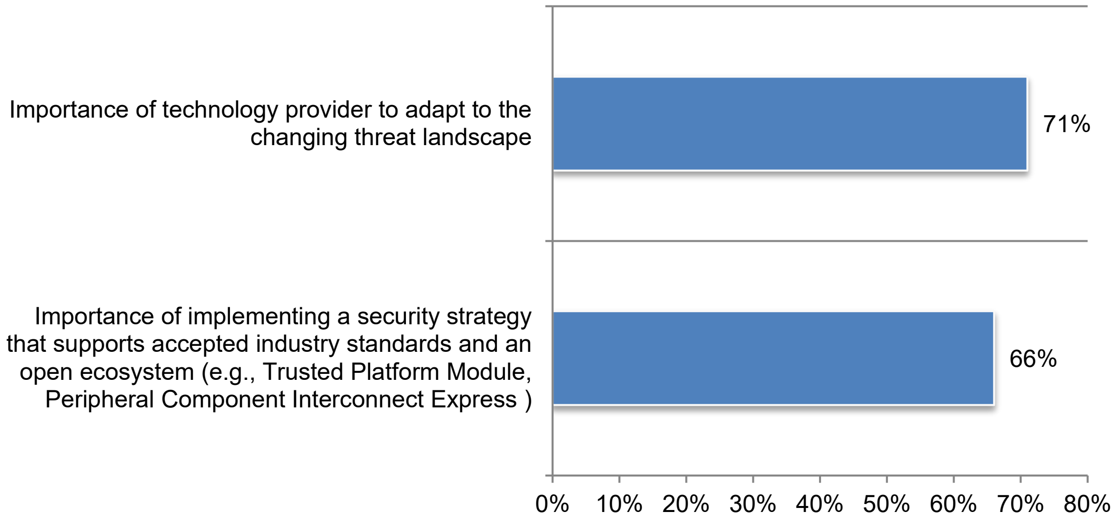
Figure 5. What security solutions are being deployed.
Yes responses presented



Security practices are important to supporting innovation and agility. Sixty-four percent of all respondents say their organizations are more likely to purchase technologies and services from technology providers that are leading edge with respect to innovation.

According to Figure 6, to support innovation, technology providers need to be able to adapt to the changing threat landscape (71 percent of respondents). Sixty-six percent of respondents say it is very important or highly important to implement a security strategy that supports accepted industry standards and an open ecosystem such as a Trusted Platform Module (TPM) and Peripheral Component interconnect Express (PCIe). Such technology provides an extra layer of security.

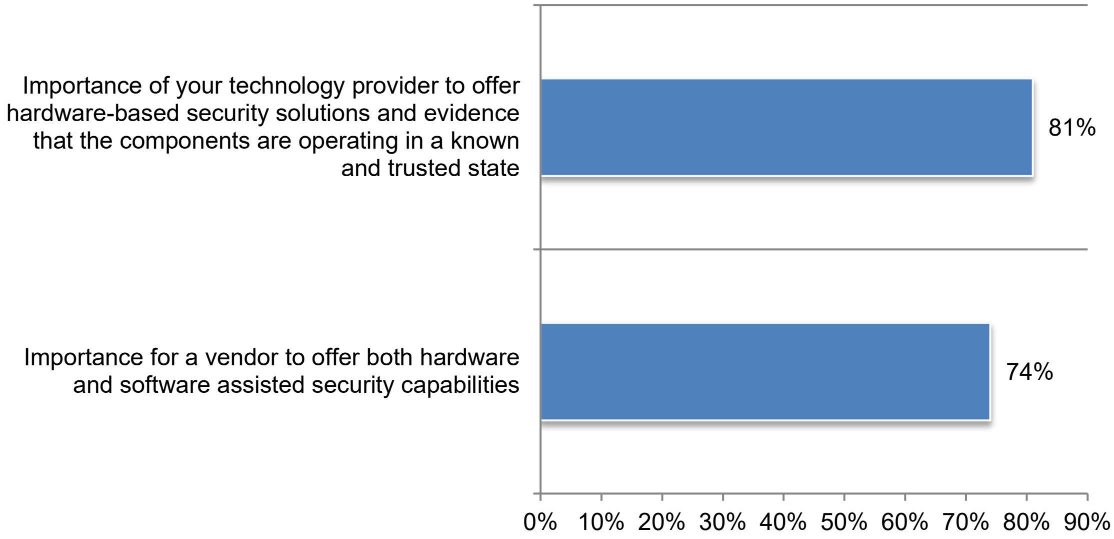
Figure 6. Important security practices to support innovation and agility
On a scale from 1 = not important to 10 = highly important, 7+ responses presented



As shown in Figure 7, for those organizations using hardware-based solutions (36 percent), 81 percent of respondents say it is important (42 percent) or highly important (39 percent) for the technology provider to offer hardware-based security solutions and evidence that the components are operating in a known and trusted state.

Further, 74 percent say it is important for a vendor to offer both hardware and software-assisted security capabilities. Only 39 percent of respondents say their anti-virus software vendor offers hardware-assisted telemetry to detect malware behavior signals below the operating system.

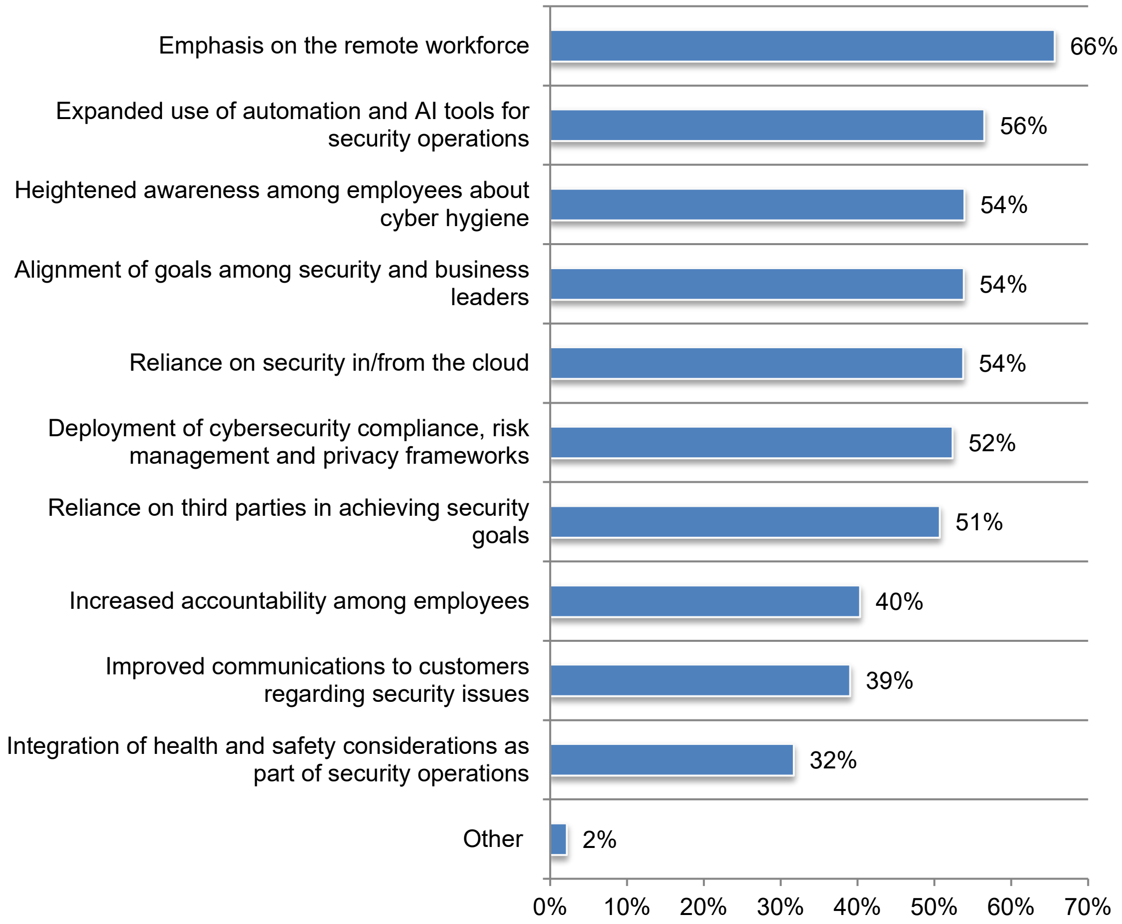
Figure 7. Importance of certain features provided by vendors
On a scale from 1 = not important to 10 = very important, 7+ responses



Pandemic pressures motivated many organizations to innovate their cybersecurity practices. With very little advance warning, organizations were forced to make changes to their cybersecurity practices because of a remote workforce. Fifty-three percent of respondents say their organizations refreshed their security strategy because of the pandemic.

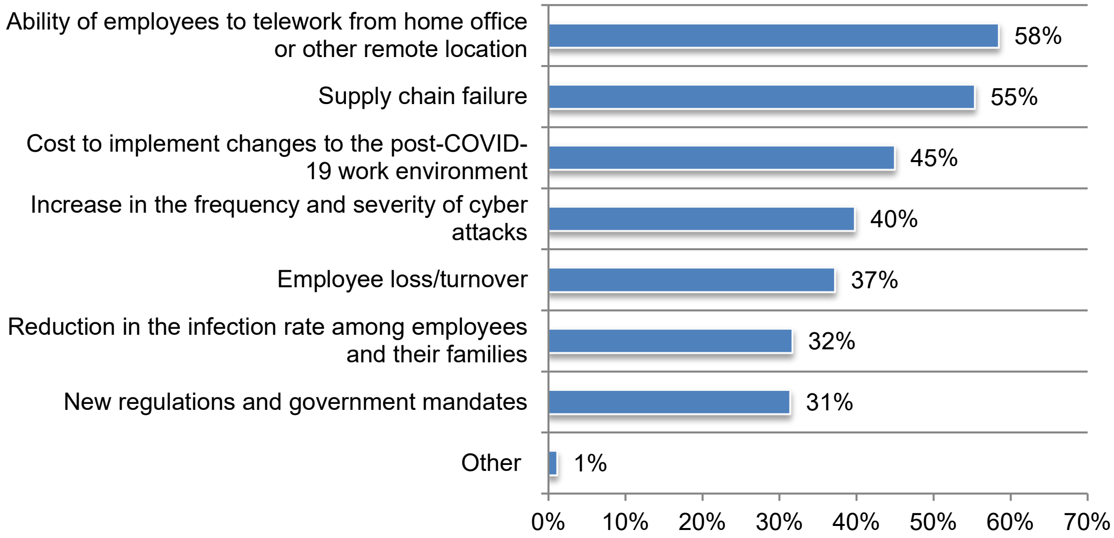
As shown in Figure 8, of these respondents, their priorities shifted to more of an emphasis on the remote workforce (66 percent) and the expanded use of automation and AI tools (56 percent). Fifty-four percent of respondents say new priorities include heightened awareness among employees about cyber hygiene, alignment of goals among security and business leaders and reliance on security in/from the cloud.

Figure 8. How have your organization's security priorities changed?
More than one response permitted



As shown in Figure 9, the number one driver to making changes due to the pandemic is the ability for employees to telework from home office or other remote locations (58 percent of respondents). This is followed by supply chain failures (55 percent of respondents) and the cost to implement changes to the post-COVID-19 workforce based on the need to ensure security and to improve efficiency through the expanded use of automation and AI tools for security operations.

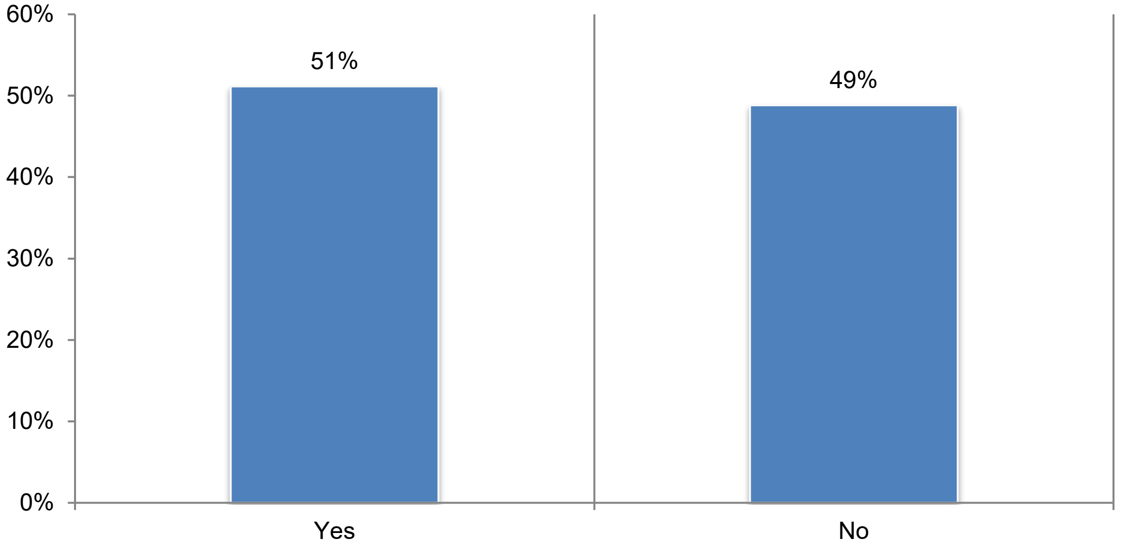
Figure 9. What were the main drivers to the changes implemented?
Three responses permitted



Organizations see the promise of Zero Trust in strengthening their security posture. According to NIST, a Zero-Trust architecture is the term for an evolving set of cybersecurity paradigms that move defenses from static, network-based perimeters to focus on users, assets and resources. Zero Trust assumes there is no implicit trust granted to assets or user accounts based solely on their physical or network location or based on asset ownership. Therefore, Zero Trust architecture applies these principles to plan industrial and enterprise infrastructure and workflows.

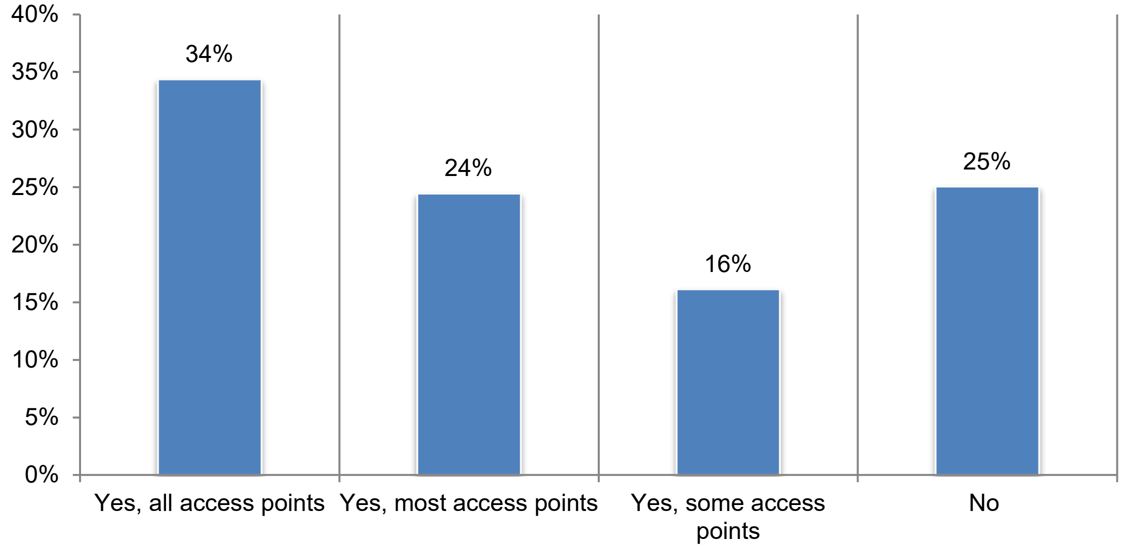
Thirty-two percent of the 36 percent of organizations using hardware-based security solutions have implemented a Zero Trust infrastructure strategy. Of these, 51 percent say hardware security capabilities have been incorporated in their Zero Trust strategies (Figure 10). Further, the pandemic and a remote workforce has increased interest in Zero Trust cybersecurity models and in hardware and firmware-level security models, according to 75 percent of these respondents.

Figure 10. If your organization implemented a Zero Trust infrastructure strategy, does it incorporate security capabilities in it?



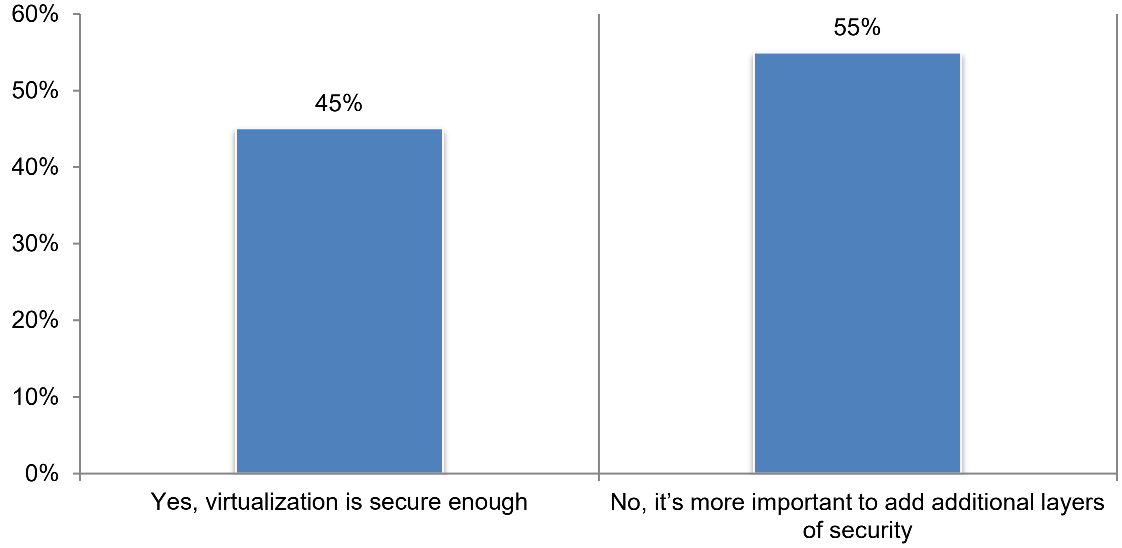
Most organizations require authentication to their data. According to Figure 11, 58 percent of respondents say access points in their organization's IT infrastructure are authenticated at all access points (34 percent) or at most access points (24 percent). Twenty-five percent of respondents say their organization does not authenticate access points and 49 percent of these respondents say it is because of the negative impact on performance.

Figure 11. Does your organization authenticate access points in its IT infrastructure?



Additional layers of security are needed along with virtualization technology, according to 55 percent of respondents. Forty-eight percent of respondents say their organizations use virtualization technology at the client, endpoint or PC level. As described in the research, virtualization technology enables organizations to run virtual versions of computer systems in a layer that's abstracted from its hardware. In fact, 45 percent of respondents consider virtualization enough security, according to Figure 12.

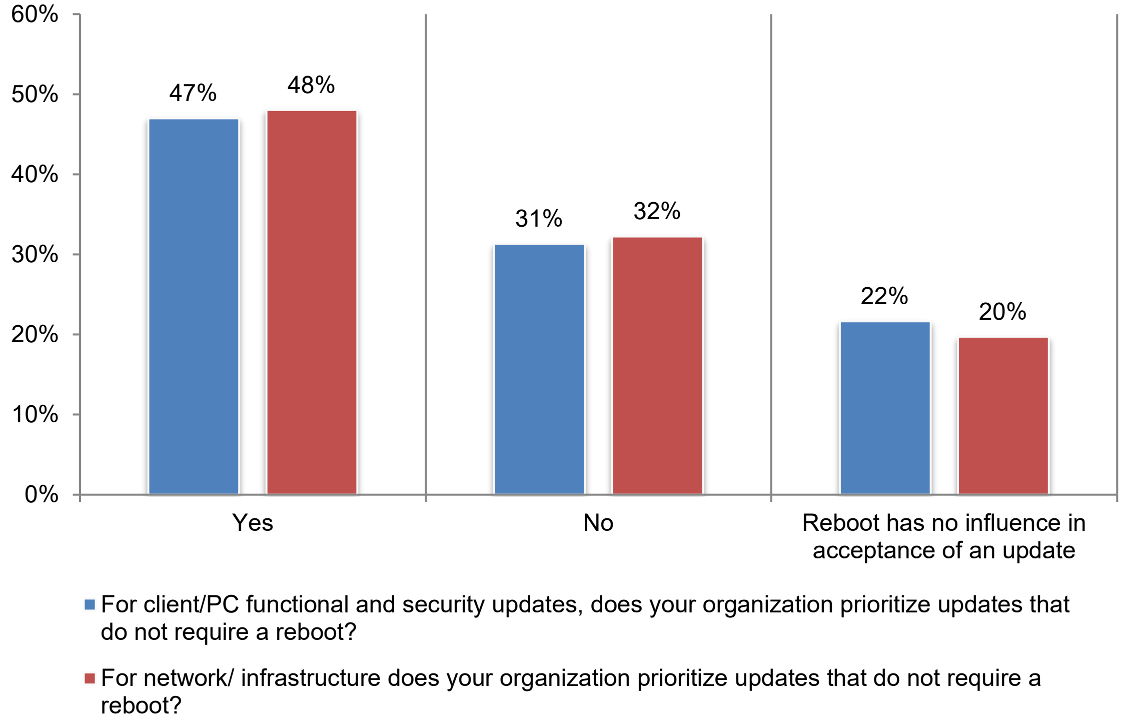
Figure 12. Do you consider virtualization enough security, or do you think it's more important to add additional layers of security?



Visibility remains essential in activating timely security updates. Less than half of organizations have visibility into newly disclosed vulnerabilities and patches/updates. Forty-eight percent of respondents say they have such visibility and on average, the security team spends 17 hours each week mapping known vulnerabilities in IoT devices.

As shown in Figure 13, security updates are also mainly prioritized for the latest product generation, according to 42 percent of respondents. For client/PC functional and security updates, and network/infrastructure our organization prioritizes updates that do not require a reboot, according to 47 percent and 48 percent of respondents, respectively.

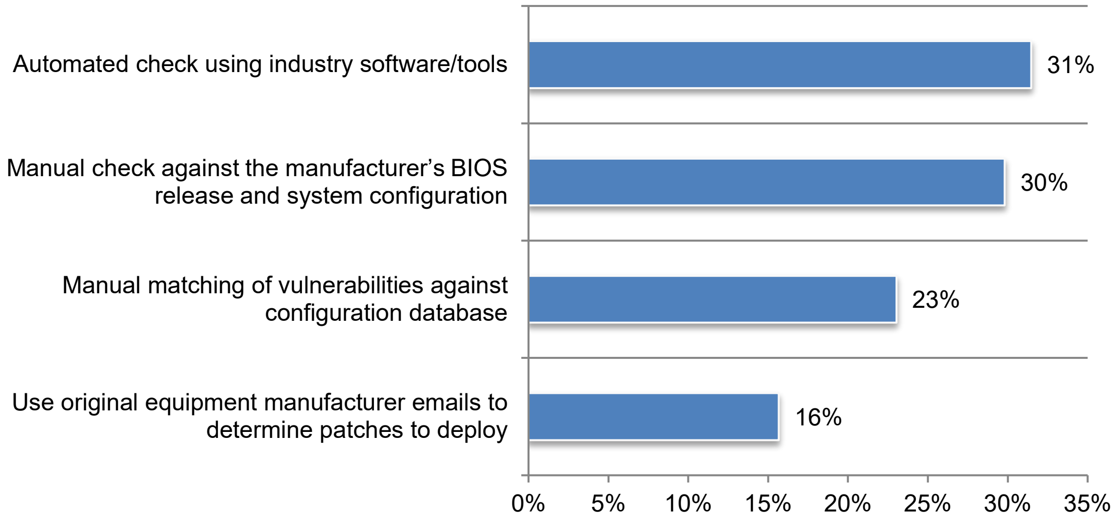
Figure 13. Does your organization prioritize updates that do not require a reboot?



Hardware and firmware security solutions make vulnerability management more effective, according to 69 percent of respondents. Of those organizations using hardware and firmware security solutions, 58 percent of respondents say their organizations have good or significant visibility into whether their hardware and firmware are operating in a known good state.

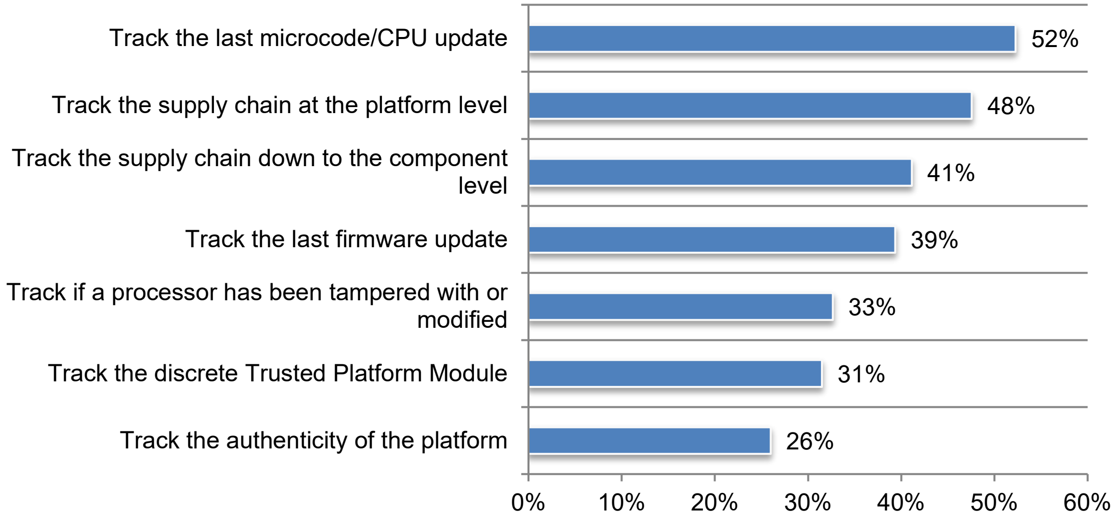
As shown in Figure 14, to plan and deploy security and functional updates for basic input output systems (BIOS) and firmware, 31 percent of respondents use automated industry software/tools. Manual methods are primarily used such as a manual check against the manufacturer's BIOS release and system configuration (30 percent of respondents) or manual matching of vulnerabilities against configuration database (23 percent of respondents).

Figure 14. How does your organization plan and deploy security and functional updates for basic input output systems (BIOS) and firmware?



More than half (52 percent) of all respondents in the research say their organizations track the security of their devices based on the last microcode/CPU update. This is followed by tracking the supply chain at the platform level (48 percent of respondents) and the supply chain down to the component level (41 percent of respondents), as shown in Figure 15.

Figure 15. How does your organization track the status and security of its device fleet?

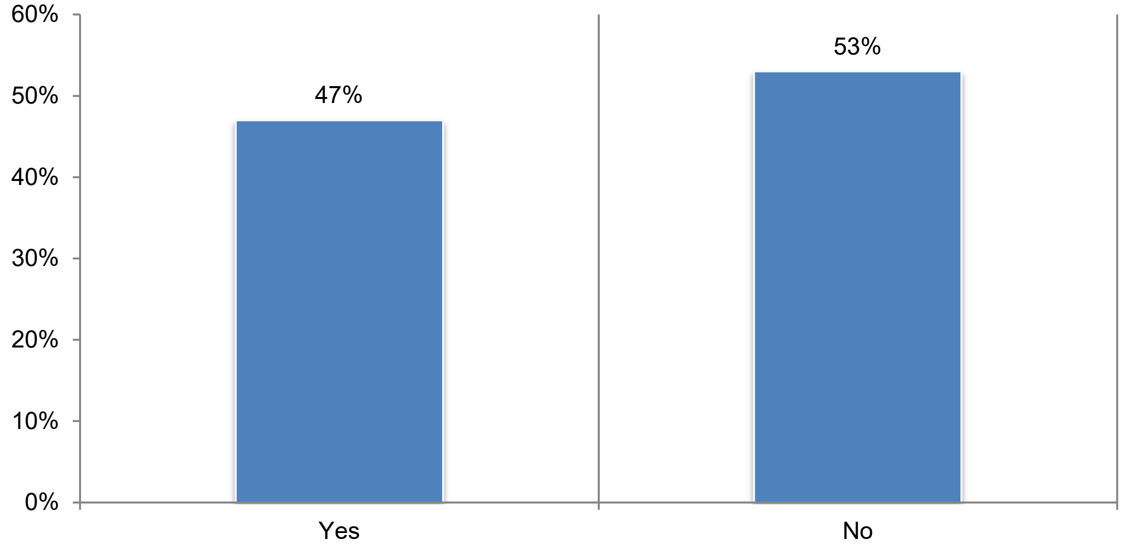


Edge cloud architecture technology

Organizations are leveraging edge-to-cloud technology solutions. In the context of this research, edge cloud architecture is defined as used to decentralize processing power to the edges of an organization's networks. Sixty-four percent of respondents say their organizations have adopted edge-to-cloud architecture and 59 percent of these respondents say they are integrating technology and best-known methods to protect against physical attacks both in the data center and at the edge.

As shown in Figure 16, less than half (47 percent) of these respondents say they have the security infrastructure in place to address vulnerabilities from the edge to the cloud.

Figure 16. Does your organization have the security infrastructure in place to address vulnerabilities from the edge to the cloud?



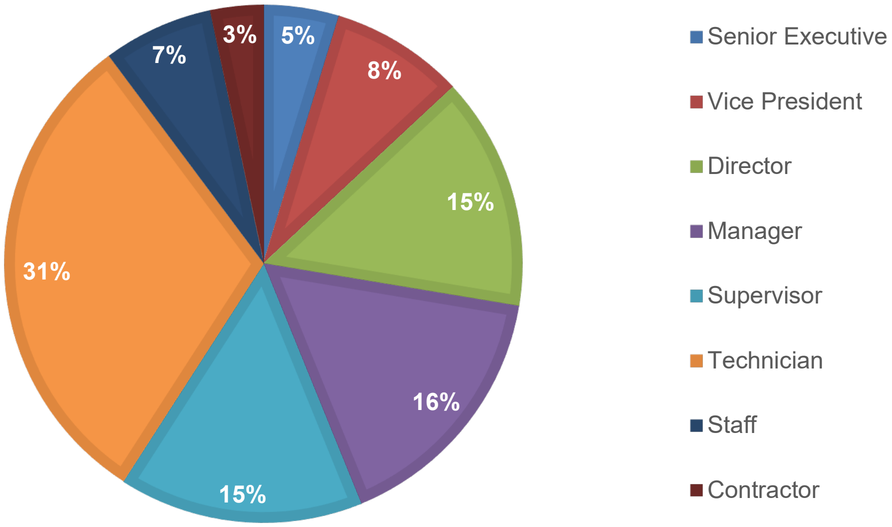
Part 3. Methodology

A sampling frame of 43,231 IT security professionals in the United States, LATAM and EMEA who are influential in IT security decision-making regarding investment in technologies and activities were selected as participants to this survey. Table 1 shows 1,569 total returns. Screening and reliability checks required the removal of 163 surveys. Our final sample consisted of 1,406 surveys or a 3.3 percent response.

Table 1. Sample response	Freq	Pct%
Sampling frame	43,231	100.0%
Total returns	1,569	3.6%
Rejected or screened surveys	163	0.4%
Final sample	1,406	3.3%

Figure 17 reports the respondent's organizational level within participating organizations. By design, more than half (59 percent) of respondents are at or above the supervisory levels. The largest category at 31 percent of respondents is staff/technician.

Figure 17. Current position within the organization



As shown in Figure 18, 20 percent of respondents said their primary role is IT security. Fourteen percent of respondents said their primary role is application security, followed by security architecture (12 percent of respondents), network engineering and quality assurance (each at 11 percent of respondents).

Figure 18. Primary role within the organization

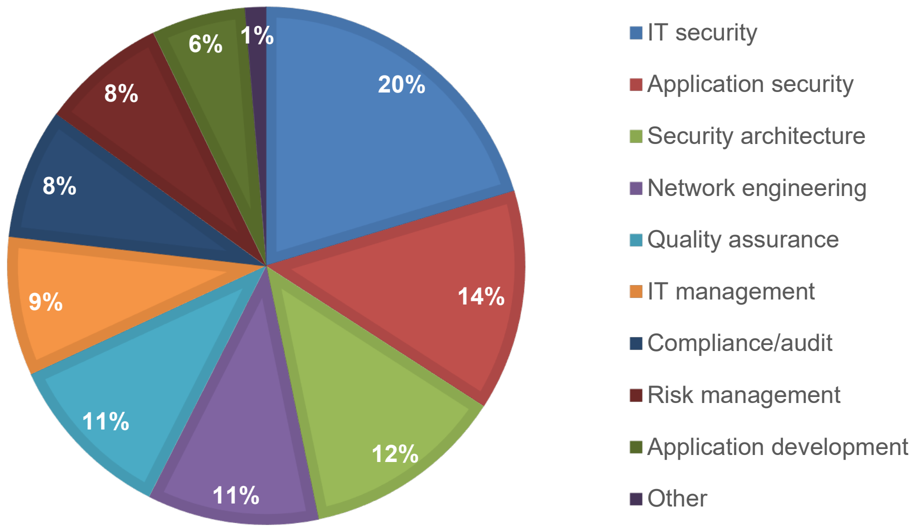
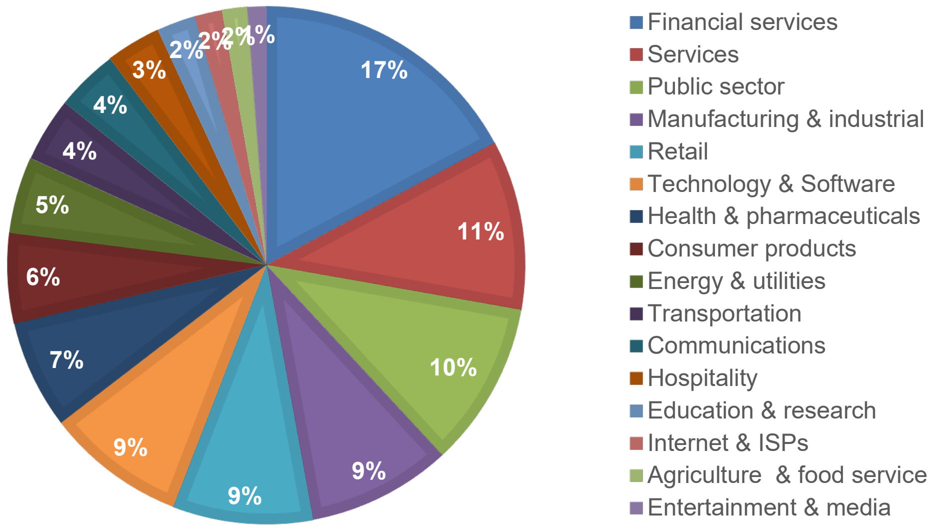


Figure 19 reports the industry focus of respondents' organizations. This chart identifies financial services (17 percent) as the largest industry focus, which includes banking, investment management, insurance, brokerage, payments and credit cards. This is followed by services (11 percent of respondents), public sector (10 percent of respondents), industrial and manufacturing (9 percent of respondents), retail (9 percent of respondents), technology and software (9 percent of respondents), and healthcare and pharmaceuticals (7 percent of respondents).

Figure 19. Primary industry focus



Part 4. Caveats to this study

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 familiar with their organization's PKI. We also acknowledge that the results may be biased by external events such as media coverage. Finally, because we used a web-based collection method, it is possible that non-web responses by mailed survey or telephone call would result in a different pattern of findings.

- 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.

Part 5. Appendix with the detailed audited findings

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 2022.

Part 1. Screening questions

Survey response	US	EMEA	LATAM	Total
Total sampling frame	16,450	13,800	12,981	43,231
Returned surveys	658	482	429	1,569
Rejected surveys	61	54	48	163
Final sample	597	428	381	1,406
Response rate	3.6%	3.1%	2.9%	3.3%

S1. How familiar are you with your organization's security innovation initiatives?	US	EMEA	LATAM	Total
Very familiar	41%	36%	37%	38%
Familiar	40%	40%	34%	38%
Somewhat familiar	19%	24%	29%	23%
No knowledge (stop)	0%	0%	0%	0%
Total	100%	100%	100%	100%

S2. Please check all the activities that you see as part of your job or role.	US	EMEA	LATAM	Total
Managing budgets	46%	38%	50%	45%
Evaluating vendors	51%	46%	42%	47%
Setting priorities	39%	42%	52%	43%
Securing systems	60%	53%	47%	54%
Ensuring compliance	35%	33%	24%	31%
Ensuring system availability	31%	28%	17%	26%
Patching vulnerabilities	44%	53%	61%	51%
Responding to cyber attacks	56%	47%	58%	54%
None of the above (stop)	0%	0%	0%	0%
Total	362%	340%	351%	352%

S3. How influential are you in IT security decision-making regarding investment in technologies and activities?	US	EMEA	LATAM	Total
I am the primary decision-maker	25%	21%	29%	25%
I am one of the primary decision-makers	30%	27%	30%	29%
I influence decision making	45%	52%	41%	46%
I have no influence on decision making (stop)	0%	0%	0%	0%
Total	100%	100%	100%	100%

Part 2. Background on your organization's security strategy

Attributions: Please rate each one of the following statements using the scale provided below each item. **Strongly Agree and Agree response combined.**	US	EMEA	LATAM	Total
Q1a. My organization's cybersecurity practices are innovative with respect to the way technology investments are made.	53%	44%	57%	51%
Q1b. My organization's cybersecurity practices are innovative with respect to the way threats are detected.	63%	58%	55%	59%
Q1c. My organization's cybersecurity practices are innovative with respect to the way risks are accessed.	41%	39%	46%	42%
Q1d. My organization is more likely to purchase technologies and services from companies that are leading edge with respect to innovation.	69%	61%	59%	64%

Q2. How important is implementing a security strategy that supports accepted industry standards and an open ecosystem (e.g. Trusted Platform Module (TPM), Peripheral Component Interconnect Express (PCIe)? Please respond based on a scale from 1 = not important to 10 = highly important.	US	EMEA	LATAM	Total
1 or 2	9%	8%	4%	7%
3 or 4	12%	10%	8%	10%
5 or 6	16%	19%	15%	17%
7 or 8	23%	30%	34%	28%
9 or 10	40%	33%	39%	38%
Total	100%	100%	100%	100%
Extrapolated value	6.96	6.90	7.42	7.07

Q3a. Have you refreshed your security strategy over the last two years (e.g., during the COVID-19 pandemic)?	US	EMEA	LATAM	Total
Yes	60%	49%	45%	53%
No (please skip to Q4)	40%	51%	55%	47%
Total	100%	100%	100%	100%

Q3b. If yes, how have your organization's priorities changed? Please select the top five priorities.	US	EMEA	LATAM	Total
Alignment of goals among security and business leaders	54%	49%	59%	54%
Deployment of cybersecurity compliance, risk management and privacy frameworks	49%	53%	57%	52%
Emphasis on the remote workforce	65%	68%	64%	66%
Expanded use of automation and AI tools for security operations	59%	57%	52%	56%
Heightened awareness among employees about cyber hygiene	50%	54%	60%	54%
Improved communications to customers regarding security issues	41%	39%	36%	39%
Increased accountability among employees	38%	43%	41%	40%
Integration of health and safety considerations as part of security operations	33%	27%	35%	32%
Reliance on security in/from the cloud	58%	52%	49%	54%
Reliance on third parties in achieving security goals	50%	55%	47%	51%
Other (please specify)	3%	3%	0%	2%
Total	500%	500%	500%	500%

Q3c. If yes, what were the main drivers to the changes implemented? Please select the top three drivers.	US	EMEA	LATAM	Total
Ability of employees to telework from home office or other remote location	63%	57%	53%	58%
Cost to implement changes to the post-COVID-19 work environment	47%	43%	44%	45%
Employee loss/turnover	40%	38%	32%	37%
Increase in the frequency and severity of cyber attacks	41%	37%	41%	40%
New regulations and government mandates	30%	31%	34%	31%
Reduction in the infection rate among employees and their families	25%	38%	35%	32%
Supply chain failure	54%	54%	59%	55%
Other (please specify)	0%	2%	2%	1%
Total	300%	300%	300%	300%

Q4. What are the top areas of security innovation within your organization today? Please select only three choices.	US	EMEA	LATAM	Total
Cloud migration	41%	35%	43%	40%
Compliance framework	21%	30%	24%	25%
Education & training	40%	33%	40%	38%
Risk management process	20%	19%	19%	19%
Security analytics	39%	36%	31%	36%
Security at the silicon level	40%	41%	38%	40%
Security automation	41%	42%	39%	41%
Third party assessment	23%	22%	21%	22%
Threat sharing	17%	18%	23%	19%
Virtualization	16%	21%	20%	19%
Other (please specify)	2%	3%	2%	2%
Total	300%	300%	300%	300%

Q5. What are the primary factors considered when making improvements to the security infrastructure? Please select the top five choices.	US	EMEA	LATAM	Total
Hardware requirements	56%	60%	61%	59%
In-house expertise	43%	51%	41%	45%
Installation costs	25%	23%	27%	25%
Interoperability issues	48%	50%	49%	49%
Personnel issues (lack of in-house expertise)	47%	45%	40%	44%
System complexity issues	60%	57%	60%	59%
System effectiveness issues (high false positive)	49%	51%	54%	51%
System performance issues (degradation)	48%	44%	43%	45%
The licensing cost	23%	28%	25%	25%
The maintenance cost	19%	16%	18%	18%
Vendor support issues	41%	38%	45%	41%
Visibility of core systems	38%	37%	34%	37%
Other (please specify)	3%	0%	3%	2%
Total	500%	500%	500%	500%

Q6. Within your organization, who is **most** responsible for security innovation and other related activities? Please select only one choice.	US	EMEA	LATAM	Total
CEO/COO	5%	6%	4%	5%
CIO/CTO	21%	25%	28%	24%
IT Security leader (CISO)	20%	18%	12%	17%
Security leader (CSO)	6%	3%	9%	6%
Security architect	6%	8%	5%	6%
Compliance leader	7%	5%	8%	7%
Security engineer	11%	9%	8%	10%
Risk management leader	3%	5%	7%	5%
Line of business leader	18%	15%	16%	17%
Human resource leader	2%	3%	3%	3%
Operations leader	1%	2%	0%	1%
Other (please specify)	0%	1%	0%	0%
Total	100%	100%	100%	100%

Q7. How has your organization’s budget for security technologies changed in the past 12 months? Please select only one choice.	US	EMEA	LATAM	Total
Significantly increased to deal with an increase in security threats	19%	18%	16%	18%
Increased to deal with an increase in security threats	27%	30%	25%	27%
Somewhat increased to deal with an increase in security threats	17%	13%	21%	17%
No change	20%	22%	26%	22%
Decreased	8%	11%	7%	9%
Significantly decreased	9%	6%	5%	7%
Total	100%	100%	100%	100%

Q8. How important is it for your technology provider to adapt to the changing threat landscape? Please provide your response on a scale from 1 = not important to 10 = highly important.	US	EMEA	LATAM	Total
1 or 2	3%	0%	3%	2%
3 or 4	8%	5%	11%	8%
5 or 6	21%	16%	18%	19%
7 or 8	27%	36%	24%	29%
9 or 10	41%	43%	44%	42%
Total	100%	100%	100%	100%
Extrapolated value	7.40	7.84	7.40	7.53

Part 3. Zero trust and hardware-based security solutions

Q9 Do your organization's current cybersecurity solutions/protocols use hardware-assisted security solutions?	US	EMEA	LATAM	Total
Yes	40%	34%	33%	36%
No, but our organization plans to in the next six months (please skip to Q24)	23%	27%	21%	24%
No, but our organization plans to in the next 12 months (please skip to Q24)	25%	21%	23%	23%
No plans to use (please skip to Q24)	12%	18%	23%	17%
Total	100%	100%	100%	100%

Q10. How much of a priority is hardware and/or firmware-based security in your organization? Please provide your response on a scale from 1 = not a priority to 10 = Very high priority?	US	EMEA	LATAM	Total
1 or 2	0%	0%	2%	1%
3 or 4	2%	1%	9%	4%
5 or 6	13%	10%	8%	11%
7 or 8	40%	43%	36%	40%
9 or 10	45%	46%	45%	45%
Total	100%	100%	100%	100%
Extrapolated value	8.06	8.18	7.76	8.02

Q11a Does your organization apply a Zero-Trust infrastructure strategy as defined in this survey?	US	EMEA	LATAM	Total
Yes	36%	31%	28%	32%
No (please skip to Q13)	64%	69%	72%	68%
Total	100%	100%	100%	100%

Q11b. If yes, does your organization incorporate hardware security capabilities in its Zero-Trust infrastructure strategy?	US	EMEA	LATAM	Total
Yes	54%	50%	48%	51%
No	46%	50%	52%	49%
Total	100%	100%	100%	100%

Please refer to the agreement scale below when responding to the following questions. **Strongly Agree and Agree response combined**	US	EMEA	LATAM	Total
Q12. Zero-Trust cybersecurity models are top-of-mind with the pandemic prompting a surge in remote working and an increased interest in hardware and firmware-level security models.	78%	69%	77%	75%
Q13a. My organization is taking steps to advance security at the hardware level, especially within the cloud infrastructure, data centers, security operation centers (SOC) and edge computing devices.	66%	58%	68%	64%
Q13b. My organization is proactively taking steps to ensure the integrity of data with improved hardware or firmware-level security solutions.	71%	60%	62%	65%
Q13c. In my organization, vulnerability management is enhanced by the rise of hardware or firm-ware security solutions.	73%	63%	68%	69%

Q14. Does your anti-virus software vendor offer hardware-assisted telemetry to detect malware behavior signals below the operating system?	US	EMEA	LATAM	Total
Yes	44%	37%	34%	39%
No	56%	63%	66%	61%
Total	100%	100%	100%	100%

Q15. How important is it for your technology provider to offer hardware-based security solutions and evidence that the components are operating in a known and trusted state? Please respond using the scale from 1 = not important to 10 = highly important.	US	EMEA	LATAM	Total
1 or 2	3%	2%	5%	3%
3 or 4	2%	1%	8%	3%
5 or 6	15%	11%	9%	12%
7 or 8	45%	46%	33%	42%
9 or 10	35%	40%	45%	39%
Total	100%	100%	100%	100%
Extrapolated value	7.64	7.92	7.60	7.71

Q16. How does your organization plan and deploy security and functional updates for basic input output systems (BIOS) and firmware? Please select only one choice.	US	EMEA	LATAM	Total
Manual check against the manufacturer's BIOS release and system configuration	31%	28%	30%	30%
Automated check using industry software/tools	31%	29%	35%	31%
Manual matching of vulnerabilities against configuration database	25%	23%	20%	23%
Use original equipment manufacturer (OEM) emails to determine patches to deploy	13%	20%	15%	16%
Total	100%	100%	100%	100%

Q17. Does your organization deploy any tools or policies to ensure hardware supply chain assurance and transparency?	US	EMEA	LATAM	Total
Yes	58%	50%	47%	53%
No	42%	50%	53%	47%
Total	100%	100%	100%	100%

Q18. In the past 12 months, what percentage of security threats targeted your organization's hardware?	US	EMEA	LATAM	Total
Less than 5%	2%	0%	6%	2%
5% to 10%	5%	8%	5%	6%
11% to 15%	12%	15%	16%	14%
16% to 20%	16%	18%	21%	18%
21% to 30%	21%	23%	26%	23%
31% to 40%	23%	27%	12%	21%
41% to 50%	16%	9%	12%	13%
50%+	5%	0%	2%	3%
Total	100%	100%	100%	100%
Extrapolated value	24.9%	21.5%	22.1%	23.1%

Q19. How much visibility does your organization have into whether its hardware and firmware are operating in a known good state? Please provide a response on a scale from 1 = no visibility to 10 = significant visibility?	US	EMEA	LATAM	Total
1 or 2	12%	11%	15%	13%
3 or 4	11%	8%	7%	9%
5 or 6	23%	20%	18%	21%
7 or 8	30%	25%	35%	30%
9 or 10	24%	36%	25%	28%
Total	100%	100%	100%	100%
Extrapolated value	6.36	6.84	6.46	6.53

Q20. How important is it for a vendor to offer both hardware and software assisted security capabilities? Please provide your response using a 10-scale from 1 = not important to 10 = very important.	US	EMEA	LATAM	Total
1 or 2	6%	4%	3%	5%
3 or 4	5%	7%	8%	6%
5 or 6	9%	18%	18%	14%
7 or 8	32%	40%	39%	36%
9 or 10	48%	31%	32%	38%
Total	100%	100%	100%	100%
Extrapolated value	7.72	7.24	7.28	7.43

Q21. Is hardware part of your organization's endpoint (PC/IoT) security strategy?	US	EMEA	LATAM	Total
Yes	68%	57%	64%	64%
No	32%	43%	36%	36%
Total	100%	100%	100%	100%

Q22. Does your organization take advantage of hardware-enabled accelerators to offset the cost of encryption?	US	EMEA	LATAM	Total
Yes	41%	38%	34%	38%
No	59%	62%	66%	62%
Total	100%	100%	100%	100%

Q23. Do you take advantage of hardware/silicon-enabled accelerators to offset the cost of authenticating endpoints before enabling access?	US	EMEA	LATAM	Total
Yes	31%	21%	24%	26%
No	69%	79%	76%	74%
Total	100%	100%	100%	100%

Part 4. Security updates and authentication

Q24. What is your organization's security update policy relative to affected product generation? Please select only one choice.	US	EMEA	LATAM	Total
Prioritize updates for the latest product generation	44%	39%	41%	42%
Hold updates until vendor provides patches for entire fleet, old and new generations	30%	28%	30%	29%
No policy, we deploy updates as they become available for any given generation	26%	33%	29%	29%
Total	100%	100%	100%	100%

Q25. For client/PC functional and security updates, does your organization prioritize updates that do not require a reboot?	US	EMEA	LATAM	Total
Yes	51%	45%	43%	47%
No	29%	34%	32%	31%
Reboot has no influence in acceptance of an update	20%	21%	25%	22%
Total	100%	100%	100%	100%

Q26. For network/ infrastructure does your organization prioritize updates that do not require a reboot?	US	EMEA	LATAM	Total
Yes	55%	41%	45%	48%
No	27%	38%	34%	32%
Reboot has no influence in acceptance of an update	18%	21%	21%	20%
Total	100%	100%	100%	100%

Q27a. Does your organization authenticate access points in your organization's IT infrastructure?	US	EMEA	LATAM	Total
Yes, all access points	32%	38%	34%	34%
Yes, most access points	23%	26%	25%	24%
Yes, some access points	17%	15%	16%	16%
No (please skip to Q27c)	28%	21%	25%	25%
Total	100%	100%	100%	100%

Q27b If yes, how do you authenticate? Please select one top choice.	US	EMEA	LATAM	Total
Password	30%	45%	41%	38%
Password MFA	21%	23%	24%	22%
Token (OTP)	12%	9%	8%	10%
Biometric	10%	8%	8%	9%
Passwordless	5%	3%	6%	5%
Machine authentication	22%	12%	11%	16%
Other (please specify)	0%	0%	2%	1%
Total	100%	100%	100%	100%

Q27c. If no, is it because of the negative impact on performance?	US	EMEA	LATAM	Total
Yes	56%	43%	45%	49%
No	44%	57%	55%	51%
Total	100%	100%	100%	100%

Q28. How does your organization track the status and security of its device fleet? Please select all that apply.	US	EMEA	LATAM	Total
Track the last microcode/CPU update	58%	49%	47%	52%
Track the last firmware update	39%	41%	38%	39%
Track the supply chain at the platform level	45%	49%	50%	48%
Track the supply chain down to the component level	48%	37%	35%	41%
Track if a processor has been tampered with or modified	36%	33%	27%	33%
Track the authenticity of the platform	27%	29%	21%	26%
Track the discrete Trusted Platform Module (TPM)	30%	34%	31%	31%
Total	283%	272%	249%	270%

Q29a. Do you have visibility into newly disclosed vulnerabilities and patches/updates?	US	EMEA	LATAM	Total
Yes	51%	48%	44%	48%
No (please skip to Q30a)	49%	52%	56%	52%
Total	100%	100%	100%	100%

Q29b. If yes, how many hours does your team spend mapping known vulnerabilities IoT devices?	US	EMEA	LATAM	Total
Less than 1 hour per week	2%	5%	6%	4%
Between 1 to 5 hours per week	6%	12%	9%	9%
Between 6 and 10 hours per week	13%	19%	21%	17%
Between 11 and 20 hours per week	32%	29%	27%	30%
Between 21 and 40 hours per week	24%	23%	22%	23%
More than 40 hours per week	23%	12%	15%	17%
Total	100%	100%	100%	100%
Extrapolated value (hours)	18.37	15.03	15.49	16.57

Part 5. Edge cloud architecture and virtualization technology

Q30a. Does your organization leverage edge to cloud technology solutions?	US	EMEA	LATAM	Total
Yes	69%	63%	59%	64%
No (please skip to Q31)	31%	37%	41%	36%
Total	100%	100%	100%	100%

Q30b. Are you integrating technology and best-known methods to protect against physical attacks (both in the data center and at the edge)?	US	EMEA	LATAM	Total
Yes	63%	58%	54%	59%
No	37%	42%	46%	41%
Total	100%	100%	100%	100%

Q30c. If yes, do you have the security infrastructure in place to address vulnerabilities from the edge to the cloud?	US	EMEA	LATAM	Total
Yes	51%	45%	43%	47%
No	49%	55%	57%	53%
Total	100%	100%	100%	100%

Q31. Does your organization use virtualization technology at the client, endpoint or PC level?	US	EMEA	LATAM	Total
Yes	51%	46%	44%	48%
No (please skip to Part 6)	49%	54%	56%	52%
Total	100%	100%	100%	100%

Q32. Do you consider virtualization enough security, or do you think it's more important to add additional layers of security?	US	EMEA	LATAM	Total
Yes, virtualization is secure enough	44%	43%	49%	45%
No, it's more important to add additional layers of security	56%	57%	51%	55%
Total	100%	100%	100%	100%

Organizational characteristics

D1. What organizational level best describes your current position?	US	EMEA	LATAM	Total
Senior Executive	5%	4%	5%	5%
Vice President	8%	9%	8%	8%
Director	16%	13%	14%	15%
Manager	18%	12%	18%	16%
Supervisor	14%	17%	15%	15%
Technician	30%	33%	29%	31%
Staff	6%	7%	8%	7%
Contractor	3%	4%	3%	3%
Other	0%	1%	0%	0%
Total	100%	100%	100%	100%

D2. What best describes your primary role in the organization?	US	EMEA	LATAM	Total
Application development	5%	7%	6%	6%
Application security	15%	11%	15%	14%
Security architecture	12%	15%	11%	13%
IT management	9%	8%	9%	9%
IT security	20%	22%	19%	20%
Quality assurance	11%	9%	12%	11%
Compliance/audit	9%	8%	7%	8%
Risk management	7%	8%	9%	8%
Network engineering	11%	10%	11%	11%
Other	1%	2%	1%	1%
Total	100%	100%	100%	100%

D3. What industry best describes your organization's industry focus?	US	EMEA	LATAM	Total
Agriculture & food service	1%	2%	2%	2%
Communications	3%	5%	4%	4%
Consumer products	5%	6%	6%	6%
Defense & aerospace	1%	0%	0%	0%
Education & research	3%	2%	2%	2%
Energy & utilities	5%	6%	3%	5%
Entertainment & media	2%	1%	0%	1%
Financial services	18%	16%	17%	17%
Health & pharmaceuticals	7%	8%	5%	7%
Hospitality	2%	4%	5%	3%
Internet & ISPs	2%	1%	2%	2%
Manufacturing & industrial	9%	8%	10%	9%
Public sector	10%	11%	10%	10%
Retail	9%	8%	9%	9%
Services	10%	10%	12%	11%
Technology & Software	9%	8%	9%	9%
Transportation	4%	4%	4%	4%
Other	0%	0%	0%	0%
Total	100%	100%	100%	100%

For more information about this study, please contact Ponemon Institute by sending an email to research@ponemon.org or call at 1.800.887.3118.

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.