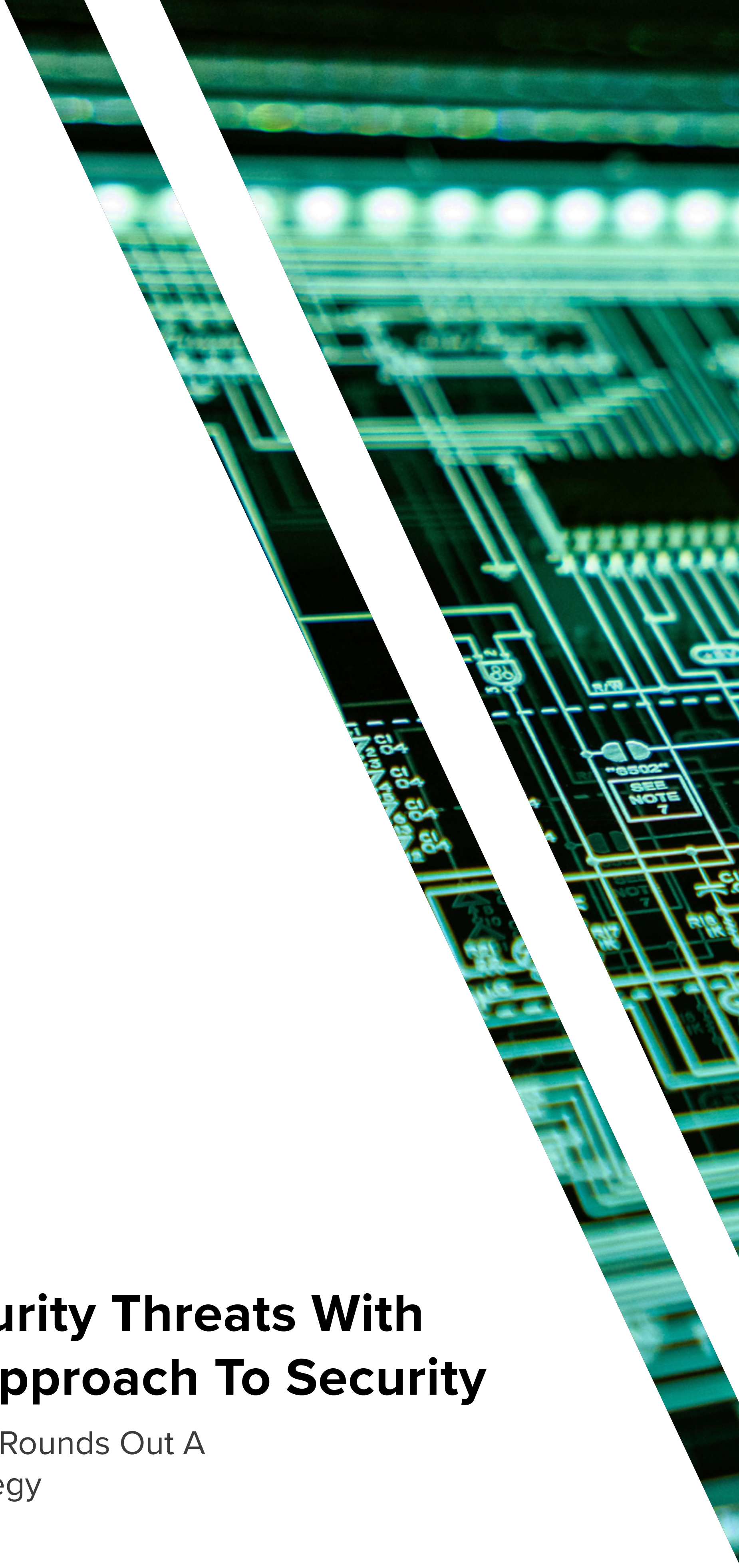
FORRESTER®



Tackle Cybersecurity Threats With An End-To-End Approach To Security

How PC Hardware Security Rounds Out A Holistic Cybersecurity Strategy

A FORRESTER CONSULTING THOUGHT LEADERSHIP PAPER COMMISSIONED BY INTEL, SEPTEMBER 2022

Table of Contents

Project Team:
Ana Brzezinska,
Senior Market Impact Consultant

Madeline Harrell,
Market Impact Consultant

Andrea Mendez Otero,
Market Impact Associate Consultant

Contributing Research:
Forrester's Technology Architecture &
Delivery research group

ABOUT FORRESTER CONSULTING

Forrester Consulting provides independent and objective research-based consulting to help leaders succeed in their organizations. Ranging in scope from a short strategy session to custom projects, Forrester's Consulting services connect you directly with research analysts who apply expert insight to your specific business challenges. For more information, visit forrester.com/consulting.

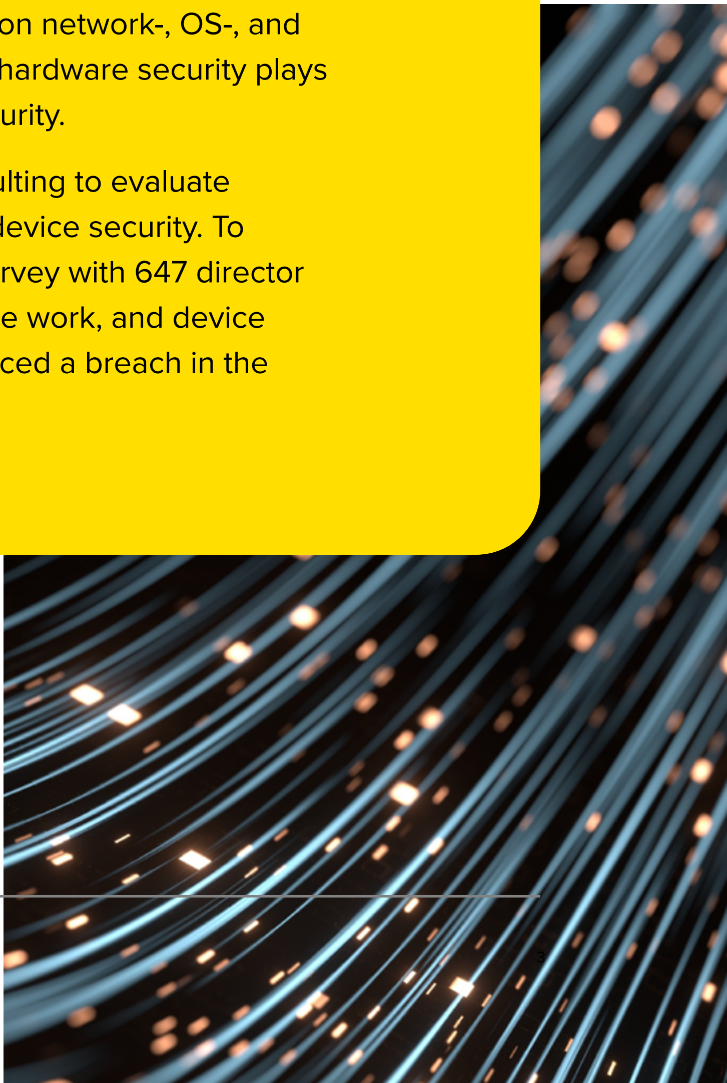
Executive Summary

Crafting a holistic cybersecurity strategy is challenging for any organization, especially in the age of hybrid work and constant threat evolution.[1] While companies need a holistic cybersecurity strategy that protects all aspects of the business, endpoints are some of the most crucial but difficult-to-protect assets.

Hardware — in this case, foundational pieces of a PC that lie below the OS in combination with the layer provided by the system vendor — and the security tools and processes that protect it must evolve alongside other aspects of a holistic security strategy. From form-factor multiplication to OS proliferation and a slew of complex endpoint management and security tools, the expansive nature of hardware security for devices makes comprehensive endpoint security a challenge for even the most sophisticated organizations.

The savviest enterprises understand that an end-to-end approach that includes hardware, network, OS, and endpoint security software is critical to a comprehensive endpoint security solution. However, most enterprises today don't follow this advice. Too often they focus on network-, OS-, and policy-level protections while ignoring the role that hardware security plays in establishing a strong foundation for endpoint security.

In March 2022, Intel commissioned Forrester Consulting to evaluate perceptions and strategies around hardware-level device security. To explore this topic, Forrester conducted an online survey with 647 director or higher-level technology selection strategy, remote work, and device investment decision-makers at organizations that faced a breach in the past 12 months.



Key Findings

Companies take cybersecurity seriously but struggle to address it holistically. Respondents indicate network security as their highest priority, with software close behind. But very few currently prioritize hardware security in favor of more easily approachable aspects of their security strategy, like cloud and privacy.

Companies are prioritizing device-level security but have difficulty crafting a holistic strategy that improves overall security posture. Our research shows that although hardware-level protections can protect companies from the increasing frequency of breaches, complexity is a hurdle and knowledge is limited.

Effectively prioritizing hardware-level security drives employee experience, revenue, and CX benefits. Including hardware-level security as part of a larger end-to-end security strategy can improve the employee experience, thus impacting customer experience and bottom line.

PC Cybersecurity Without Hardware Protections: Incomplete At Best And Dangerous At Worst

Cybersecurity is a top priority among IT decision-makers (ITDMs), especially as companies adjust to hybrid work.[2] But far too many respondents retain a legacy network-centric view of security, emphasizing a traditional perimeter-based approach that is ineffective in a world where data increasingly resides outside the corporate network.[3] Unfortunately, this means that ITDMs often neglect other areas of the cybersecurity stack, such as client hardware-level security, and focus on network and software security. Just 67% of respondents said hardware-level security is a priority.

The good news is that this is changing. Respondents understand the need to adjust their security strategies to include hardware-level protections rooted deep in silicon for an in-depth defense, but the complexity of changing strategies keeps them in the dark and vulnerable to continued breaches. In surveying 647 director or higher-level technology selection strategy, remote work, and device investment decision-makers at organizations that faced a breach in the past 12 months, we found that despite the growing importance of hardware security among leaders today, most organizations don't do it well, impacting:

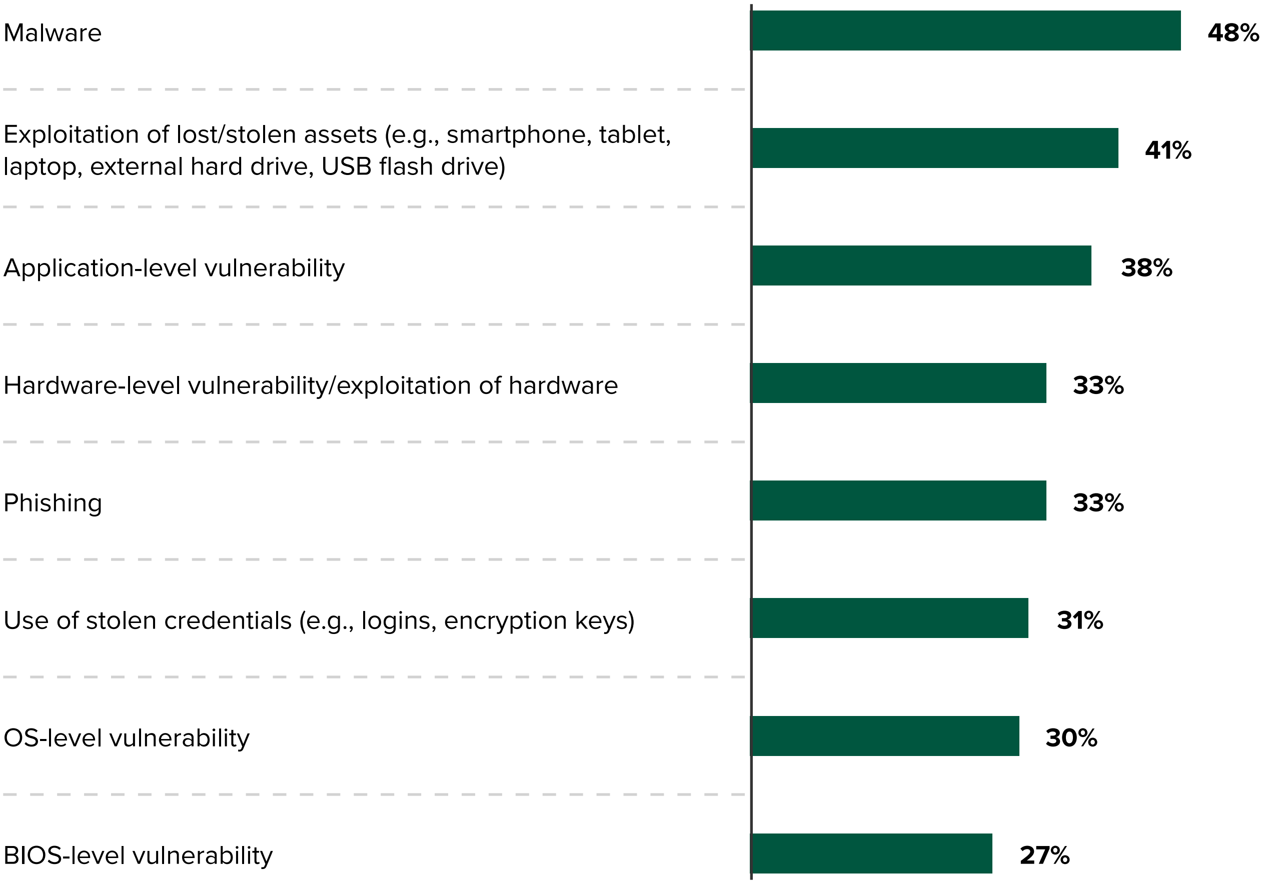
- **Customer and brand trust.** Due to continued security breaches — often due to vulnerabilities in hardware — customers are losing trust in organizations. More than one-third (34%) of respondents reported decreased customer trust, 31% reported decreased trust of their partner ecosystems, and 28% reported loss of customers because of breaches.
- **Breach recovery time and cost.** Recovering from a breach takes up valuable time and resources, costing an average of 4.2% of total revenue and about 1,187 hours to recover. While there are many enablers of breaches, 41% of respondents indicated that breaches were due

On average, breaches cost firms 4.2% of their revenue and take 1,187 hours to recover.

to exploitation of endpoint assets (see Figure 1). Many breach targets were physical endpoints, with computers topping the list. Breaches not only are security issues but also affect business continuity and hamper employees' efforts to get back to work and be productive. Ransomware and malicious code also keep ITDMs up at night; respondents listed malicious code injection protection as the most important to overall endpoint security capabilities.

Figure 1

"You indicated earlier that your organization faced a breach within the past 12 months. How was a breach enabled in your organization?"

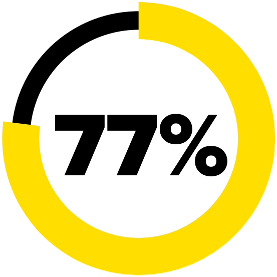


Base: 647 director or higher-level technology selection strategy, remote work, and device investment decision-makers at organizations that faced a breach in the past 12 months
Source: A commissioned study conducted by Forrester Consulting on behalf of Intel, March 2022

- **Employee experience and productivity.** Continued security breaches and extensive auditing after those breaches affect employees' productivity. Forty-one percent of respondents reported increased auditing frequency due to breaches, while another 39% reported employees' decreased productivity or disruptions to productivity due to the same.
- **Key cybersecurity goals.** Due to past endpoint breaches — and their impact on employees' productivity — respondents know hardware-level security is important and worth the effort to keep it functioning properly. This is spurring them to prioritize it in the next 12 months. Furthermore, post-breach, they are working to prevent more attacks with security investments. Forty percent of respondents said that as a result of a breach, they invested in hardware-level security. But nearly two-thirds agreed they are still at risk with their current hardware approach, indicating a need to take a more holistic approach to device-level security.

Despite Its Importance, PC Hardware Security Has Perception Issues

Despite respondents increasingly prioritizing hardware in their security strategy, most still face hardware vulnerabilities because many ITDMs lack awareness of the role that hardware plays in the overall security posture. For example, many understand that hardware is the root of trust for PC security, but they don't understand how it connects to the other segments of their security strategy, like the network. When looking for device-level security, silicon-layer protections are a necessity for in-depth defense. And if companies don't choose the right platform, they aren't protected. Companies struggle with hardware security today because of:



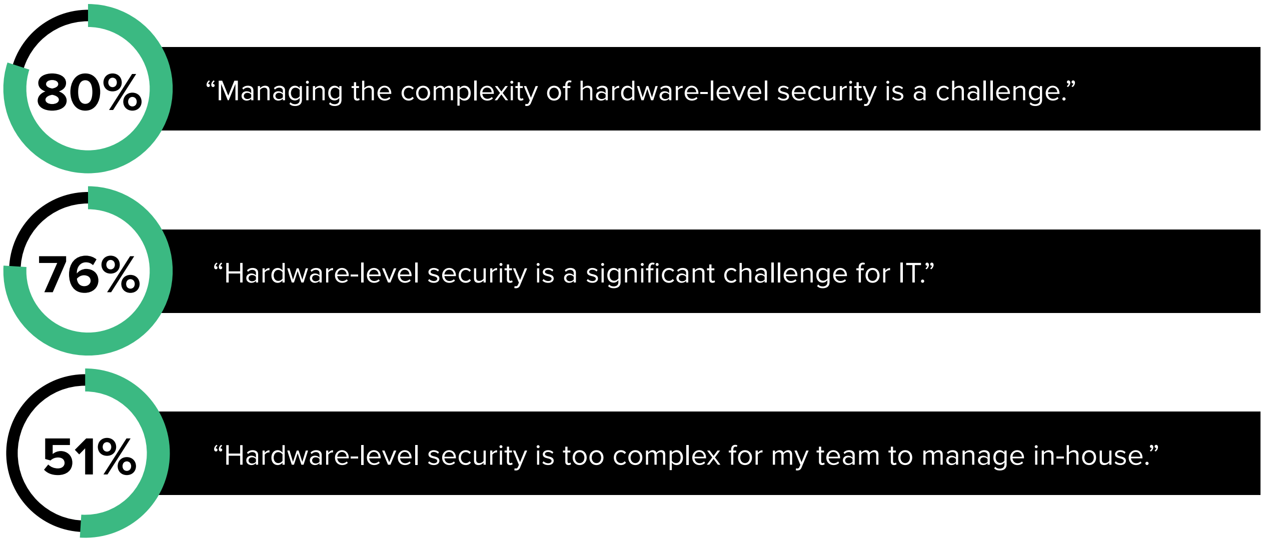
agree hardware-level security is worth the effort to keep it functioning properly.

- **Complexity.** Companies struggle to tackle the complexity of hardware security, admittedly: 76% of respondents agreed it's a challenge, and 51% agreed it's too complex for their team to manage in-house without relying on third-party providers. That's even with about two teams per organization managing endpoint security. More than a quarter of respondents indicated difficulty integrating their many endpoint security tools and managing a mixed environment of BYO and corporate-owned devices. Furthermore, managing hardware-level security complexity was the top challenge among endpoint security activities for IT teams (see Figure 2). Because a holistically effective strategy addresses the sum of all endpoint security activities, ITDMs can struggle with crafting it. There is also a misconception about the complexity of hardware and software security alignment. ITDMs need to select security capabilities that best fit their organization's unique needs and preoptimized software that best meets those needs.

- **Management and resources.** IT department challenges in endpoint security largely include device management and resources, like the difficulty of managing endpoint and security technologies and a lack of resources like staff, time, skills, and executive support. For example, it's common for organizations to have multiple products to manage end-user computing devices, deploy software packages, and patch vulnerabilities.[4] And justifying spending more time and money on hardware investments that remain largely unseen from users' perspective is difficult.

Figure 2

"Please rate your level of agreement with the following statements around hardware-level security."



Base: 647 director or higher-level technology selection strategy, remote work, and device investment decision-makers at organizations that faced a breach in the past 12 months
Source: A commissioned study conducted by Forrester Consulting on behalf of Intel, March 2022

- **Departmental alignment across IT and LOB.** Not everyone is on the same page about the importance of hardware security. Eighty-three percent of IT respondents said that improving hardware-level security is a high or critical priority for the next 12 months, but that is likely because IT knows the most about the benefits of device-level security. Line-of-business (LOB) decision-makers — with budget purview — must also identify how investments in device-level security positively impact the business. But hardware-level security matters to everyone, not just IT.[5] For respondents who only purchase end-user devices via IT, the main impact of breaches was employees' decreased productivity and increased auditing frequency. Among respondents from organizations that allow LOBs to make purchasing decisions, increased auditing frequency was a top issue, followed by significant monetary impact. IT and LOBs are seeing the negative impact of breaches, whether they're productivity-related or a direct attack on the bottom line.

- **General awareness.** Companies struggle to understand how targeted hardware investment helps OS and endpoint security software policy configuration for different classes of security software. Respondents ranked hardware root of trust and silicon-assisted security as the least important components of their endpoint security strategy, below encryption, cloud services, and privacy controls. This indicates a focus on other parts of their security strategies, pushing hardware to last on the list. This is likely due to not understanding how to integrate hardware security as part of a larger overall endpoint security strategy. So the question becomes: “What role does silicon-assisted security play in overall system security, and how can you strengthen that connection?”

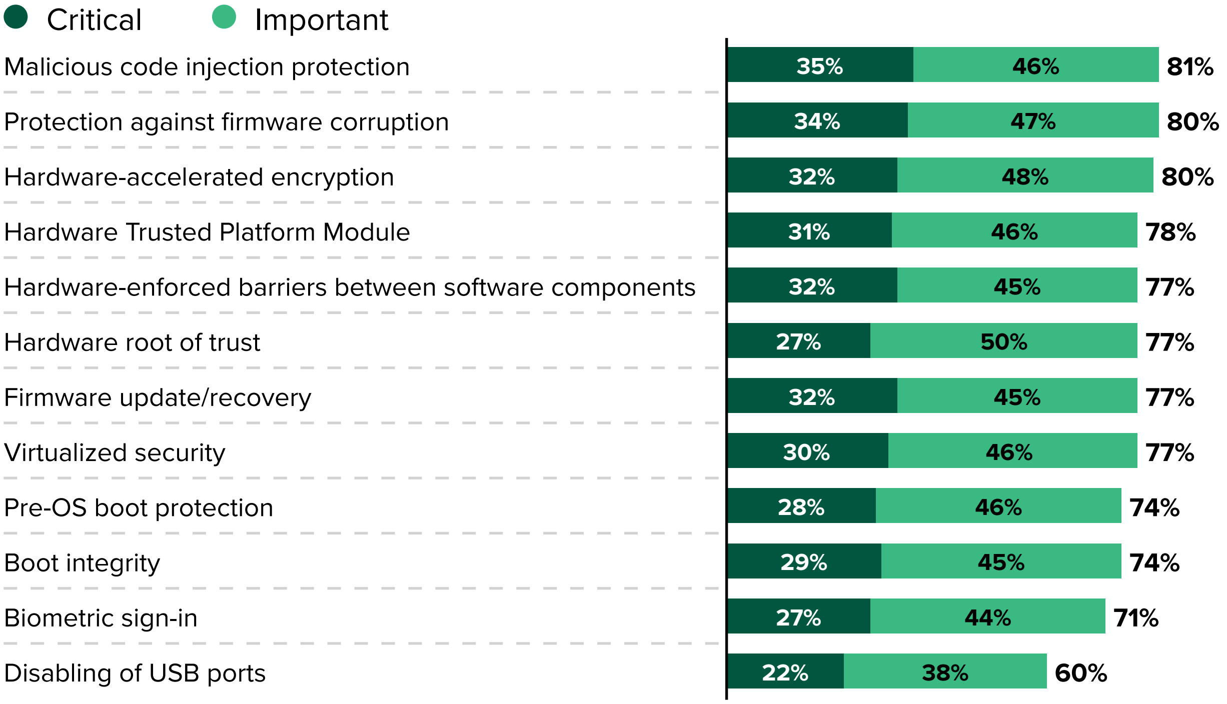
Enlist The Help Of Device-Level Security To Improve The Effectiveness Of Your Entire Security Stack

Despite the challenges, security and IT teams must embed hardware-level security to help prevent breaches. Luckily, 87% of respondents said that they are prioritizing investment in security initiatives over the next 12 months (starting in Q3 2022). Companies are also increasing strategic implementation of hardware-level security by improving their device management policies at the software level; 84% said that effective hardware-level security will lead to a broader security approach within their organization. Benefits that result from strategically investing in hardware-level security to enable the full stack include:

- **Policy-level protections.** Hardware security can improve OS and hardware-enabled endpoint security software. And it's sometimes required to enable specific settings in the OS. Respondents reported benefits related to hardware-level embedded security like fewer breaches and security incidents (46%) and increased trust in execution for hardware-isolated data protection. They also associated it with the ability to verify the trustworthiness of devices (45%) and data (42%) (see Figure 3).
- **Management benefits.** Respondents recognized the IT benefits of focusing on hardware-level security and embedding it with endpoint security and IT. These included easier management for the IT team (52%), simplified security event and incident management (37%), and a reduced number of third-party security agents on the device (34%) (see Figure 4).
- **Employee experience and customer experience.** The most notable employee benefit of hardware-level embedded security is the overall improved end-user experience. Hardware-level embedded security enables this with easier security protocols, troubleshooting, and better access to IT. It also improves employees' experiences with PCs by improving boot times and protecting sensitive personal data in memory stores in the event of a breach or stolen device. Improving the employee experience improves the customer experience: 84% of respondents said that effective hardware-level security increases customer trust.

Figure 3

"How important are each of the following to your overall endpoint security capabilities?"



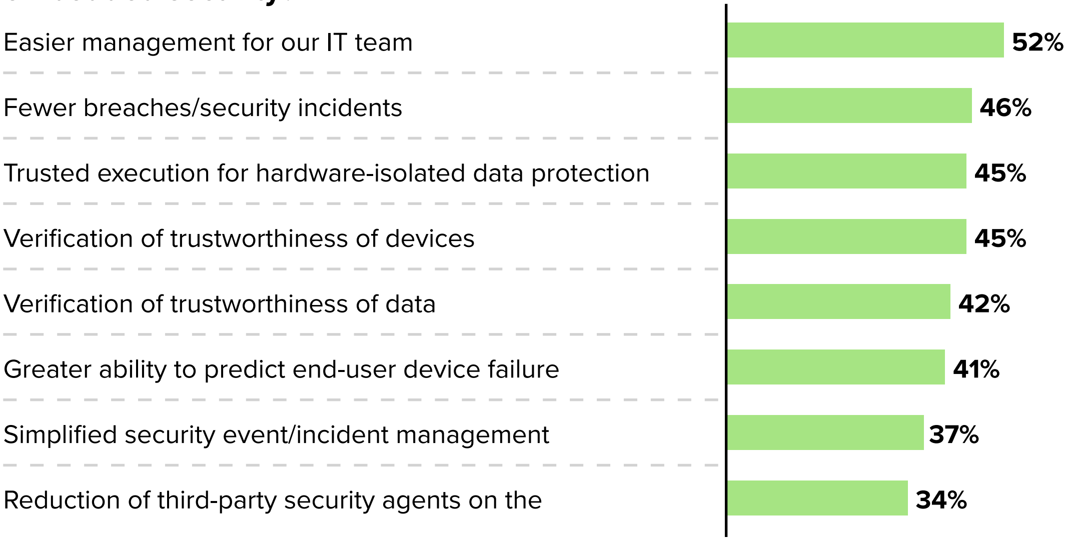
Base: 647 director or higher-level technology selection strategy, remote work, and device investment decision-makers at organizations that faced a breach in the past 12 months

Note: Total percentages may not equal separate values due to rounding.

Source: A commissioned study conducted by Forrester Consulting on behalf of Intel, March 2022

Figure 4

"What are the benefits, related to endpoint security and IT, of hardware-level embedded security?"



Base: 647 director or higher-level technology selection strategy, remote work, and device investment decision-makers at organizations that faced a breach in the past 12 months

Source: A commissioned study conducted by Forrester Consulting on behalf of Intel, March 2022

Key Recommendations

It’s clear that organizations can’t ignore the benefits of integrating device-level security into a holistic cybersecurity strategy. The question is: "Where should organizations start?" Despite the technology’s reputation for complexity and high cost, you can still build a business case to integrate client hardware security into your technology stack.

Forrester’s in-depth survey of IT decision-makers about hardware security yielded several important recommendations:

Start with a strong device procurement process.

The easiest way to implement hardware security is to buy devices that already have it embedded. Many OEM device manufacturers partner with silicon providers to enable specific capabilities that work for their organization. Include these requirements within RFPs from the start rather than thinking about hardware security post-sale. That way, your organization can focus on purchasing the right tools with the right foundational security features embedded in the hardware and add additional protections, like endpoint detection and response, afterward.

Link the benefits of hardware to anywhere work.

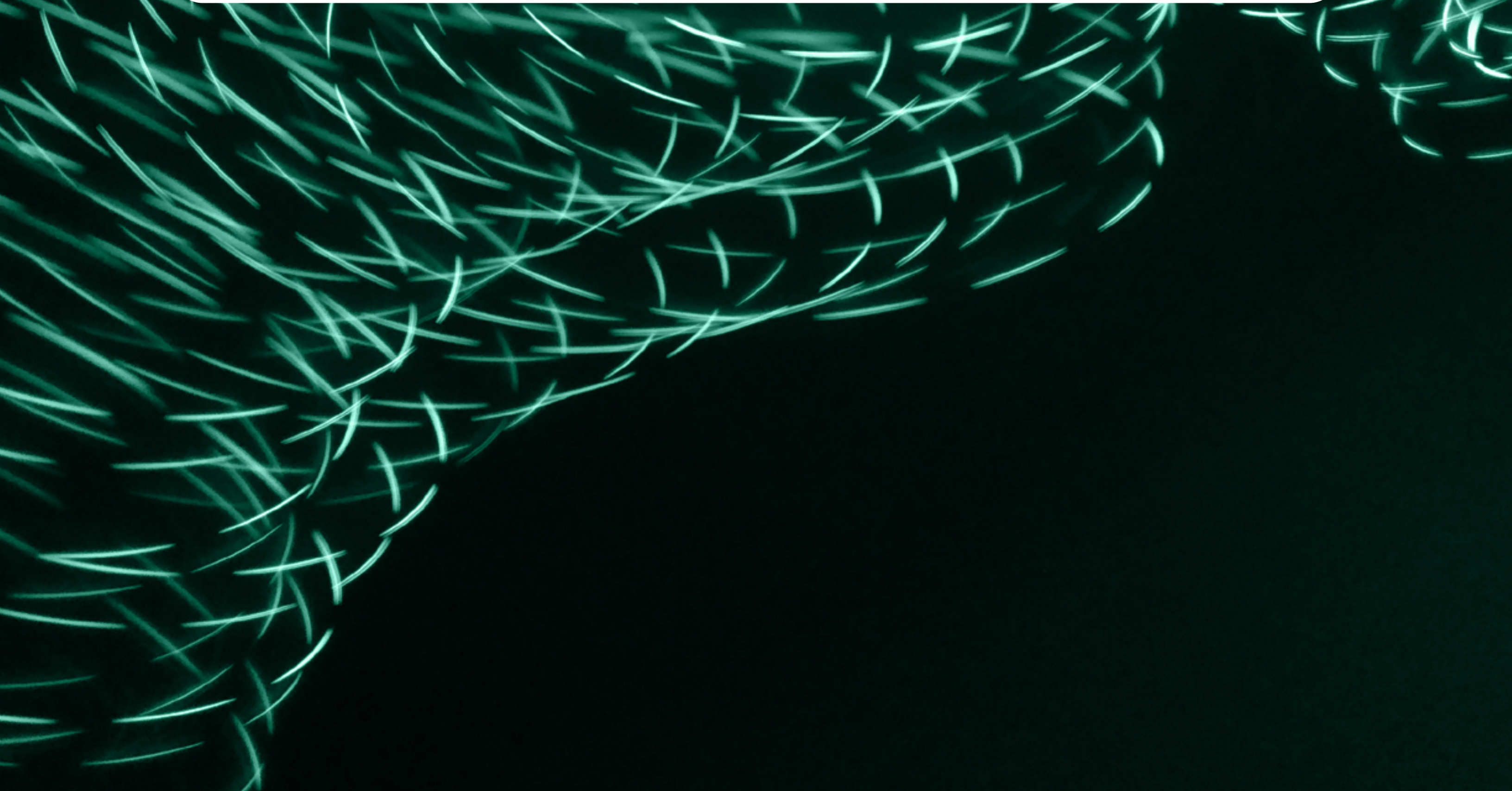
Our research showed that 51% of organizations have plans to pursue hybrid work and 15% have plans to move to a fully remote model.[6] Hardware security will be instrumental in enabling future-of-work strategies. Why? Because the only way to effectively manage offline endpoints not connected to a corporate network is through hardware-level features, an increasingly common phenomenon among distributed endpoints. Embedded hardware protections will also help endpoints stay more secure during shipping to remote workers’ home offices.

Deploy hardware security in device refreshes.

Many organizations are refreshing their device rosters to take advantage of the latest OS releases. This is a great opportunity to leverage device-level security because many new OSes rely on the most recent hardware innovations to optimize security, management, and user experiences. Organizations can also benefit from increased protections in the OS and hardware if they conduct both upgrades simultaneously.

Educate LOB decision-makers on the benefits of buying devices with hardware security capabilities.

Business decision-makers choose a large percentage of hardware purchases — a key blind spot for IT leaders seeking visibility over endpoint assets. Provide a recommendations list to business purchasers that includes devices with advanced hardware protections. To sell these groups on the value of these devices, focus on the business benefits that the right security solutions deliver.



Appendix A: Methodology

In March 2022, Intel commissioned Forrester Consulting to evaluate perceptions and strategies around hardware-level device security. Forrester conducted an online survey with 647 director or higher-level technology selection strategy, remote work, and device investment decision-makers at organizations that faced a breach in the past 12 months to explore this topic. Respondents were offered a small incentive as a thank you for time spent on the survey. The study began in February 2022 and was completed in March 2022.

Appendix B: Demographics

GEOGRAPHY	
United Kingdom	**17%**
United States	**17%**
India	**17%**
Germany	**17%**
Brazil	**17%**
Japan	**15%**

NUMBER OF EMPLOYEES	
>20,000	**11%**
5,000 to 19,999	**23%**
1,000 to 4,999	**15%**
500 to 999	**12%**
100 to 499	**8%**
1 to 99	**32%**

RESPONDENT LEVEL	
C-level executive	**22%**
Vice president	**32%**
Director	**46%**

DEPARTMENT	
IT	**100%**

TYPES OF BREACHES IN PAST 12 MONTHS (Multiple responses accepted)	
External attack targeting our organization	**58%**
Internal incident within our organization	**55%**
Lost/stolen assets	**55%**
Attack or incident involving our business partners/ third-party suppliers	**50%**

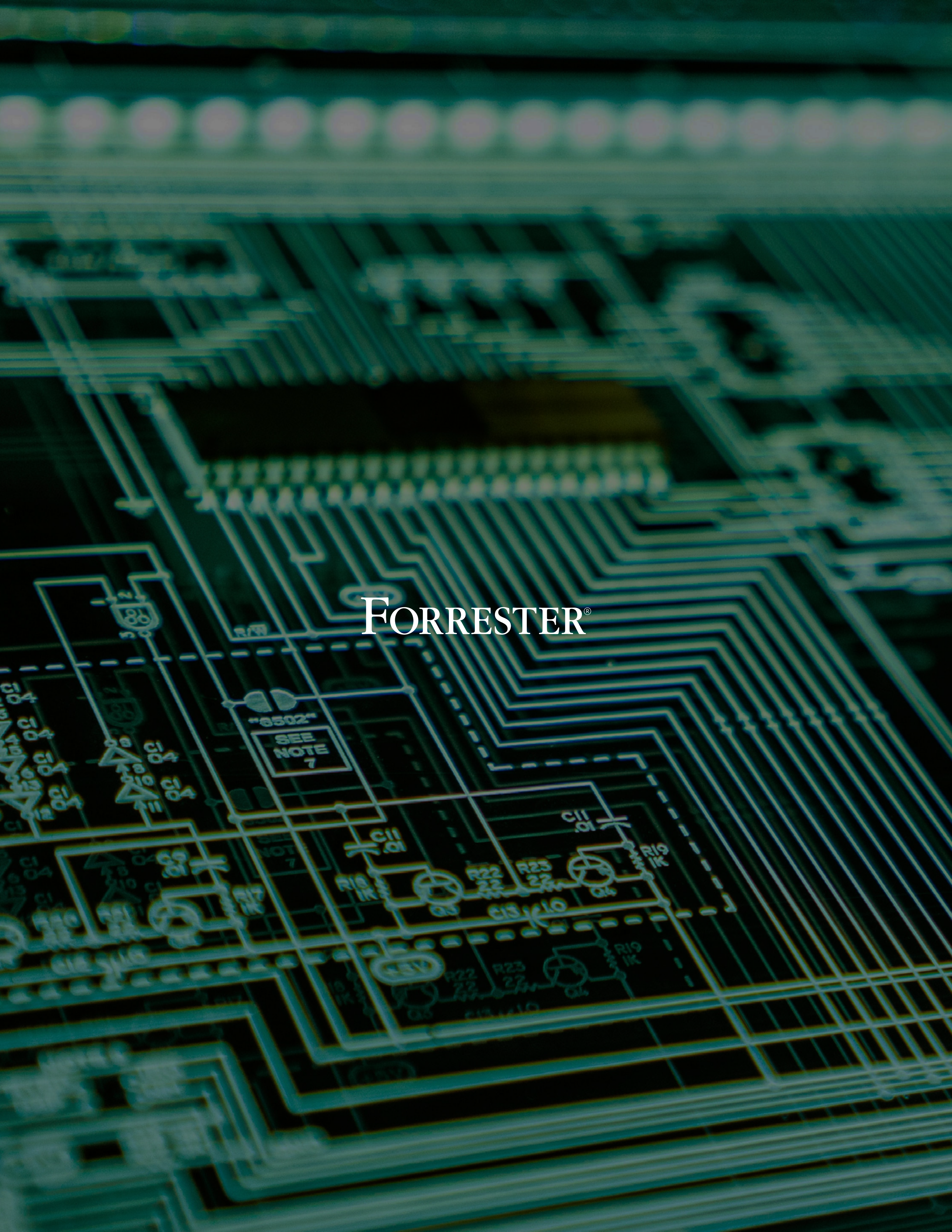
INDUSTRY	
Technology and technology services	**15%**
Retail	**10%**
Financial services and insurance	**8%**
Manufacturing and materials	**8%**
Telecommunications services	**5%**
Healthcare	**5%**
Business and professional services	**5%**
Transportation and logistics	**4%**
Chemicals and metals	**4%**
Consumer services	**4%**
Consumer product goods and manufacturing	**4%**
Construction	**4%**
All others reporting 3% and less	**24%**

Percentages do not total 100 because of rounding.

Appendix D: Endnotes

[1] “The Anywhere-Work Guide For Tech Pros, 2022,” Forrester Research, Inc., May 16, 2022.
[a3] “The Definition Of Modern Zero Trust, 2022,” Forrester Research, Inc., January 24, 2022.
[4] “The Forrester Wave™: Unified Endpoint Management, Q4 2021,” Forrester Research, Inc., November 2, 2021.
[5] “The Future Of Endpoint Management, 2022,” Forrester Research, Inc., June 6, 2022.
[6] “The Anywhere-Work Preflight Checklist, 2022,” Forrester Research, Inc., May 16, 2022.

No product or component can be absolutely secure.



FORRESTER®