Enterprise Strategy Group™

The Growing Role of AI in Endpoint Management and Security Convergence

Gabe Knuth | Senior Analyst

ENTERPRISE STRATEGY GROUP

APRIL 2025

Research Objectives

Organizations continue to face increasing complexity in endpoint management and security that is driven by the rapid expansion of remote work, rising device and OS sprawl, vulnerability management and incident response challenges, and continuing threats like ransomware. At the same time, the growing influence of AI and automation is reshaping both offensive and defensive strategies—empowering defenders with new tools while enabling bad actors to launch more sophisticated attacks.

To gain further insight into these trends, how organizations are attempting to overcome challenges, and the results of their efforts, Enterprise Strategy Group, now part of Omdia, surveyed 364 IT and cybersecurity professionals in North America (US and Canada) responsible for evaluating, purchasing, and supporting endpoint management and/or security technologies.

This study sought to:

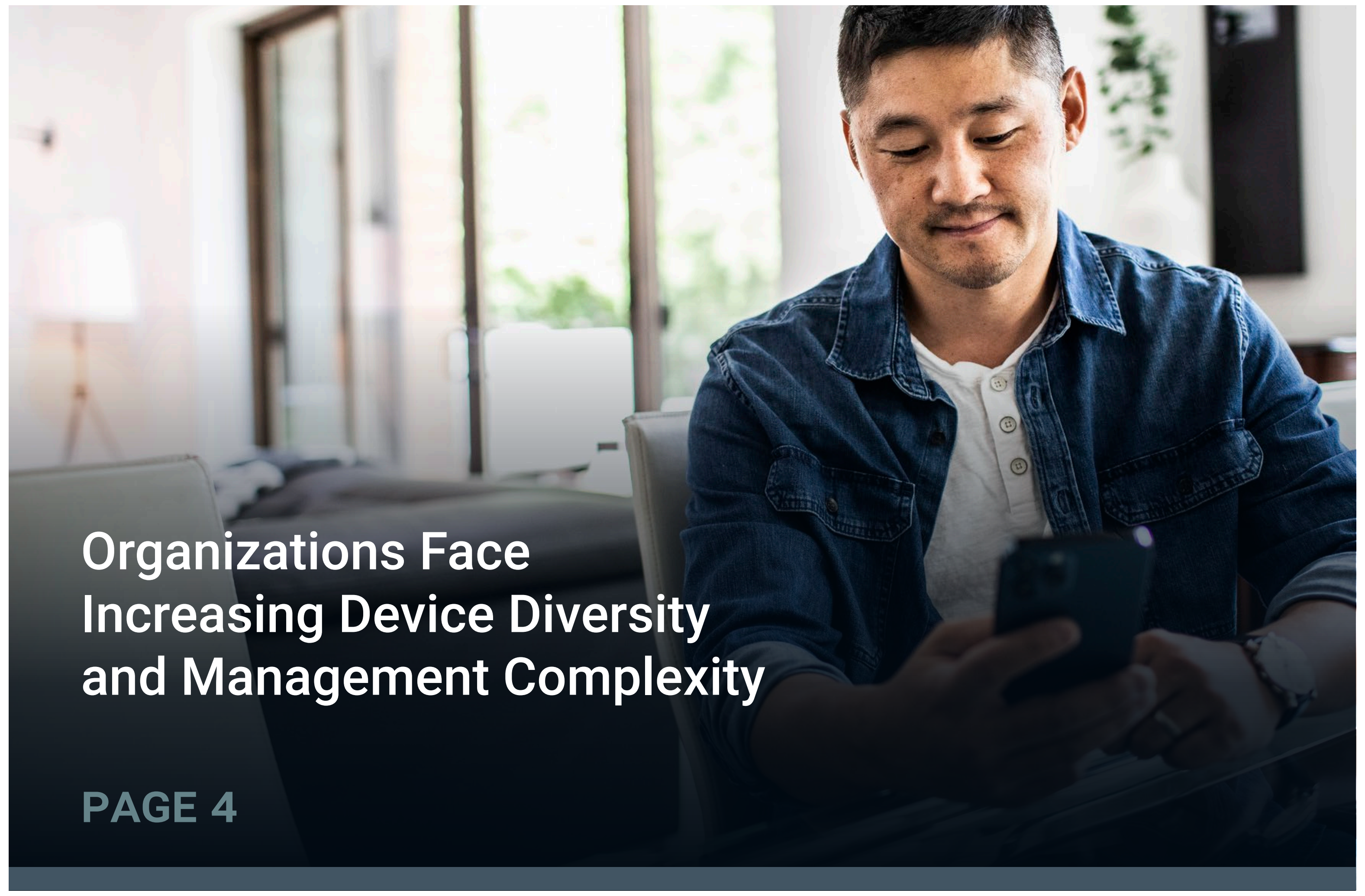
Assess the state of endpoint management and security as well as the challenges and priorities that drive decision-making.

Compare the results of this research to similar research from 2022, and reveal trends in the convergence of IT and security teams, devices in use, and experienced security events.

Understand the shifting trends in buying teams as convergence takes hold as well as future priorities and likely spending intentions.

Highlight emerging trends, threats, and solutions brought about by an evolving market that is increasingly contending with the benefits and dangers of AI.

Key Findings



Organizations Face Increasing Device Diversity and Management Complexity

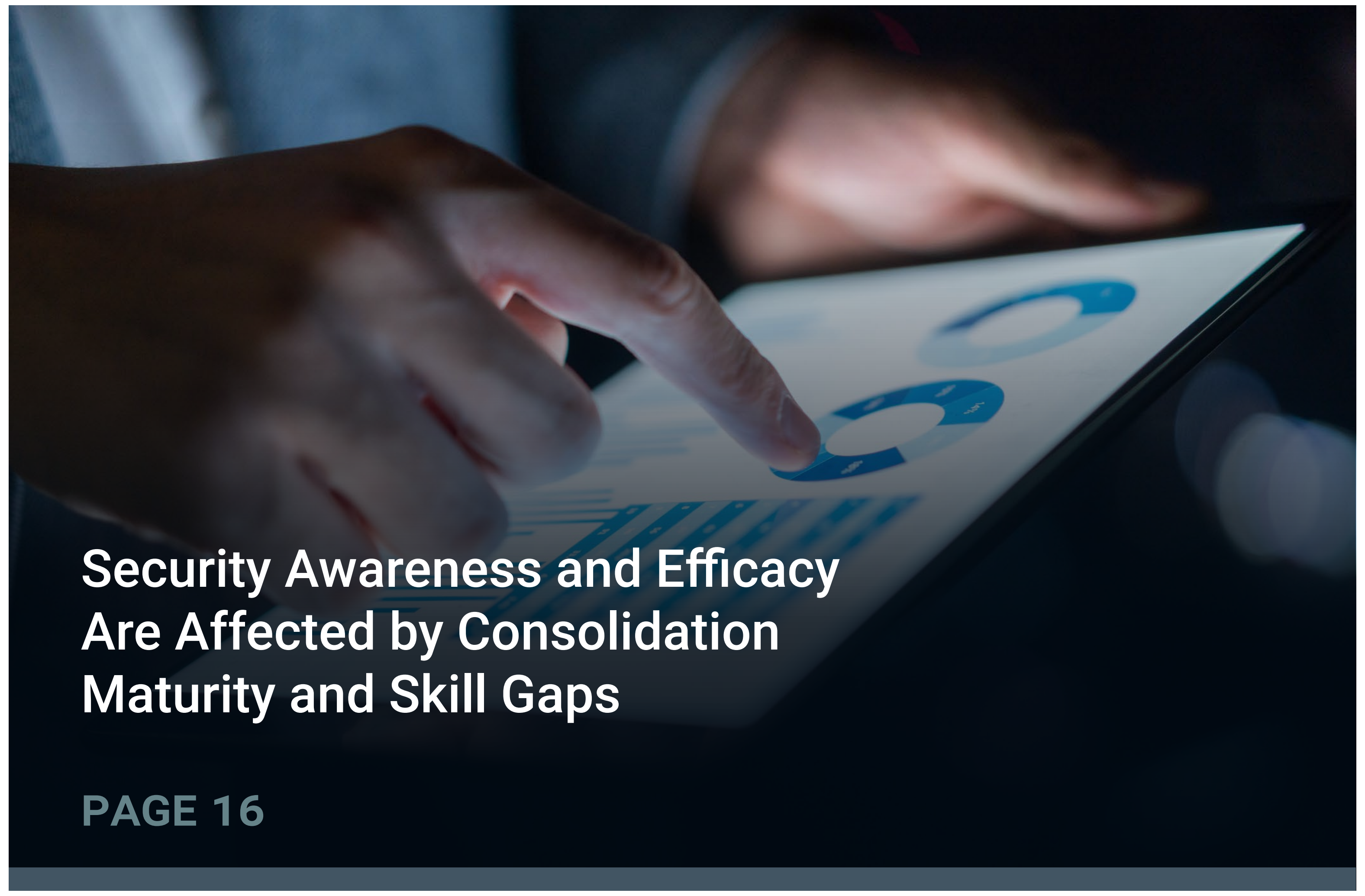
PAGE 4

Management and Security Tool Sprawl Persists Amid Changing Tool and Team Consolidation Efforts

PAGE 9

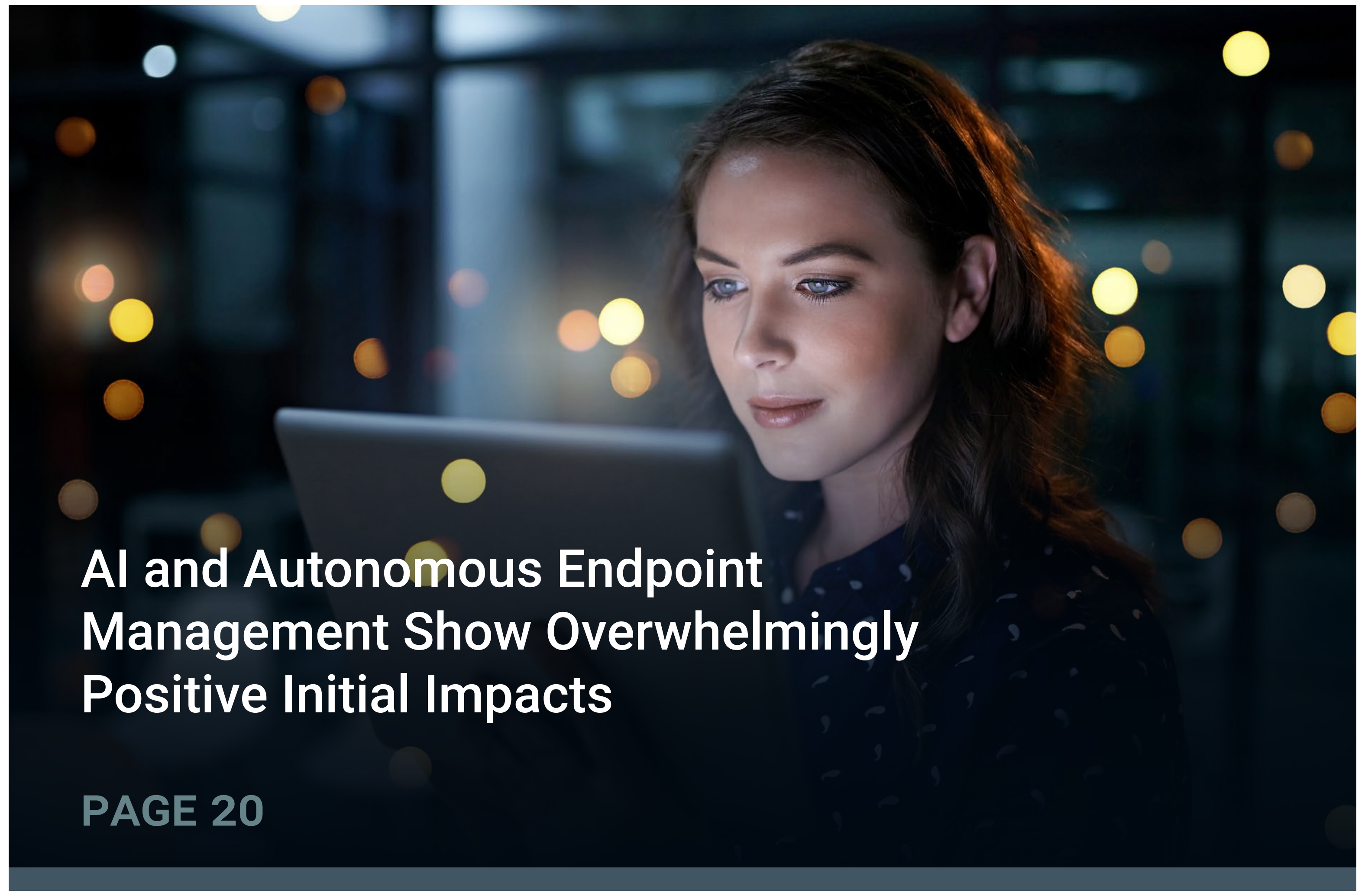
Most Unmanaged Devices Are Not Unmanaged by Choice

PAGE 13



Security Awareness and Efficacy Are Affected by Consolidation Maturity and Skill Gaps

PAGE 16



AI and Autonomous Endpoint Management Show Overwhelmingly Positive Initial Impacts

PAGE 20

Strategic Investments in Technology and Services Are Key to Success

PAGE 23

BACK TO CONTENTS

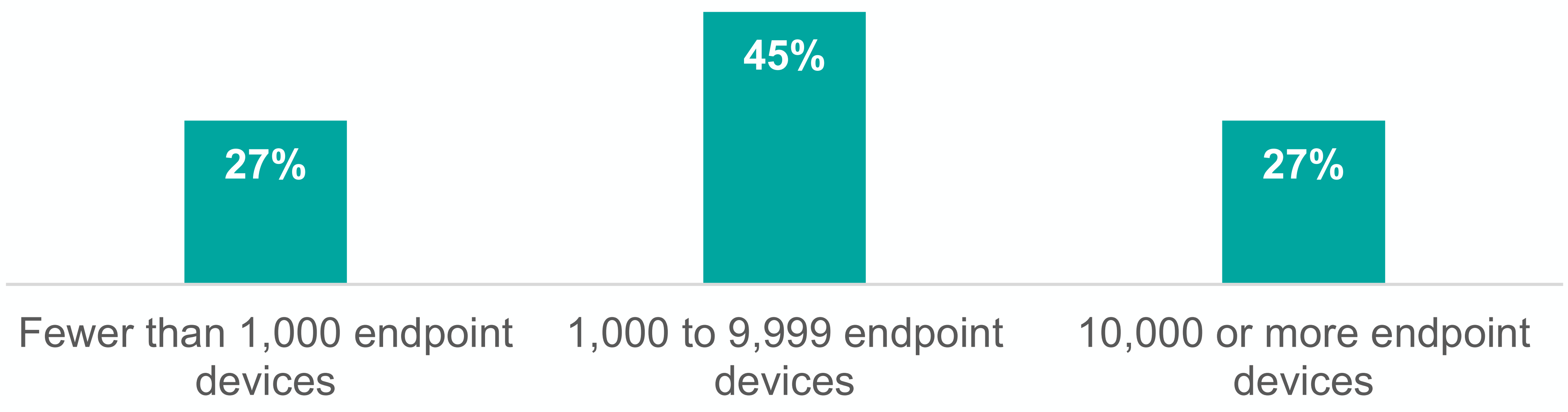
Organizations Face Increasing Device Diversity and Management Complexity

Endpoint Management and Security Are Becoming More Difficult

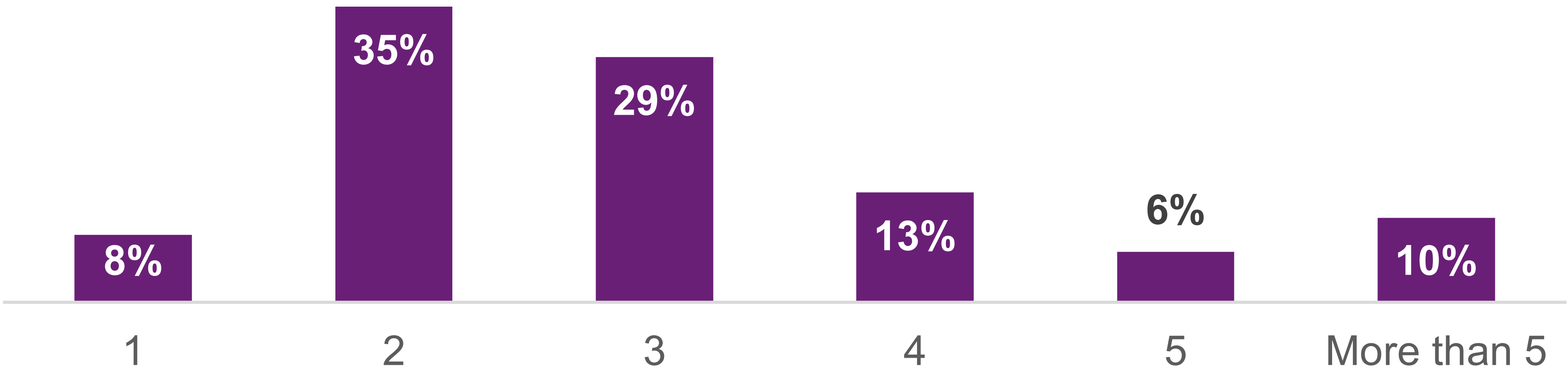
Most organizations are managing thousands—and in many cases, tens of thousands—of endpoint devices. Nearly three-quarters (72%) of organizations report having at least 1,000 devices in play, spanning laptops, mobile devices, and more. This level of device sprawl, especially across both managed and unmanaged assets, underpins the operational challenges teams face as they try to maintain visibility, enforce policies, and respond to threats in real time. Compounding the challenge, employees are using multiple devices to get their work done. In fact, 93% of organizations say the typical employee uses two or more endpoints daily. That includes laptops, smartphones, tablets, and other devices, all of which need to be secured, patched, and monitored.

This level of per-user sprawl puts additional pressure on IT and security teams already stretched thin by growing device counts and limited visibility across environments. Because of this, roughly 40% of respondents noted that endpoint management and/or security are now more difficult compared with two years ago.

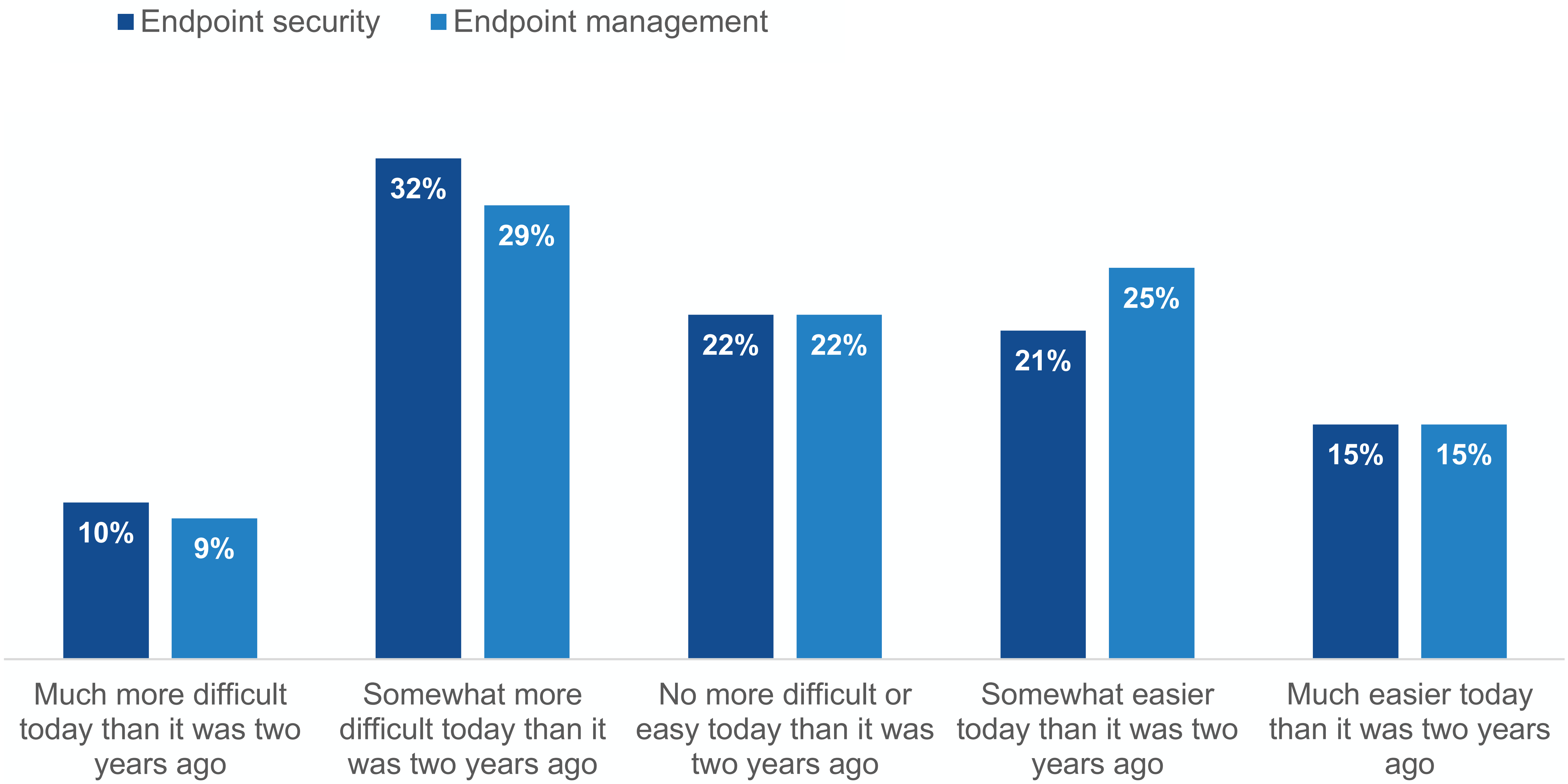
Total endpoint devices in use.



Average endpoint devices per employee.



Change in difficulty of endpoint management and security.

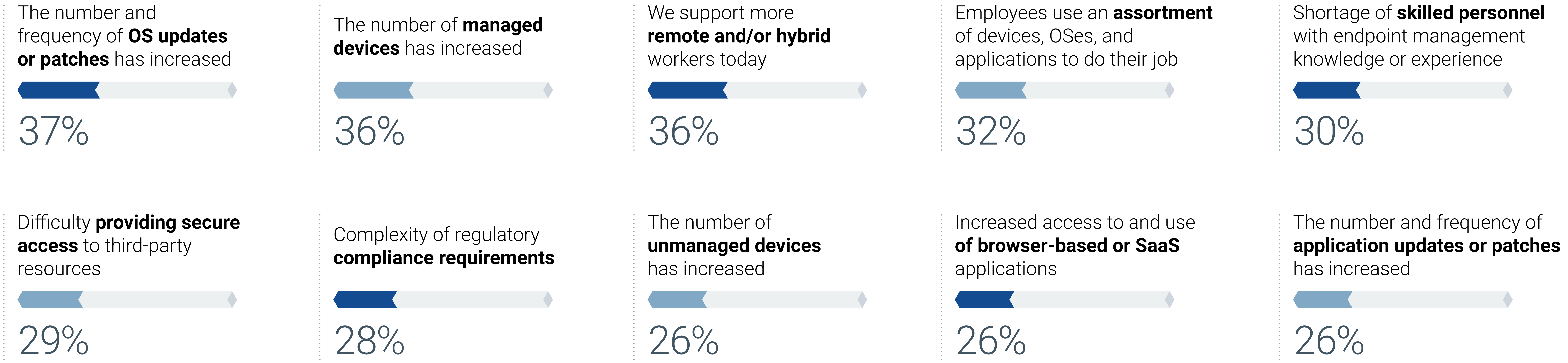


The Core Drivers Behind Rising Complexity in Endpoint Management and Security Can Be Summed Up in Two Words: More and Less

Organizations are dealing with more threats, more frequent OS and application updates, more devices (both managed and unmanaged), and more remote or hybrid workers. The growing diversity of operating systems, applications, and user needs only adds to the challenge of managing and securing these workspaces.

If there's a theme around what organizations have less of when it comes to managing and securing devices, it includes time, expertise, and visibility. Respondents point to a lack of skilled staff, insufficient training, and limited time to learn or optimize new tools as contributing factors—highlighting a growing resource gap at a time when demands continue to rise.

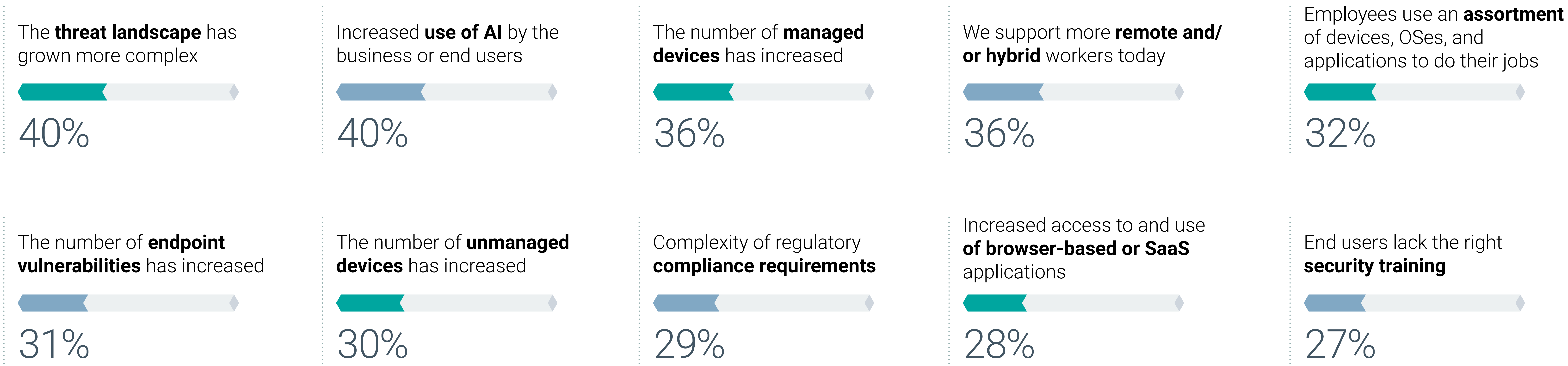
Top factors driving increased endpoint management complexity.



The number and frequency of **OS updates or patches** has increased	37%
The number of **managed devices** has increased	36%
We support more **remote and/or hybrid** workers today	36%
Employees use an **assortment** of devices, OSes, and applications to do their job	32%
Shortage of **skilled personnel** with endpoint management knowledge or experience	30%
Difficulty **providing secure access** to third-party resources	29%
Complexity of regulatory **compliance requirements**	28%
The number of **unmanaged devices** has increased	26%
Increased access to and use **of browser-based or SaaS** applications	26%
The number and frequency of **application updates or patches** has increased	26%

BACK TO CONTENTS

Top factors driving increased endpoint security complexity.



The **threat landscape** has grown more complex

40%

Increased **use of AI** by the business or end users

40%

The number of **managed devices** has increased

36%

We support more **remote and/ or hybrid** workers today

36%

Employees use an **assortment** of devices, OSes, and applications to do their jobs

32%

The number of **endpoint vulnerabilities** has increased

31%

The number of **unmanaged devices** has increased

30%

Complexity of regulatory **compliance requirements**

29%

Increased access to and use **of browser-based or SaaS** applications

28%

End users lack the right **security training**

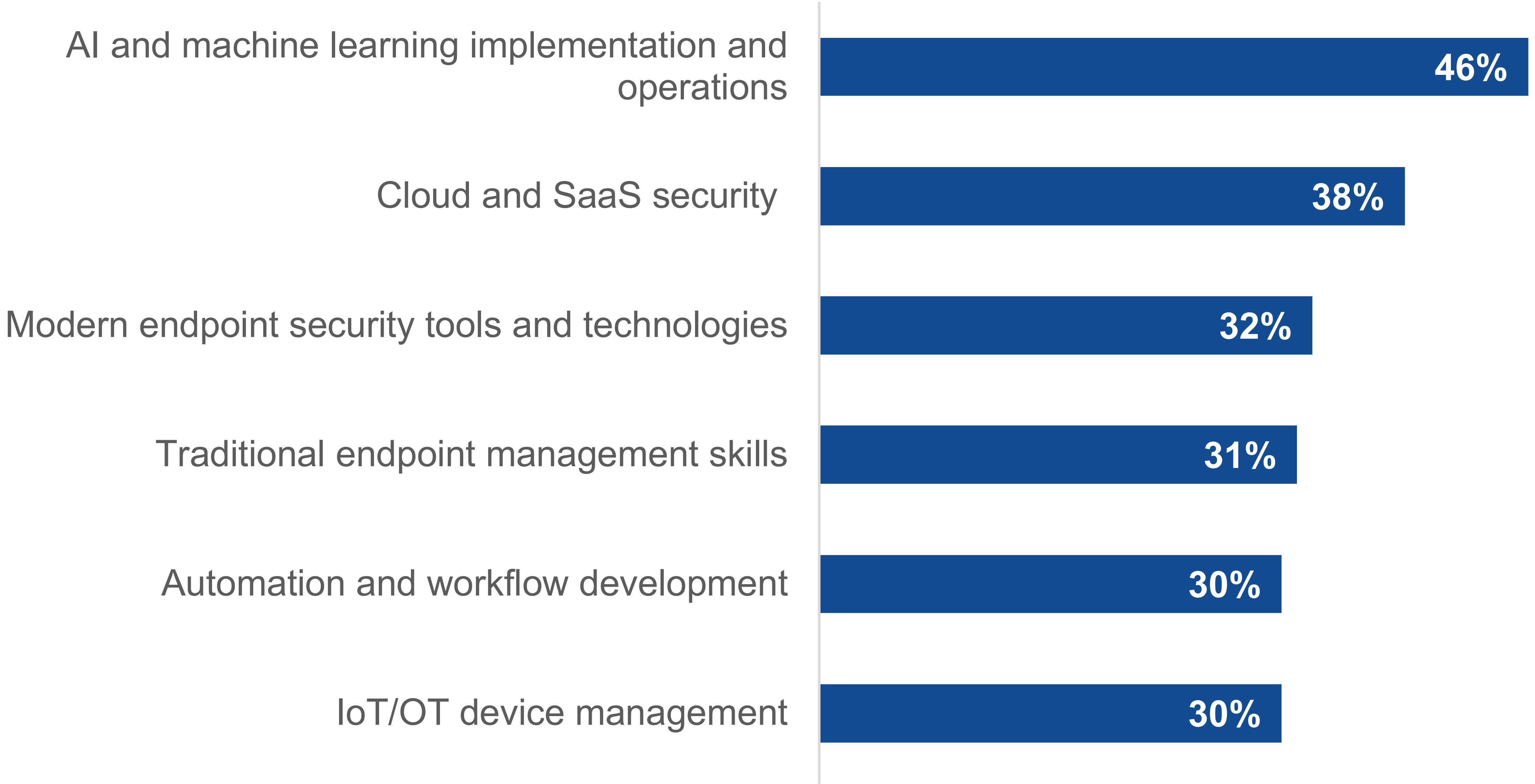
27%

Skill Gaps and AI Threaten to Make Endpoint Matters Worse

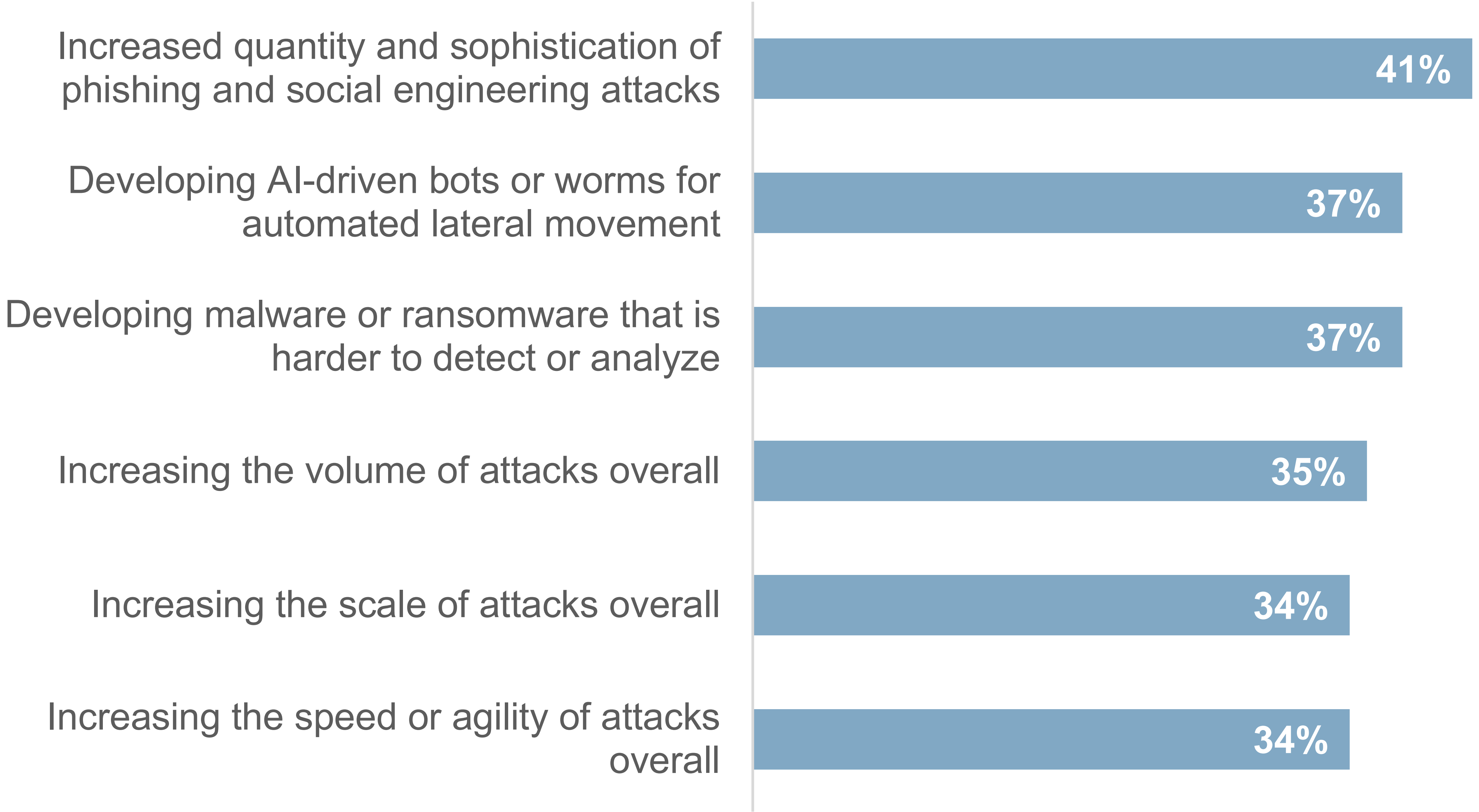
While many organizations understandably struggle to support new technologies with adequately knowledgeable and experienced staff, a significant portion noted headcount gaps in both newer areas like AI/ML and cloud security and traditional endpoint management, as well as automation and workflow development and IoT device management. Perhaps most concerning is that AI is enabling bad actors to take advantage of the very gaps in skill from which organizations suffer across a variety of areas, in addition to a general increase in both the quantity and sophistication of attacks.

This, as will be seen later, has a direct influence on an organization's ability to manage and protect itself, let alone know whether it is under attack.

Top skill gap areas for endpoint management and security.



Top ways AI is used by attackers targeting end-user devices.



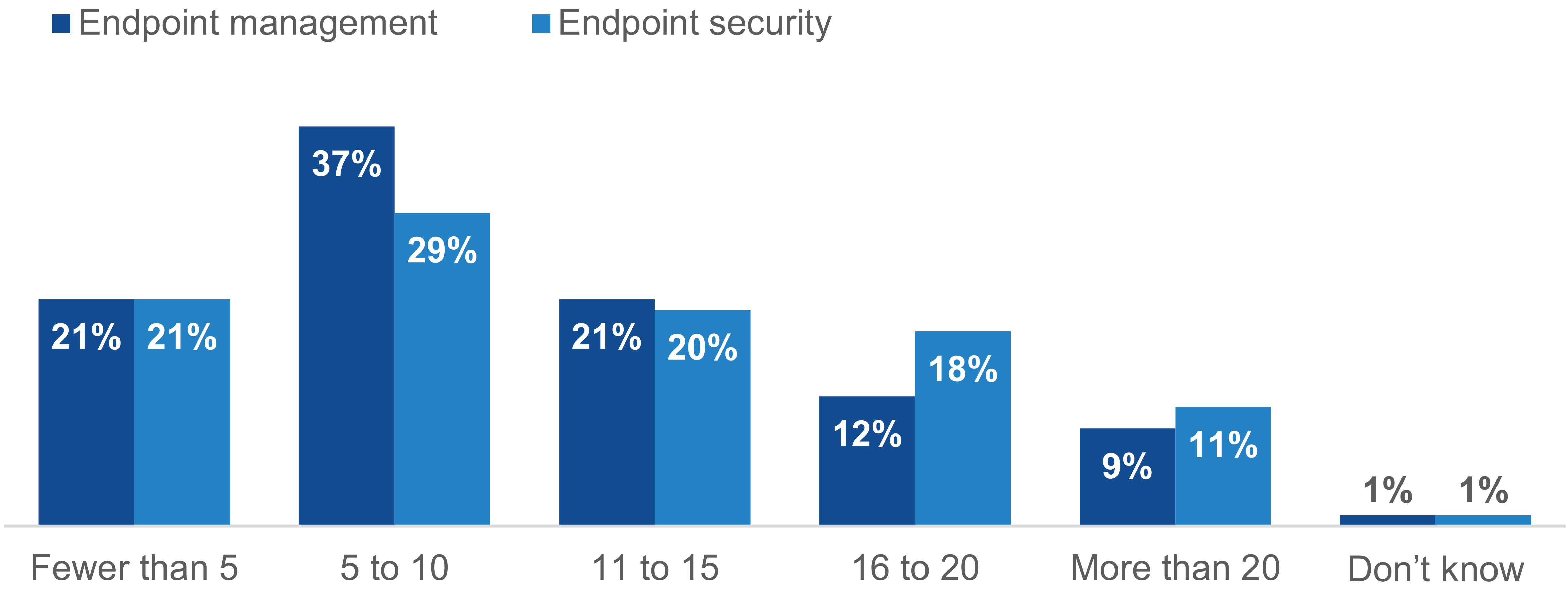
Management and Security Tool Sprawl Persists Amid Changing Tool and Team Consolidation Efforts

Tool Sprawl Is Real and Driven by Numerous Factors

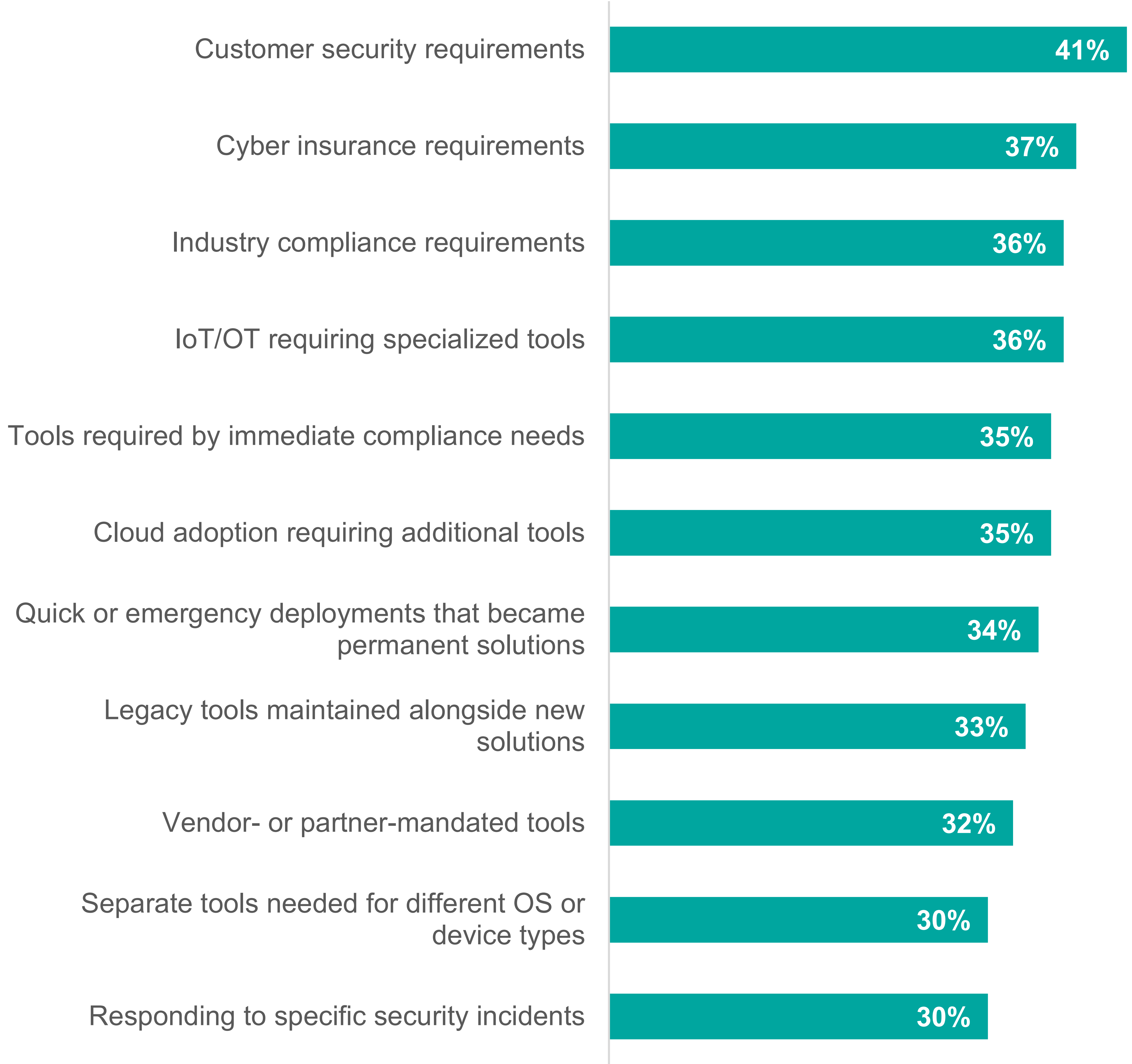
Most organizations are juggling multiple tools for both endpoint management and security, with the majority using between five and 15 tools in each category. Nearly 30% say they're managing 16 or more tools for endpoint security alone. While respondents were asked separately about their management and security tools, it's likely that some tools span both functions. Still, the overall takeaway is clear: Teams are supporting a large number of tools, which can add friction, increase cost, and complicate integration. The fact that 21% report using fewer than five tools for each category hints at some consolidation—but for most, there's still a long way to go.

The most common factors driving sprawl across endpoint security and management tools include requirements spanning customer security, cyber insurance, and industry compliance, as well as specialized tools for IoT/OT.

Number of endpoint management and security tools deployed.



Top ten factors contributing to management and security tool sprawl.



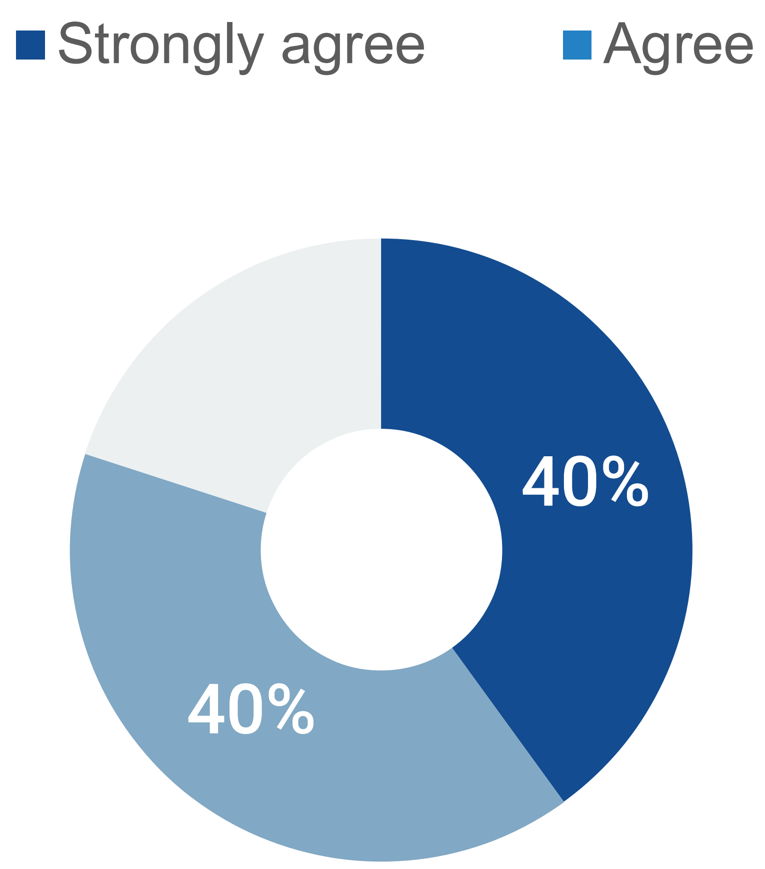
Tool Consolidation Seen as a Positive

Eight in ten organizations believe that consolidating endpoint management and security tools would positively impact their ability to manage and secure endpoints, which is a position that is reinforced throughout this research. Furthermore, 50% of respondents believe that overlapping tool functionalities negatively impact their organization's ability to secure and manage endpoints.

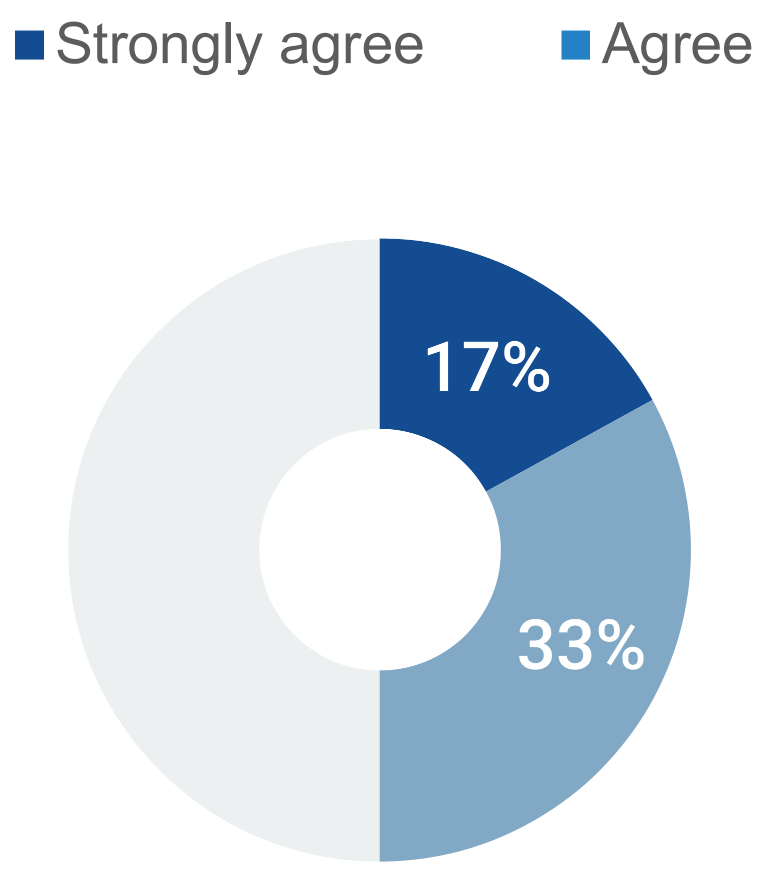
It's no surprise, then, to see that the primary approach to consolidation taken by organizations is to consolidate endpoint management and security vendors, followed by observability and monitoring technologies.

Tool consolidation and functional overlap avoidance are top of mind.

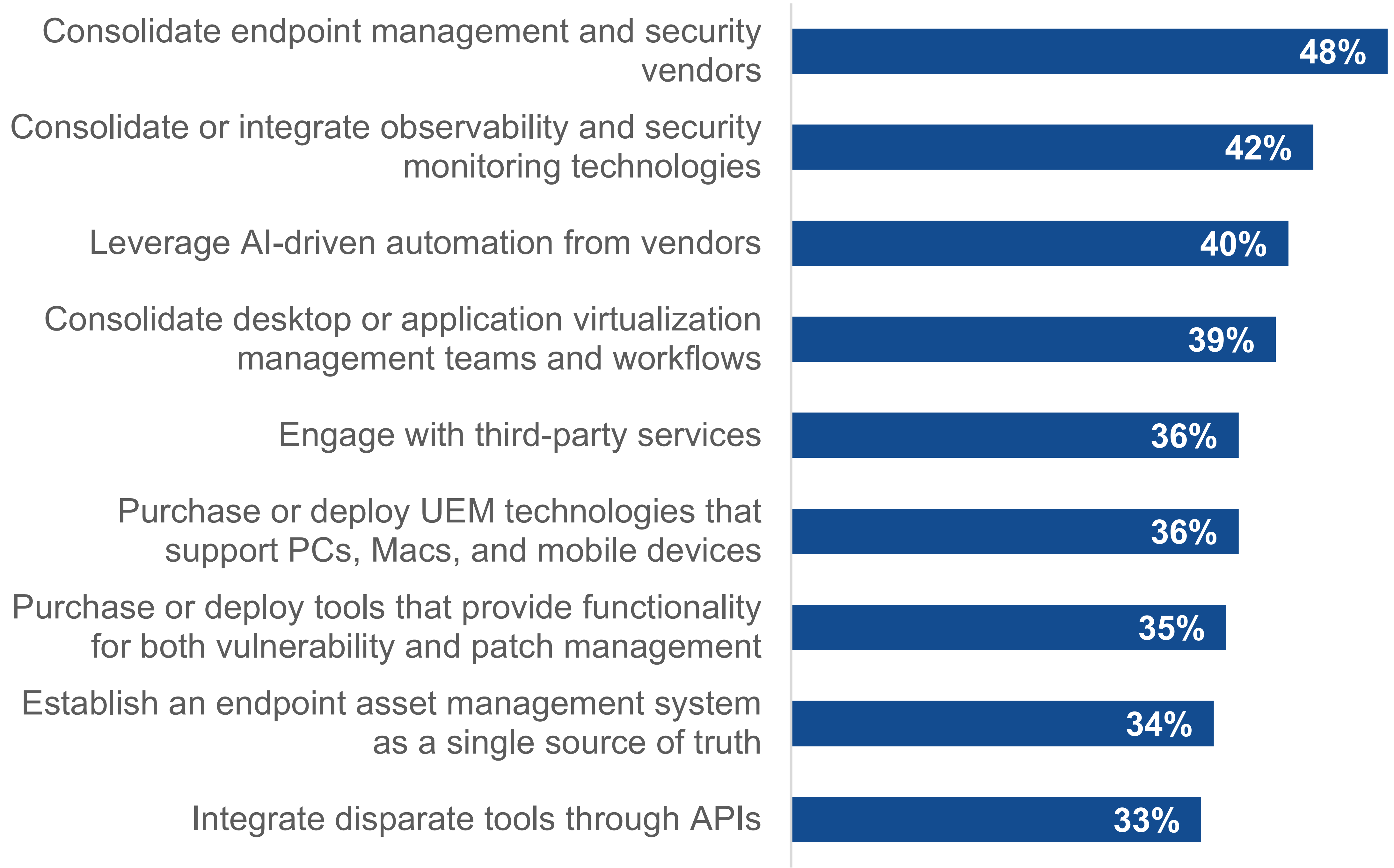
Consolidating tools used for endpoint management and security would positively impact our ability to manage and secure endpoints.



Overlapping functionality across tools causes problems that negatively impact endpoint management and security.



Actions taken to support endpoint management and security consolidation.



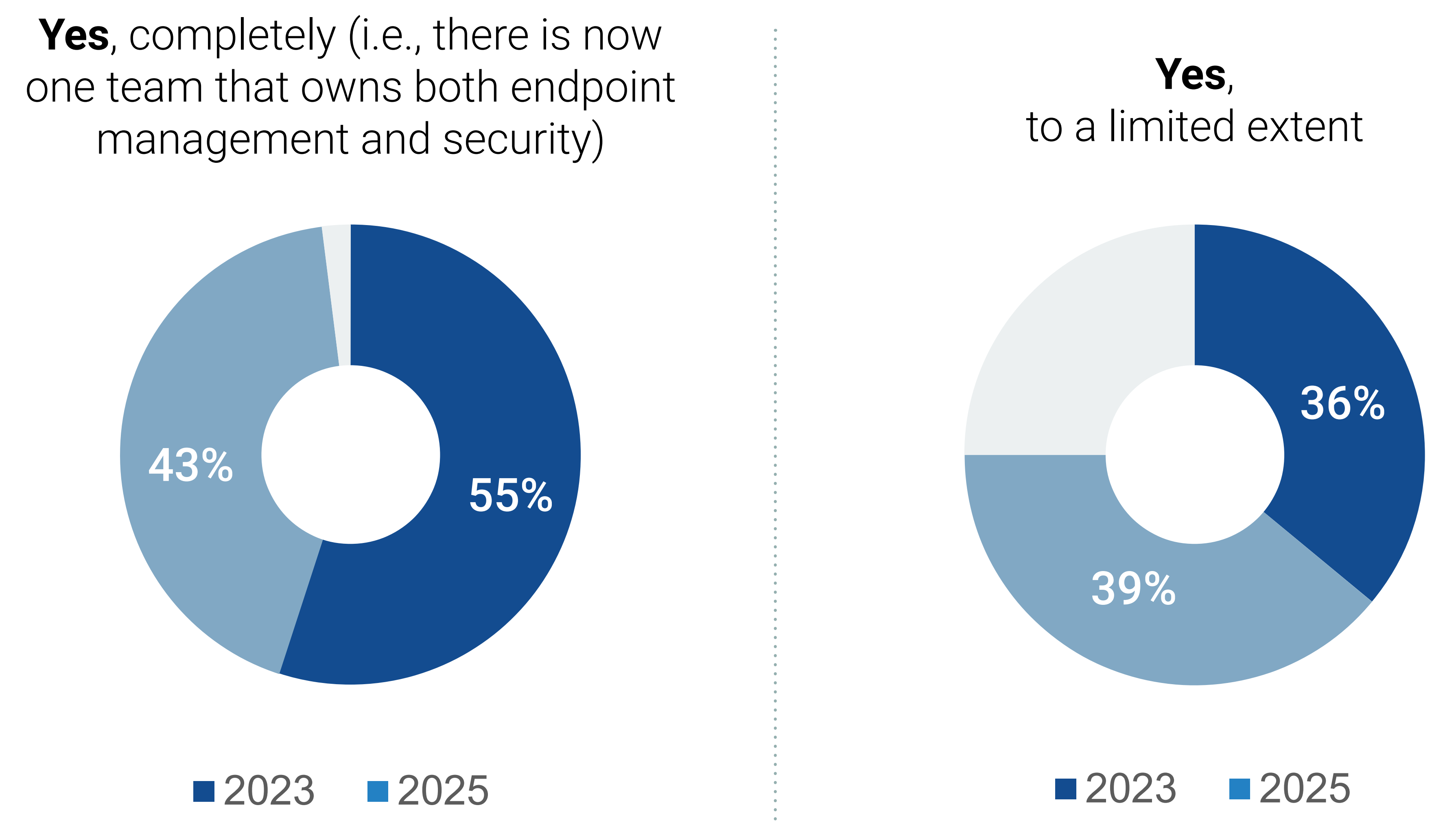
Team Consolidation Efforts Seem to Have Stalled

Though tool consolidation is top of mind, momentum toward overall management and security team consolidation has slowed. While it's still a priority, driven by the desire to improve operational efficiency and coordination as well as security response times and effectiveness, the percentage of respondents that identify as having *completely* consolidated their teams into one has fallen from 55% to 43% over the past two years.

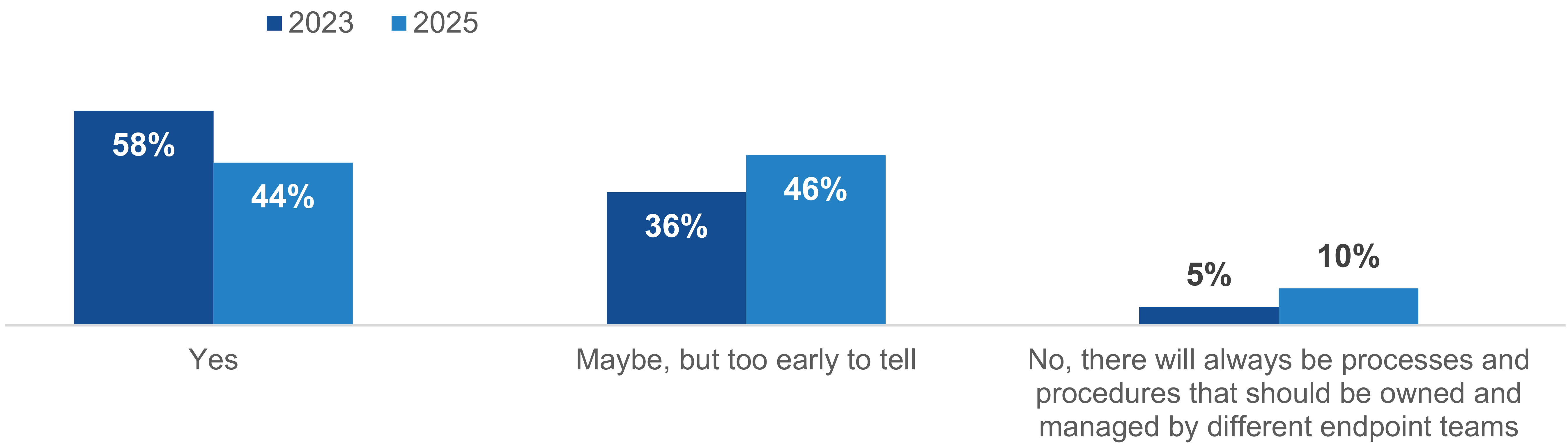
Likewise, there is a drop-off in consolidation aspirations among organizations that have not yet *completely* integrated the personnel supporting endpoint management and security functions. Specifically, the number of these organizations that anticipate fully combining management and security efforts under one team has dropped from 58% in 2023 to 44% in 2025.

For those that have consolidated or expect to, most often the resulting team becomes part of IT operations as opposed to security operations, which could explain why some say there will always be some procedures that will be owned by other teams.

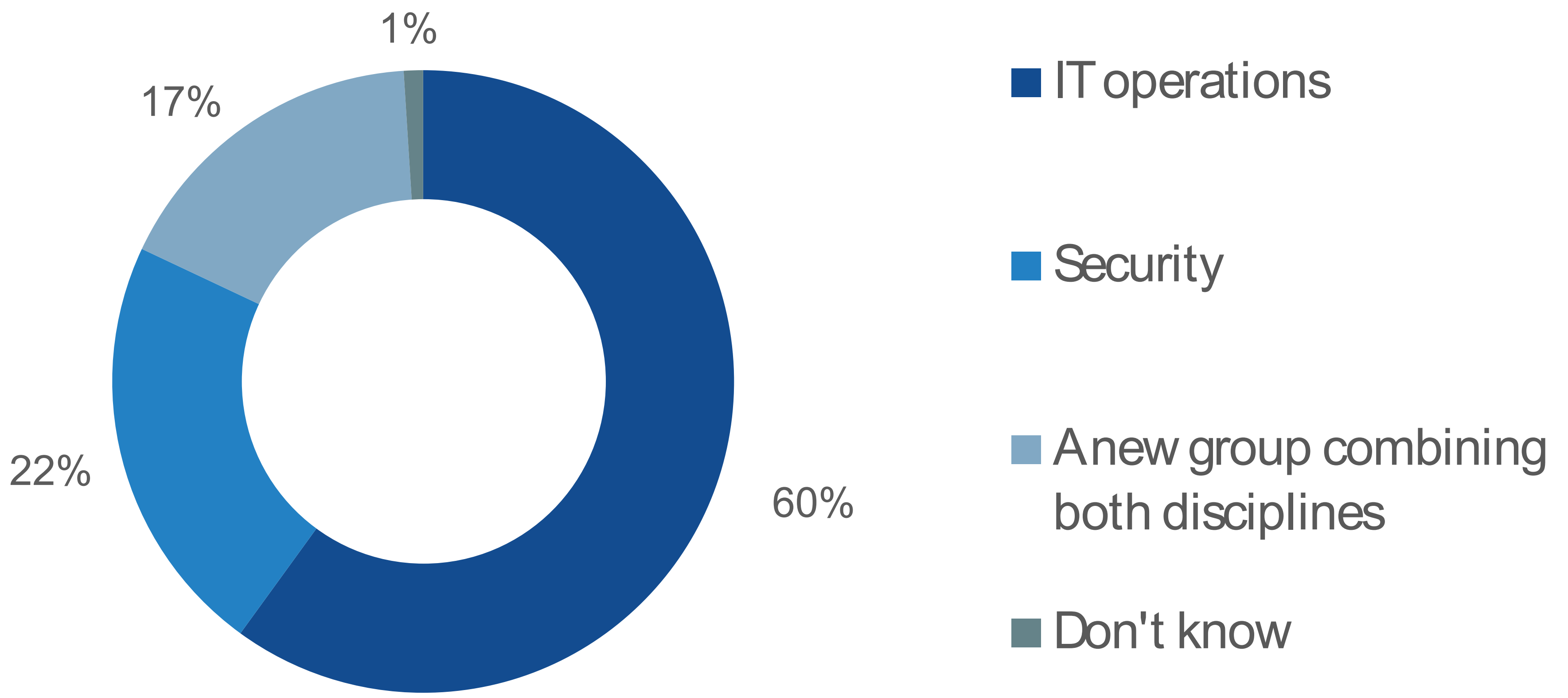
Have organizations consolidated teams managing endpoint management and security functions?



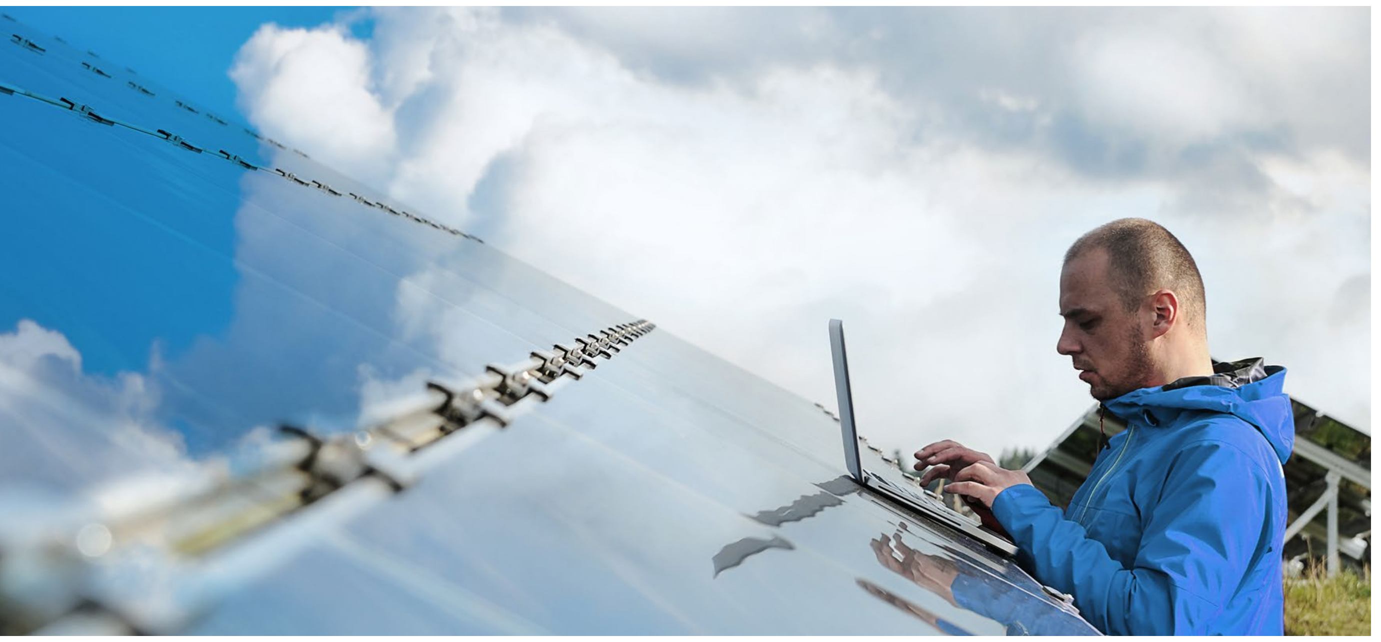
Are organizations planning to consolidate teams managing endpoint management and security functions?



Team that owns the consolidated endpoint management and security function.



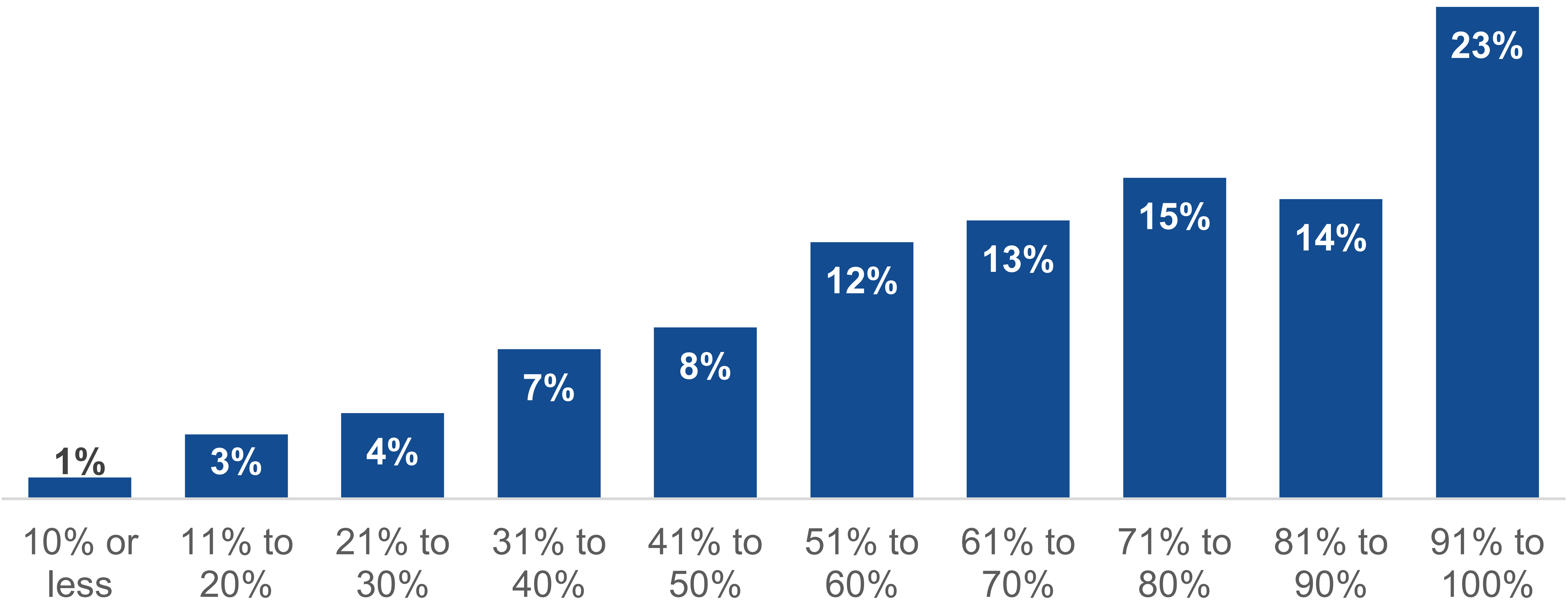
Most Unmanaged Devices Are Not Unmanaged by Choice



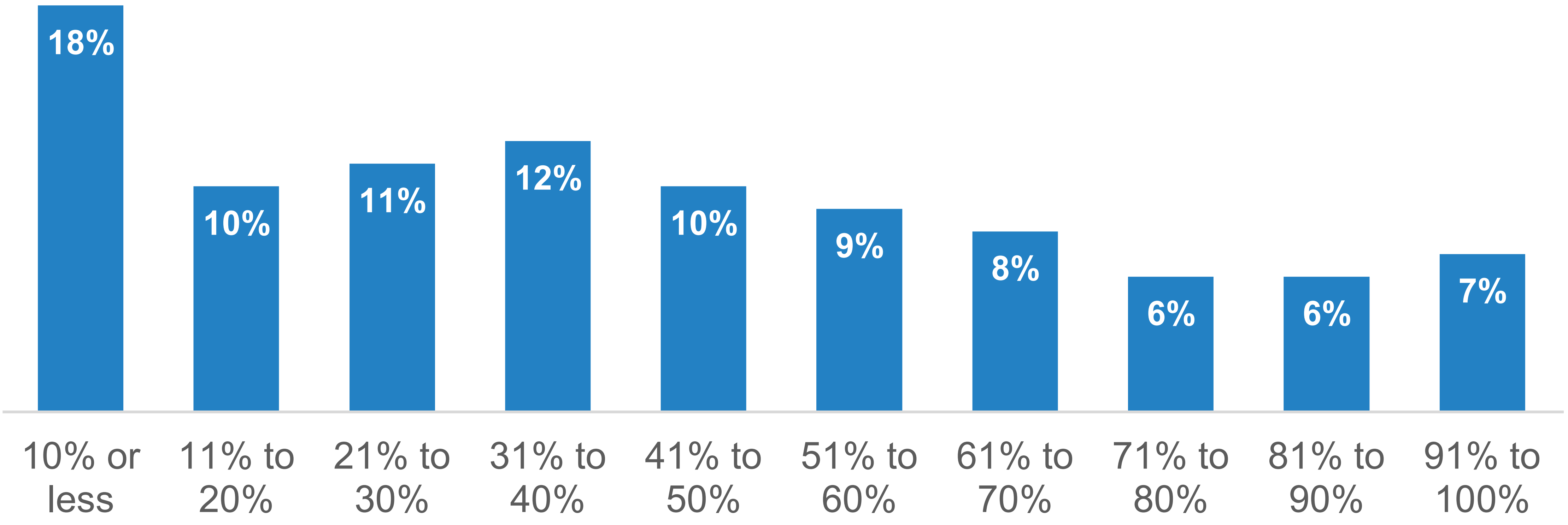
Endpoint Device Management Is a Mixed Bag With Similarly Mixed Results

Respondents indicated an average of 68% of their organization's devices are centrally managed by IT or some third-party provider. The real story, however, is in the *unmanaged* devices. Typically, unmanaged devices fall into two categories: "strategically unmanaged," whereby security is ensured via alternative means like zero-trust strategies, VPNs, browser security, or desktop virtualization, and "unintentionally unmanaged," whereby devices go unmanaged not because of a strategy, but due to oversight, lack of visibility, or capability gaps. The research shows that 59% of unmanaged devices belong to the latter category, which means that nearly one in five devices in a given organization are both *unmanaged* and *unsecured*.

Percentage of total devices that are centrally managed.



Percentage of unmanaged devices that are strategically unmanaged.

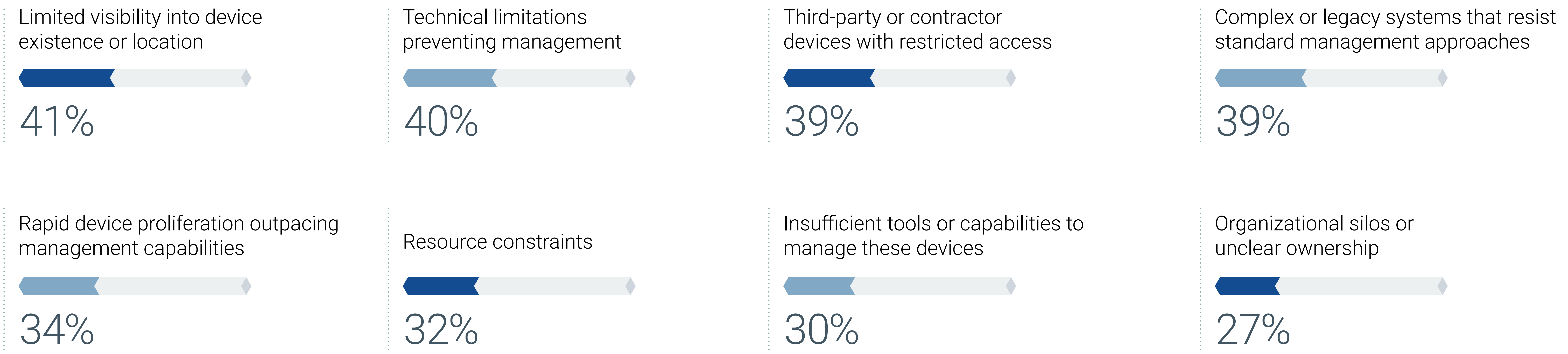


Visibility, Access, and Complexity Top the List of Reasons Devices Go Unmanaged

When asked about why these devices go unintentionally unmanaged, organizations indicated concerning technical and visibility limitations, along with other common challenges related to complexity, more devices, and resource constraints.

Given the overall confidence in their abilities, this paints a paradoxical picture that would indicate that operations may not be as robust as they seem. As is illustrated in the next section, this can result in critical oversights.

Top factors that lead to unintentionally unmanaged devices.



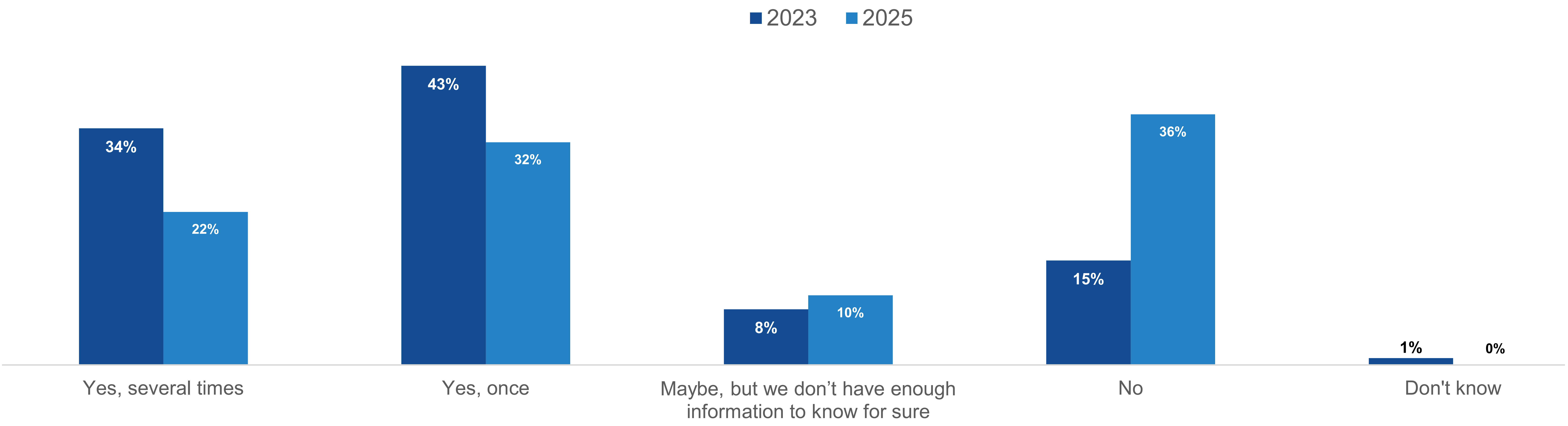
Security Awareness and Efficacy Are Affected by Consolidation Maturity and Skill Gaps

Poor Device Management Continues to Fuel Cyberattacks, but Fewer Attacks Are Reported

A significant number of organizations experience cyberattacks due to unknown, unmanaged, or poorly managed endpoints; however, the number of respondents who answered in the affirmative on this is down significantly. Specifically, more than three-quarters (77%) said they had in 2023 versus just more than half (54%) in 2025.

How can the situation be getting more difficult, with so many skill gaps and unintentionally unmanaged devices, yet we see reduced cyberattacks? The answer is, for better and worse: awareness.

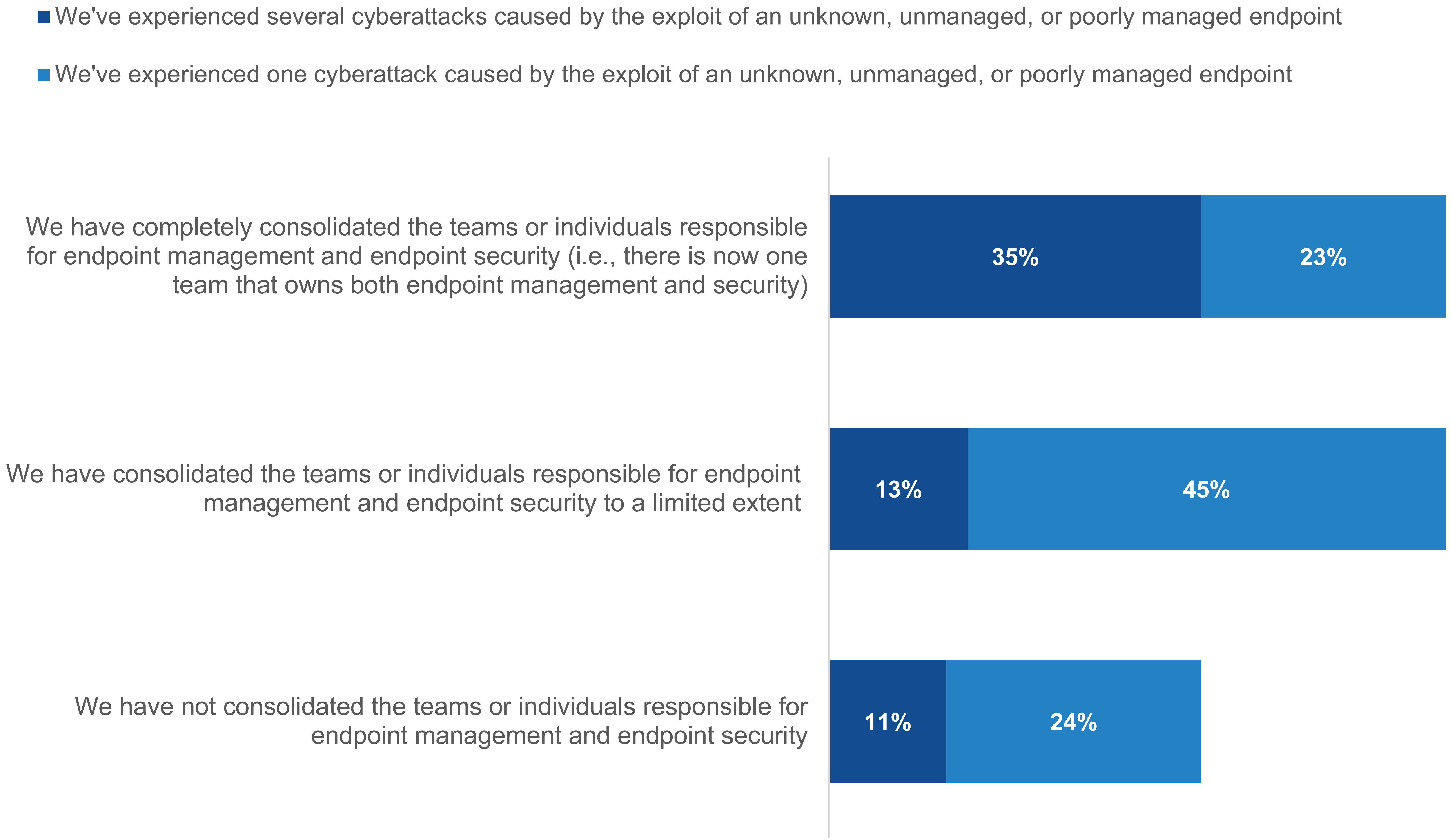
Have organizations experienced cyberattacks related to unknown, unmanaged, or poorly managed devices?

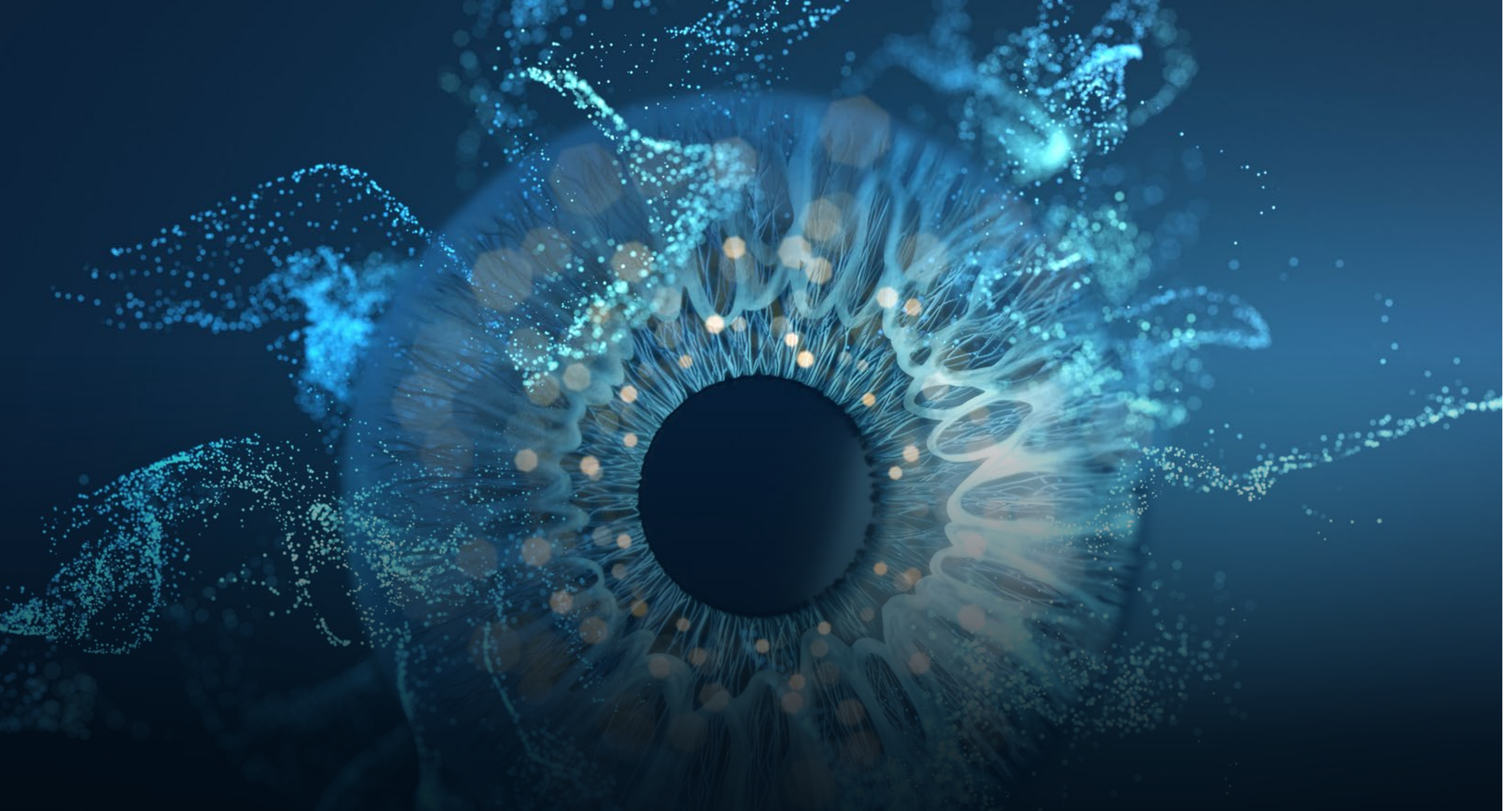


Awareness (and Lack Thereof) Contributes to a Perceived Reduction in Security Events

When looking at those organizations that had reported cyberattacks through the lens of the degree of endpoint management and security personnel consolidation they reported having completed, it shows a clear connection between consolidation and greater awareness of the security events that have occurred. In essence, consolidated teams see more events because they are better at finding them, whereas groups that are not consolidated are not as good at identifying those events and are more likely to say they haven't experienced any.

Frequency of cyberattack detection based on extent of endpoint management and security personnel consolidation.





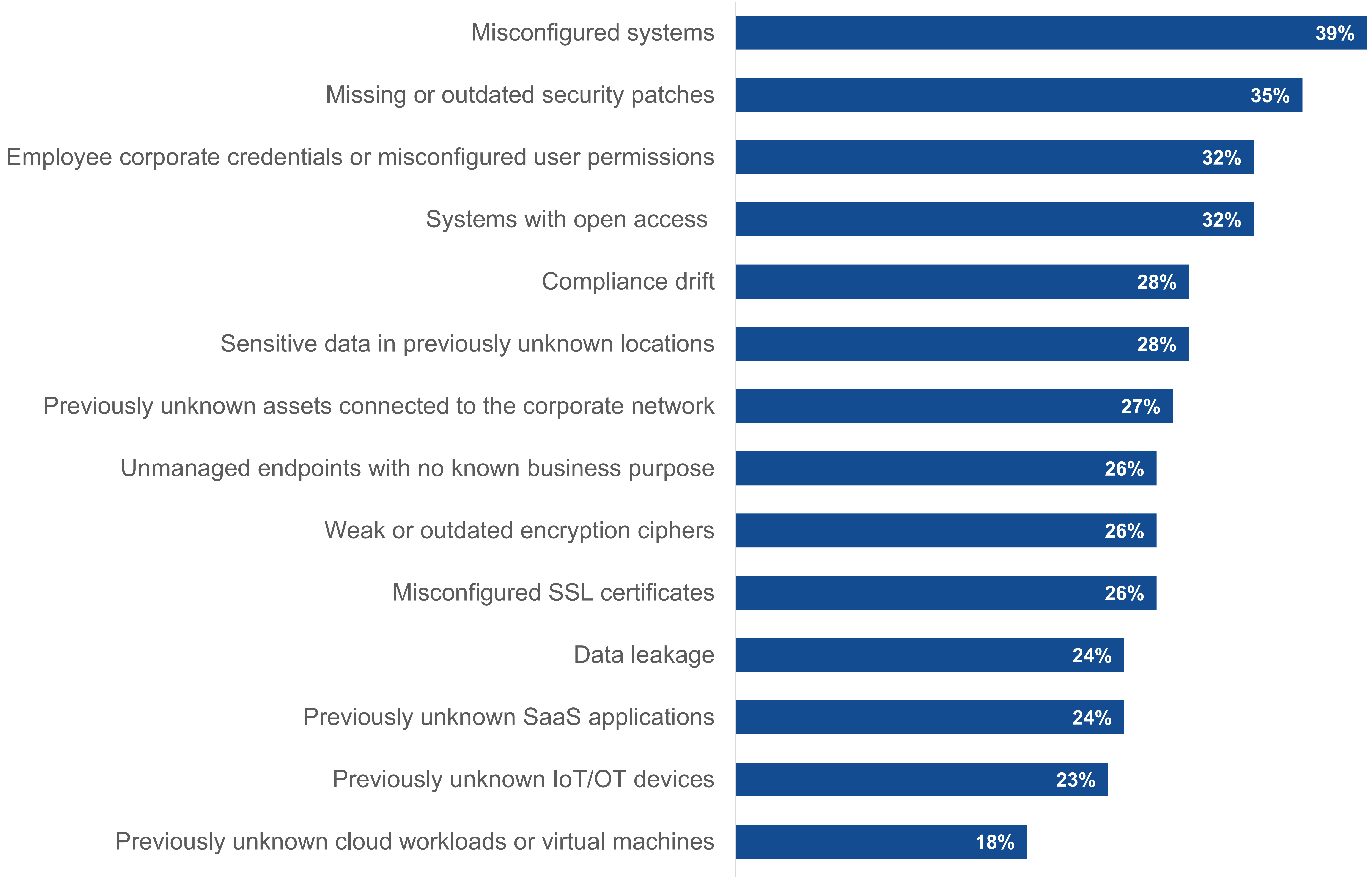
Increasing Visibility Raises Awareness

Likewise, when organizations started looking for problems, they found them. Often, discoveries were related to:

- Basic security hygiene issues (misconfigured systems, 39%, and outdated patches, 35%).
- Access control problems (credential misconfigurations, 32%, and open access, 32%).
- "Unknown" assets representing significant blind spots across environments.

These aren't minor technical issues; they are serious vulnerabilities that could lead to breaches or compliance violations. The 28% discovering sensitive data in unexpected locations is particularly concerning. Critically, these problems existed before these tools were deployed, but they were unknown.

Discoveries stemming from endpoint management and security monitoring.



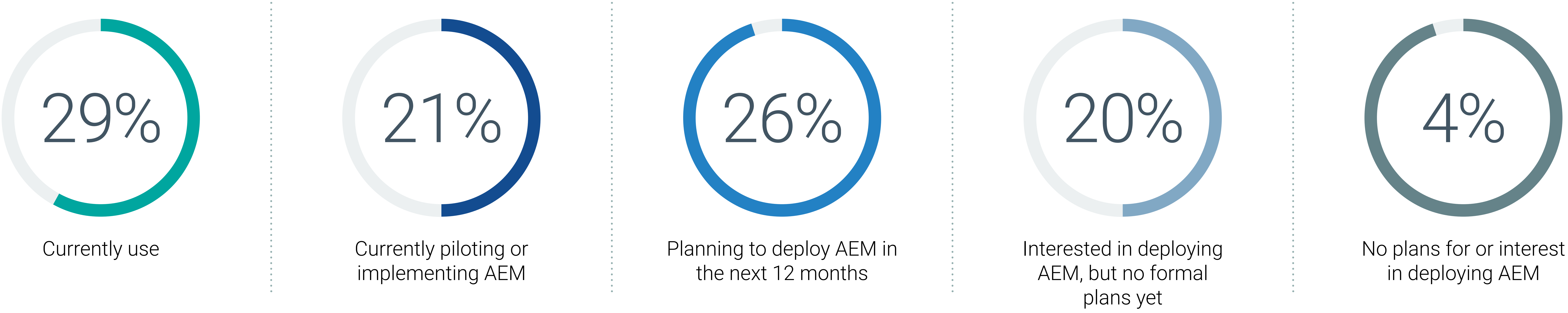
AI and Autonomous Endpoint Management Show Overwhelmingly Positive Initial Impacts

Interest in Autonomous Endpoint Management Is Significant

Autonomous endpoint management (AEM) is an emerging approach to device administration that automates workflows across endpoint management and security processes. It leverages AI, machine learning, and automation to perform tasks such as proactive risk identification, vulnerability detection and remediation, patch and configuration management, and predictive maintenance with minimal human intervention.

Given the increasing complexity and wide-ranging skill gaps observed in this research, it's no surprise that AEM is met with extreme enthusiasm, with just 4% saying the have no plans for or interest in deploying it.

Autonomous endpoint management usage plans.

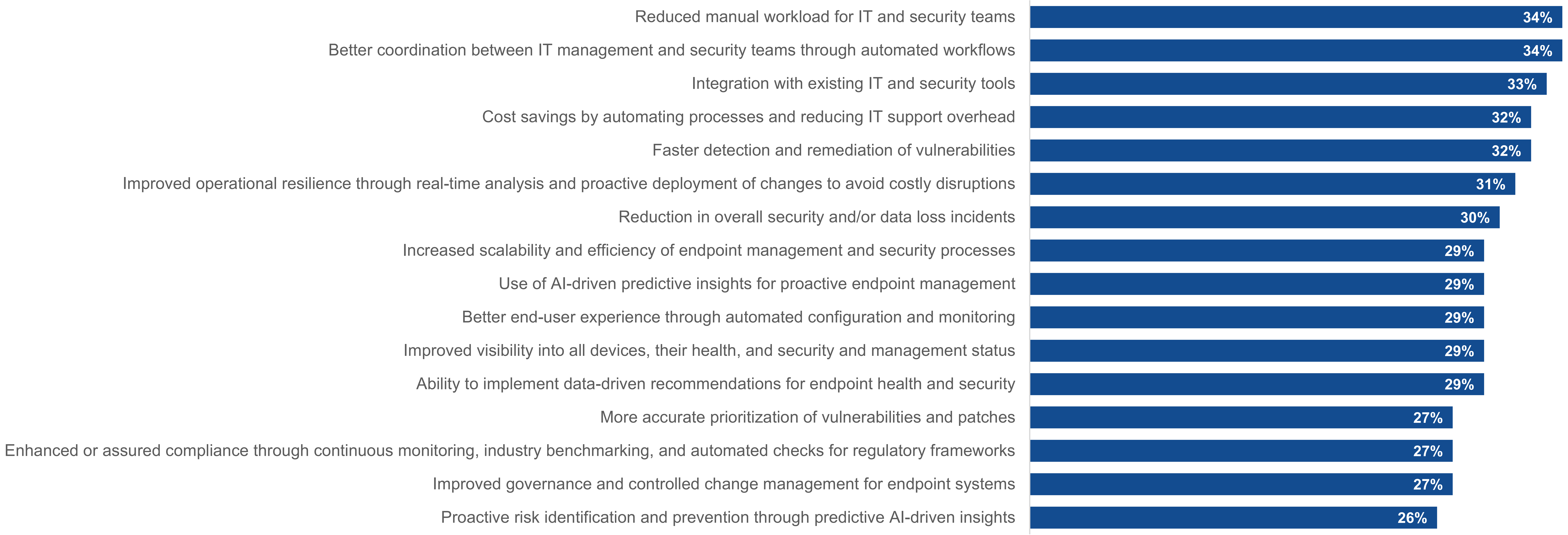


BACK TO CONTENTS

Early Benefits of AEM Are Promising

Organizations exploring AEM are already seeing—or expecting—meaningful benefits. Top-cited outcomes include reduced manual workload, streamlined workflows, and better integration across tools. Security and visibility improvements also rank highly, with respondents pointing to faster threat detection, fewer incidents, and more proactive risk management via AI-driven insights.

Realized or expected benefits of autonomous endpoint management.



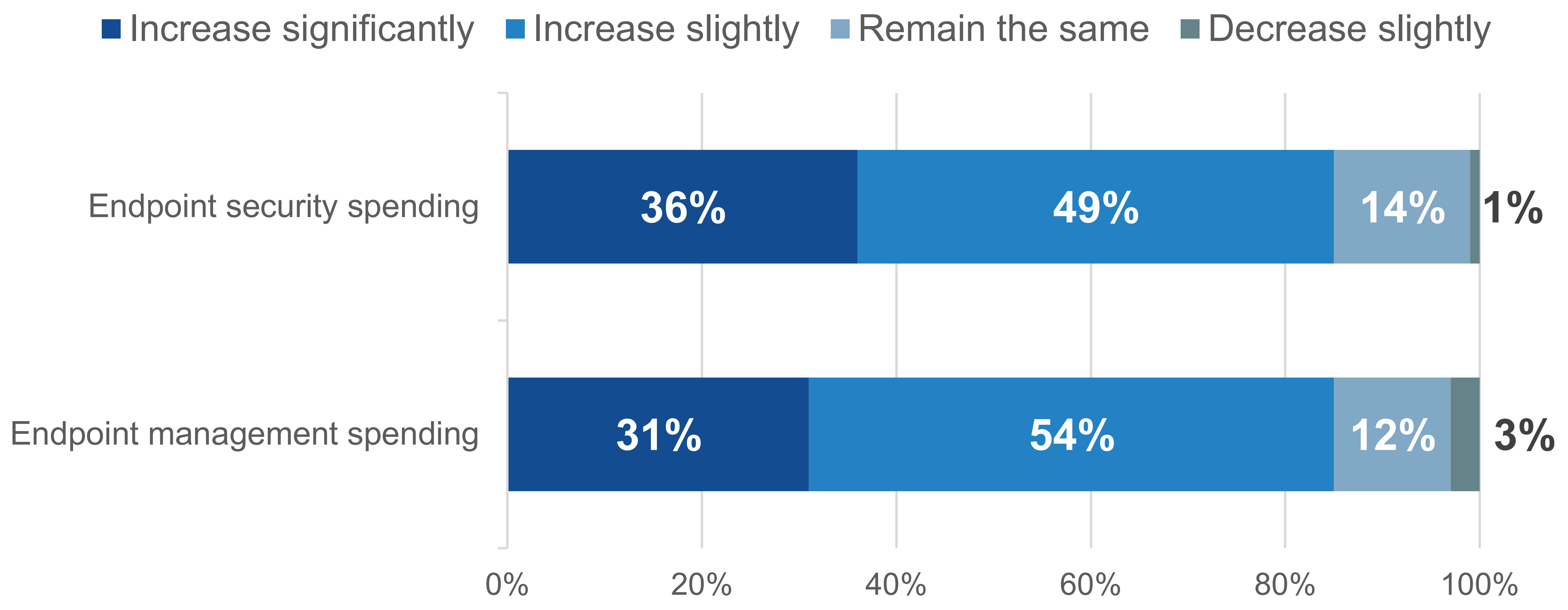
Strategic Investments in Technology and Services Are Key to Success

Widespread, Significant Investments in Endpoint Management and Security Will Continue

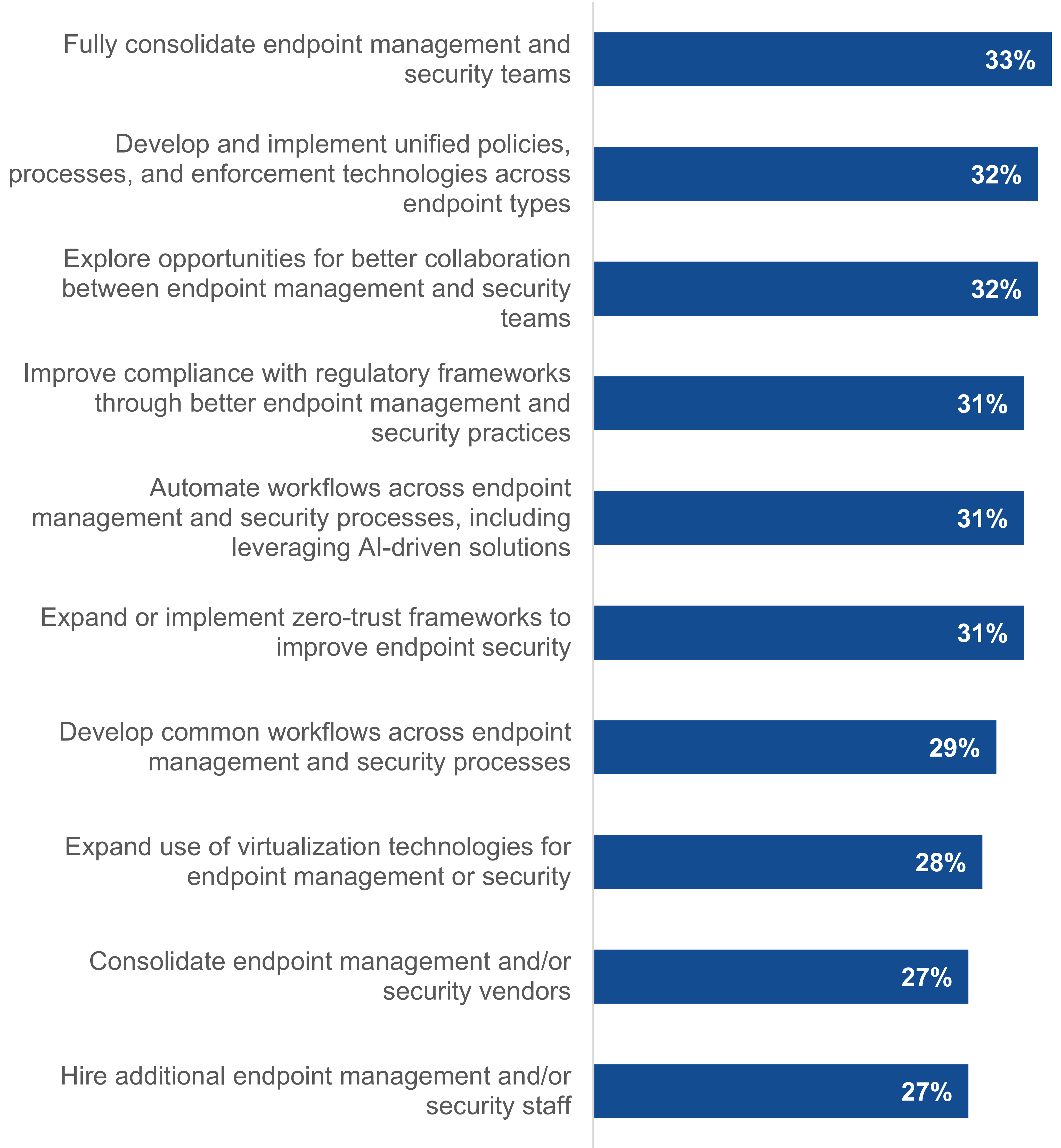
Organizations aren't just pushing through the complexity—they're investing heavily to improve how they handle it. Indeed, 85% of respondents expect to increase spending on both endpoint management and security over the next 12 to 24 months, with roughly a third expecting significant increases in each area

These investments appear to be directed at both tactical needs and long-term strategic shifts. Priorities include consolidating teams and tools, standardizing policies, automating workflows (often with AI), and improving collaboration across IT and security functions. Regulatory compliance, zero-trust frameworks, and expanded virtualization also rank high on the list—indicating a clear focus on both risk mitigation and operational maturity.

Endpoint management and security spending poised for growth over the next 18-24 months.



Top ten actions organizations will take over the next 12-24 months in support of improving endpoint management or security.

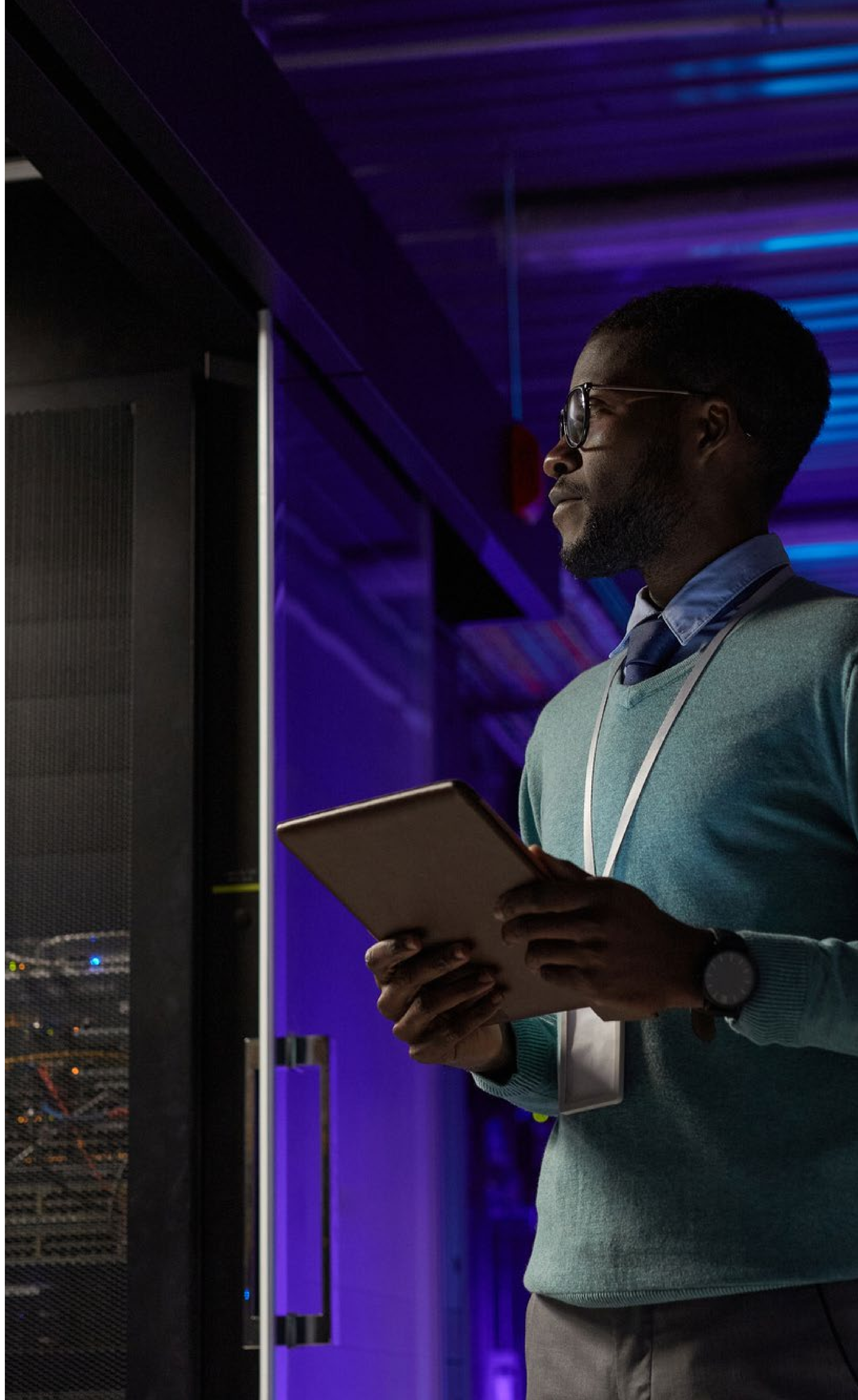


TANIUM™

ABOUT

Tanium Autonomous Endpoint Management (AEM) offers the most comprehensive solution for intelligently managing endpoints across industries, providing capabilities for asset discovery and inventory, endpoint management, vulnerability management, risk and compliance, threat hunting & incident response, and digital employee experience. The platform supports 34M endpoints worldwide, including 40% of the Fortune 100, delivering increasingly efficient operations and an improved security posture at scale, with confidence, and in real-time. For more information on The Power of Certainty™, visit www.tanium.com and follow us on LinkedIn and X.

LEARN MORE

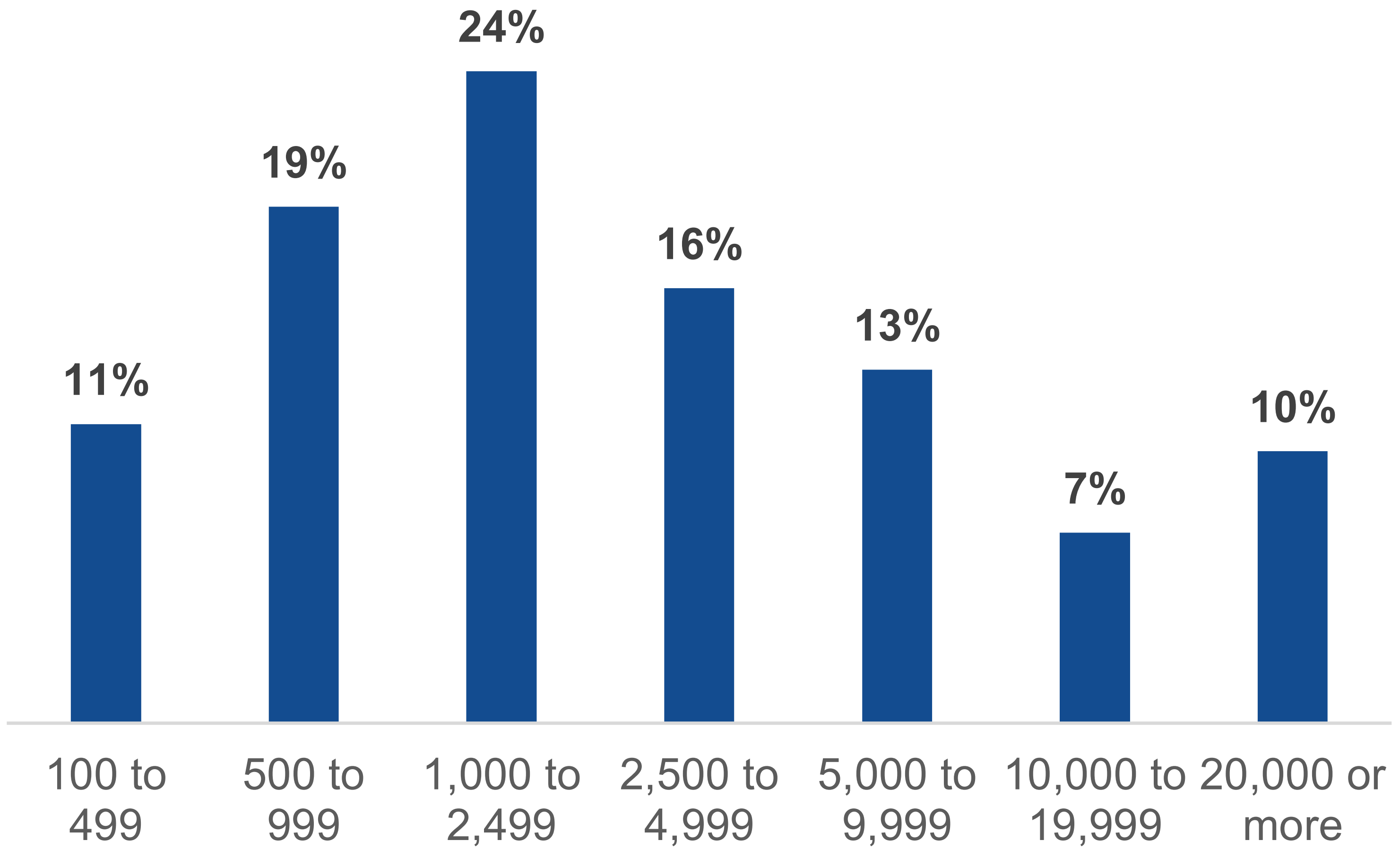


RESEARCH METHODOLOGY AND DEMOGRAPHICS

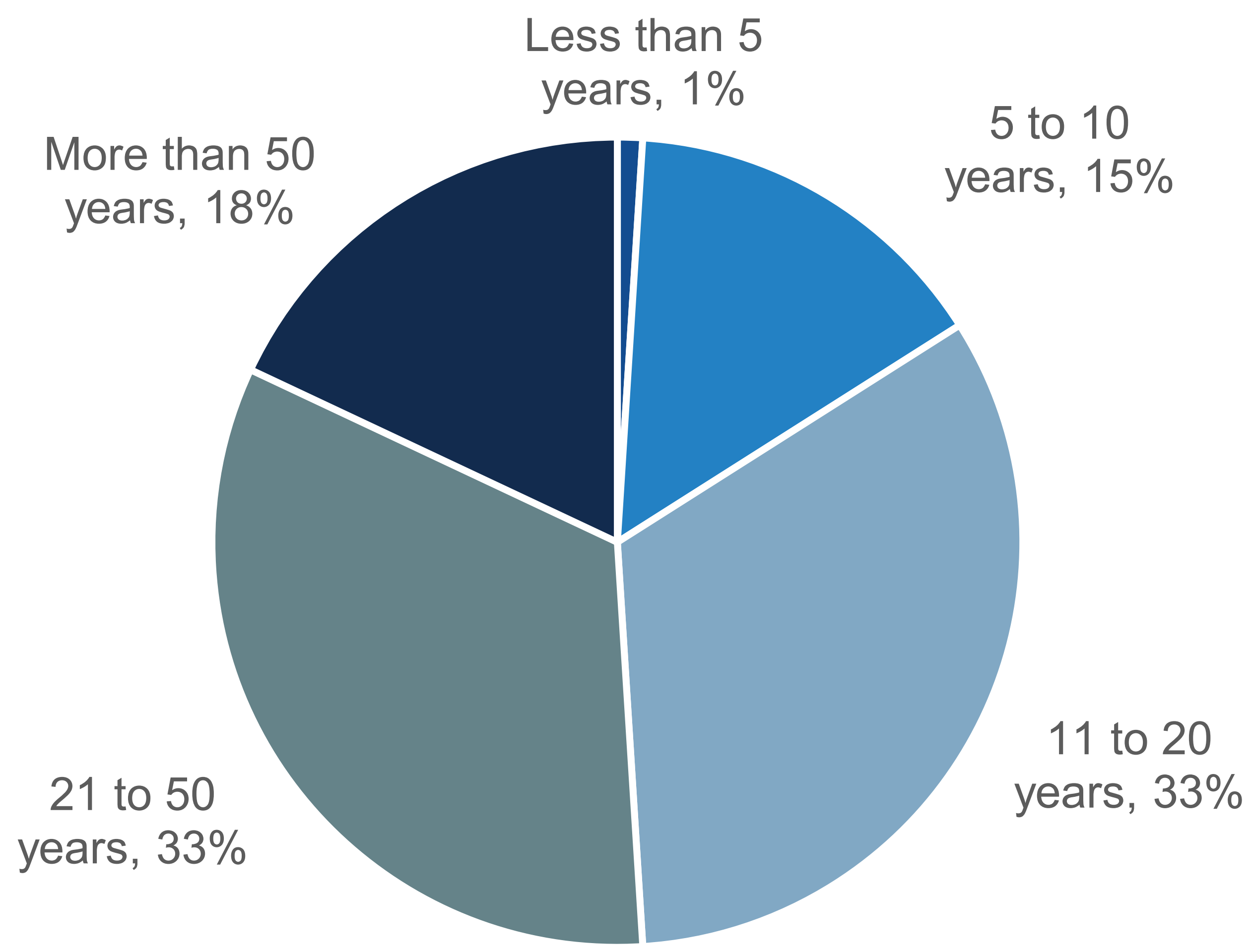
To gather data for this report, Enterprise Strategy Group, now part of Omdia, conducted a comprehensive online survey of IT and cybersecurity professionals from private- and public-sector organizations in North America (United States and Canada) between February 7, 2025 and February 27, 2025. To qualify for this survey, respondents were required to be involved with endpoint management and security technology and processes. All respondents were provided an incentive to complete the survey in the form of cash awards and/or cash equivalents.

After filtering out unqualified respondents, removing duplicate responses, and screening the remaining completed responses (on a number of criteria) for data integrity, we were left with a final total sample of 364 IT and cybersecurity professionals.

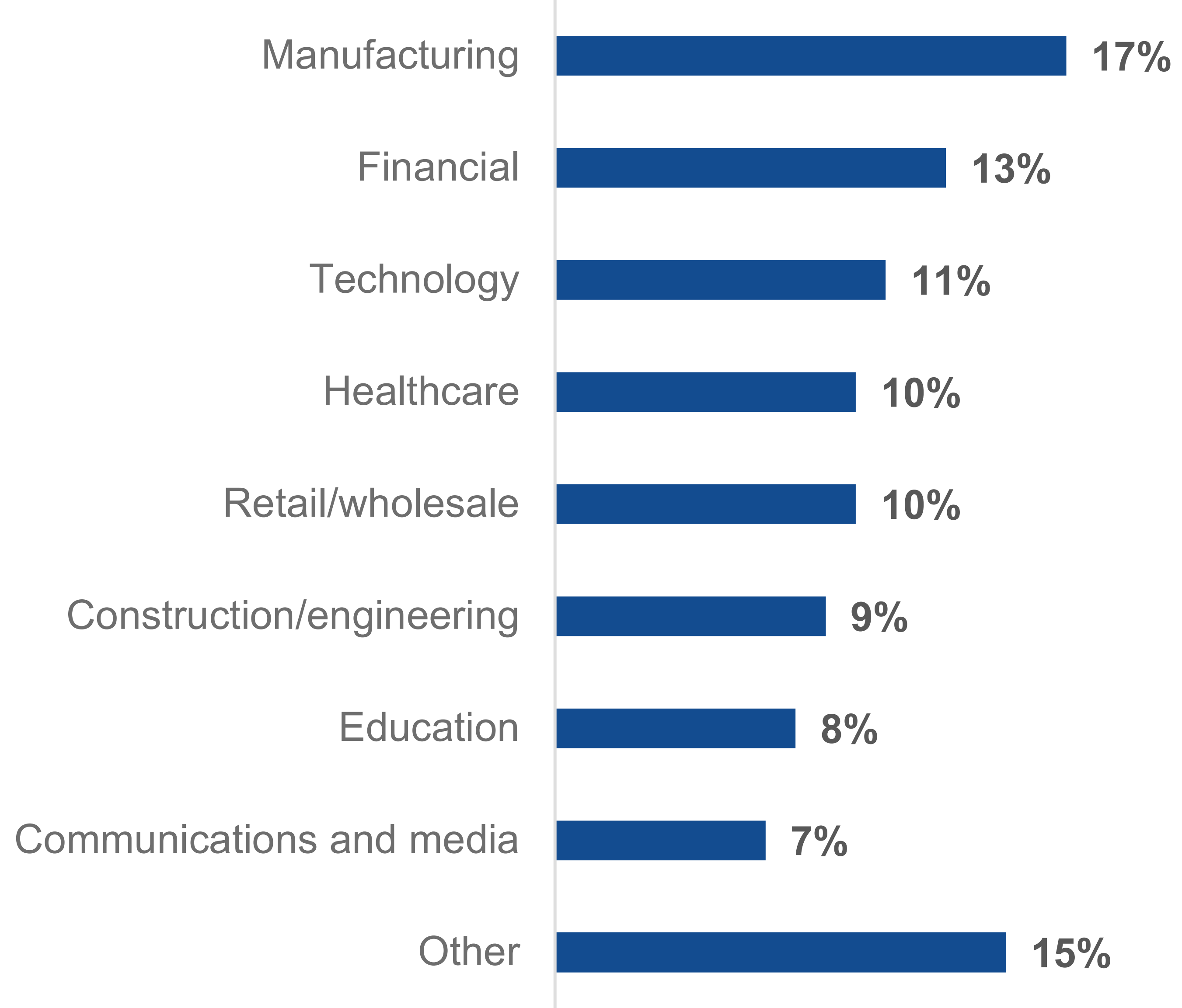
Respondents' organizations by number of employees.



Respondents' organizations by years in operation.



Respondents' organizations by industry.



Enterprise Strategy Group™

Enterprise Strategy Group is an integrated technology analysis, research, and strategy firm providing market intelligence, actionable insight, and go-to-market content services to the global technology community.