



Enterprise Strategy Group | Getting to the bigger truth.™

Unified Endpoint Management and Security in a Work-from-anywhere World

Dave Gruber, Principal Analyst

Mark Bowker, Senior Analyst

MARCH 2022

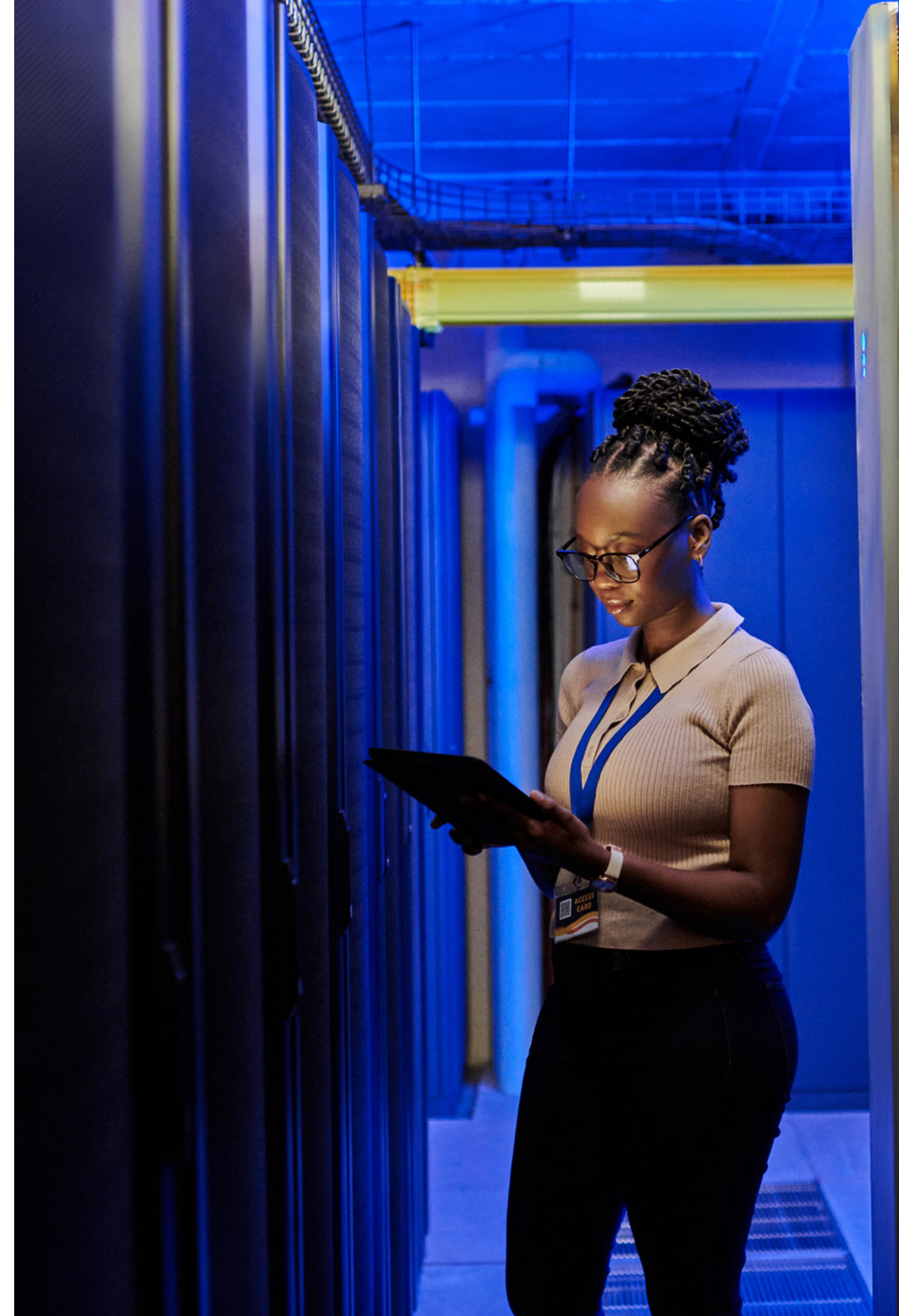
CONTENTS

Endpoint Expansion and Diversity Continue **3**

Buyers Want More from Endpoint Security Platforms **7**

The Convergence of Endpoint Management and Security Platforms **13**

The Bigger Truth **17**



A man in a blue shirt and glasses is shown in profile, looking at a smartphone. In the background, a laptop and a tablet are visible on a desk. The scene is set in a modern office environment.

Endpoint Expansion and Diversity Continue

Unified Endpoint Management and Security Beyond Traditional Devices

Organizations are facing new levels of diversity in device types and operating environments. With hybrid work dominating most organizations, management and security of both corporate-owned and non-corporate-owned devices used to interact with applications and sensitive data are required.

In parallel, IoT devices will soon outnumber traditional endpoint devices and VR/AR devices are emerging to create immersive experiences, all of which are adding a new level of complexity in securing infrastructure.

“ Organizations are facing new levels of diversity in device types and operating environments.”

| Device types currently protected and secured by endpoint device security solutions.



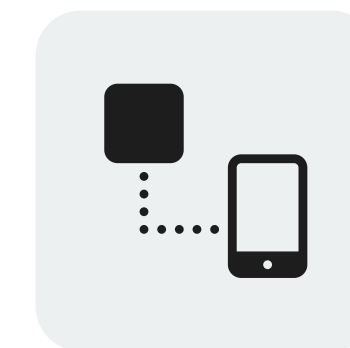
88%

Corporate-owned laptops and desktop devices



54%

Corporate-owned mobile devices



46%

IoT devices in corporate offices



41%

IoT industrial controls systems



38%

Employee-owned laptops and desktop devices (used for work)



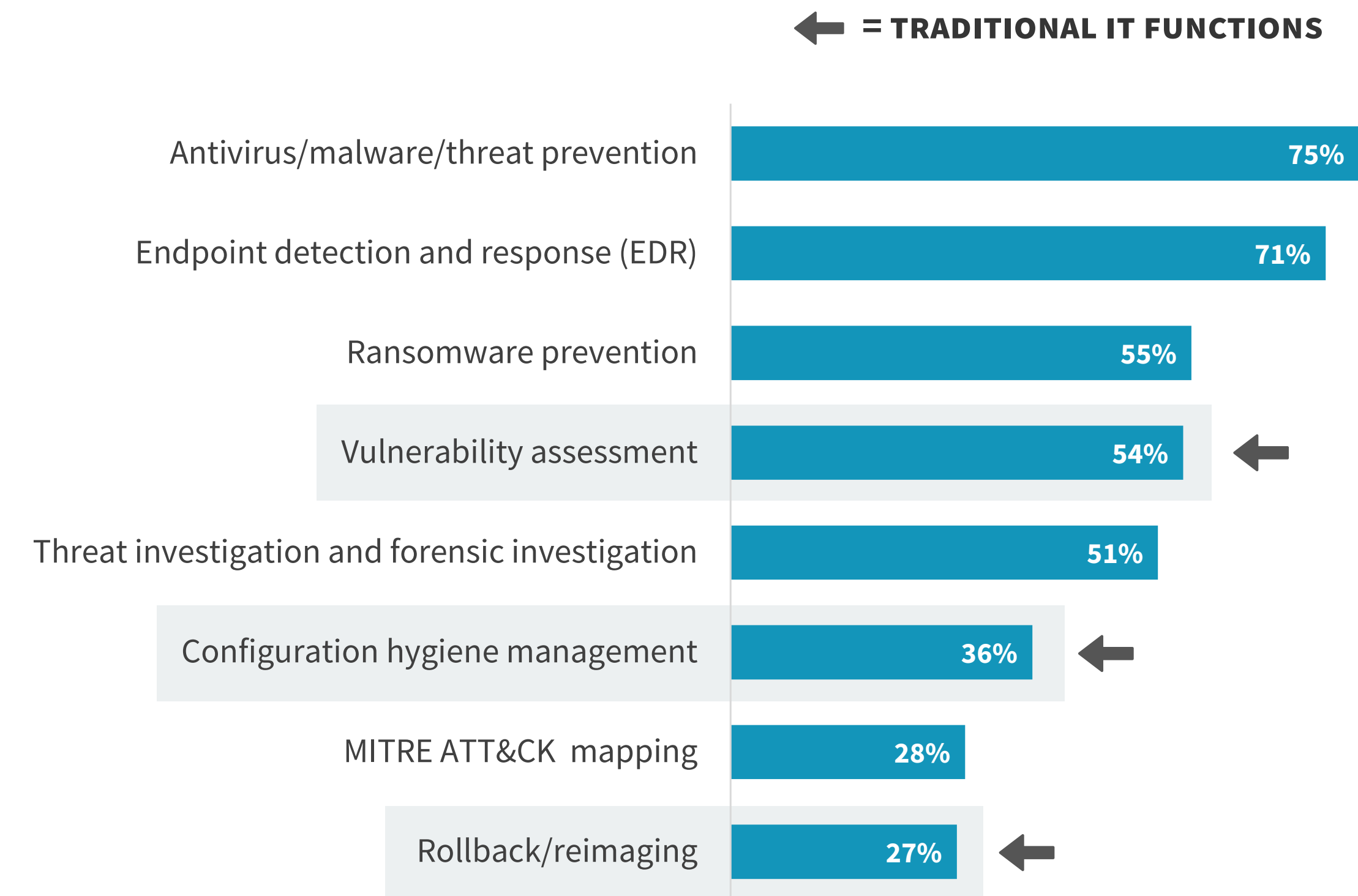
35%

Employee-owned mobile devices (used for work)

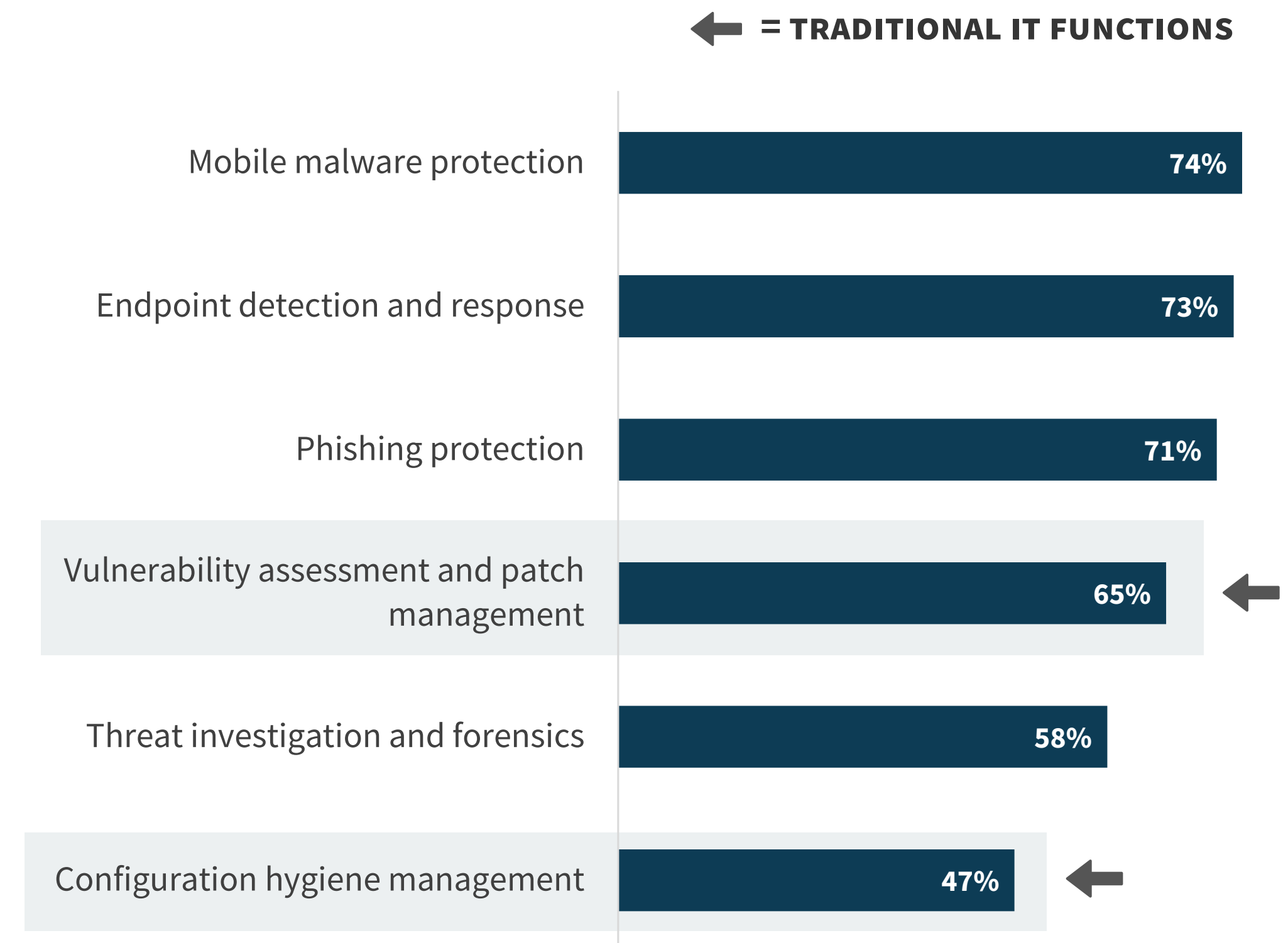
Management and Security Requirements Converge

In support of these diverse environments, IT and security teams require new mechanisms capable of providing visibility, assessment, and 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.

| Corporate-owned laptops and desktops.



| Corporate-owned mobile devices.



Use cases for IoT Devices

As IoT projects accelerate in support of corporate office automation use cases and the many industrial, healthcare, manufacturing, and other industry-specific use cases, IT and security teams require broad management, prevention, detection, and response capabilities that must span devices and operating environments often outside of their control. OT, IT, and security teams must work together to deliver on operational and security objectives, while welcoming new devices and use cases regularly.

| Desired IoT device type support.



65%

Office automation IoT devices



58%

Facility management IoT devices

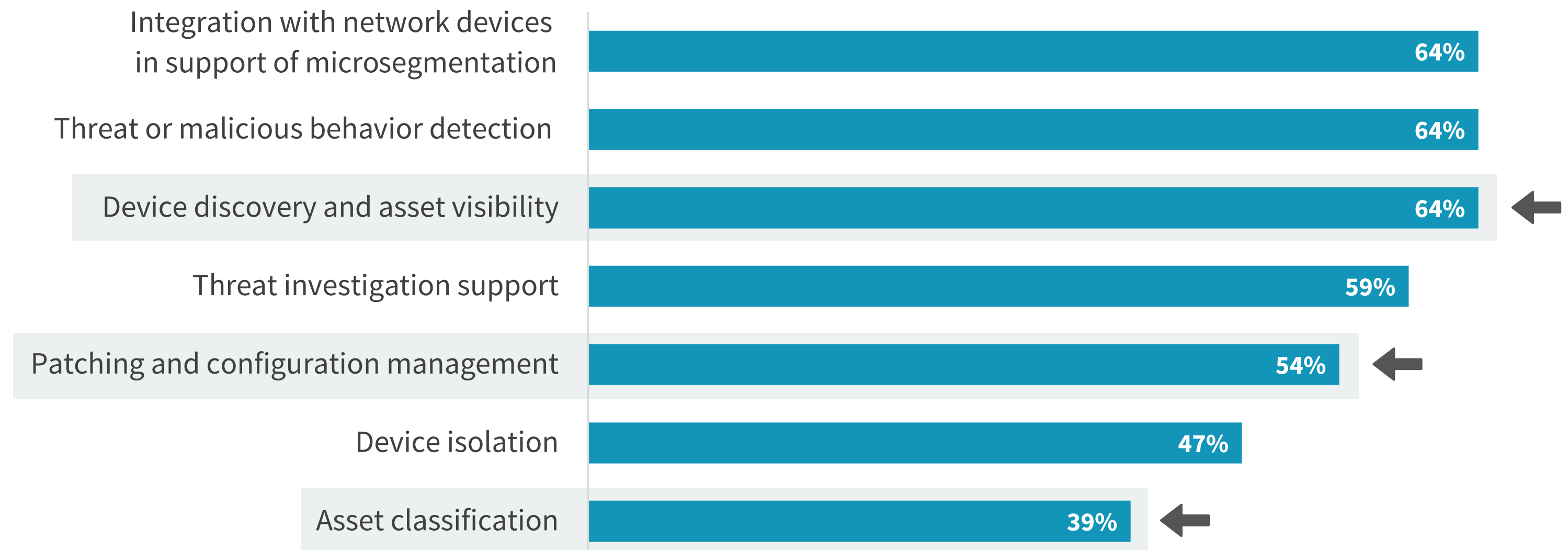


53%

Industrial IoT devices

| Desired IoT security capabilities.

← = **TRADITIONAL IT FUNCTIONS**



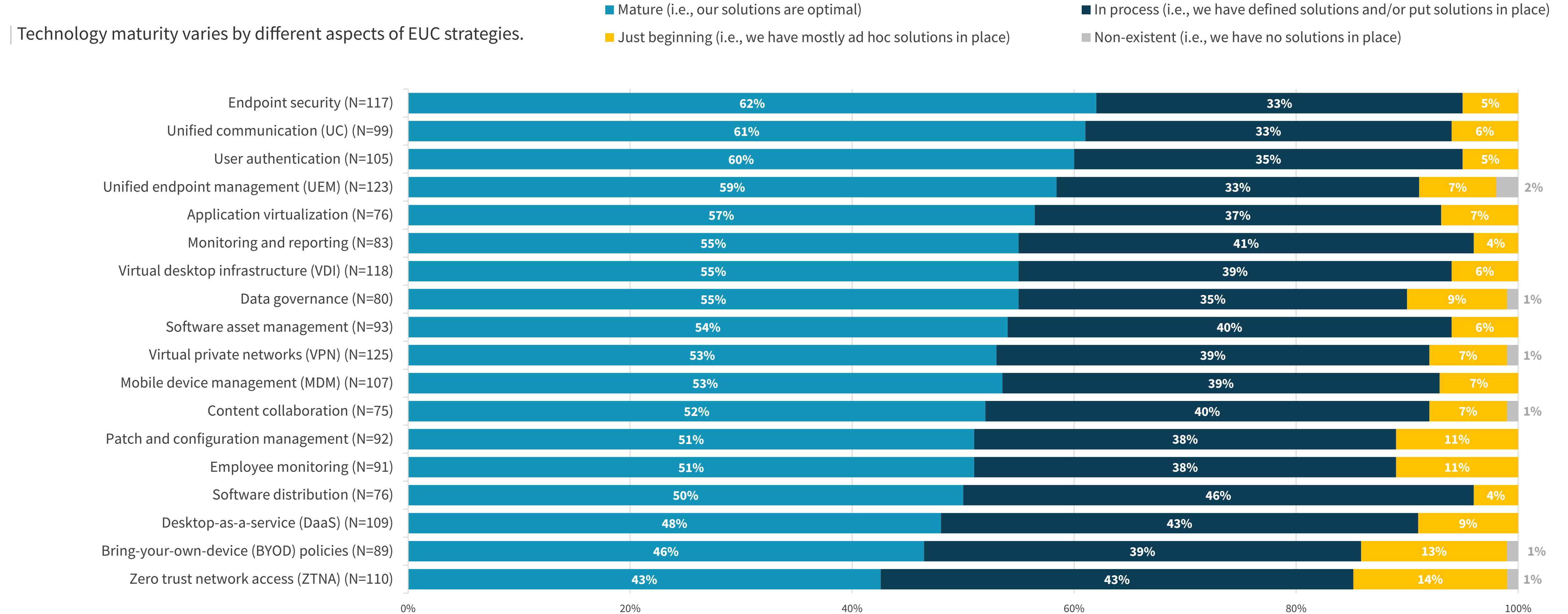
Buyers Want More from Endpoint Security Platforms

DLP and endpoint management are
converging with endpoint security



EUC is a Work in Progress for Most

While significant investments continue to be made across people, processes, and technologies required to manage and secure progressively more diverse environments, there is work to be done by most. Yet, siloed investments often generate additional complexity, driving many to desire convergence between management and security capabilities to simplify implementation and ongoing management functions.



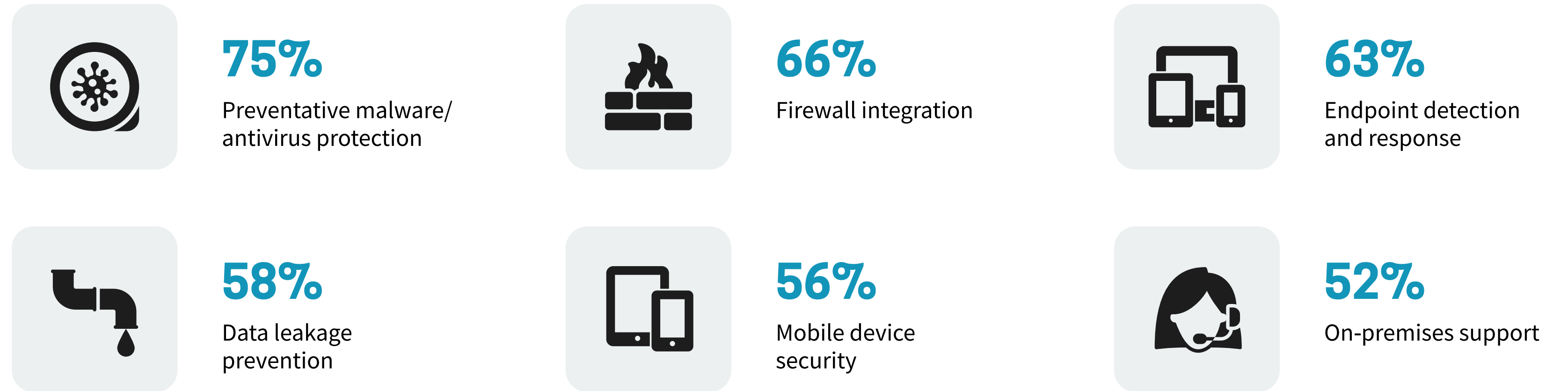
Endpoint Security Feature Priorities

Mobile device security is a priority for more than half of respondents, while concerns around data security are now a top-5 requirement for endpoint security solutions. On-premises support is still desired by more than half, despite the continuing trend for cloud-delivered solutions.

Data Security Is Increasingly Important

Hybrid, work-from-anywhere requirements have escalated the importance of data security for most. Data encryption is considered a core requirement for more than two-thirds, while fears of data leakage across the many corporate and collaboration SaaS applications is driving the requirement for both point and enterprise-wide data leakage protection solutions.

| Top endpoint security feature priorities.



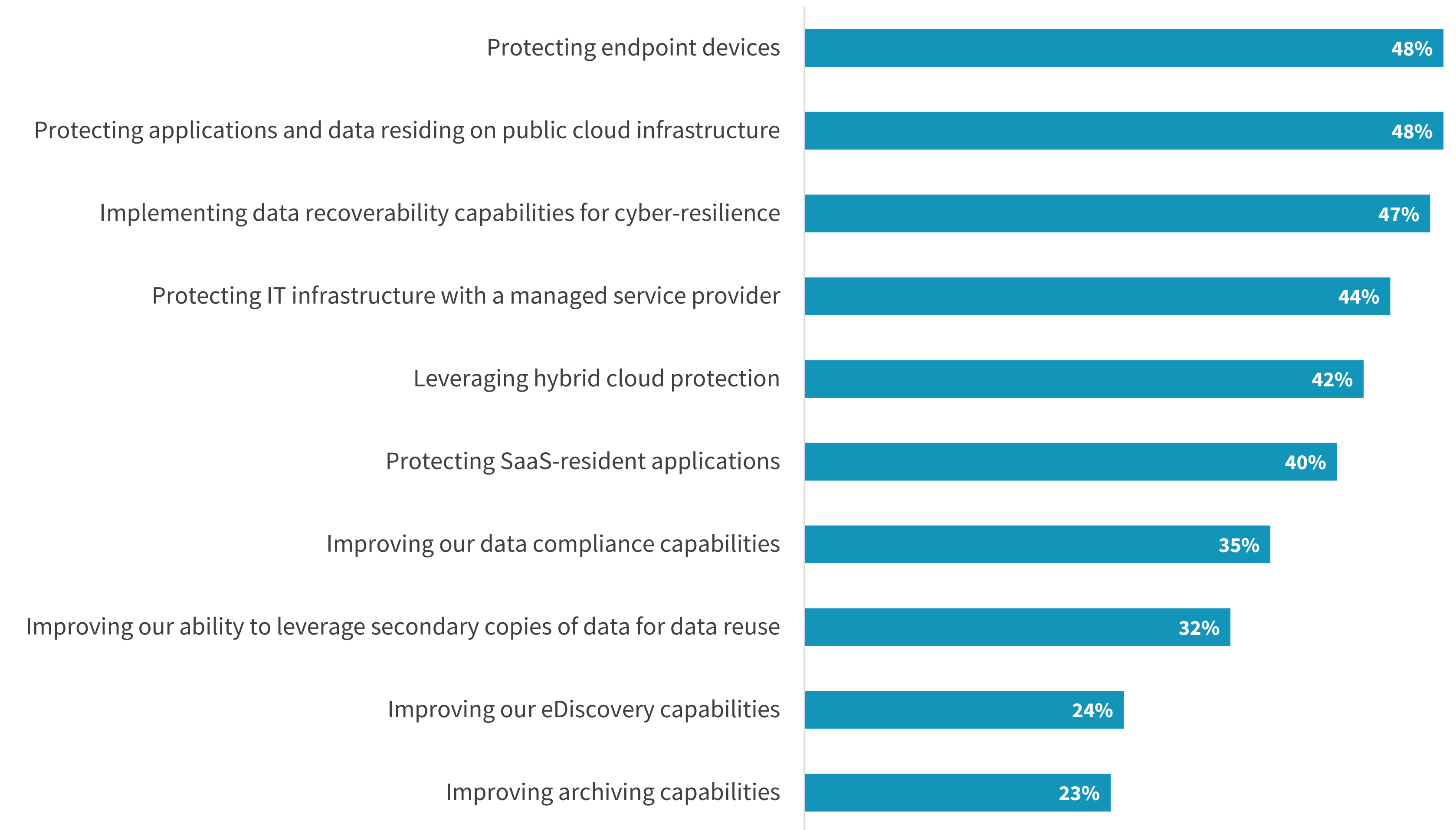
| Work-from-anywhere requirements have increased data security concerns for endpoints.



Protecting Endpoints and Cloud Apps/Data, as Well as Supporting Cyber Resilience, Are Data Protection Priorities Earmarked for Investment

IT and security teams need data protection to extend across devices, applications, and workloads, with cyber resilience top of mind. Cloud complexity from hybrid, multi-cloud, and SaaS applications add new challenges for effective data protection solutions.

| Top 10 data protection areas where organizations are making significant investments.



Most Believe Endpoint Security Is Integral to Zero Trust

Zero trust is a journey, requiring investments across multiple IT and security controls, which in turn requires IT and security teams to plan and implement in close collaboration.

With 71% already underway with zero trust projects, new security, identity, and management requirements are driving upgrades to management and security solutions.

While organizations are looking at upgrading endpoint security capabilities in support of zero trust and XDR initiatives, they may not be considering unified endpoint management (UEM) in the same light. UEM is critical to being able to effectively detect and respond to threats on mobile devices.

A comprehensive zero trust solution must have basic capabilities that only a UEM can provide. Device and Application trust come to mind. While not core to traditional EDR/XDR functions, they provide important DLP and threat mitigation capabilities.

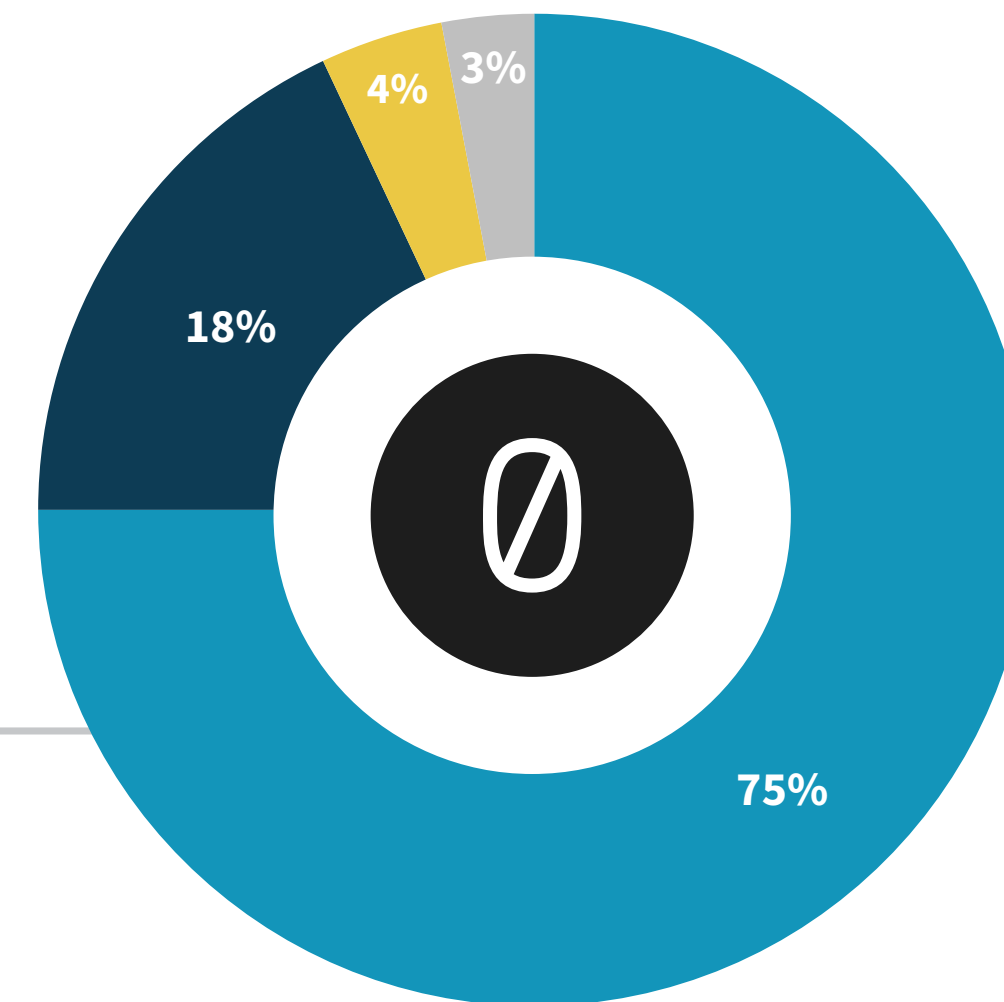


71%

of organizations are already underway with ZT implementations.

| Many organizations are adopting a zero trust strategy.

“ **Three-quarters are swapping out endpoint security in support of ZT strategies.** ”



- Yes, we have an active project underway to upgrade our endpoint security in support of our zero trust strategy
- Yes, this is something we are considering, but don't have an active zero trust project underway
- No, we don't consider endpoint security as part of our zero trust strategy
- Don't know



46%

will use XDR to supplement existing EDR solutions.

With advanced attacks involving multiple threat vectors, security teams are challenged to gain the visibility and speed required to prevent, detect, and respond to threats before damage is done. The XDR movement promises to address these issues, upleveling detection and response beyond the endpoint to include network, cloud, identity, email, and more.

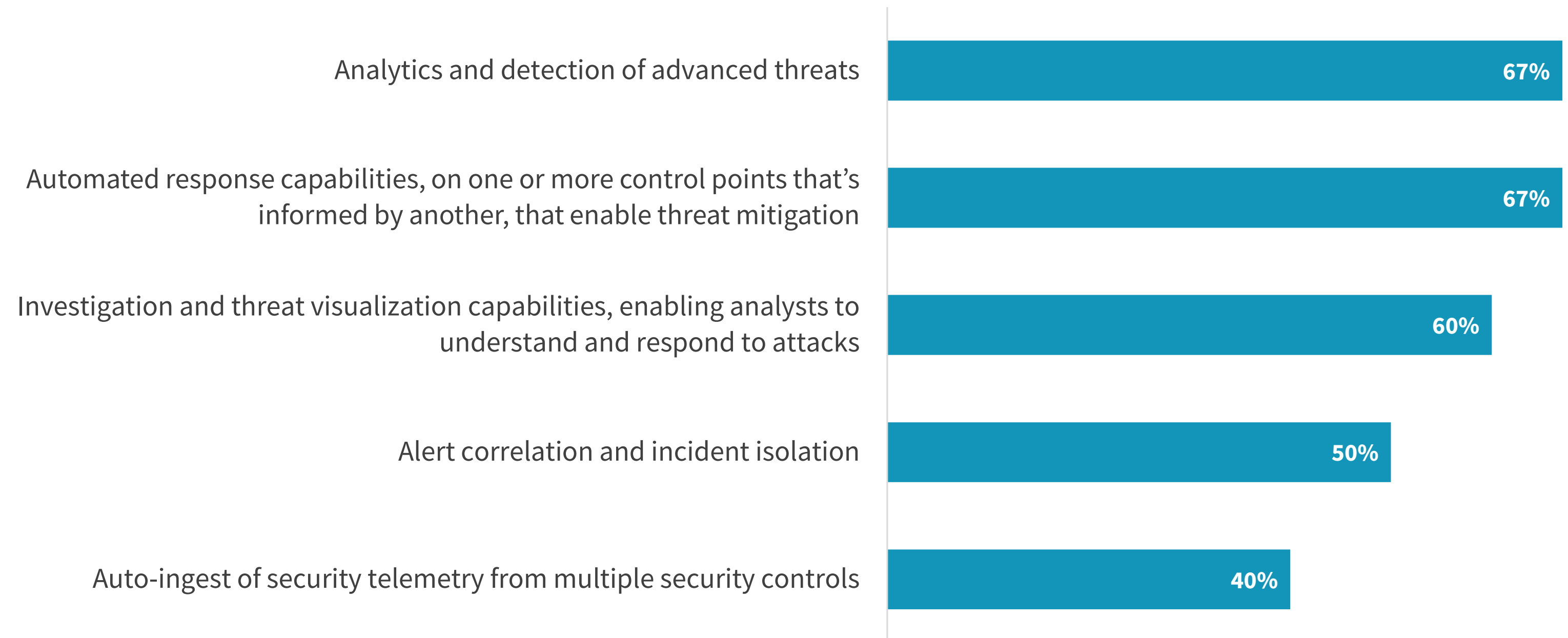
An XDR solution is only as good as the use cases that can be covered. So, when thinking about XDR, organizations should consider all use cases including Hybrid workforce. Insider Threat and Hybrid use cases on IOS, Android, and Mac are often overlooked, or weak at best. UEM solutions offer a way to add these important use cases to the mix.



50%

of respondents think XDR will replace EDR either immediately or over the next two years.

| Advanced threat detection must be proven before replacing EDR.



The Convergence of Endpoint Management and Security Platforms

A long-exposure photograph of a city street at night. The image shows light trails from cars and buildings in the background, creating a sense of motion and activity. The text is overlaid on the left side of the image.



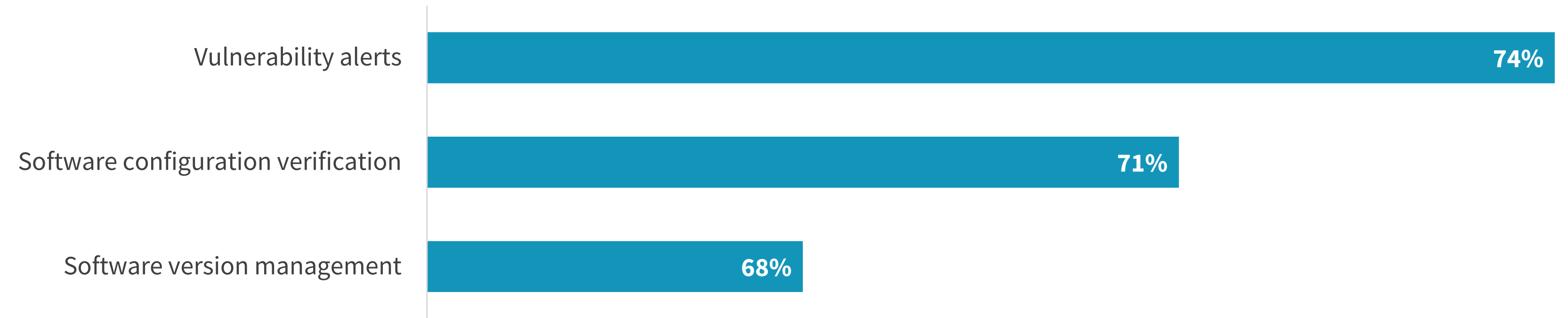
55%

believe in converged endpoint management and security.

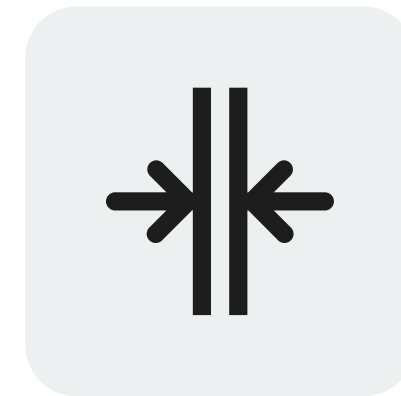
Overlapping requirements and workflows are driving many to desire a more integrated approach to endpoint security and endpoint management. Software and configuration management, patching, and vulnerability mitigations all cross IT and security objectives. However, barriers may exist in driving cooperative projects to bring these capabilities together.

While it is seemingly a smart decision to combine management and security functions into a single solution, misaligned objectives and the separation of budget ownership is making it challenging to do so.

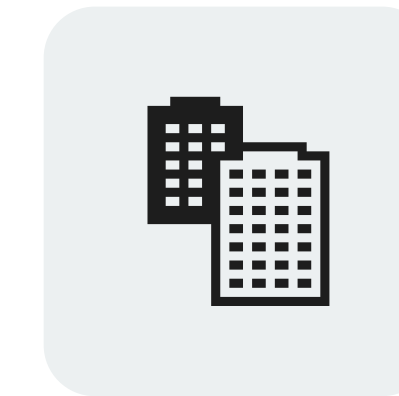
| What use cases are desired?



| Many see barriers to getting there.



Misaligned IT and security objectives make it too difficult to converge them into a single solution, **49%**



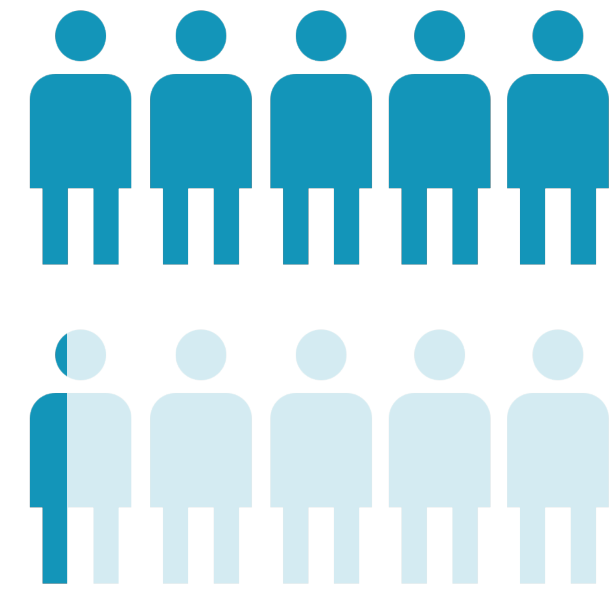
These two solutions are **purchased and operated by different organizations,** **43%**

Convergence Continues

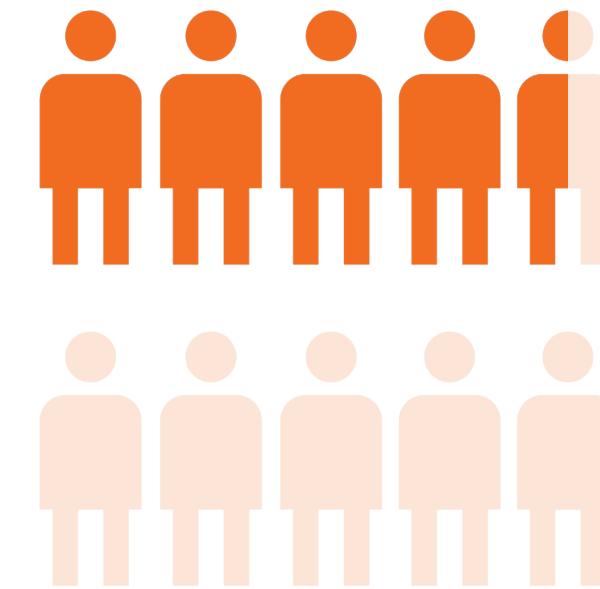
While most organizations will admit to increased complexity created by the proliferation of IT and security tools in use, not everyone agrees that consolidation is the best solution. Security teams have historically taken a best-of-breed approach. However, many are reaching a break-point driving the move to consolidation driven by complexity.

Yet, consolidated solutions and best-of-breed are often not compatible. Even the best consolidated solutions often lack the use-case coverage required to support newer advanced threats. An open approach is therefore key to be able to provide use-case coverage and enable integration of innovative point solutions, new technologies, and additional threat intelligence.

| Organizations are split on how to reduce complexity.

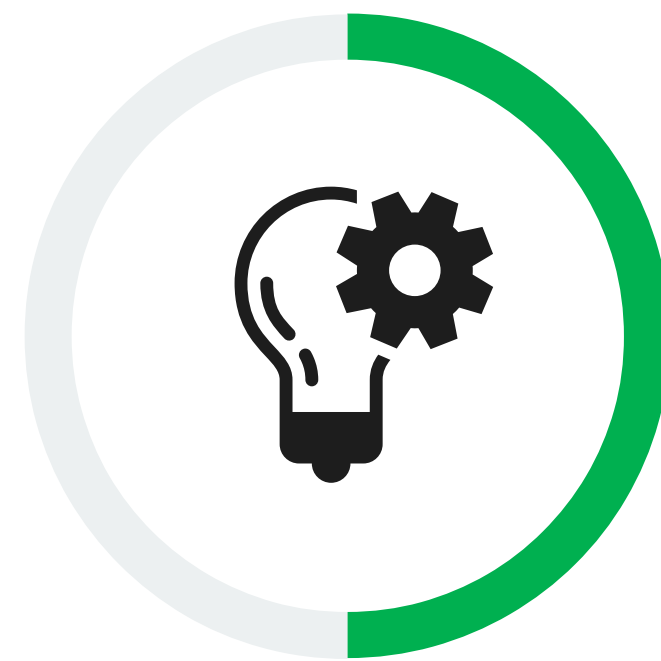


53%
desire
convergence



45%
prefer
best-of-breed

| Top driver of convergence.



46%
of respondents say
reduction in complexity is the driver.

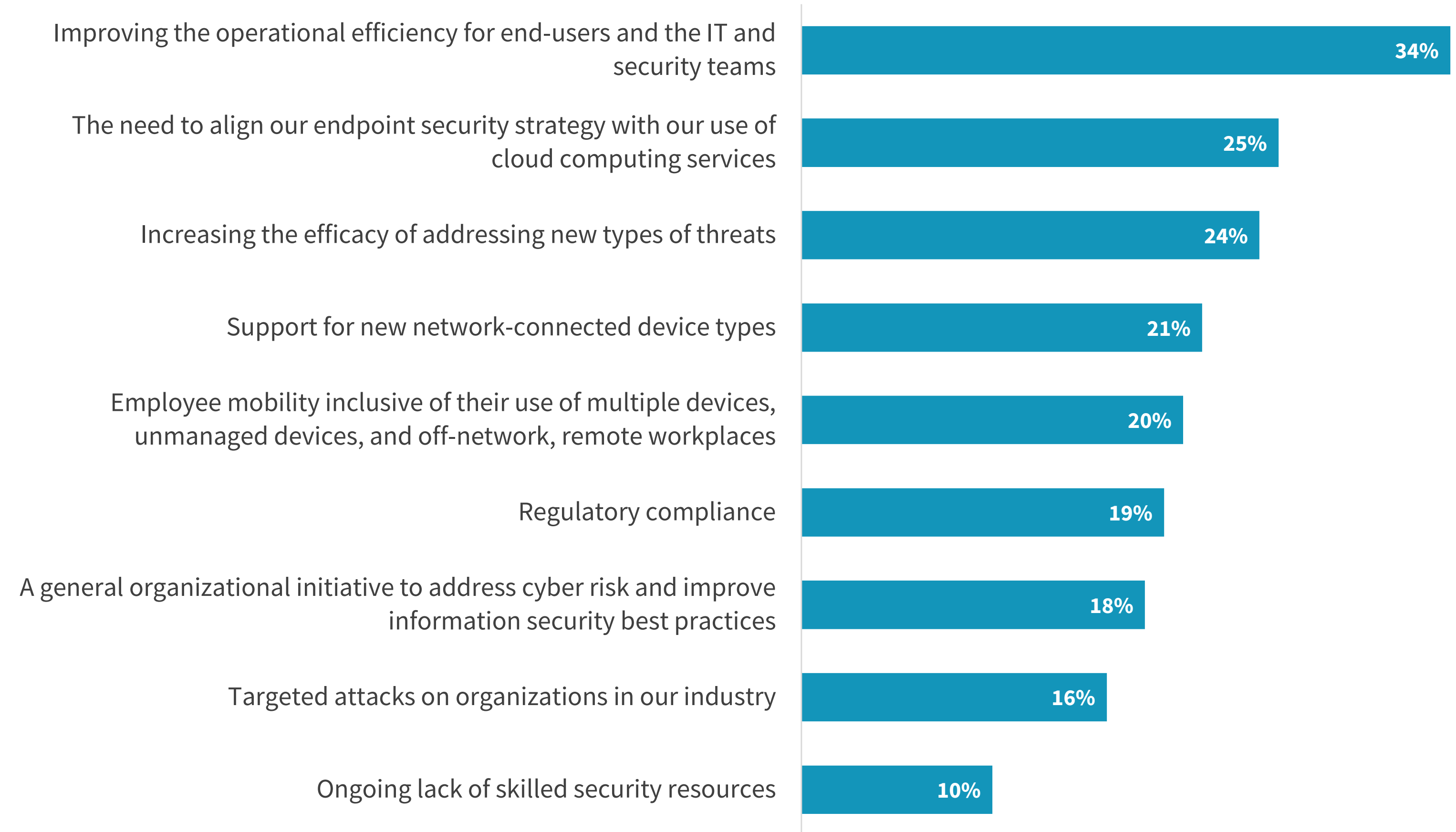
Looking Ahead:

What will influence endpoint security strategy moving forward?

- **Efficiency matters most.**
- **Connecting endpoint and cloud security together with advanced threat defense follows.**
- **IoT & mobile protection.**

At the end of the day, operational efficiency is king for all. While efficacy is the ultimate goal, efficiency challenges have become hurdles to achieving this goal, driving many to prioritize efficiency investments over efficacy investments. Organizations are looking to bring management and security capabilities closer together, reducing complexity, and aligning IT and security teams with a common view of risk remediation.

| Top considerations having the most significant influence on an organization’s endpoint security strategy.



The Bigger Truth

While endpoint management and security programs have long operated in silos, complexity and risk are driving new requirements for integration and risk mitigation alignment.

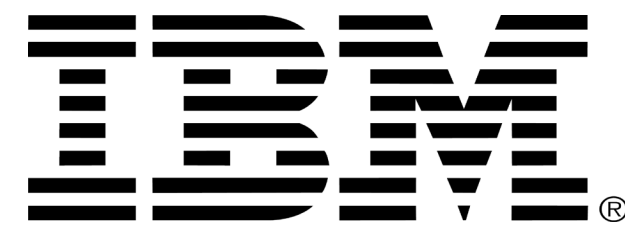
As adversaries capitalize on newly discovered vulnerabilities, IT and security teams require the ability to rapidly assess risk and align mitigation strategies, enabling faster response.

As attack surface diversity and growth continues, converging endpoint management and security processes and systems will help drive both efficacy and efficiency, leading to a reduction of risk.

Learn more about how IBM UEM solutions can help.

[LEARN MORE](#)

[Schedule a Demo](#)



All product names, logos, brands, and trademarks are the property of their respective owners. Information contained in this publication has been obtained by sources TechTarget, Inc. considers to be reliable but is not warranted by TechTarget, Inc. This publication may contain opinions of TechTarget, Inc., which are subject to change. This publication may include forecasts, projections, and other predictive statements that represent TechTarget, Inc.'s assumptions and expectations in light of currently available information. These forecasts are based on industry trends and involve variables and uncertainties. Consequently, TechTarget, Inc. makes no warranty as to the accuracy of specific forecasts, projections or predictive statements contained herein.

This publication is copyrighted by TechTarget, Inc. Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of TechTarget, Inc., is in violation of U.S. copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact Client Relations at cr@esg-global.com.



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.

© 2022 TechTarget, Inc. All Rights Reserved.