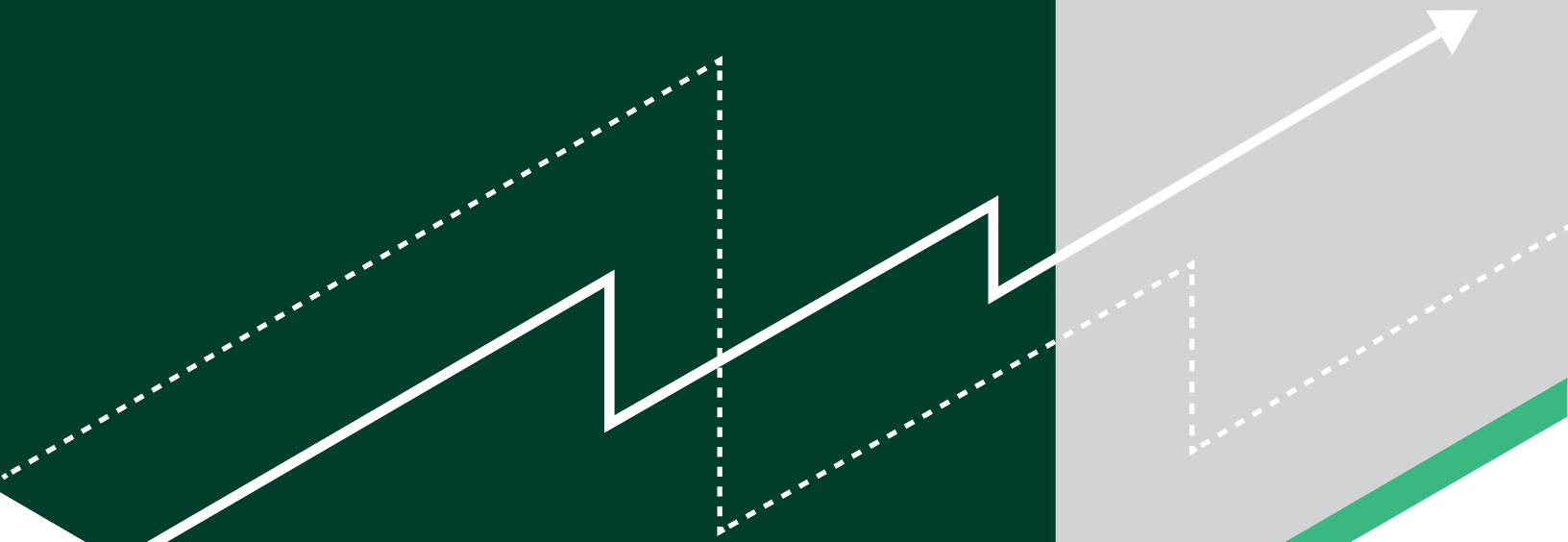
A Forrester Consulting
Thought Leadership Paper
Commissioned By HP

June 2021

Balance Endpoint Protection And Productivity Through Zero Trust



FORRESTER®

Table Of Contents

Project Director:
Madeline Harrell,
Market Impact Consultant

Contributing Research:
Forrester's Security & Risk research group

FORRESTER®

Executive Summary

As companies adapt to an increasingly remote workforce, security leaders are struggling with an explosion of devices requiring sensitive corporate data access outside of the traditional security perimeter. Attackers leverage gaps in protection measures exposed by this expanding attack surface to move laterally through corporate networks and compromise sensitive assets. To limit this risk, companies must adopt a Zero Trust (ZT) strategy for endpoint devices that eliminates default assumptions of trust between endpoint hardware, apps, data, and network resources, while continuously evaluating risk for access control decisions.

By adopting a Zero Trust strategy, security and risk (S&R) professionals will more effectively manage and compartmentalize risk associated with providing sensitive corporate resource access to remote workers and their devices. This requires coordination between the different endpoint threat prevention and detection technologies, including native OS security and hardware security measures. Ultimately this puts S&R professionals in a better position to handle new and existing threats while helping to balance security with employee experience (EX).

HP commissioned Forrester Consulting to evaluate the potential benefits and challenges of a Zero Trust approach to endpoint security. Forrester conducted an online survey of 607 director-level and above IT security professionals with responsibility over network security/hardware security to uncover these trends.

KEY FINDINGS

- **Companies are aware of the growing importance of securing their data, devices, and networks wherever work gets done.** Though incident response is still a high priority, with 79% of respondents indicating that threat detection is a critical or high priority, companies are taking a more proactive approach to endpoint security through threat prevention and actively securing data as part of a mobile security posture.
- **There is a strong case for Zero Trust to combat lateral movement of malicious actors and subsequent breach of company/employee data.** In the past year, more than one-third (34%) of respondents experienced a compromise of company data from lateral movement, a homeworker device, or an overall increase in security incidents.
- **A Zero Trust approach not only helps prevent and detect data breaches but has business and EX benefits as well.** Nearly a third of respondents indicated that without adopting a Zero Trust strategy, they have a poor security culture in the workplace. Not only does adopting ZT reduce overall risk, but it also increases employee productivity.

Companies Must Secure Endpoints As Part Of A Zero Trust Security Strategy

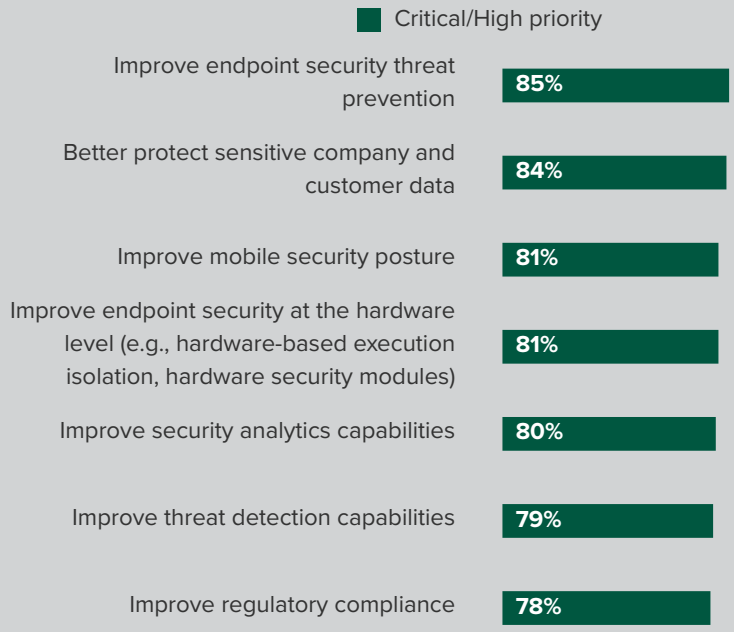
As the number and type of endpoints open to lateral movement by malicious actors increase, so too does risk.

› **Companies are increasingly focused on endpoint security, especially at the hardware level.** There is a strong focus on the protection of company and customer data, and endpoints are the spokes enabling access to all of that infrastructure and data. Eighty-five percent of respondents said that improving endpoint security threat prevention is a high or critical priority for the next 12 months, followed by better protecting sensitive company and customer data. This includes employee-provisioned devices, employee devices, and any device connected to home networks where remote employees are working (e.g., Internet of Things [IoT], printers, etc.). Improving endpoint security at the hardware level was also a key priority (81%), showing that endpoint security and securing hardware are top of mind for IT/security teams (see Figure 1).

More than one-third (34%) experienced a compromise of company data from lateral movement, a homeworker device, or an overall increase in security incidents.

Figure 1

"To what extent is your IT organization prioritizing the following information/IT security goals and initiatives over the next 12 months?"



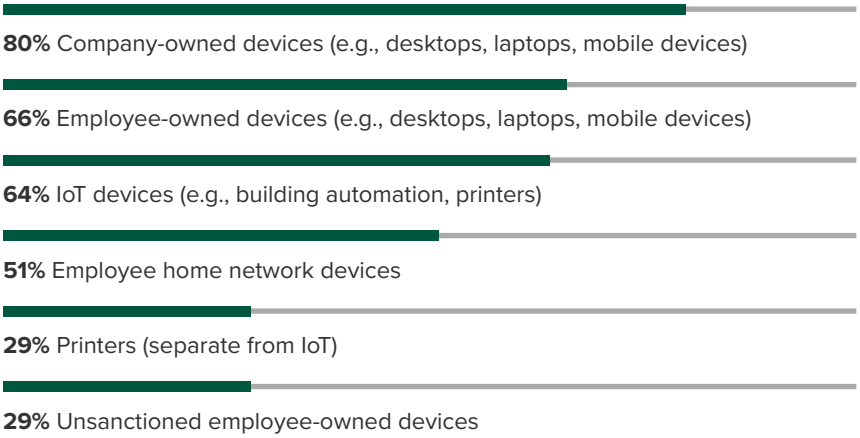
Base: 607 director-level and above IT security professionals with responsibility over network security/hardware security at SMB/midmarket and enterprise companies in NA, EMEA, and APAC
Note: Top 7 of 13 responses shown
Source: A commissioned study conducted by Forrester Consulting on behalf of HP, April 2021

FORRESTER®

- **Threats via homeworkers are putting enterprises at increased risk.** The rapid increase in remote and hybrid workforces has expanded most companies' attack surfaces, highlighting a need to secure all endpoints with access to company networks, including at-home Internet of Things devices, and printers. Eighty percent are securing company-owned devices, 66% are securing employee-owned devices, yet only 64% are securing Internet of Things devices (including printers) (see Figure 2). The reality is that based on the steady increase in attacks and breaches, these should all be closer to 100%. Companies can no longer afford to lag behind in securing employee and IoT endpoints — these have become part of the attack surface due to the increase in remote working.
- **While companies have been adjusting to the increase in remote workers, malicious actors wasted no time in targeting companies with weaknesses in their endpoint security.** Over the past year, more than one-third (34%) experienced a breach of company data from lateral movement or a homeworker device — or experienced an overall increase in security incidents. 32% experienced a breach of company data involving an employee-owned device. Zero Trust is imperative to combat malicious actors moving through companies' environments and subsequent compromise of company and employee data.

Figure 2

"Which endpoints do you include to be secured as part of your endpoint security strategy?"



Base: 607 director-level and above IT security professionals with responsibility over network security/hardware security at SMB/midmarket and enterprise companies in NA, EMEA, and APAC
Source: A commissioned study conducted by Forrester Consulting on behalf of HP, April 2021

Internal And Technical Challenges Can Hinder Adoption Of A Zero Trust Approach

IT teams see the value in adopting a Zero Trust approach to endpoint security but face internal and technical challenges when trying to jump-start their adoption journey. Companies admit to struggling to protect their endpoints with their current security software. Forty-seven percent of companies indicate that the efficacy of their current endpoint security software is inadequate in the face of today's threats (see Figure 3). Furthermore, there are not enough barriers to prevent attackers from moving laterally between endpoints, servers, or applications. While there is a strong case for adopting a ZT approach, getting executive leadership on board can still be a struggle:

- **While ZT is the clear answer to endpoint security struggles, IT teams face organizational roadblocks.** IT decision-makers state that when it comes to their approach to endpoint security, there is too much friction between IT and security teams (43%). Forty-five percent of IT decision-makers state that they lack the executive buy-in to begin ZT implementation. What does leadership believe they stand to lose by adopting ZT? Leadership believes that the adoption of Zero Trust would disrupt employee workflows, they don't have the budget for an implementation partner, and they lack the processes to handle it internally.
- **ZT adoption is not without its technical challenges.** Even looking past the organizational challenges, companies still aren't sure where to start once they begin their adoption journey. The top technical challenges keeping IT teams from easily adopting ZT are the need to improve identity access management capabilities and the lack of compliance expertise in-house. Forty-two percent say they just aren't sure where to start or stop adoption. Whether they adopt new technology that provides a built-in, user-friendly implementation experience or pay for expertise via a third-party service, IT teams can benefit from being given a roadmap to ZT. There is no need to reinvent the ZT wheel.
- **The employee experience suffers-and so too does the business — without Zero Trust.** While executive leadership fears disrupting employee workflows, over half of respondents (57%) state that prior to adopting ZT, too much employee time was being spent on security-related activities. Whether they are wasting time trying to log in to a VPN or getting the right code in the right place for a two-factor authentication, too much employee time is spent on security. With companies cracking down on security for their expanding attack surface, employees also face a lack of autonomy in choosing where they work (37%) and whether they can bring their own device (56%). As companies return to the office or move to a more hybrid model of in-office/at-home work, the ability to offer employees flexibility and autonomy around where and how they work will only increase in value.

Figure 3

"What are your biggest challenges with your current approach to endpoint security?"

47% The efficacy of our current endpoint security software is inadequate for today's threats

43% There aren't enough barriers to prevent attackers from laterally moving between endpoints and/or applications

43% There is too much friction between IT and security teams

37% Our security technologies and policies are too static to handle evolving workforce risks

"What employee experience challenges did you face prior to adopting a Zero Trust approach?"

57% Too much employee time spent on security-related activities (e.g., VPNs, 2FA)

56% Lack of flexibility around bring-your-own-device (BYOD)

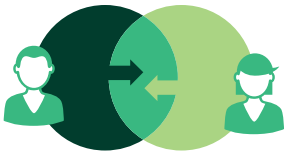
37% Lack of employee autonomy to choose where they work

35% Low employee satisfaction

Base: 607 director-level and above IT security professionals with responsibility over network security/hardware security at SMB/midmarket and enterprise companies in NA, EMEA, and APAC
Note: Top 4 responses shown
Source: A commissioned study conducted by Forrester Consulting on behalf of HP, April 2021

Zero Trust Successfully Prevents And Detects Threats And Enables Employees

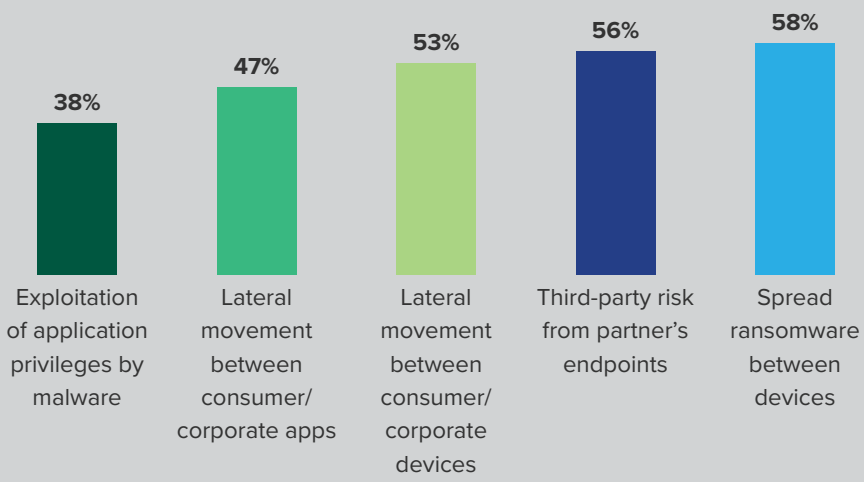
While some IT teams scramble to educate executive teams on the indelible benefits of Zero Trust while preparing to enable an increasingly remote or hybrid workforce, early and current adopters are already reaping the benefits of ZT. A Zero Trust approach to endpoint security allows IT teams to not only detect current threats to bring them to resolution, but it also enables teams to act proactively to prevent breaches before they happen. Without as many potential threats to protect against, IT and security teams can spend more time being productive rather than wasting time on extraneous security activities. With this added freedom for increased productivity, ZT also offers employees the increased autonomy and flexibility they crave, all while bumping companies' employee satisfaction ratings.



- **A ZT approach would address top technology concerns, such as preventing lateral movement of malicious actors.** After adopting ZT for endpoints, companies have experienced or would expect to experience an improved ability to not only detect but also prevent data breaches. In fact, more than half of respondents express that a ZT approach for endpoints would specifically address the spread of ransomware between devices, as well as third-party risk from partner's endpoints (56% and 58%, respectively). When it comes to lateral movement between consumer/corporate applications and devices, Zero Trust also helps to stop island-hoppers in their tracks (53% and 47%, respectively) (see Figure 4).

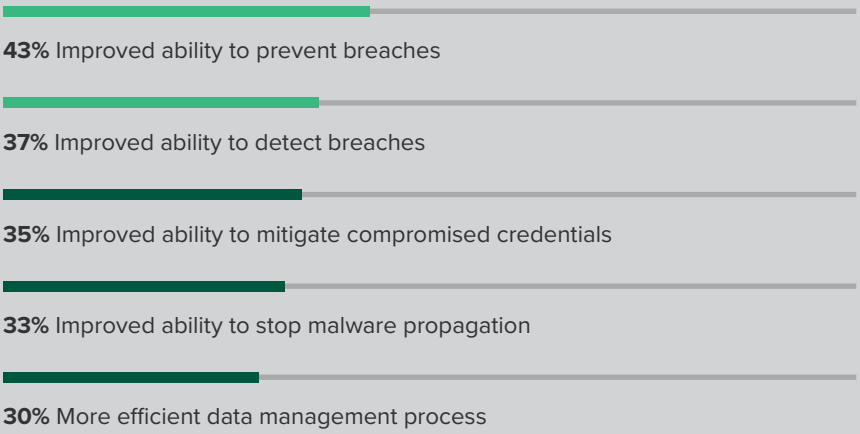
Figure 4

"What threats could specifically be addressed by a Zero Trust approach for your endpoints?"



More than 50% are confident that ZT would address lateral movement risk from third-party partner endpoints and ransomware.

"What technology benefits would you expect to see or have you seen from adopting a Zero Trust security framework?"



Base: 607 director-level and above IT security professionals with responsibility over network security/hardware security at SMB/midmarket and enterprise companies in NA, EMEA, and APAC
Note: Top 5 responses shown
Source: A commissioned study conducted by Forrester Consulting on behalf of HP, April 2021

FORRESTER®

- **ZT offers increased employee autonomy and satisfaction.** While ZT offers a more robust way to protect all of your endpoints, it also helps companies take care of their employees. With the technological benefits of decreased lateral movement between devices and securing employee-owned devices, employees can be free to work from anywhere and enjoy their sought-after increase in autonomy (54%). With less employee time being spent on security-related activities like logging in to sluggish VPNs and being authenticated, they can spend more time on innovative work. Overall, 57% of companies expect/have experienced an increased overall employee satisfaction after adopting a Zero Trust approach (see Figure 5).
- **ZT is good for business: it increases employee productivity while reducing overall risk.** Zero Trust gives companies peace of mind around their ability to prevent and detect attacks by malicious actors by cutting lateral movement at the source; it also gives employees the time and freedom they need to be productive and satisfied in their roles. But in a more general sense, ZT provides companies with a change in their organization's security culture. Fifty-one percent say adopting a ZT security framework helps increase prioritization of security at their company, followed closely by increased productivity (48%) and reduced overall risk (47%). A ZT approach can reduce time spent on typical administrative security tasks and give back more time to focus on preventing and detecting high-priority intrusions. Nearly 40% also say it helped them garner increased stakeholder buy-in, reduce cost on compliance initiatives, and increase organizationwide agility. Adopting a Zero Trust framework gives companies a new more effective strategy for protecting their customer and company data, enabling happier, more productive employees, and giving security the room to prioritize maturing overall security functions .

Figure 5

"What employee experience benefits have you experienced/would you expect from adopting a Zero Trust approach?"

57% Increased overall employee satisfaction

54% Improved ability to work from anywhere/increased employee autonomy

53% Less employee time spent on security-related activities (e.g., VPNs, 2FA)

48% More flexibility around BYOD

41% Improved company security culture

31% Improved employee engagement with techology through better UX

"What business benefits would you expect to see or have you seen from adopting a Zero Trust security framework?"

51% Increased prioritization of security

48% Increased organizationwide productivity

47% Reduced overall risk

39% Increased stakeholder buy-in

39% Reduced cost on compliance initiatives

39% Increased organizationwide agility

38% Reduced capital and/or operational expenditures on security

Base: 607 director-level and above IT security professionals with responsibility over network security/hardware security at SMB/midmarket and enterprise companies in NA, EMEA, and APAC
Source: A commissioned study conducted by Forrester Consulting on behalf of HP, April 2021

Key Recommendations

Forrester's in-depth survey of S&R decision-makers about endpoint security yielded several important recommendations:

Take a prevention-first approach to reduce security complexity. Adopt threat prevention tools focused on reducing your attack surface. This will lower your security complexity and improve your overall endpoint security resilience. These include hardware security, anti-exploit technologies, app security, data security, and secure configuration management. Each of these lowers the likelihood an attacker will compromise an employee endpoint, creating extra work for incident response teams.

Identify and segment your sensitive data and apps across all employee endpoints. Your endpoint security policies and standards must support a Zero Trust strategy, aligning risk with defined levels of data and app segmentation. This requires visibility and control at the endpoint hardware and software layers.

Your threat analysis should correlate event data gathered from multiple endpoint layers. Your endpoint protection layer must cover all enterprise hardware, software, and user activities, correlated with external threat intelligence, to identify and block malicious activity. Enriching behavioral analysis with security telemetry pulled from the operating system and hardware layers increases overall precision and helps unify native security capabilities with third-party products.

Focus on delivering a strong employee experience through Zero Trust adoption. Zero Trust doesn't mean eliminating trust with your employees. In fact, when properly utilized, Zero Trust can enable more employee freedom to work in the way they want with fewer restrictions compared to a draconian blanket policy with no flexibility. This requires precise understanding of real-time risk relative to the user, device, apps, and data, with flexible controls based on the detected level of risk. A balance can then be achieved, only restricting employees when it's appropriate and thereby enabling faster, safer access to sensitive work resources.

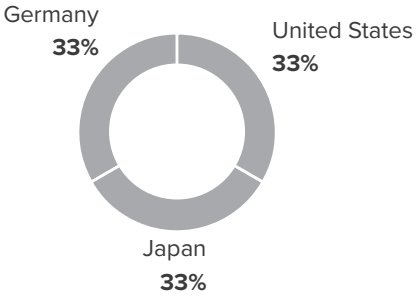
Build a strategic endpoint security roadmap looking out three to five years. Bring together key stakeholders between your security and IT operations teams involved in protecting and managing end-user devices at least once a year, and evaluate your current investments in endpoint security technologies. Identify overlap between your third-party and paid security tools, both current overlap and potential future overlap based on the current level of maturity and commoditization of the capabilities in question. For example, full disk encryption, antimalware, and application control features are enterprise-ready and able to replace third-party technologies today. Meanwhile, other capabilities such as host firewall, execution isolation, and secure configuration management might be poised for future replacement.

Appendix A: Methodology

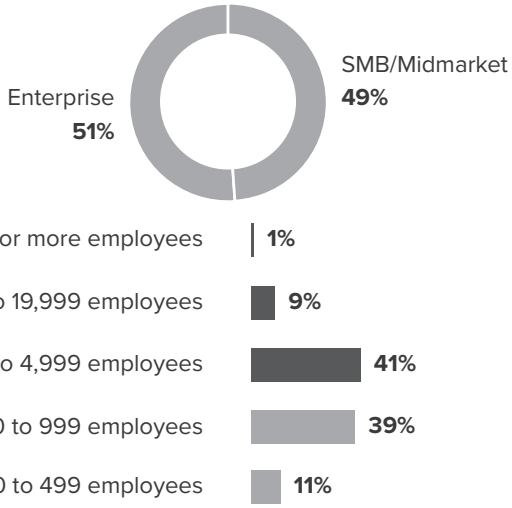
In this study, Forrester conducted an online survey of 607 director-level and above IT security professionals with responsibility over network security/hardware security at SMB/midmarket and enterprise companies in NA, EMEA, and APAC to evaluate their adoption of a Zero Trust approach to endpoint security. Questions provided to the participants asked about the current state of their endpoint security, the challenges they face with endpoint security, and the benefits of adopting Zero Trust. The study began in March 2021 and was completed in April 2021.

Appendix B: Demographics/Data

COUNTRIES



COMPANY SIZE

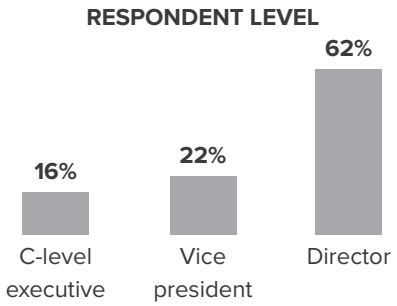


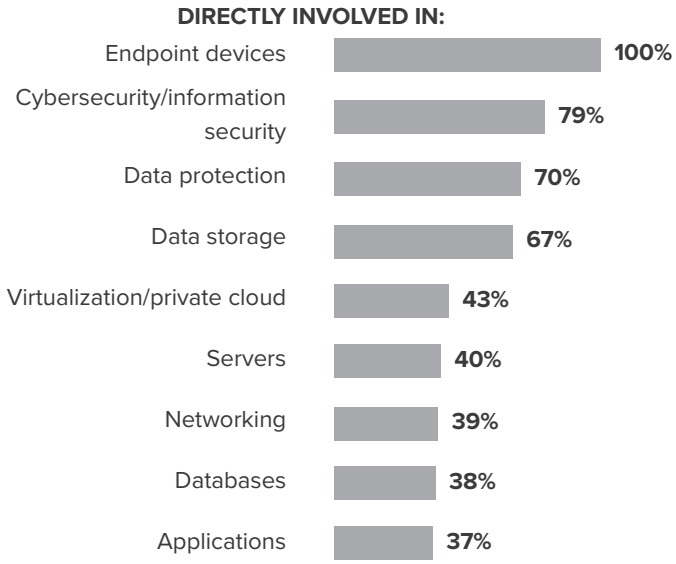
INDUSTRY

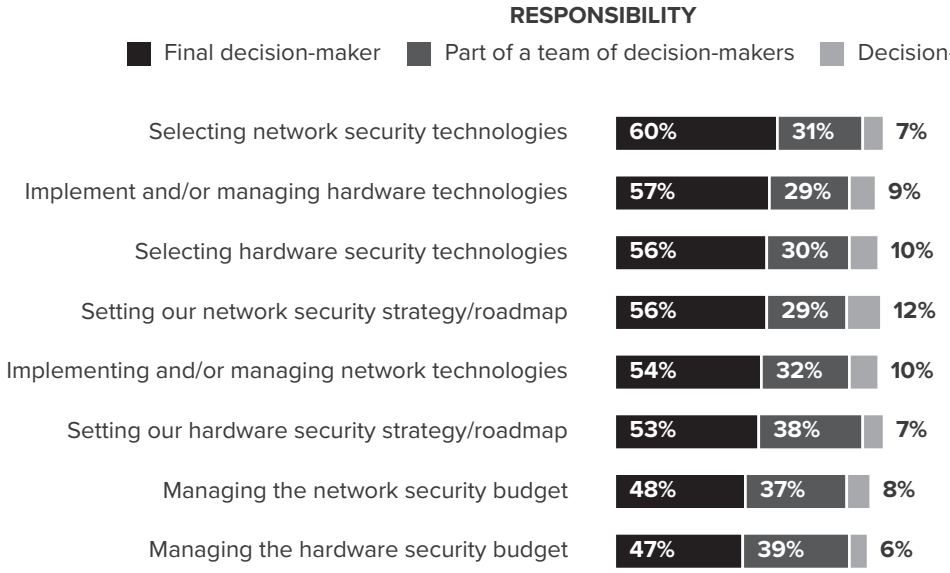
Technology and/or technology services	12%
Media and/or leisure	9%
CPGs and/or manufacturing	9%
Manufacturing and materials	8%
Financial services and/or insurance	7%
Telecommunications services	6%
Agriculture, food, and/or beverage	6%
Retail	5%
Healthcare	5%
Construction	5%
Business or professional services	5%
Transportation and logistics	4%
Energy, utilities, and/or waste management	4%
Electronics	4%
Chemicals and/or metals	4%
Travel and hospitality	2%
Advertising and/or marketing	2%
Legal services	1%
Education and/or nonprofits	1%
Consumer services	1%

Base: 607 director-level and above IT security professionals with responsibility over network security/hardware security at SMB/midmarket and enterprise companies in NA, EMEA, and APAC
Source: A commissioned study conducted by Forrester Consulting on behalf of HP, April 2021

FORRESTER®







Base: 607 director-level and above IT security professionals with responsibility over network security/hardware security at SMB/midmarket and enterprise companies in NA, EMEA, and APAC
Source: A commissioned study conducted by Forrester Consulting on behalf of HP, April 2021

FORRESTER®