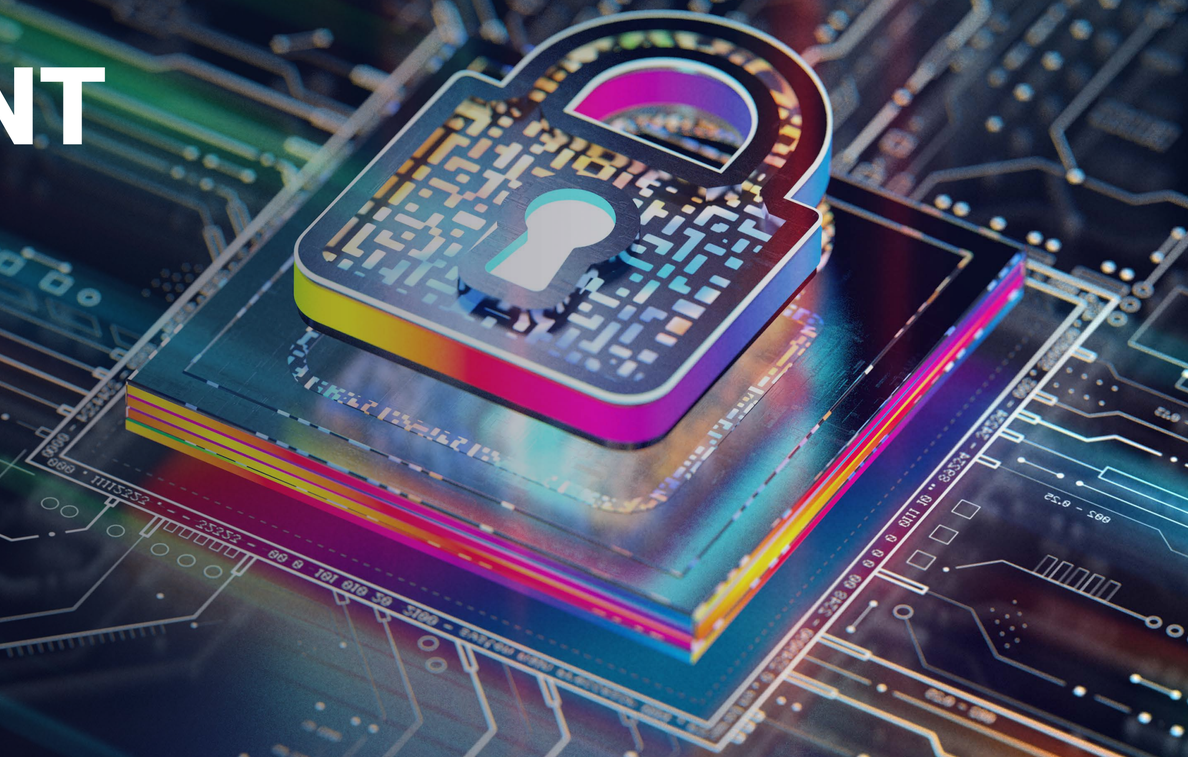
Enterprise Strategy Group™ by TechTarget

MANAGING THE ENDPOINT VULNERABILITY GAP

The Convergence of IT and Security to Reduce Exposure



Gabe Knuth, Senior Analyst
Dave Gruber, Principal Analyst

FEBRUARY 2023

Research Objectives

Requirements from widespread work-from-anywhere policies have escalated the need for endpoint management and security convergence. IT and security teams need broad management, prevention, detection, and response capabilities that span endpoint devices and operating environments that are often outside of their control, which is driving many to desire convergence between management and security capabilities to simplify implementation, ongoing management, and risk mitigation.

IT and security teams require new mechanisms capable of providing common visibility, assessment, mitigation of software and configuration vulnerabilities, threat prevention, and support for threat investigation and response activities. These management and security activities are deeply intertwined, requiring integrated workflows between IT and security teams.

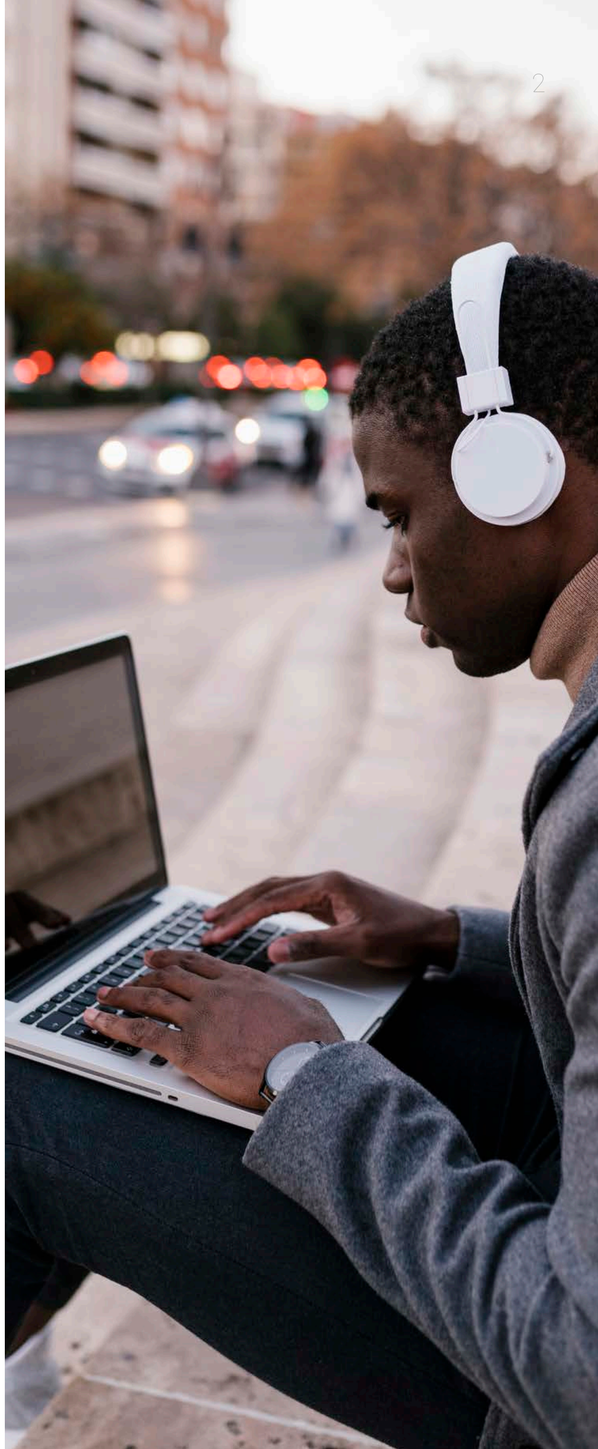
In order to gain further insights into these trends, TechTarget's Enterprise Strategy Group (ESG) surveyed 381 IT and cybersecurity decision makers involved with endpoint management and security technologies and processes at midmarket (100 to 999 employees) and enterprise (1,000 or more employees) organizations in North America (US and Canada).

This study sought to:

Identify challenges, strategies, and trends in endpoint management and security.

Determine how endpoint management and security functions and systems are converging.

Highlight opportunities for improving endpoint management and security fueled by functional convergence.



KEY FINDINGS

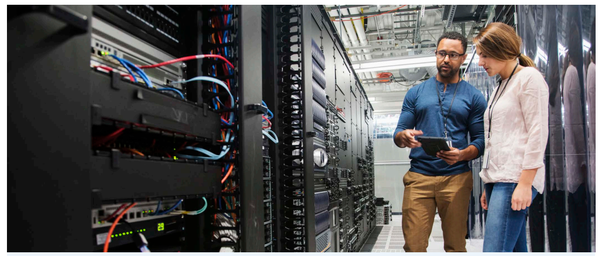
CLICK TO FOLLOW

Broad industry macrotrends are impacting both endpoint management and security.

PAGE 4

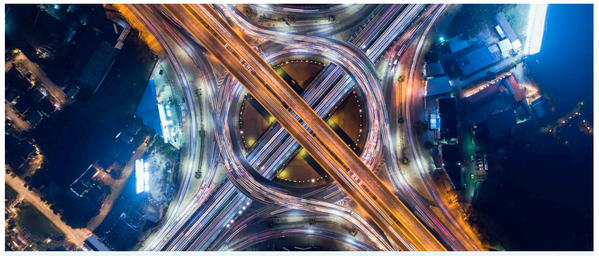
Unmanaged device utilization is on the rise, as are security incidents involving them.

PAGE 9



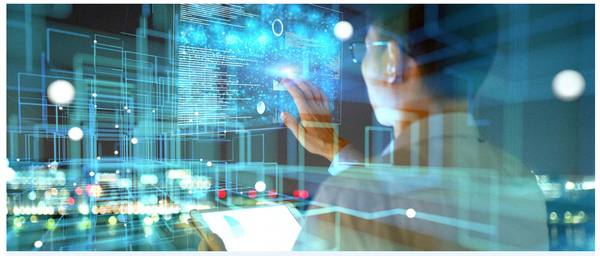
Management and security tool sprawl is driving the desire for better integration and tool consolidation.

PAGE 13



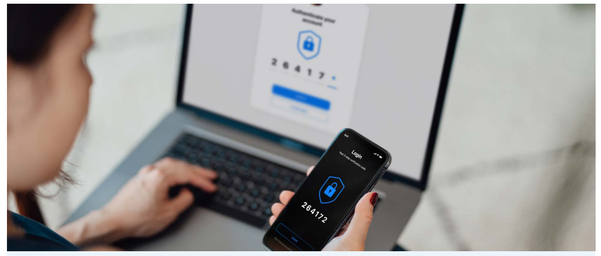
IT and security convergence is well underway, but challenges are plentiful.

PAGE 17



Desktop and app virtualization adoption is on the rise, addressing both management and security challenges.

PAGE 22



IoT presents a significant opportunity for consolidation.

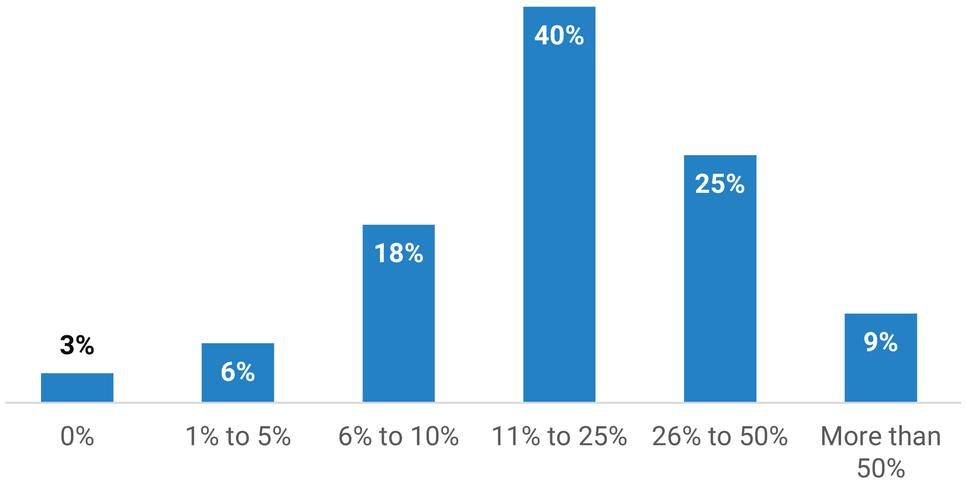
PAGE 25

Broad industry macrotrends are impacting both endpoint management and security.

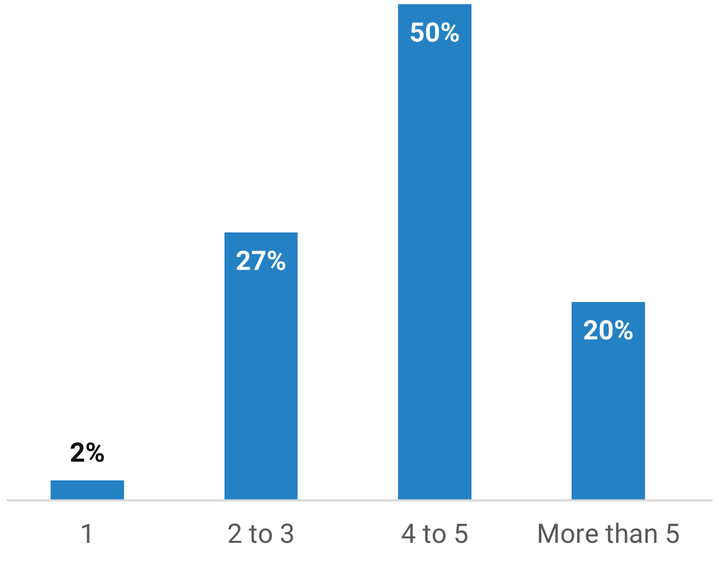
Hybrid Work Strategies Are Pervasive and Usage of Multiple Devices Is The Norm

Modern IT environments were becoming far more distributed even before pervasive work-from-home initiatives stemming from the pandemic caused a spike in remote work. Many organizations continue to support remote and hybrid work strategies for their employees, with almost all stating at least some portion of their workforce works outside of an office setting, and 34% reporting that more than a quarter of their employees work remotely. Employees are also using and interacting with more devices to get work done—both corporate-managed and personally-owned. Across the board, 97% of organizations indicate the average employee interacts with more than one device daily, and the majority report at least four devices per employee. Coupled with the proliferation of hybrid users, there are more devices along a less-defined edge than ever before.

Percentage of employees who work remotely.



Average number of devices employees interact with daily.



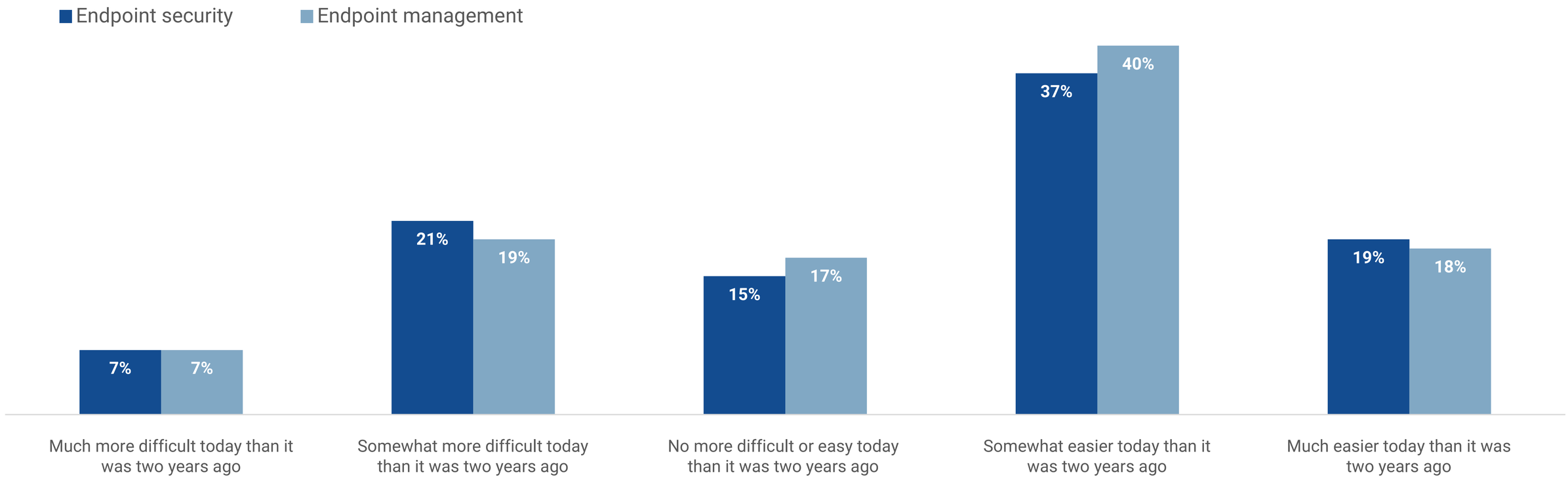
> “97% of organizations indicate the average employee interacts with **more than one device daily.”**

BACK TO CONTENTS

Consensus Is that Endpoint Security and Management Have Gotten Easier

This is likely because a few years ago, teams had to scramble to support pandemic-related work-from-home or shelter-in-place policies, so the procedures for managing endpoints had to be modernized to support the remote user. That initial motivation to rapidly modernize has been refined over the last few years as mandates and preferences to work remotely persist, leading to an overall easier and smoother operating environment today that supports hybrid users regularly.

Difficulty of securing and managing devices compared to two years ago.

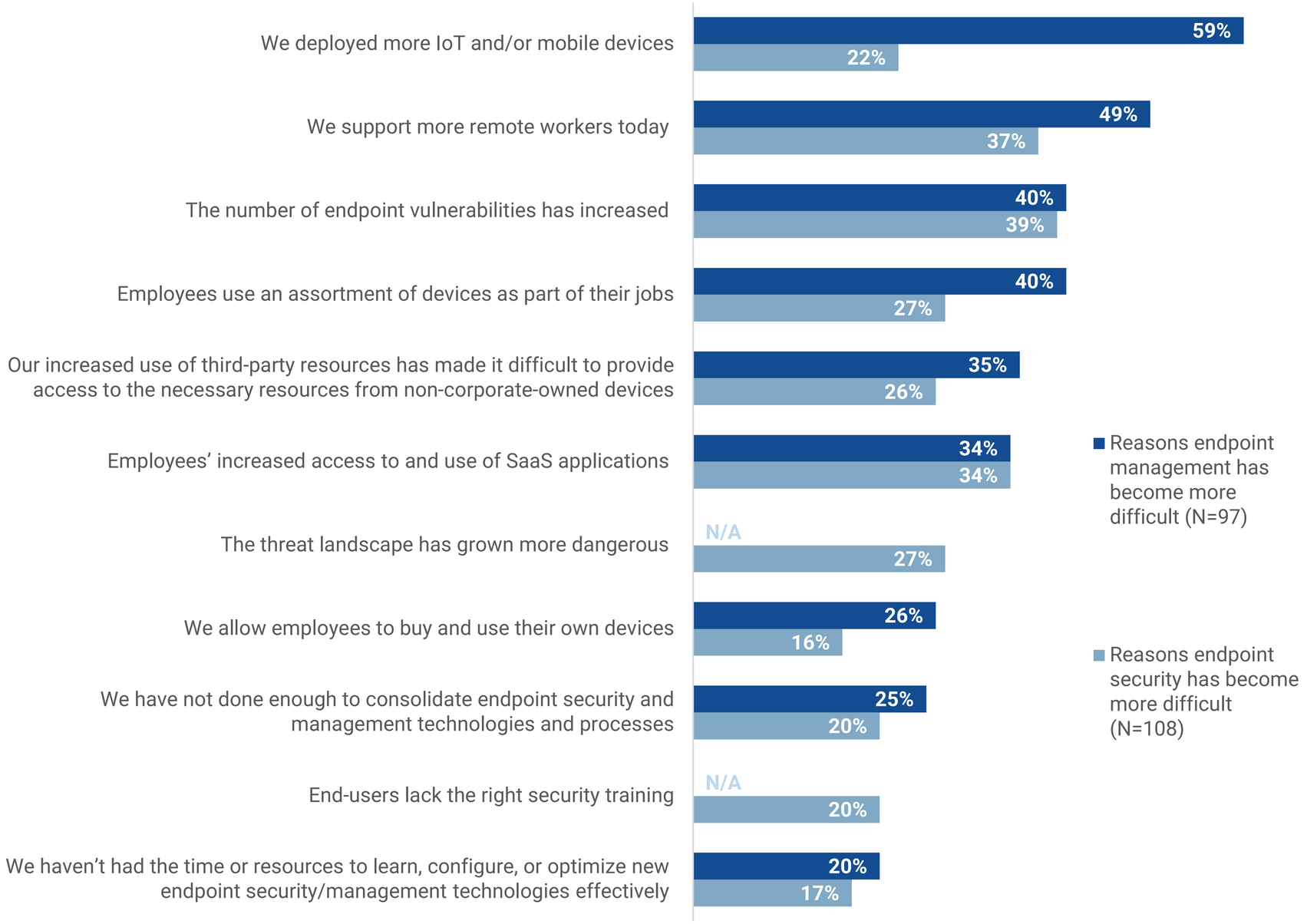


BACK TO CONTENTS

What Is Driving Increased Difficulty Securing and Managing Endpoints?

For those reporting increased difficulty securing and managing endpoints, the one-word answer to this question is “sprawl.” Organizations noted they are deploying more IoT and mobile devices, utilizing more SaaS apps (and increasing the use of them), and accommodating more bring-your-own-device usage. This all results in not only increased management responsibilities, but also exposure to more potential vulnerabilities.

Reasons securing and managing devices have become more difficult.



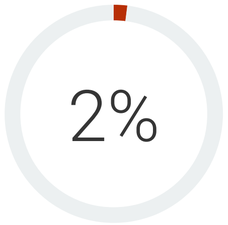
BACK TO CONTENTS

Despite Endpoint Security Confidence, Most Still Have Blind Spots

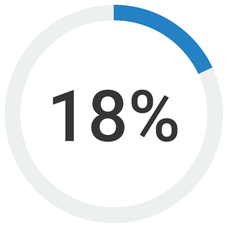
How pervasive is security monitoring for endpoints, including scanning for vulnerabilities, detecting deviations from approved configuration settings, and identifying rogue software and misconfigured security software? While 80% of organizations are actively monitoring at least half of their devices, only 10% do so for all of their endpoints. This means that while organizations have an idea of what the majority of their devices are doing, there are opportunities to expand.

This also indicates numerous blind spots in these programs, so the organizations that actively monitor fewer devices are much likelier to have experienced several endpoint-specific cyber-attacks. Fortunately, those same organizations are also overwhelmingly planning on increasing their spending on security and endpoint management, presumably to get a handle on monitoring, among other priorities.

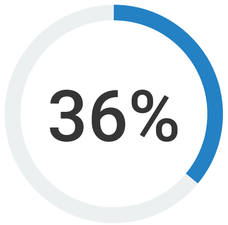
| Percentage of endpoints that are actively monitored.



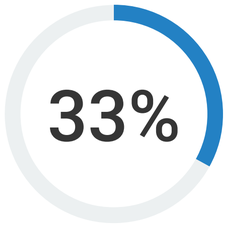
MONITOR LESS THAN 25% OF THEIR ENDPOINTS



MONITOR BETWEEN 25% AND 49% OF THEIR ENDPOINTS



MONITOR BETWEEN 50% AND 74% OF THEIR ENDPOINTS



MONITOR BETWEEN 75% AND 99% OF THEIR ENDPOINTS

MONITOR 100% OF THEIR ENDPOINTS

Organizations Actively Monitoring Fewer Devices Likelier to Have Experienced Several Cyber-attacks…

Percentage of organizations that have experienced **several cyber-attacks** due to unmanaged endpoints:

- **47%** actively monitor <50% of endpoints
- **32%** actively monitor 50%-74% of endpoints
- **30%** actively monitor 75+% of endpoints

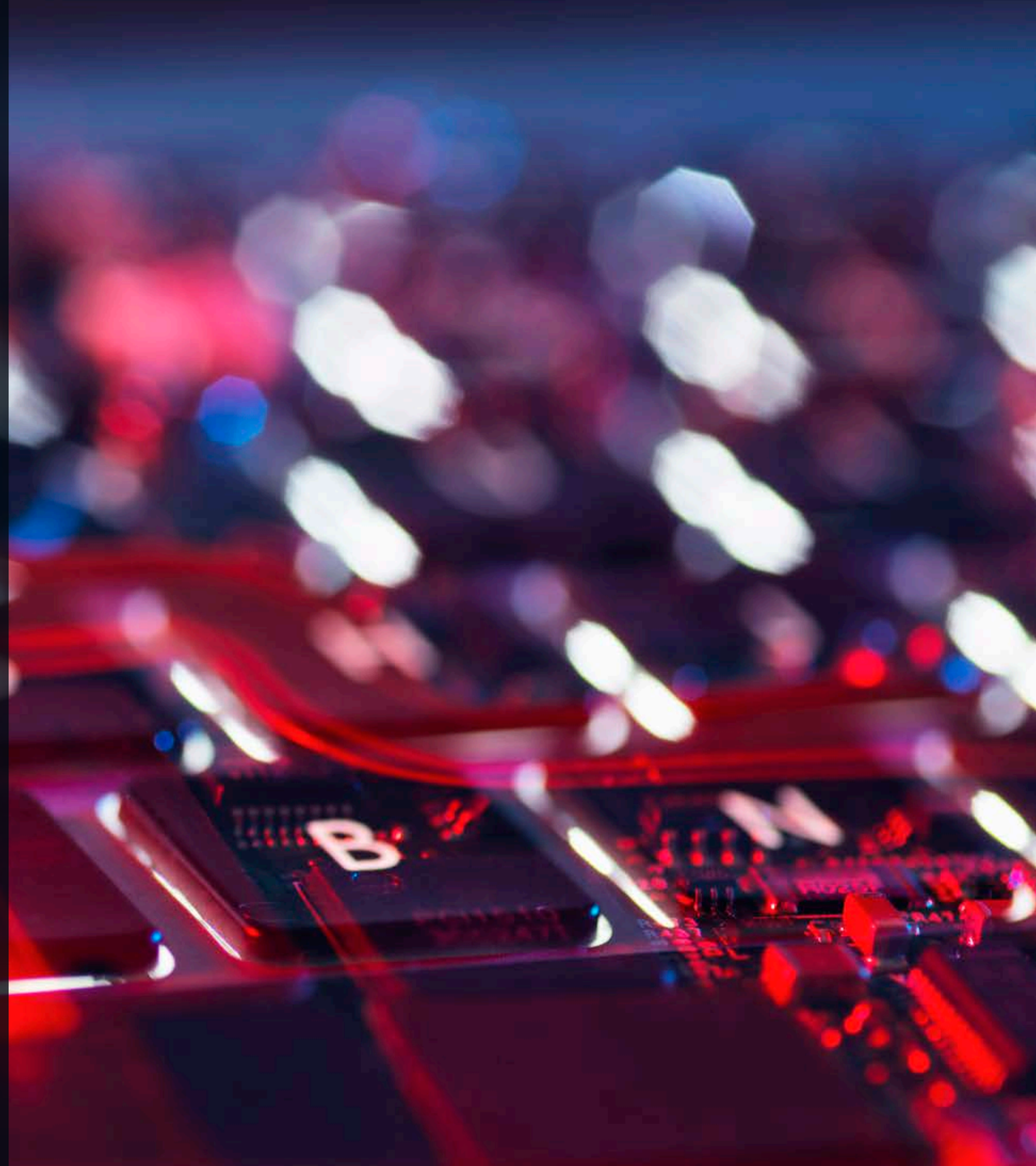
…But Are Also Likelier to Significantly Increase Endpoint Security Spending

Percentage of organizations that expect to **significantly increase** endpoint security spending:

- **59%** actively monitor <50% of endpoints
- **44%** actively monitor 50%-74% of endpoints
- **40%** actively monitor 75+% of endpoints

BACK TO CONTENTS

Unmanaged device utilization is on the rise, as are security incidents involving them.

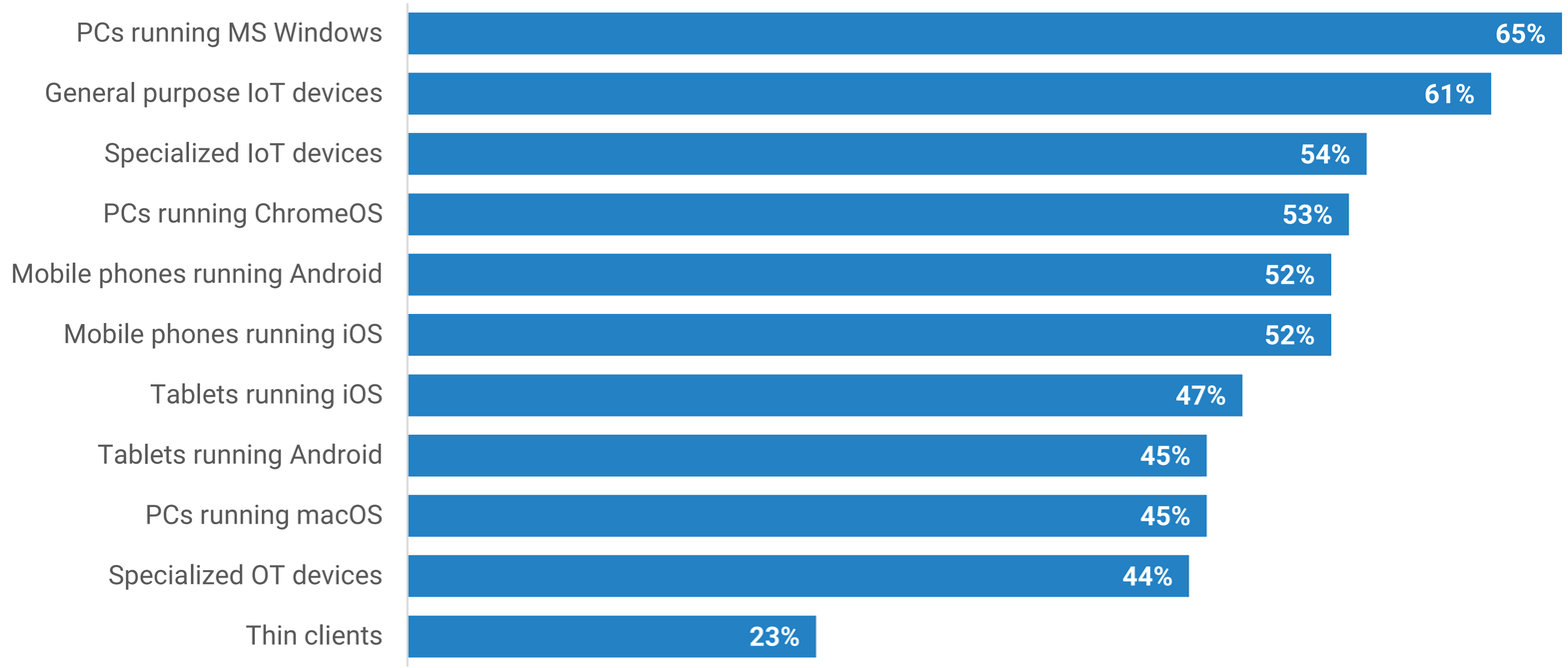


Device Diversity Is on the Rise, Driving Up Instances of Unmanaged Devices

Organizations are supporting a lot of endpoint devices and, increasingly, a wide array of device types ranging from PCs, IoT devices, mobile phones, and tablets to even thin clients. This leads to many different operating systems, as well as monitoring, security, and management platforms and approaches. Each device type increases not only management responsibilities, but also the potential attack surface. Ultimately, this means a larger security footprint and more devices that need some kind of management, even if it's zero trust.

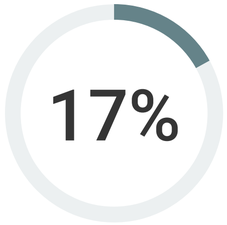
Compounding the issue of increasing device diversity is the fact that organizations report having a significant number of unmanaged devices in their environments. Indeed, more than one-quarter (28%) of respondents reveal that at least one in five of their organization's endpoint devices are unmanaged. As this problem persists, or even expands, new hybrid security strategies that leverage modern security approaches and technologies are needed.

Types of endpoint devices currently under management.



Approximate percentage of all endpoint devices considered **unmanaged**.

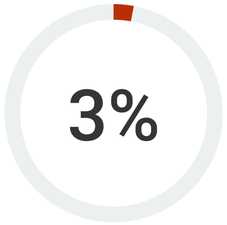
SAY LESS THAN 5% OF DEVICES ARE UNMANAGED



SAY 5% - 10% OF DEVICES ARE UNMANAGED

SAY 11% - 20% OF DEVICES ARE UNMANAGED

SAY 21% - 30% OF DEVICES ARE UNMANAGED



SAY MORE THAN 30% OF DEVICES ARE UNMANAGED

BACK TO CONTENTS

Have organizations experienced cyber-attacks caused by an unknown, unmanaged, or poorly managed endpoint?

Of the organizations that have experienced **several** cyber-attacks, **what percentage of their endpoints are unmanaged?**

Majority Have Experienced Attacks Relating to Device Management

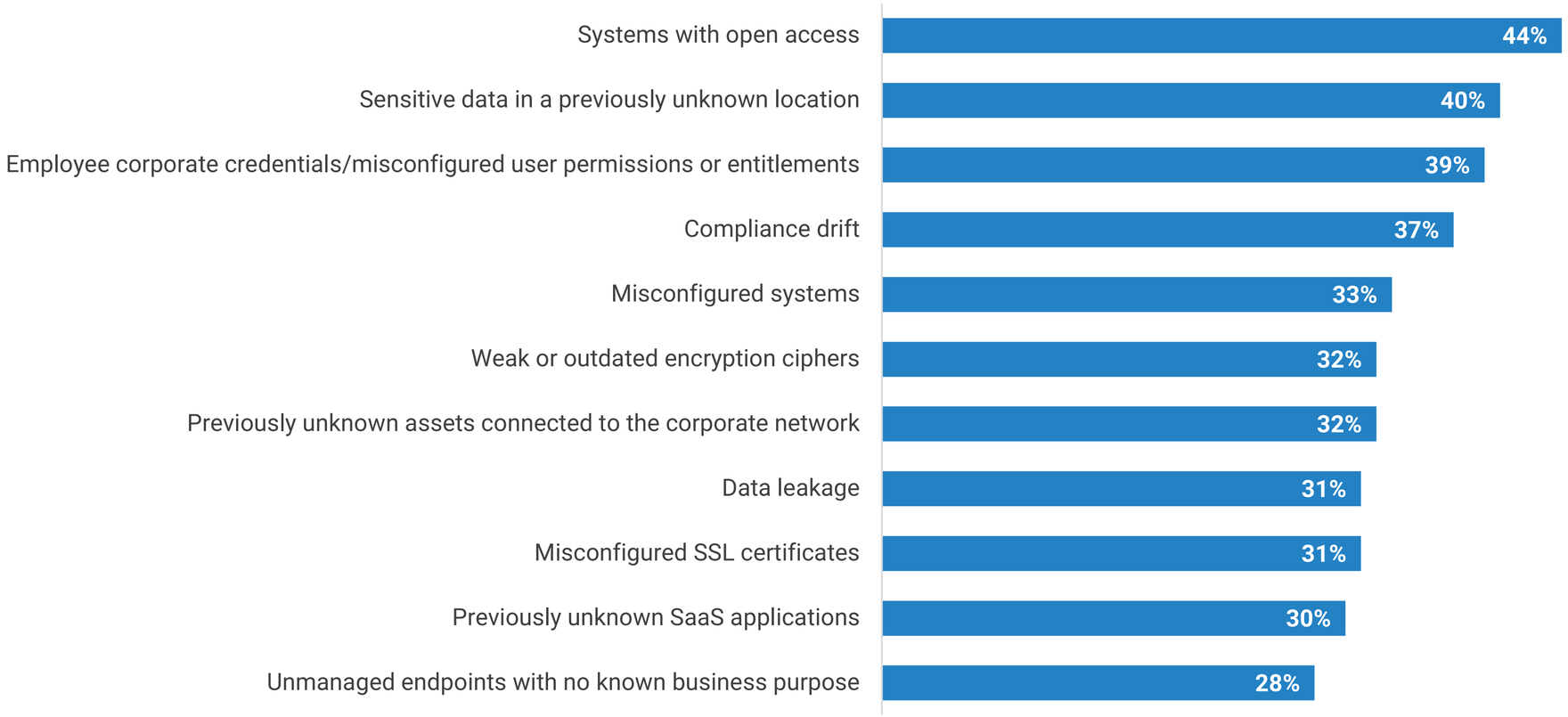
These trends have real-world effects, with more than three-quarters of organizations reporting that they experienced at least one (43%) or several (34%) cyber-attacks caused by an unknown, unmanaged, or poorly managed endpoint devices. Tellingly, organizations with higher percentages of unmanaged devices are more likely to report experiencing several cyber-attacks stemming from these unmanaged devices. Specifically, those organizations exceeding the 20% threshold in terms of unmanaged devices are nearly 11x likelier than those with less than 5% unmanaged devices to have experienced several endpoint-focused cyber-attacks.

BACK TO CONTENTS

Use of Endpoint Management and Monitoring Solutions Can Help to Identify Potential Exploits

Through the use of endpoint management and security monitoring, organizations have discovered a myriad of potential breach points that could be used as vectors of cyber-attacks. For example, 44% of organizations found systems with open access, while four in ten identified sensitive data in a previously unknown location. This demonstrates that even companies that think their endpoint environments are in good shape can benefit from monitoring.

Vulnerabilities discovered as part of endpoint management and security monitoring.



> **“44% of organizations found systems with open access,** while four in ten identified sensitive data in a previously unknown location.”

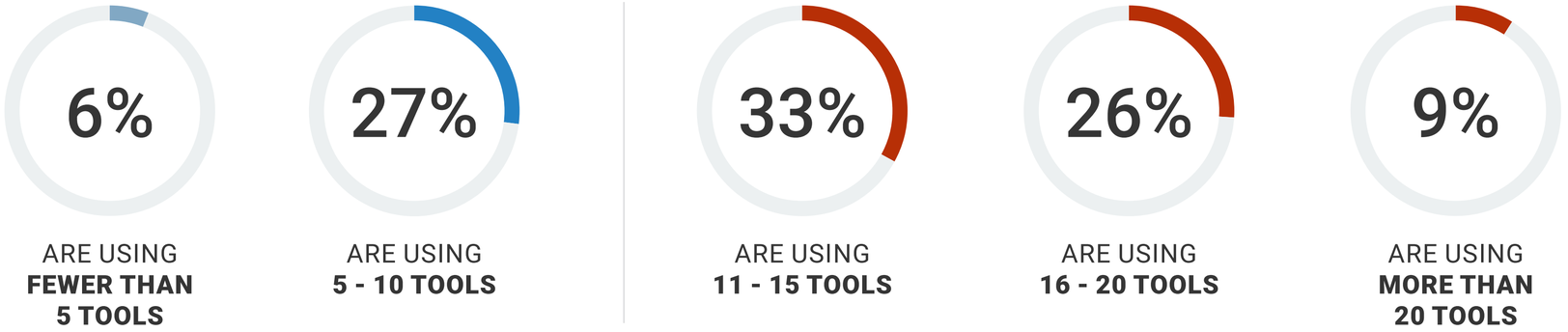
BACK TO CONTENTS

Management and security tool sprawl is driving the desire for better integration and tool consolidation.

Significant Proliferation of Security and Management Tools

As previously seen, organizations are supporting more device types and accompanying OSes, which equates to more management and security tools. But when does it become unsustainable to keep adding tools? More than two-thirds of respondents say their organization is using more than 10 of these tools. Multiple tool use adds layers of management complexity, and it's questionable whether this even helps to reduce attacks.

| Number of different tools and technologies used for endpoint management and security.



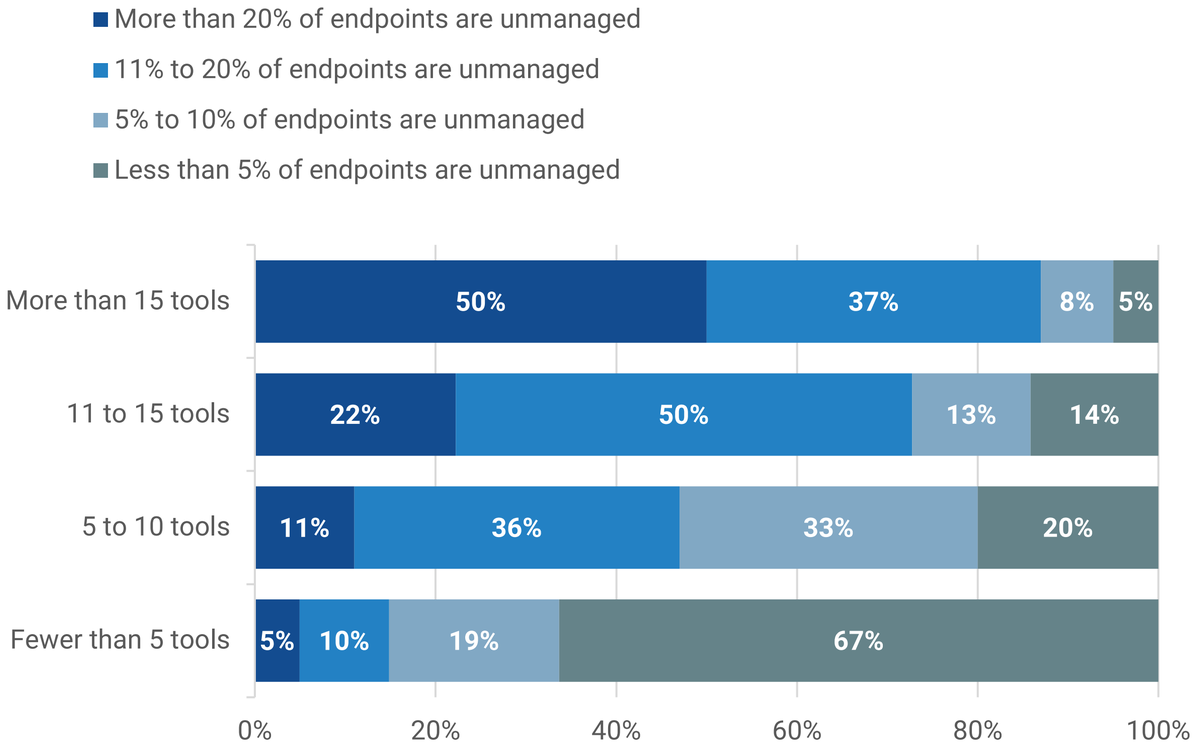
"More than two-thirds of respondents say their organization **is using more than 10 of these tools.**"

BACK TO CONTENTS

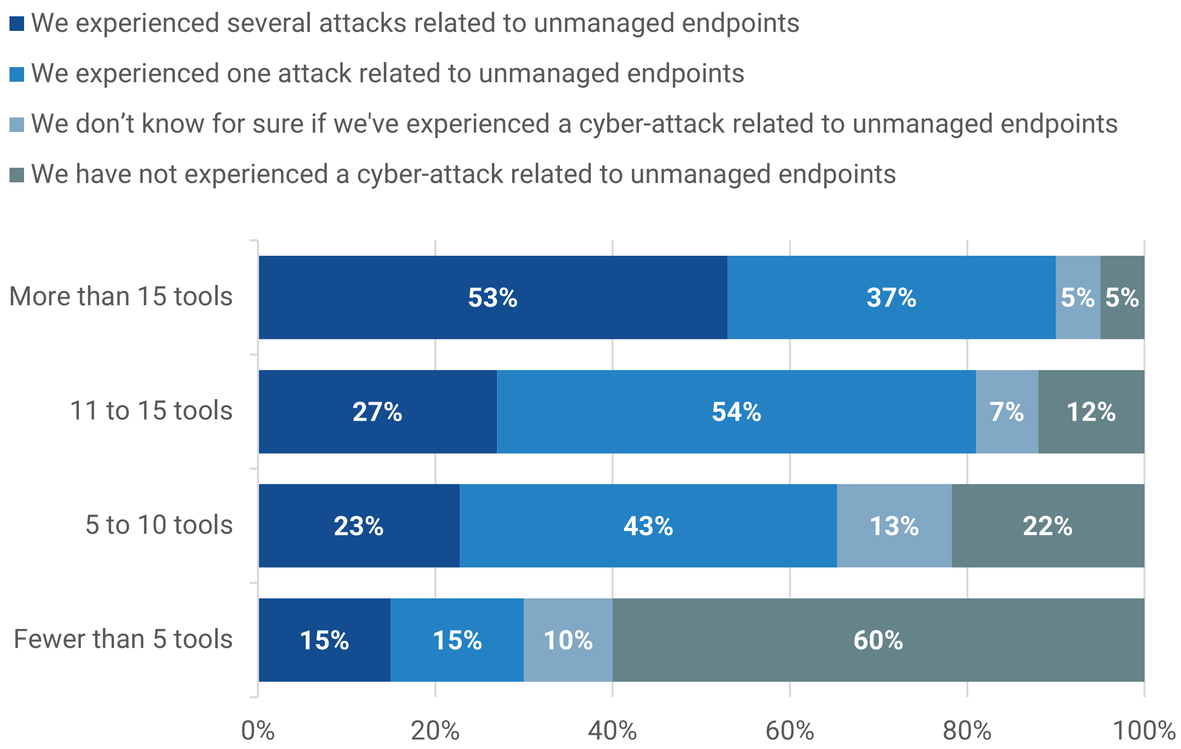
Endpoint Security and Management Tool Sprawl Is Having an Effect

What is the profile of those organizations leveraging more endpoint security and management tools? There is a high correlation between those using more tools and those who not only have larger percentages of unmanaged devices but also have been victimized by endpoint attacks more than once. Specifically, half of organizations with more than 15 endpoint security/management tools report more than 20% of their devices are unmanaged, compared with only 5% of those with fewer than five tools. Likewise, more than half (53%) of organizations with more than 15 tools have experienced several cyber-attacks related to unmanaged endpoints, compared with only 15% of those with fewer than five tools. Some of this can be explained by overall organizational size and complexity, but it brings up the question of whether there is a point of diminishing returns.

Percentage of endpoint devices that are unmanaged by the total number of endpoint security and management tools deployed.



Percentage of organizations that have experienced cyber-attacks due to unmanaged endpoints by the total number of endpoint security and management tools deployed.

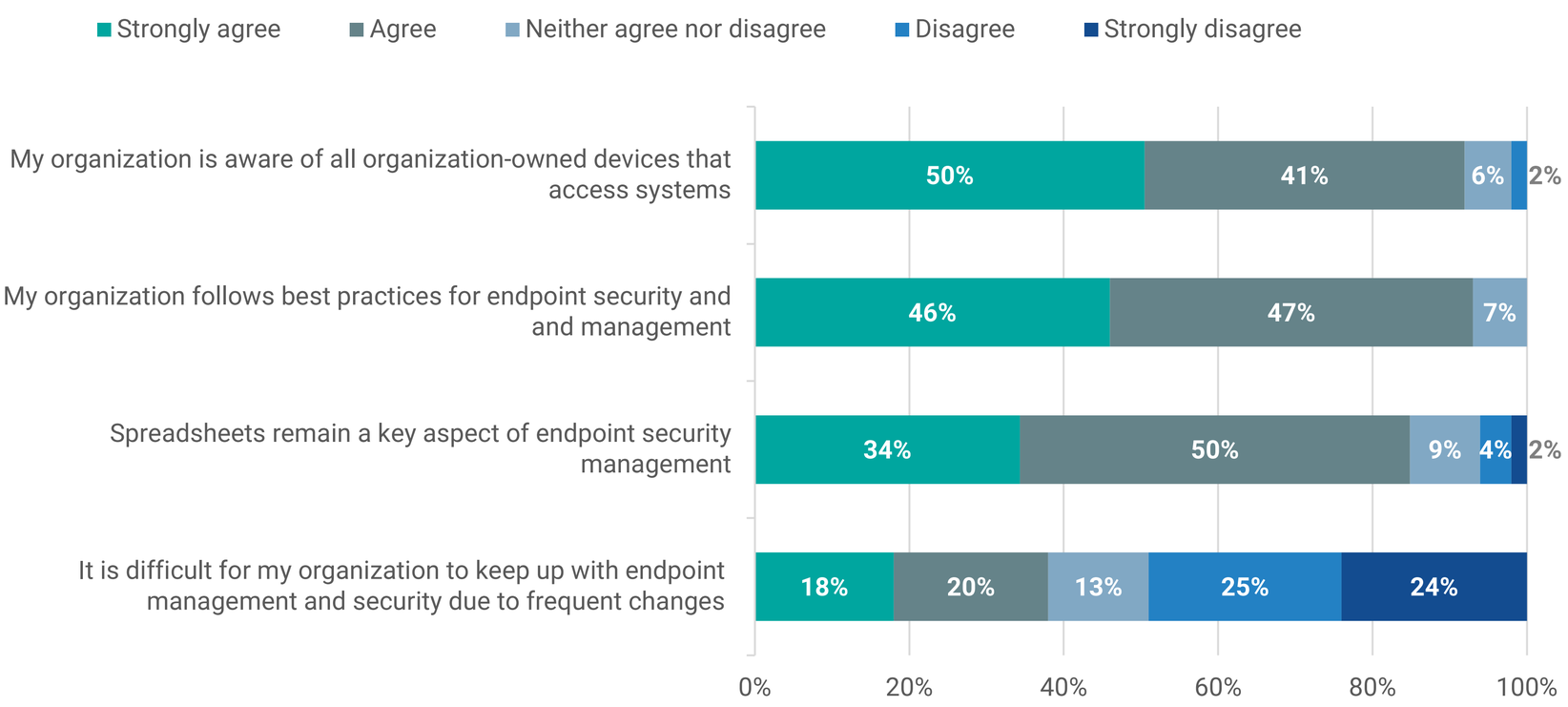


BACK TO CONTENTS

Spreadsheets Do *Not* Equate to Best Practices

While more than 90% of respondents feel like they have awareness of their organization-owned devices and follow best practices for endpoint security and management, more than one-third (38%) still find it difficult to keep up with endpoint management and security due to frequent changes. With 84% reporting a continued use of spreadsheets as a key aspect of their endpoint security management program, more integrated, automated management and security tools are needed. Organizations need ways to introduce more automation into their practices for processes that aren't getting enough focus, such as automated risk assessments and remediation/patching, device visibility, and cross-team collaboration.

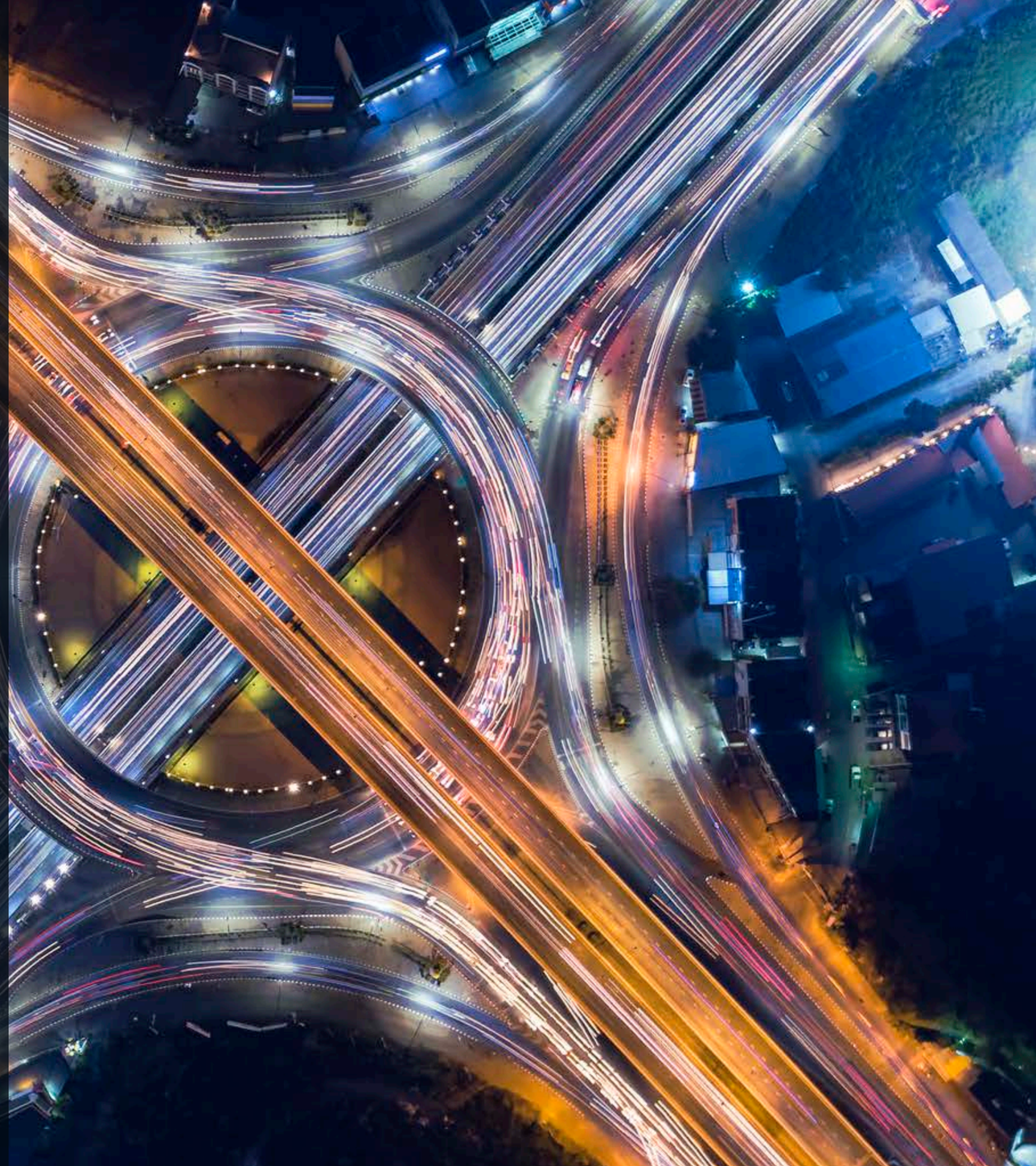
Opinions on endpoint management and security.



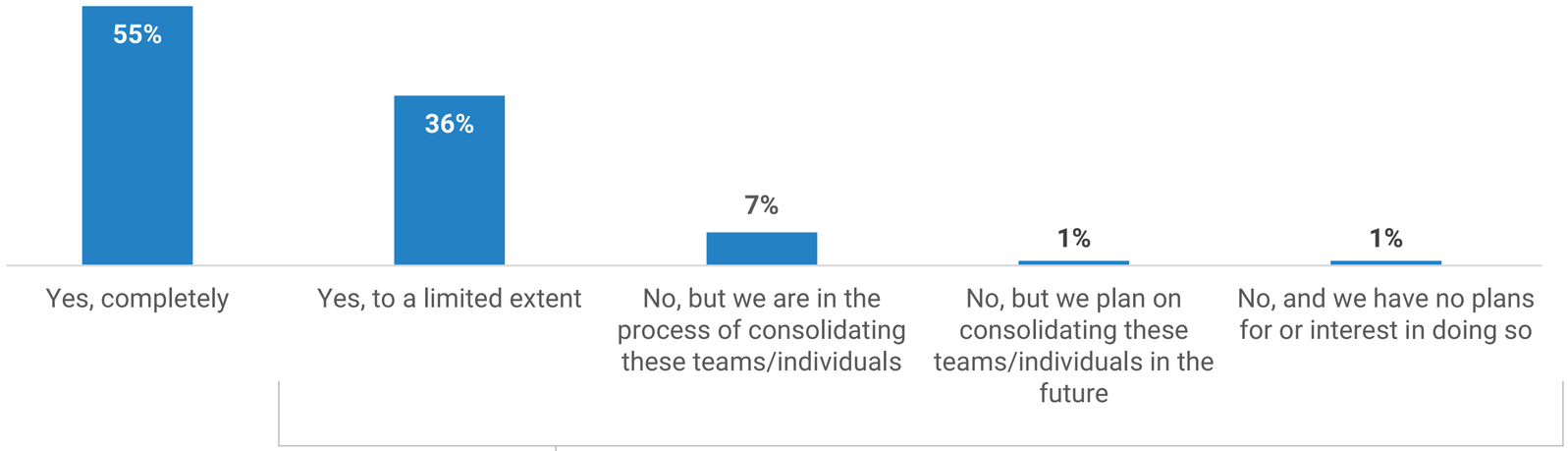
> "With 84% reporting a continued use of spreadsheets as a key aspect of their endpoint security management program, **more integrated, automated management and security tools are needed.**"

BACK TO CONTENTS

IT and security convergence is well underway, but challenges are plentiful.

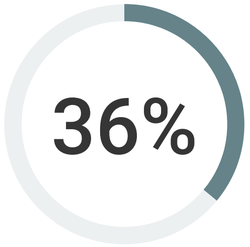


Have organizations consolidated the teams or individuals responsible for endpoint management and security?



Will these organizations eventually have one team responsible for both endpoint management and security?

Yes

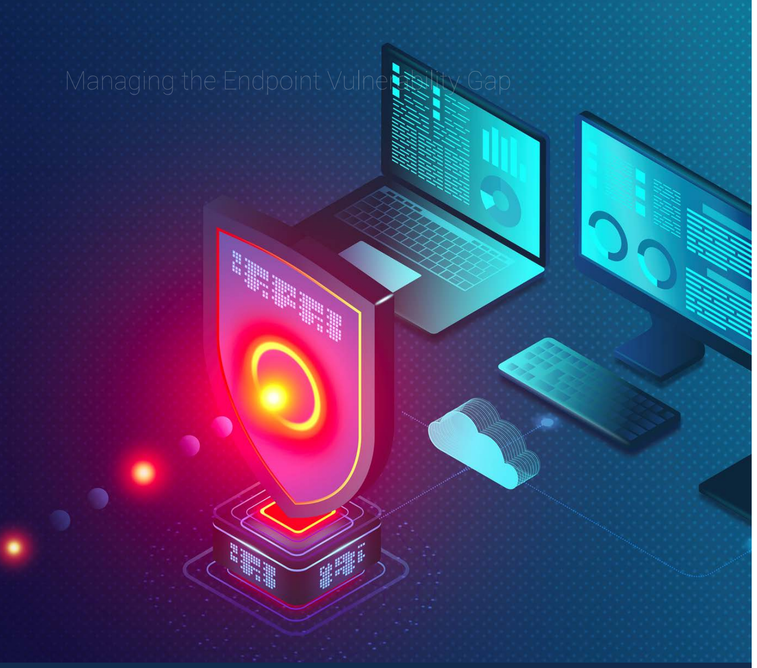


Maybe,
but too early to tell

Endpoint Management and Security Are Overwhelmingly Converging

Organizations are showing a clear preference to combine endpoint security and management rather than maintaining separate teams/responsibilities, with more than half (55%) reporting that they've already completely converged the two functions. Furthermore, the vast majority of those still operating separately can see a time when they will eventually operate as one. Endpoint management and security technology solution providers need to accelerate the convergence of tools to support this fast-moving organizational trend.

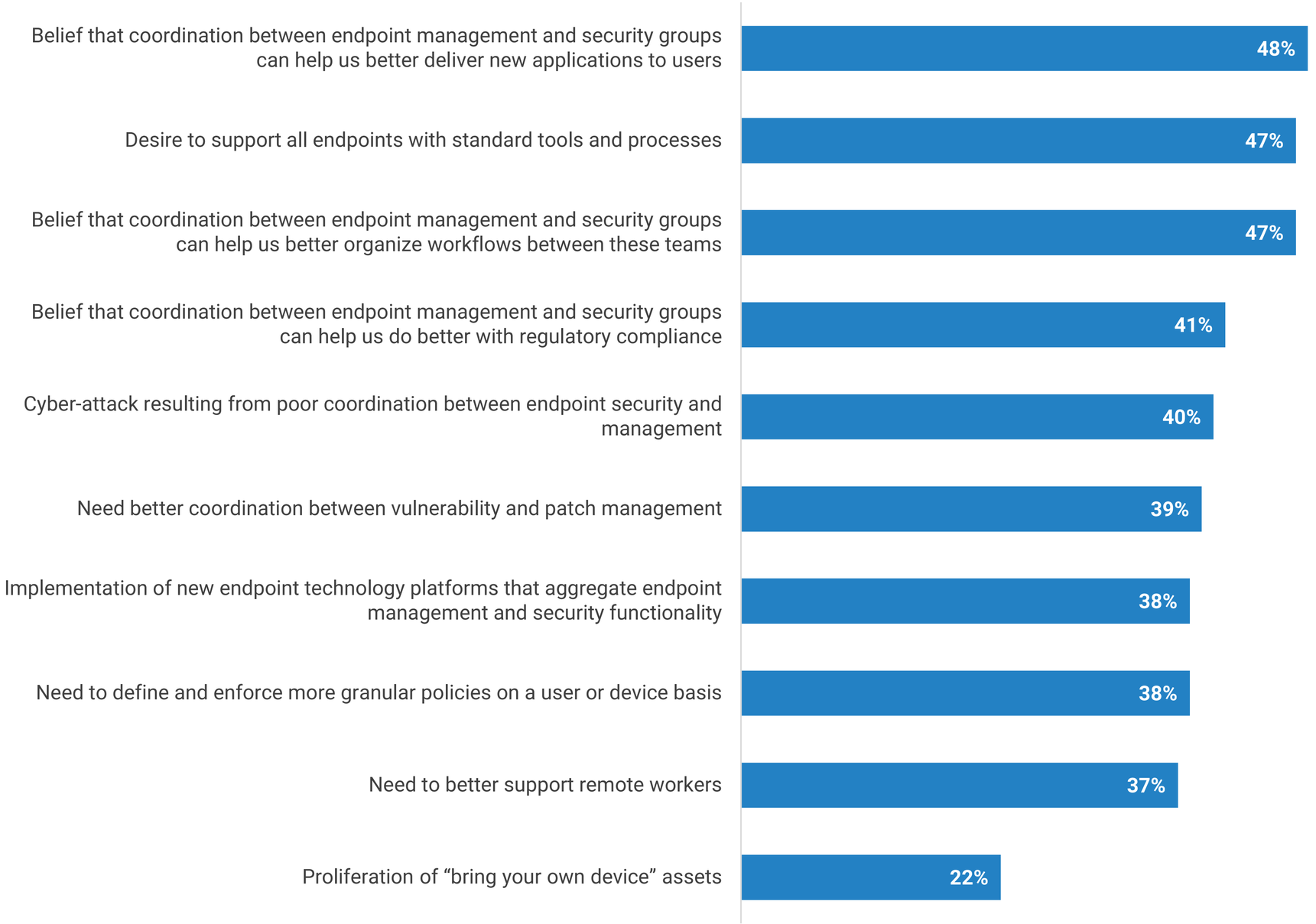
BACK TO CONTENTS



Key Endpoint Management and Security Consolidation Drivers

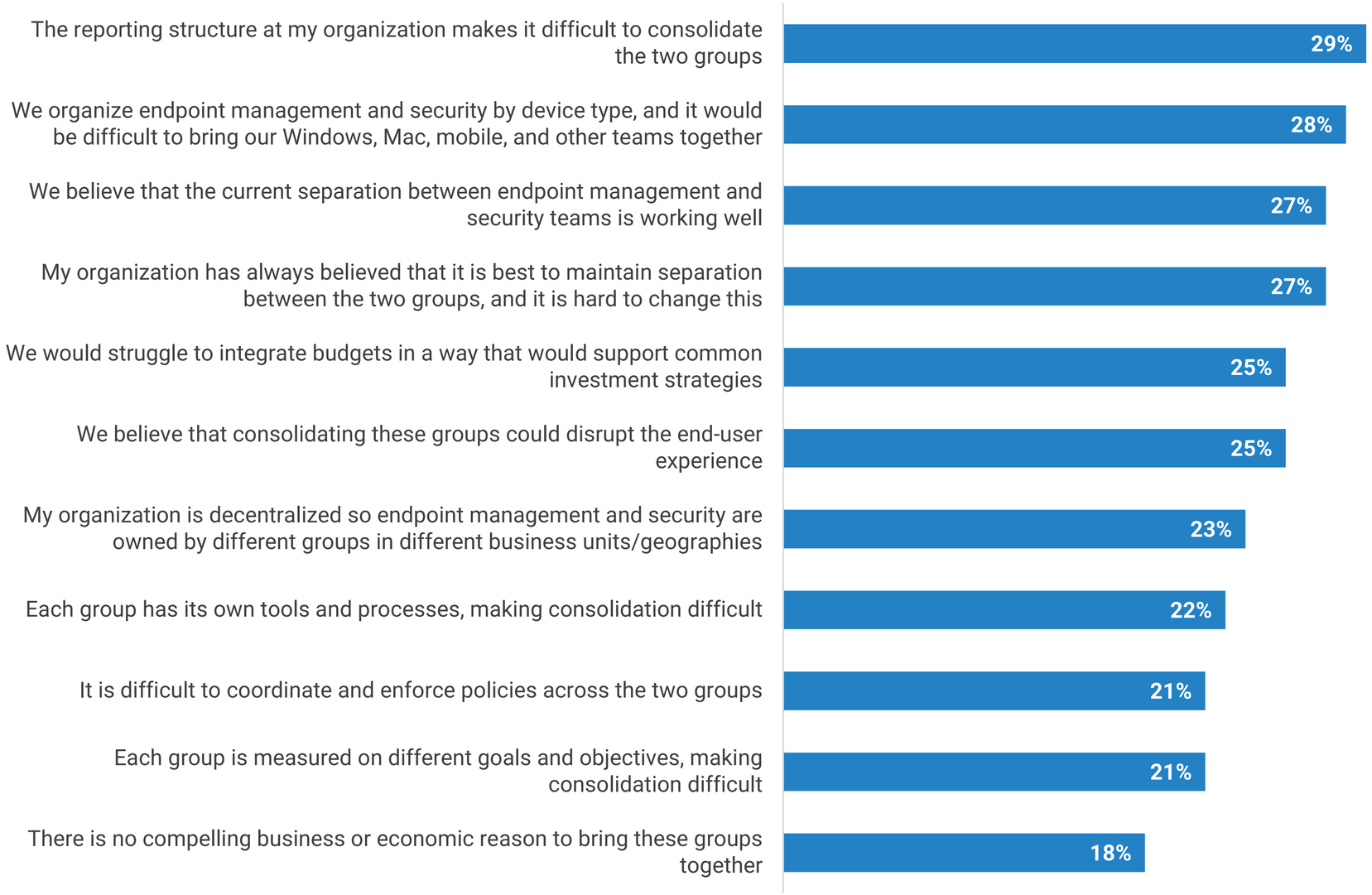
Key drivers for organizational consolidation of endpoint management and security include optimizing new application delivery, standardization and streamlining of processes and workflows, and improvements to security and compliance posture.

Endpoint management and security consolidation drivers.



BACK TO CONTENTS

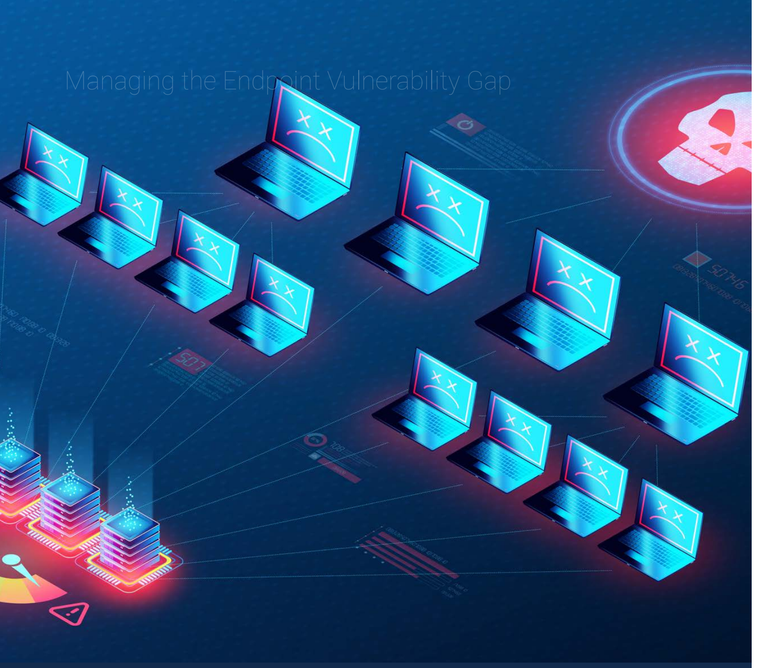
Biggest impediments to greater consolidation of endpoint management and security.



Impediments to Further Consolidation Are Plentiful

Despite the excitement around consolidation, numerous challenges, both technical and dogmatic, are creating headwinds for consolidation initiatives. Breaking through long-standing, entrenched, and siloed practices requires careful planning and a brave leap of faith for many. For others, systems re-architecture and integration will require additional investments and may slow the process.

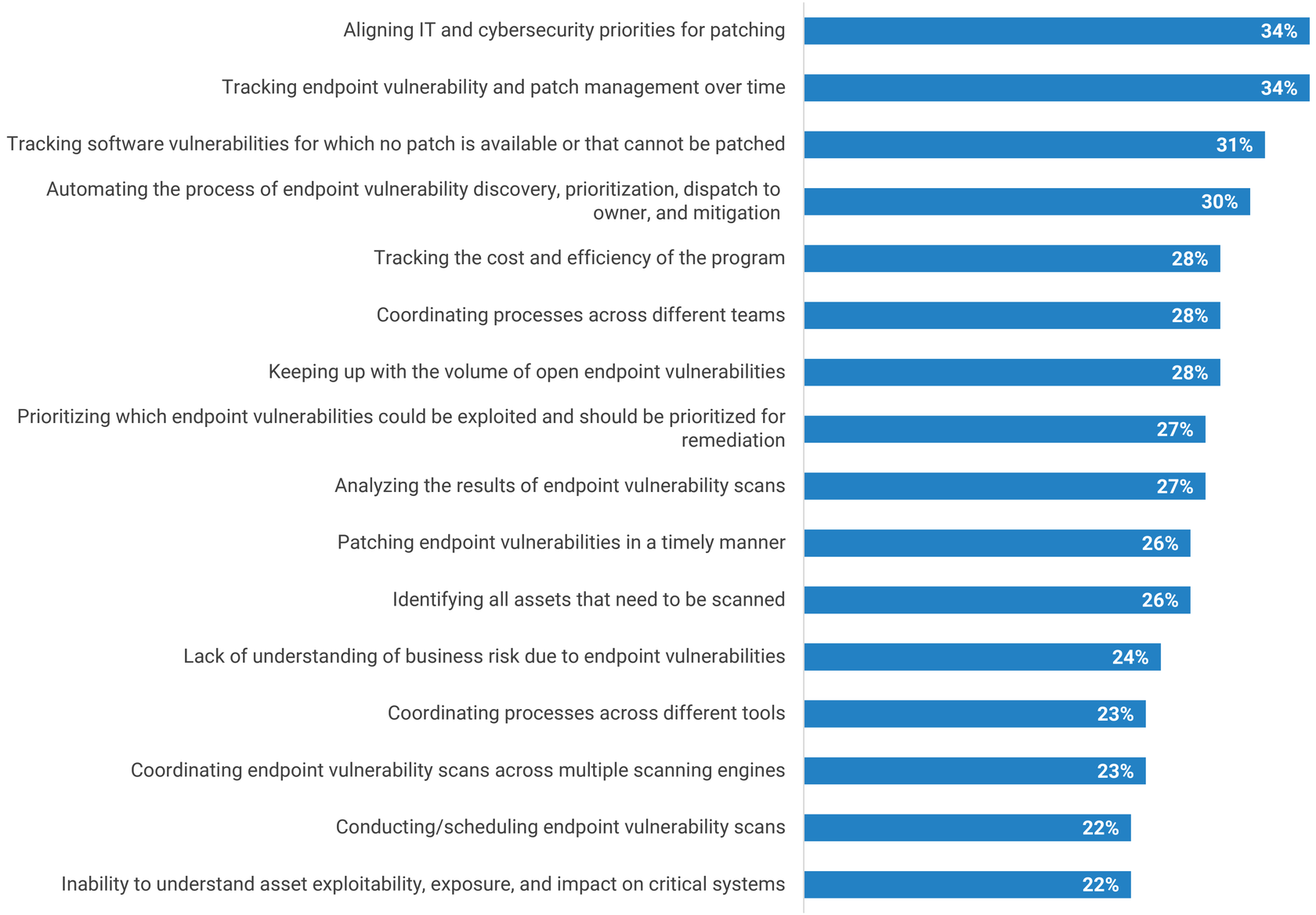
BACK TO CONTENTS



A Deeper Look at Vulnerability Management

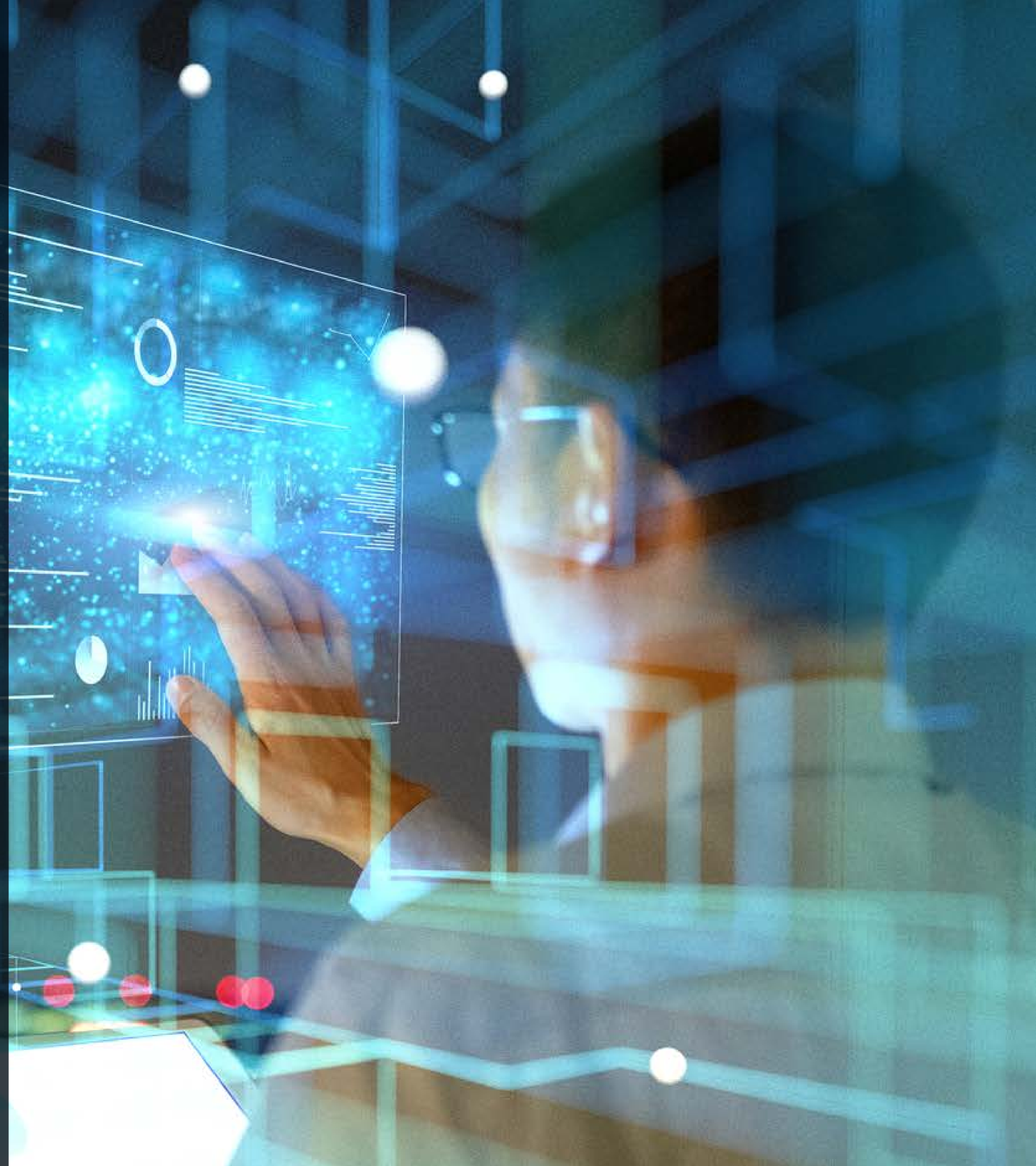
With vulnerability management central to the consolidation agenda, looking more closely at the biggest challenges associated with endpoint vulnerability management reveals that issues persist in aligning patching priorities between IT and security. Tracking endpoint patching over time further challenges many, requiring process improvements to close the loop between patching and assessment.

Biggest challenges associated with endpoint vulnerability management.



BACK TO CONTENTS

Desktop and app virtualization adoption is on the rise, addressing both management and security challenges.



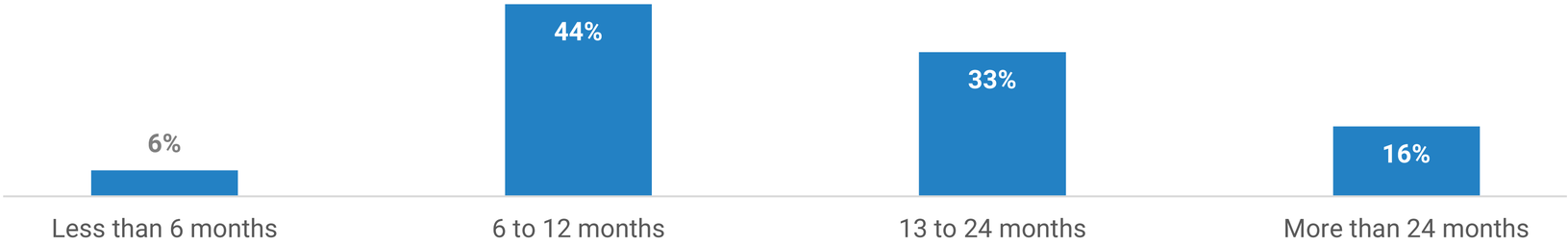
Desktop Virtualization Usage Is Extensive, though Relatively Immature

Desktop virtualization is in widespread use around the world and across industries. Nearly two-thirds (61%) report full production use, while another 29% are in various stages of pilot programs. While some organizations have been using these technologies for a long time and merely expanded their usage over the past few years, most respondents indicated that these deployments were relatively new. For those who have been using it for 24 months or less, there may be some growing pains and opportunities for optimization. However, virtualizing end-user computing environments remains a huge priority for remote access and security strategies, which is especially important for organizations supporting increasingly remote or hybrid workforces.

In general, respondents noted that they would increase use of desktop/application virtualization, with the most notable result being that the number of organizations that expect to virtualize more than three-quarters of their desktops will increase by 7x in the next three years.

Usage of desktop or application virtualization.

Length of desktop/application virtualization solution deployment.



The number of organizations that expect to virtualize more than three-quarters of their desktops will **increase by 7x in the next three years.**

BACK TO CONTENTS

Initial and/or primary users of desktop or application virtualization environments.

55%
Remote employees/ telecommuters

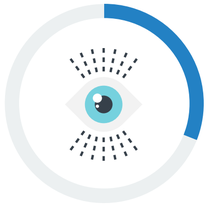
51%
Research and development

48%
Mobile employees

48%
Knowledge workers

42%
Clerical/ data entry

41%
Field service technicians



31%
Manufacturing/logistics (“shop floor”)

30%
Call center

29%
Contractors/ temporary employees

19%
Offshore employees

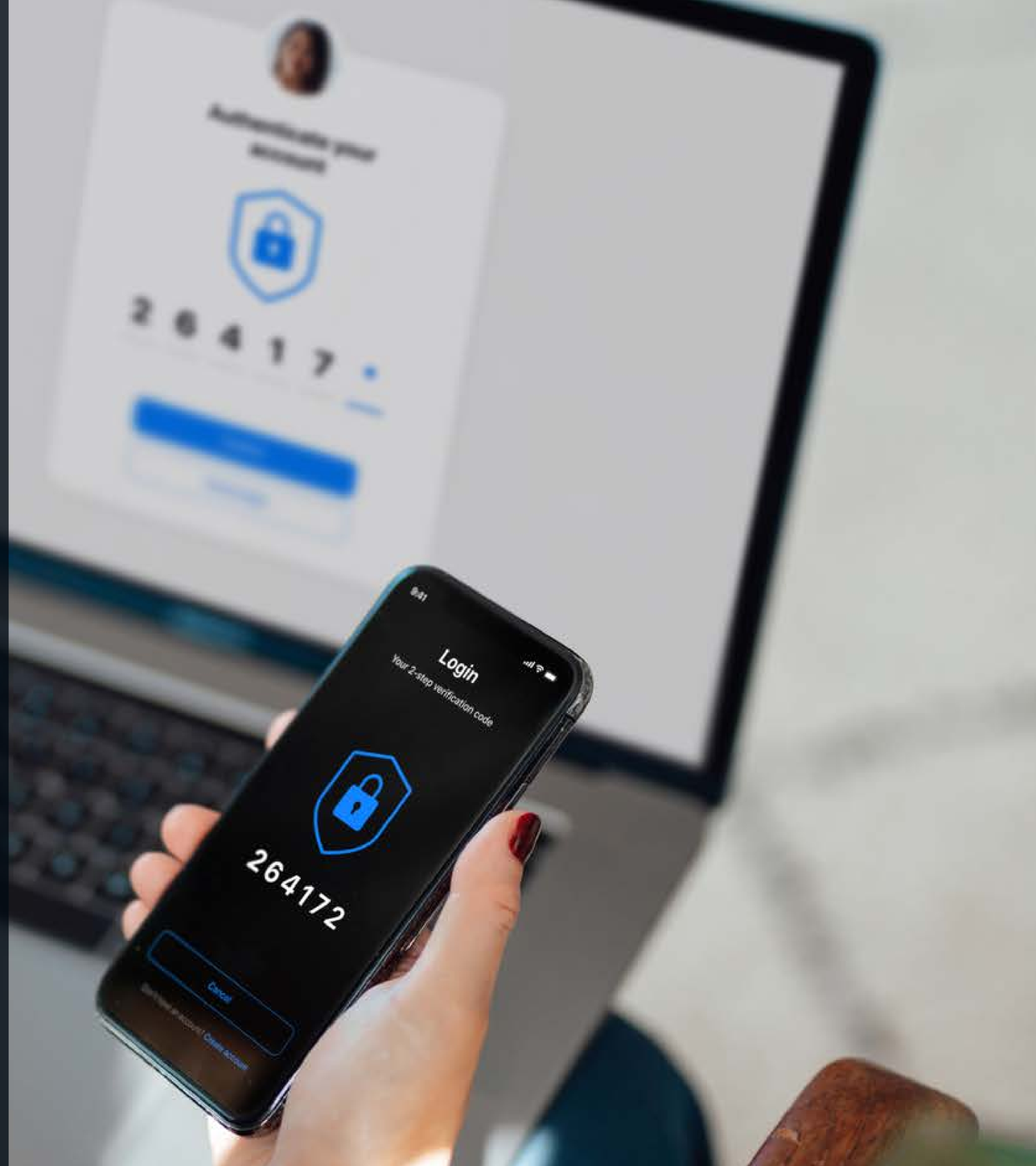
> “The pervasive work-from-home mandates **clearly changed hosted desktop strategies...**”

Remote Employees Top the List of Primary Virtualization Environment Users

While supporting remote employees has always been a use case for desktop virtualization, it is now the most commonly cited due to the increase in telecommuters stemming from work-from-home initiatives. The pervasive work-from-home mandates clearly changed hosted desktop strategies as organizations look to these solutions to facilitate employee connectivity and collaboration outside of the office environment, especially as remote work preferences persist when mandates relax.

BACK TO CONTENTS

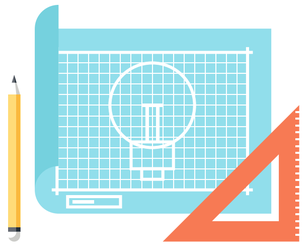
IoT presents a significant opportunity for consolidation.



IoT Growth Is Driving the Need for Consolidation

IoT management is becoming more associated with endpoint management, joining mobile devices, traditional desktops/laptops, and remote apps/desktops. With rapid growth of IoT devices and little standardization on management, many are anxious to close this gap, prioritizing the consolidation of IoT device management and security. Consolidation here will include workflows, vendors, and tools. When it comes to consolidation, high focus areas include IoT management and security, asset inventory and management, vendor consolidation, and the management of desktop or application virtualization solutions.

Beyond developing common policies, processes, and enforcement technologies across PCs, Macs, and mobile devices, adding the management and security of IoT devices to endpoint management and security oversight and operations is seen as the road to most improving overall endpoint management and security.



55%

of organizations have integrated IoT management and IoT security responsibilities as part of their efforts to consolidate endpoint management and security teams.

31%

of organizations believe adding management/security of IoT devices to endpoint management and security operations would yield significant improvements.

BACK TO CONTENTS

SYXSENSE®

Syxsense is a cloud-based unified security and endpoint management platform that helps organizations manage and secure the PCs, desktop servers, and virtual, mobile and IoT devices connected to their networks. Syxsense encompasses vulnerability scanning, patch management and endpoint security and remediation — enabling organizations to align their core IT management processes with their cybersecurity strategies.

LEARN MORE

ABOUT ENTERPRISE STRATEGY GROUP

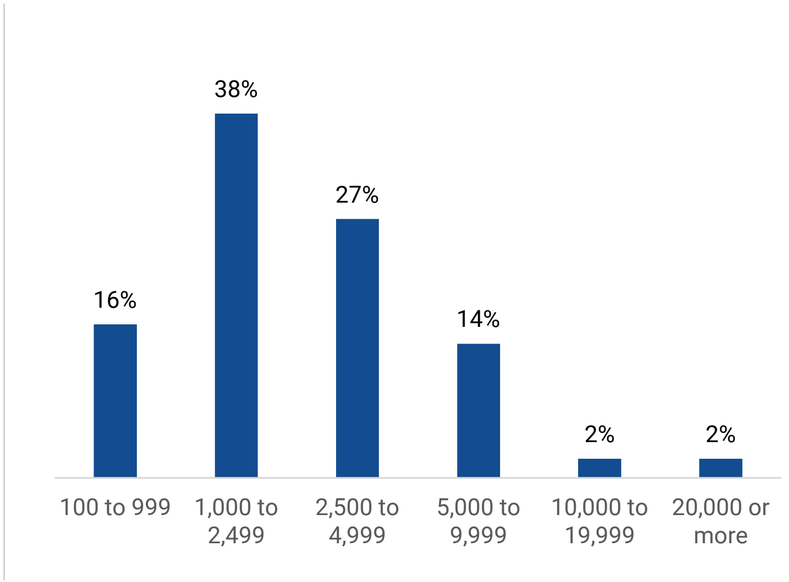
TechTarget's Enterprise Strategy Group is an integrated technology analysis, research, and strategy firm providing market intelligence, actionable insight, and go-to-market content services to the global technology community.

Research Methodology and Demographics

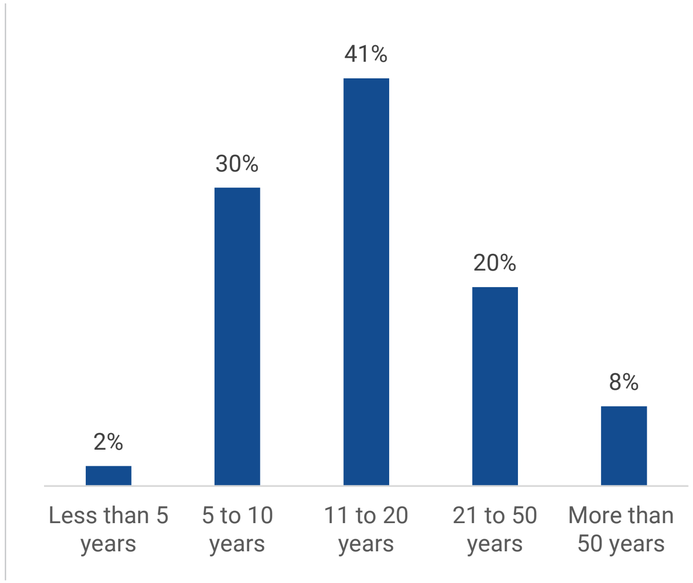
To gather data for this report, ESG conducted a comprehensive online survey of IT and cybersecurity professionals from private- and public-sector organizations in North America between November 15, 2022 and November 28, 2022. To qualify for this survey, respondents were required to be IT and cybersecurity professionals involved with endpoint management and security technologies 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 381 IT and cybersecurity professionals.

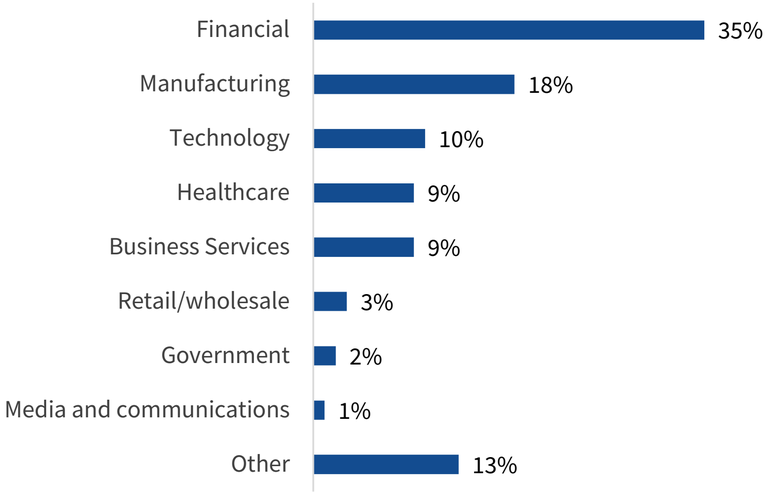
RESPONDENTS BY NUMBER OF EMPLOYEES



RESPONDENTS BY AGE OF COMPANY



RESPONDENTS BY INDUSTRY



BACK TO CONTENTS

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.