

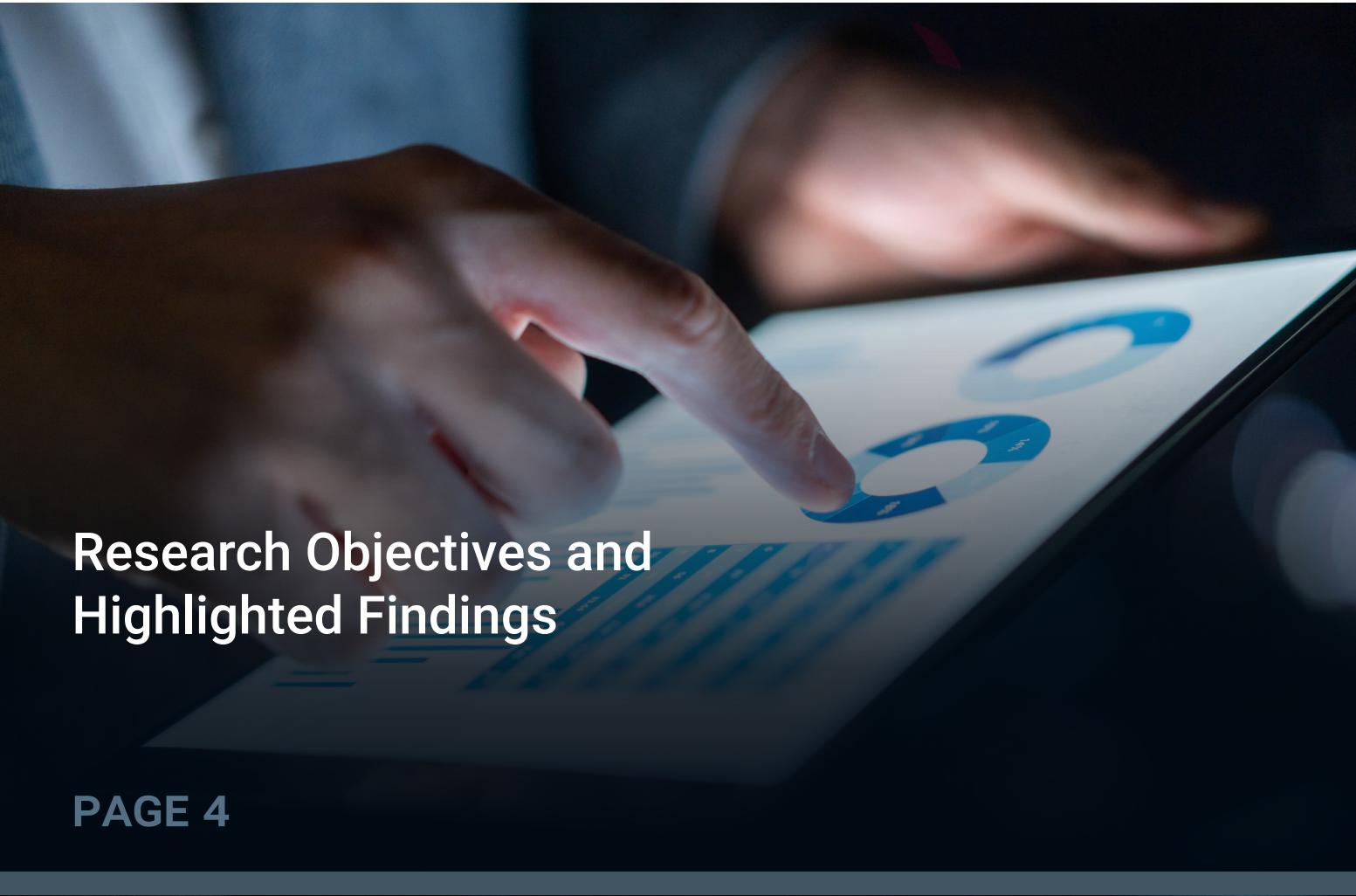
Validating the Impact of Digital Experience Monitoring Solutions

Utilizing Digital Experience Monitoring
Solutions to Elevate Zero Trust



This Enterprise Strategy Group eBook was commissioned by
Zscaler and is distributed under license from TechTarget, Inc.

Contents



Research Objectives and Highlighted Findings

PAGE 4



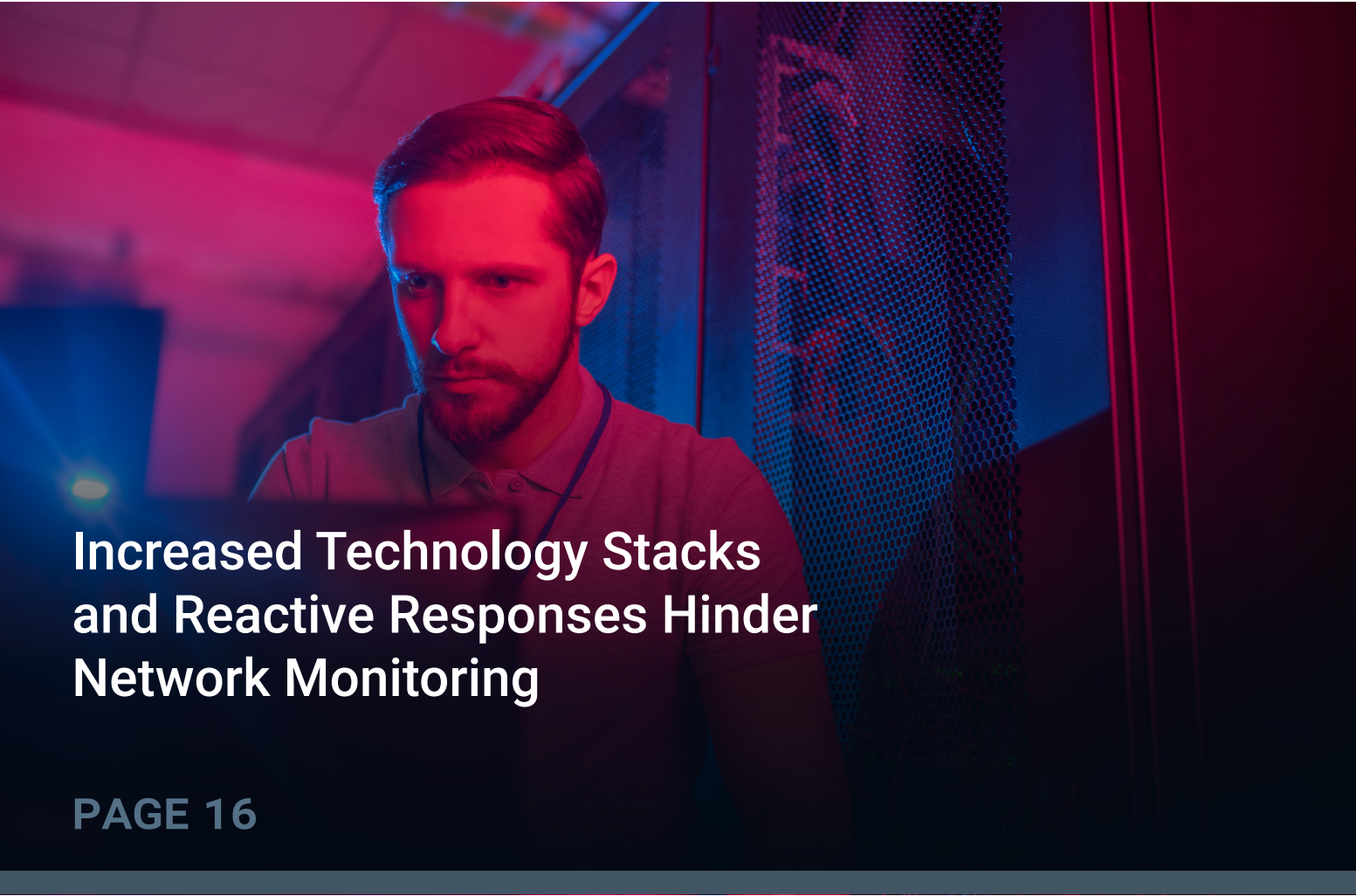
Exploring Zero Trust and Digital Experience Monitoring Integrations

PAGE 5



Maintaining and Monitoring the Digital Experience of Employees Has Only Gotten More Difficult

PAGE 11



Increased Technology Stacks and Reactive Responses Hinder Network Monitoring

PAGE 16



DEM Is Already Moving the Needle for Some, Especially When Fortified With AI Capabilities and Root Cause Analysis

PAGE 20



Conclusion

PAGE 26



Introduction

Businesses are under more pressure than ever to ensure all of their network environments operate with maximum efficiency and minimal exposure to security risks and incidents. Zero trust initiatives are implemented with the intention of providing enterprise-wide strategies to mitigate potential threats across the digital landscape. The success of zero trust initiatives largely depends on the value of the data and insights analyzed for actionable measures. Gaining insights into the performance of the variety of applications, services, and tools used to monitor networks is, therefore, imperative.

Digital experience monitoring (DEM) acts as an IT management solution, assessing performance and aiding teams by continuously monitoring system health to optimize user-application connections. DEM solutions can support zero trust initiatives by providing end-to-end visibility and monitoring capabilities across the network infrastructure on a unified platform.

Objectives

This eBook, along with its accompanying research survey, aims to delve into the adoption and impact of DEM solutions within organizations. It seeks to understand how DEM influences employee productivity and experiences, as well as its effects on the efficiency and effectiveness of network operations, IT security monitoring teams, and other personas.

Additionally, the research explores zero trust as a comprehensive security strategy and some of the challenges and trends around it. Zero trust is examined in the context of DEM solutions and capabilities that have been implemented in support of organizations’ zero trust security and observability initiatives.

Highlighted Findings

Organizations must improve their current approaches to experience monitoring: Organizations face challenges in gaining deep insights into digital environments due to complex monitoring solutions. Specifically, 71% struggle with endpoint performance metrics, and 69% find application performance metrics challenging.

Zero trust adoption rates are climbing: Currently, 91% of surveyed enterprises have implemented zero trust initiatives, with 77% indicating significant security performance improvements.

DEM solutions effectively support zero trust initiatives: 66% of organizations say the primary reason they invested in DEM solutions was to achieve their zero trust goals more effectively. 92% of all respondents reported that DEM solutions were critical or important to their proactive responsiveness to potential incidents and issues.



An aerial night view of a city skyline, likely San Francisco, with the Transamerica Pyramid as a central landmark. The city lights are visible against a dark blue sky with scattered clouds. Overlaid on the image are several glowing blue arcs and points, suggesting a digital network or data flow. The text is positioned in the lower-left quadrant of the image.

Exploring Zero Trust and Digital Experience Monitoring Integrations

The Majority of Organizations Are Implementing Zero Trust Initiatives

The following definition was shown to all survey respondents to ensure a consistent frame of reference for all survey questions: **Zero trust** strategies assume the network is compromised and brokers default-deny resource-specific access through a least-privilege approach supported by continuous authentication, authorization, and risk evaluation for every request.

Zero trust operates on three fundamental principles:

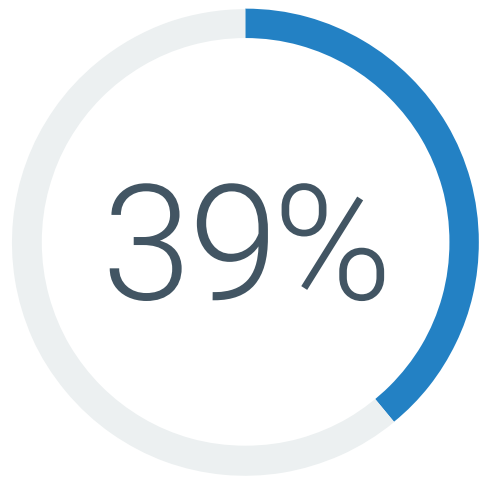
- 1. **Terminate all connections:** Firewalls inspect files upon delivery, often resulting in delayed alerts for malicious content. Zero trust solutions terminate every connection and enable real-time analysis of all traffic, preventing threats like ransomware and malware more effectively.
- 2. **Secure data with detailed, context-based policies:** Zero trust policies verify access requests and rights based on user identity, device, location, content type, and requested application, adapting privileges as contexts change.
- 3. **Negate risk by minimizing attack surfaces:** Zero trust establishes direct connections for users to access necessary apps and resources, bypassing networks. This approach helps reduce risks associated with lateral movement and potential compromise of devices. Consolidating tools distributed across an enterprise, similarly, helps reduce potential attack surfaces.

Security threats, both internal and external, are exacerbated by increasing attack surfaces that require continuous monitoring. The need to expand monitoring across networking landscapes often leads to increased complexity. Additionally, continuing adoption and interest in containers and microservices are factors driving the adoption of zero trust. As such, 91% of all respondents already have implemented, or are in the process of implementing, zero trust initiatives.

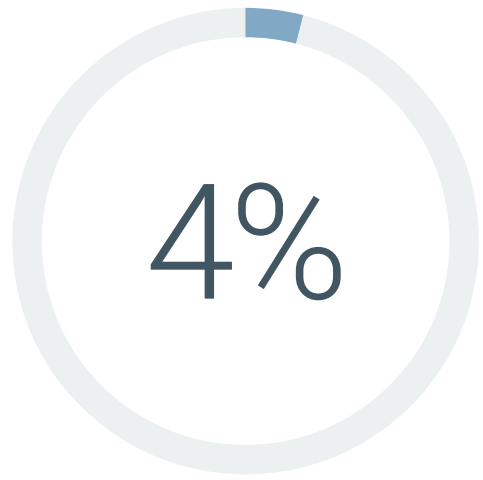
Zero trust initiatives have passed the tipping point.



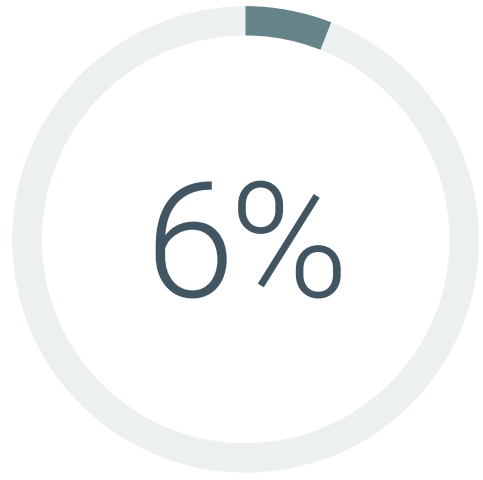
Yes, we have a **broad zero trust initiative underway**



Yes, we have **begun to implement zero trust initiatives for certain use cases**



No, but we are **actively planning a zero trust initiative**



No, and we currently have **no plans for a zero trust initiative**

Advancing Zero Trust Initiatives Is Often a Catalyst for Investments in DEM Solutions

Many tools are required to garner insights around network performance and security (i.e., DEM, network performance management [NPM], application management [APM], endpoint monitoring, etc.). Research generated by TechTarget’s Enterprise Strategy Group provided insights specifically around DEM and its applicability to supporting zero trust.

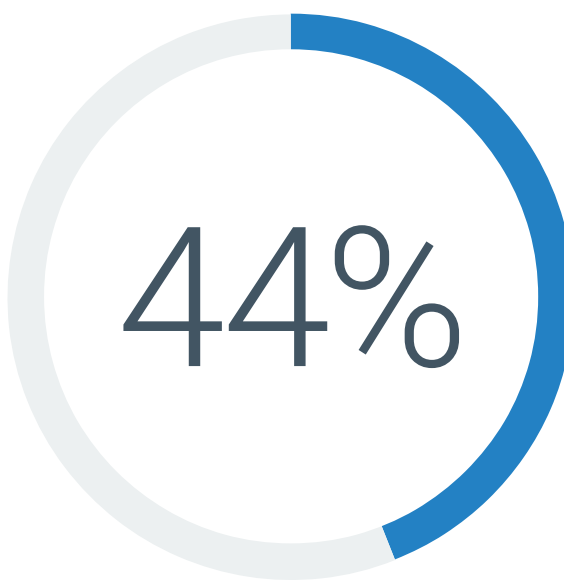
Within the context of the survey, the following definition was provided to all survey respondents: **digital experience monitoring solutions** *measure and assess end-user experience, while enhancing visibility. Instead of focusing on a single application, these tools provide insights into the business impact of technical issues. They empower organizations to identify and resolve business challenges that arise across various applications.*

Data revealed that, while the majority of organizations invest first in zero trust initiatives, 66% primarily invested in DEM solutions to more effectively achieve their zero trust goals.

Which of the following did your organization start investing in first?

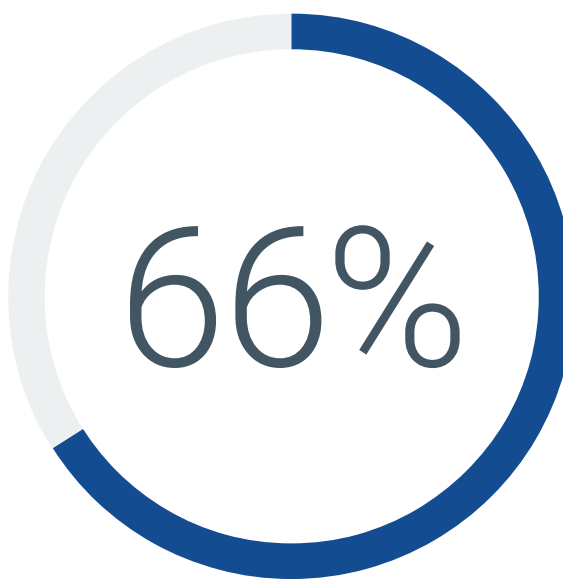


Security controls to advance our zero trust initiative(s)

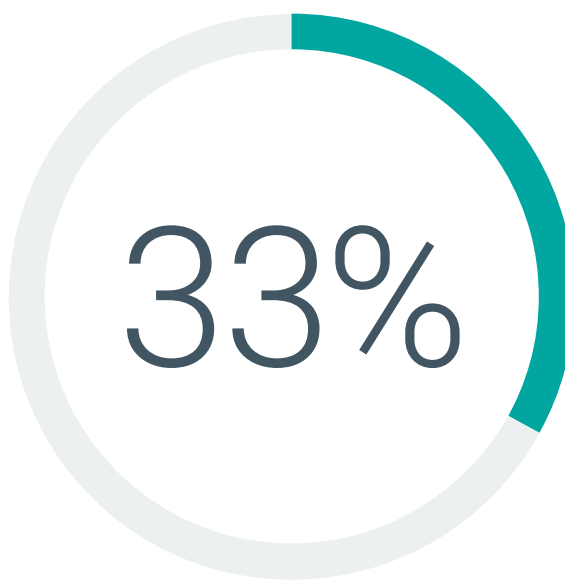


Digital experience monitoring solutions

To what degree did your organization primarily invest in DEM to more effectively achieve its zero trust goals?



This was the main reason



This was one of many reasons



“Data revealed that, while the majority of organizations invest first in zero trust initiatives, **66% primarily invested in DEM solutions to more effectively achieve their zero trust goals.**”

“When asked what the most positive contributions of their DEM solutions were, **3 of the top 5 capabilities reported by respondents lean toward greater awareness and visibility.**”

Visibility- And Awareness-based Functions Contribute to More Effective Network Monitoring

Improving the employee experience in network monitoring requires an understanding of the capabilities needed to perform the solutions’ responsibilities. When asked what the most positive contributions of their DEM solutions were, 3 of the top 5 capabilities reported by respondents lean toward greater awareness and visibility.

With capabilities aligned to zero trust precepts such as real-time monitoring and alerts (36%), complete end-to-end visibility (36%), and AI-based detection and recommendations (35%), DEM solutions are well positioned to support organizations’ network management and monitoring needs.

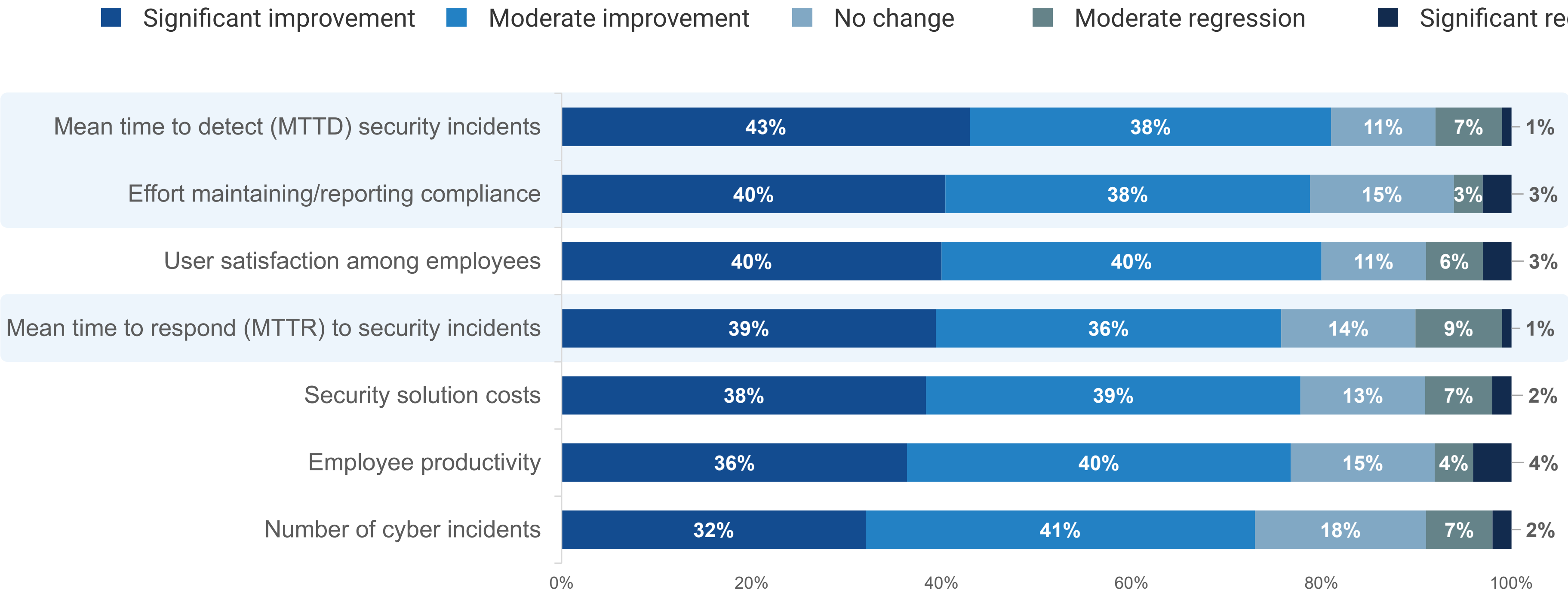
Organizations should leverage observability tools features to improve network monitoring.



Zero Trust Initiatives Are Already Making a Material Impact

The benefits of a strong zero trust strategy are wide ranging. 80% of organizations reported that their zero trust initiatives have improved end-user satisfaction amongst employees. The initiatives also improved employee productivity (76%), as zero trust aids employees in many tasks, such as reducing mean time to detect (MTTD) for security incidents (81%), managing compliance (78%), and decreasing mean time to respond (MTTR) to incidents (75%).

Network team members recognize the value in zero trust.



“80% of organizations reported that their zero trust initiatives **have improved end-user satisfaction amongst employees.**”

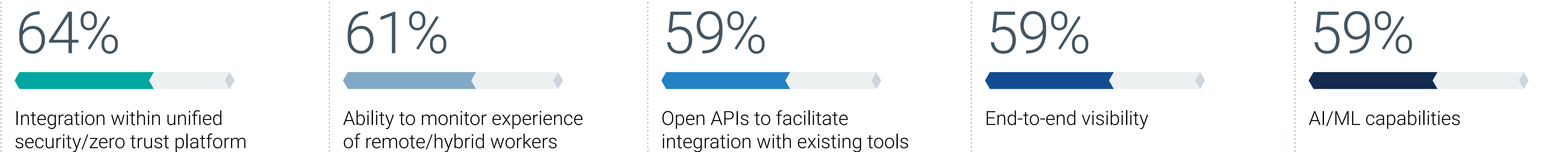
“The majority of organizations (64%) considering DEM investments **prioritize its integration** within a unified zero trust platform.”

DEM Integration With Zero Trust Initiatives Is Most Commonly Reported Critical Capability

It is clear that zero trust initiatives are capable of improving network monitoring KPIs. The potential to enhance employees’ network monitoring experience and productivity is appealing. It’s, therefore, unsurprising that the majority of organizations (64%) considering DEM investments prioritize its integration within a unified zero trust platform.

By integrating DEM technology into zero trust architectures, the capabilities these solutions provide will enhance the ability to better execute core tenets of zero trust.

Validating the case for integrating DEM with zero trust initiatives.





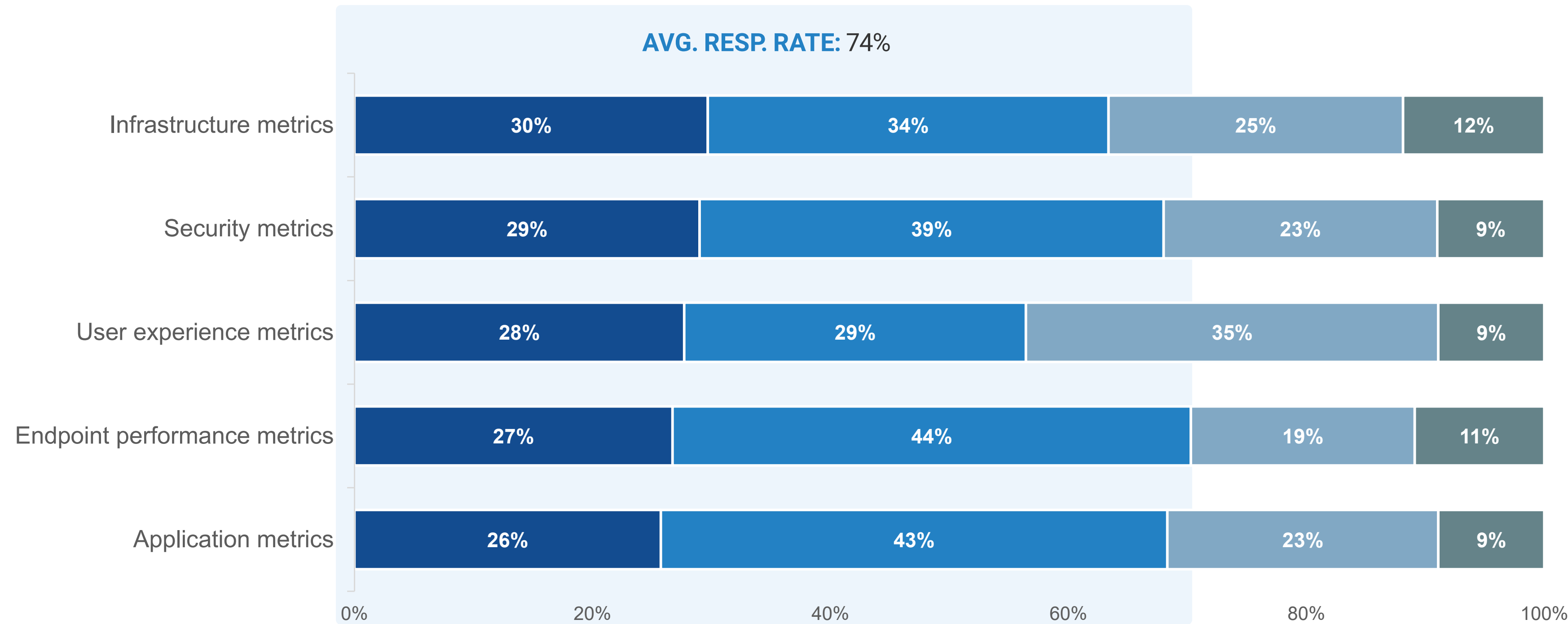
**Maintaining and Monitoring the Digital
Experience of Employees Has Only Gotten
More Difficult**



Measuring Employee Experience Is No Easy Task

Measuring employee experiences is difficult. Organizations reported difficulty throughout a variety of metrics, including infrastructure, security, user experience endpoint performance, and application metrics. On average, 74% of all respondents found that measuring employee experience amongst all applications and digital service areas was challenging or extremely challenging.

Organizations are challenged extrapolating meaningful metric data. Extremely challenging Challenging Not very challenging Not at all challenging

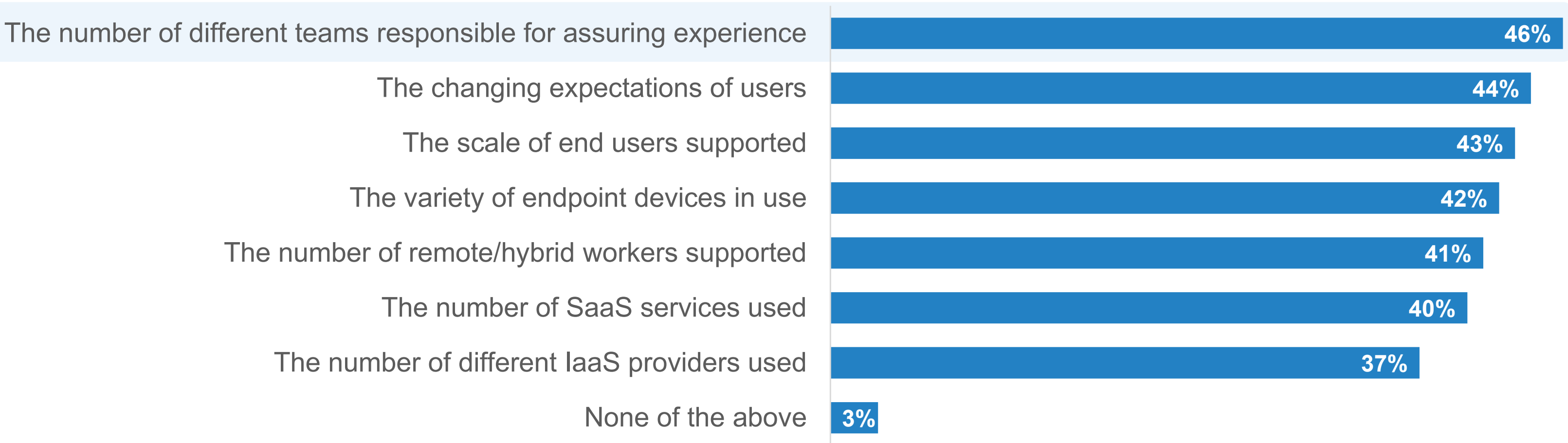


“74% of all respondents found that measuring employee experience amongst all applications and digital service areas **was challenging or extremely challenging.**”

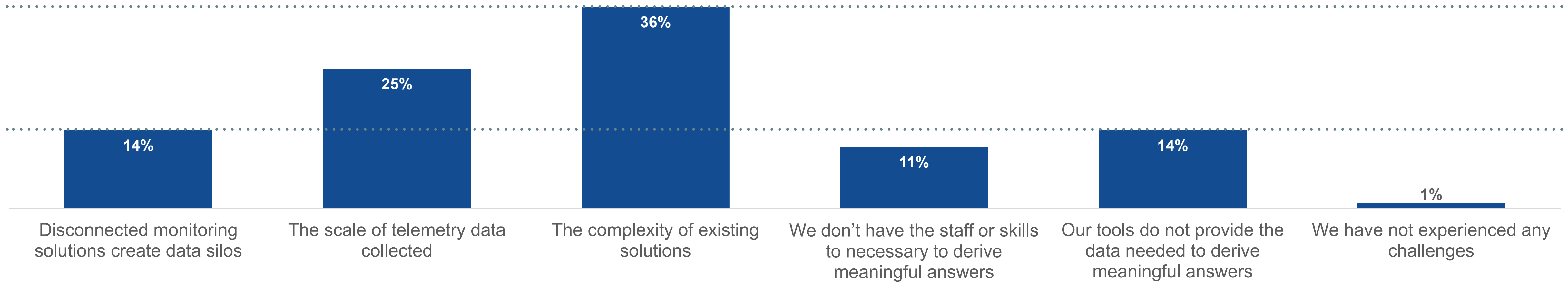
Team Size and the Complexity of Solutions Hamper Digital Experience Insights

Gaining digital experience insights across enterprises has a bevy of potential bottlenecks and impediments. The complexity of existing solutions was identified by 36% of organizations as the greatest barrier to gaining insights. The array of tools distributed across organizations, coupled with difficulties in aligning teams across different groups (46%) contributes to heightened complexity. Streamlining insights through a unified platform can greatly help to alleviate this.

Team size and solution complexity add to the challenge of effective insights.



AVG. RESP. RATE: 16%

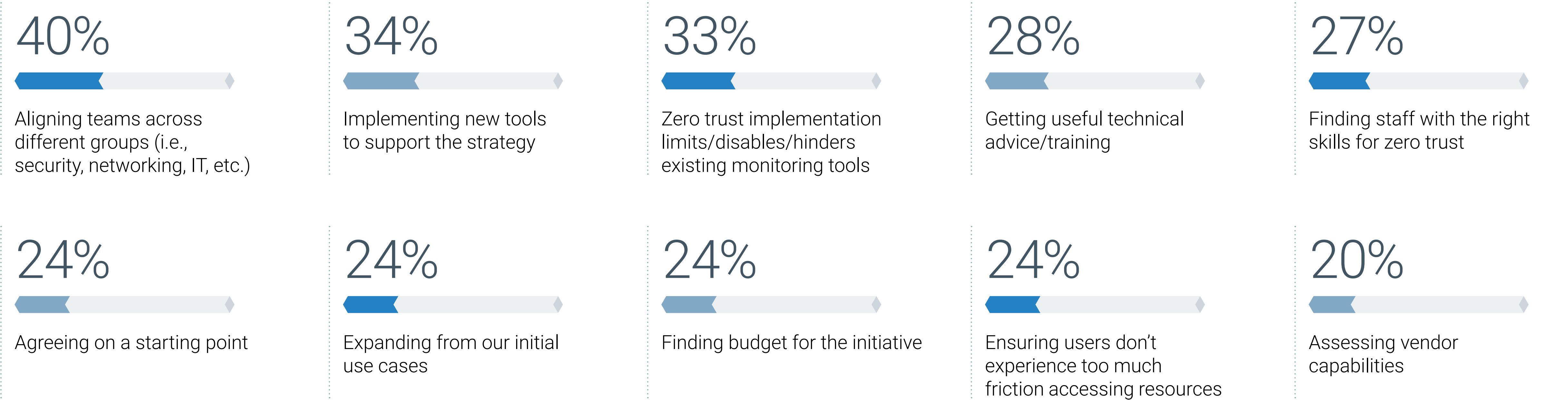


Zero Trust Is Not Without Its Hurdles to Overcome

While capable of improving network monitoring and, ultimately, employees’ user experiences, zero trust is not without its challenges. 34% of organizations reported that implementing new tools to support their zero trust initiative(s) has been one of their greatest zero trust challenges, while 33% reported that zero trust implementation limiting, disabling, or hindering their existing monitoring tools was challenging.

Additionally, aligning teams in different groups, arguably a precursor to operating in silos, is a challenge for 40% of organizations implementing zero trust.

Challenges permeate zero trust initiatives.



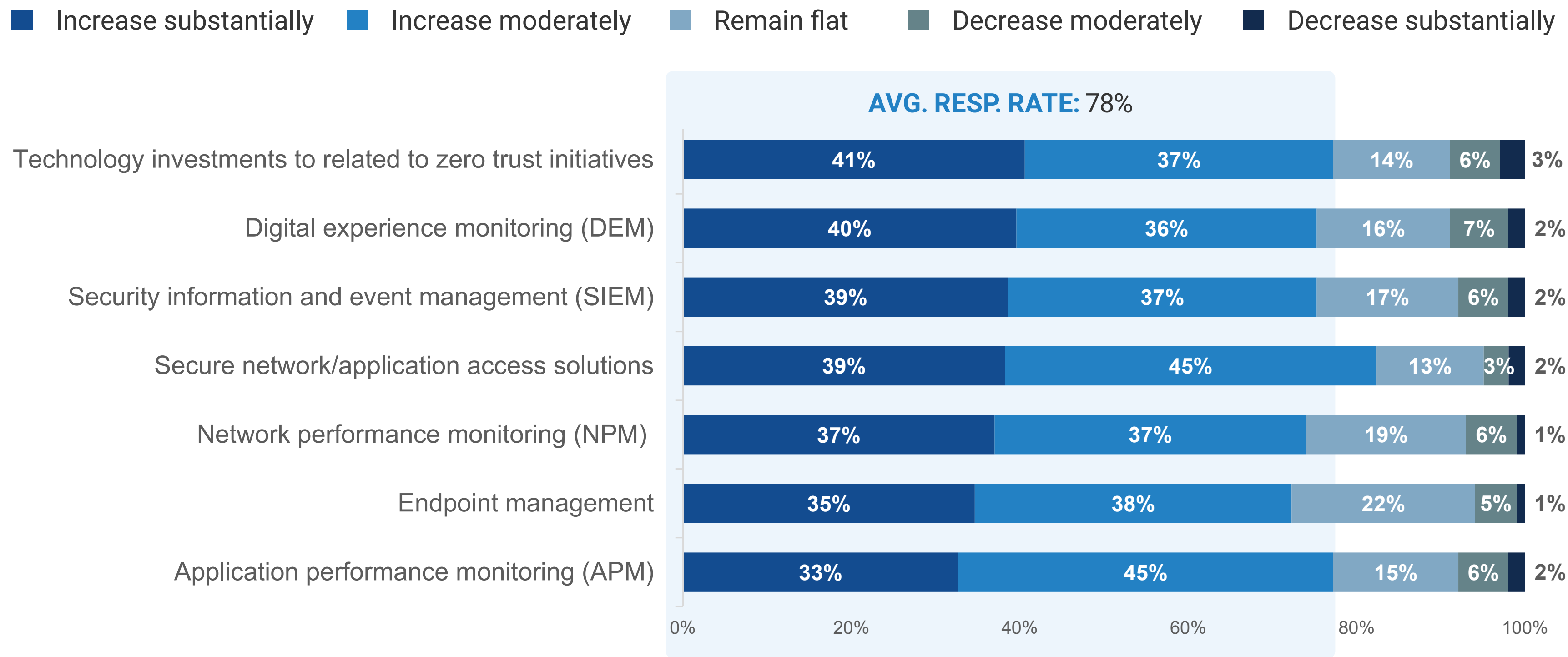
Zero Trust Is Worth the Investment

In spite of some of the identified challenges associated with zero trust initiatives, organizations demonstrate confidence in the value of zero trust, as evidenced by their intended future spending.

Among respondents anticipating increased spending, 41% are expecting to substantially increase their spending on zero trust initiatives, while 40% expected to substantially increase their investment in DEM solutions.

With 78% of respondents anticipating moderate or substantial investment growth in the technologies related to zero trust initiatives over the next 12 to 24 months, it is evident that organizations believe that zero trust is worth the investment.

Solutions supporting zero trust are projected to see increased levels of spending.





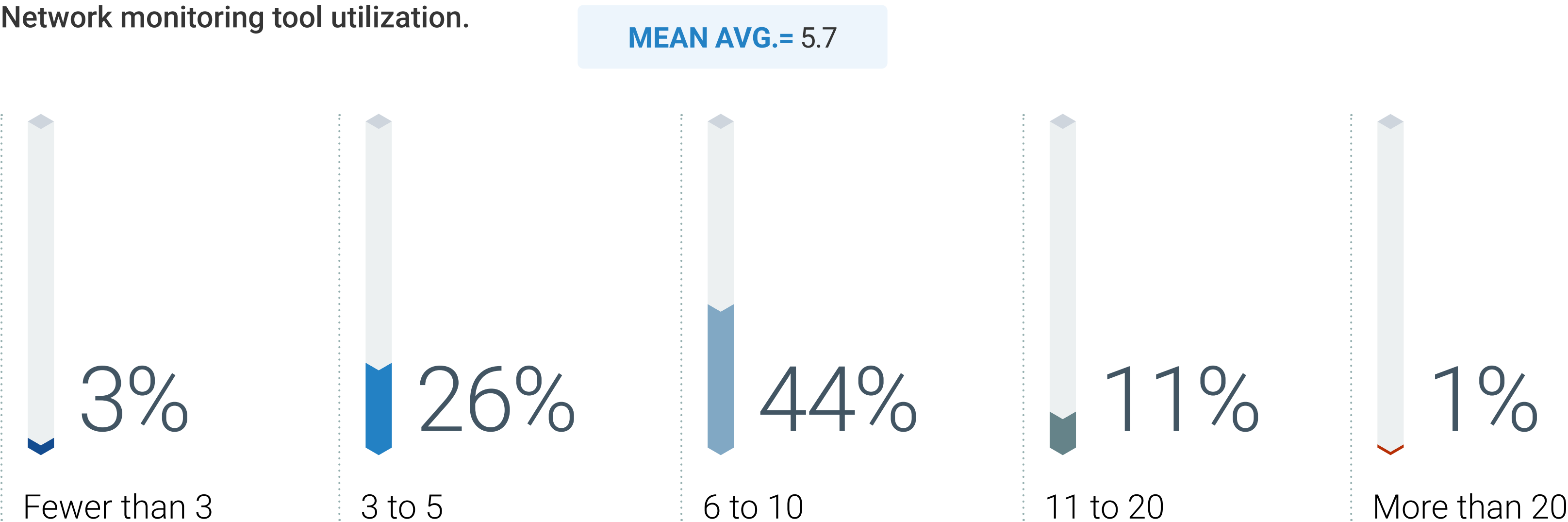
Increased Technology Stacks and Reactive Responses Hinder Network Monitoring

Measuring the Efficiency Lift ServiceOps Maturity Delivers

As teams get bigger, so too does the potential for an increase in the number of network monitoring tools utilized. In fact, 44% of respondents reported that they use 6 to 10 different monitoring tools, with the estimated mean average for the number of monitoring tools used by organizations being 5.7 tools.

Each monitoring tool adds an extra layer to the IT infrastructure and the potential for siloed visibility. Consolidating monitoring systems can enhance security by providing a comprehensive view of the network, reducing attack thresholds, and improving threat and performance visibility.

Network monitoring tool utilization.



“Consolidating monitoring systems can enhance security by providing a comprehensive view of the network, reducing attack thresholds, and improving threat and performance visibility.”

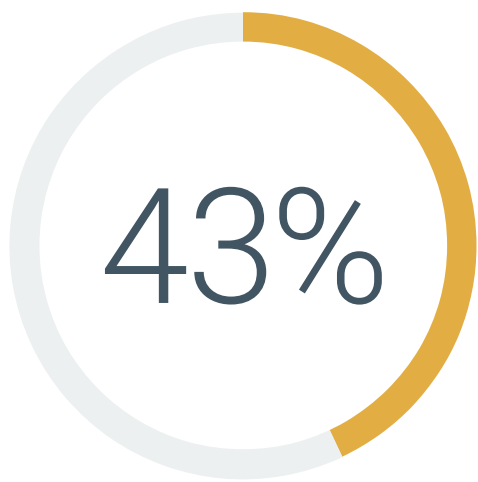
“**58% of organizations are at least sometimes reactive** when issues arise, taking action after employees notice the issues.”

Organizations Need to Get Ahead of Issues Sooner Rather Than Later

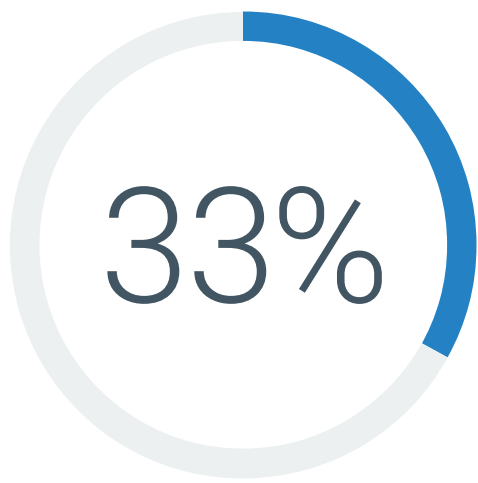
Along with the number of tools utilized potentially impeding network and performance monitoring, being reactive instead of proactive can result in less efficient management of issues when they arise. This can lead to loss in productivity, an increase in IT infrastructure exposure to incidents or threats, and slower MTTR. 58% of organizations are at least sometimes reactive when issues arise, taking action after employees notice the issues.

By leveraging AI and robust root cause analysis (RCA) found in top-tier DEM solutions, organizations have a greater potential to shift toward a proactive approach, identifying and taking action on issues before employees notice them.

Monitoring teams should strive to be more proactive in addressing issues.



Generally proactive: we are able to identify and take action on issues before employees notice them



It's a **mix**

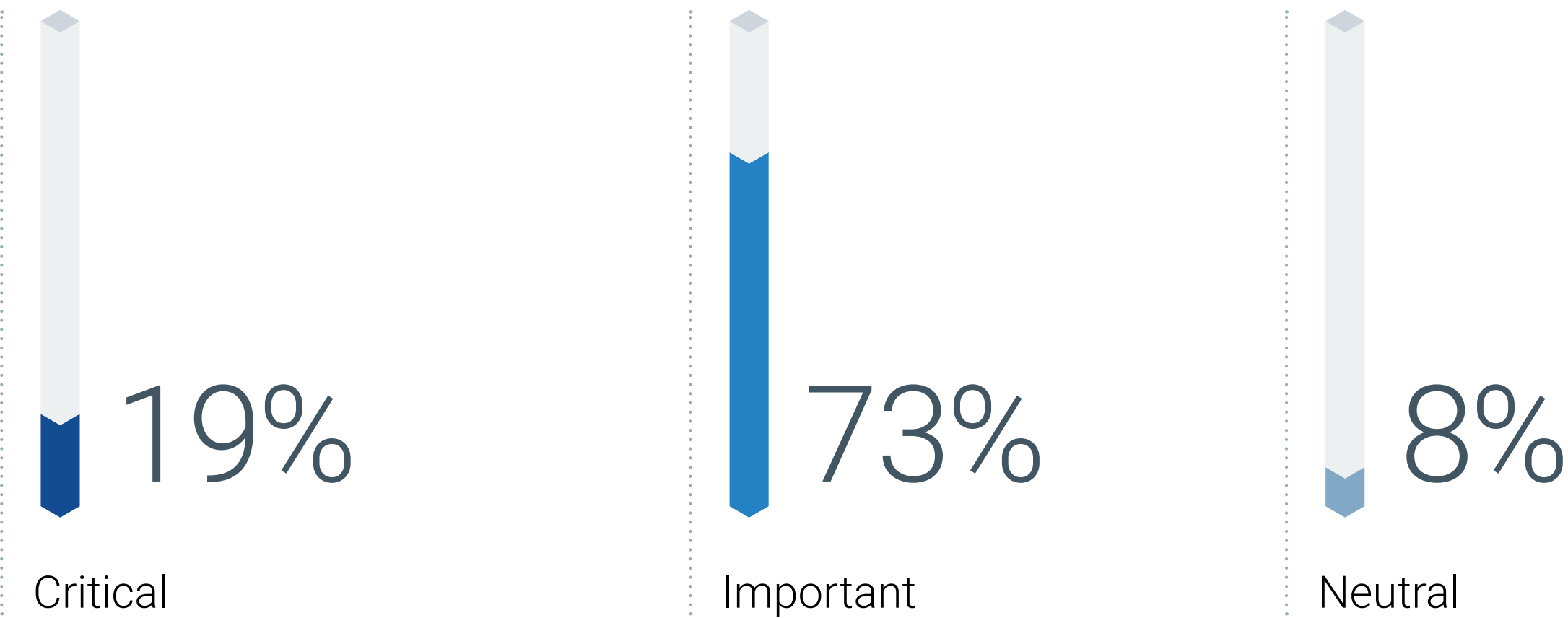


Generally reactive: we identify and take action on issues after employees notice the issues and submit helpdesk tickets

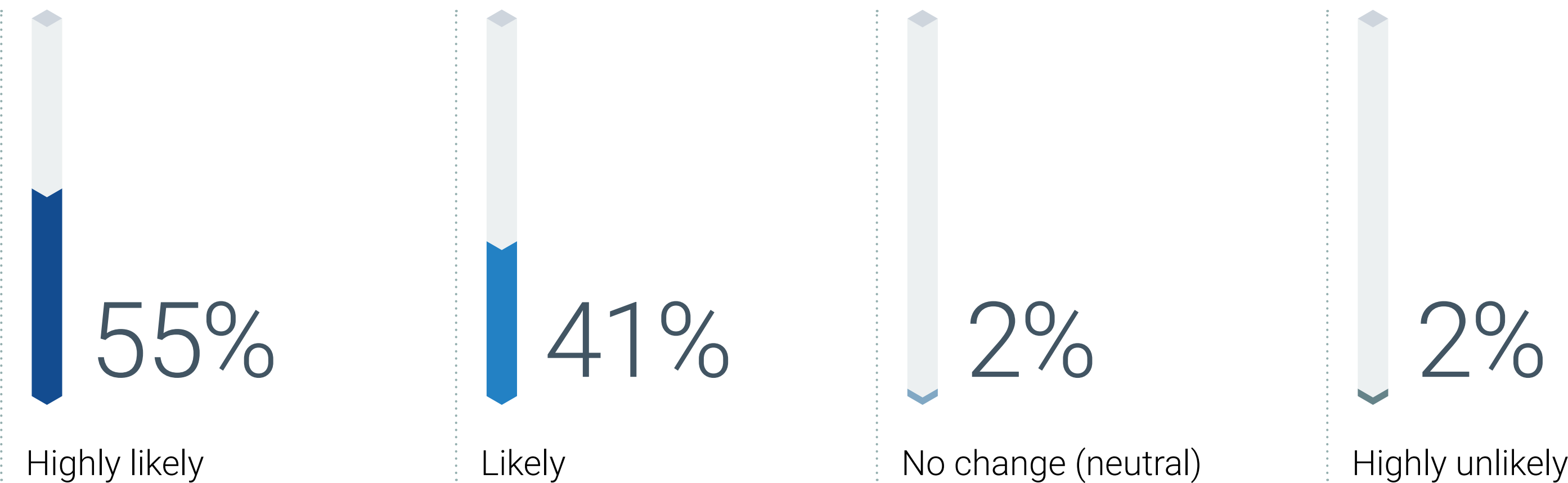
DEM Solutions Can Be the Bridge Between Being Proactive Instead of Reactive

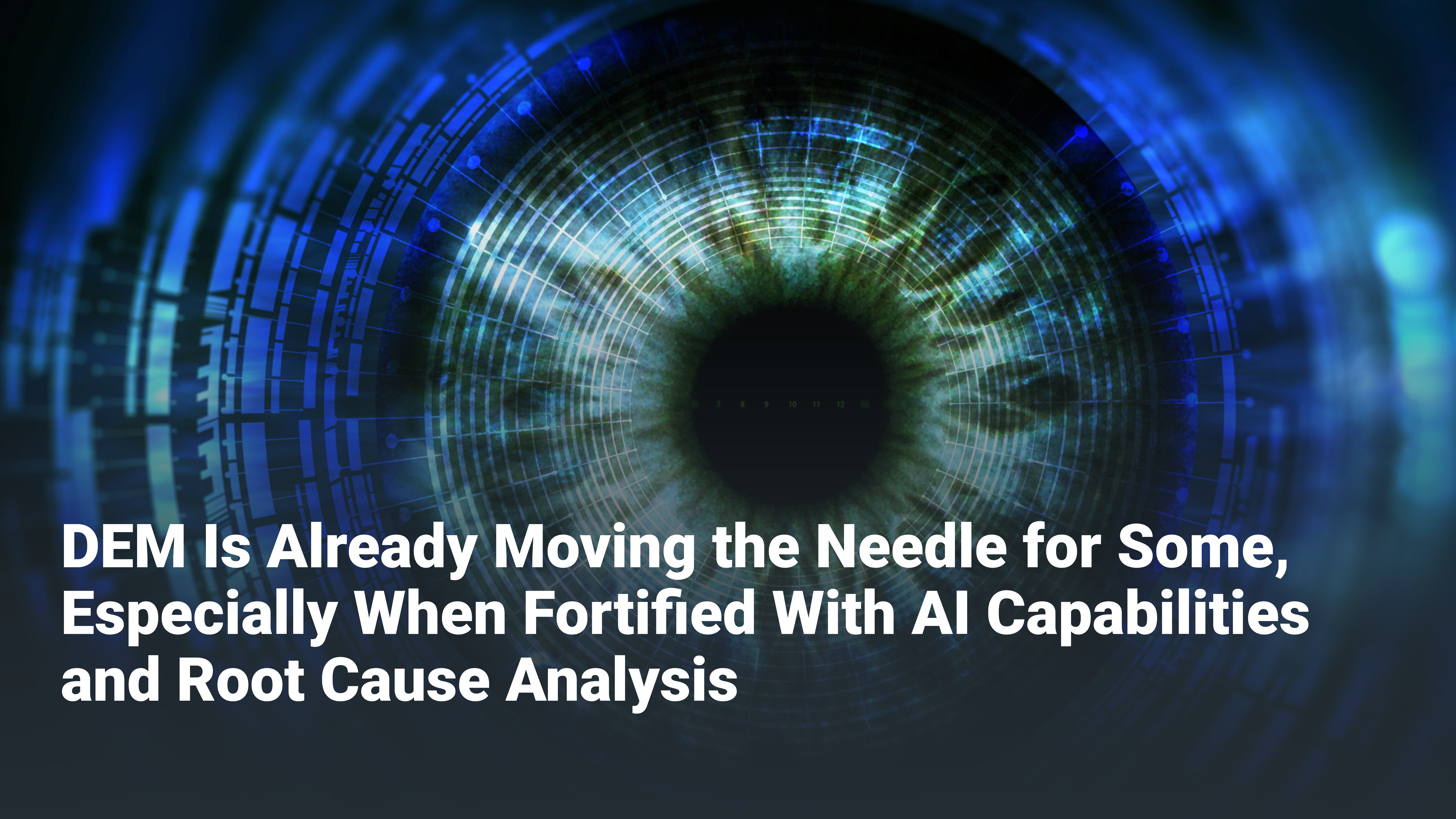
Effective use of DEM solutions can greatly assist organizations in being more proactive. 92% of respondents reported that DEM solutions were critical or important to their proactive responsiveness to potential incidents and issues. However, 96% of respondents feel stuck in a mostly reactive mode and feel better use of DEM would help them become more proactive.

DEM solutions are essential to proactive network monitoring.



Most organizations feel better use of DEM would help them become more proactive.





**DEM Is Already Moving the Needle for Some,
Especially When Fortified With AI Capabilities
and Root Cause Analysis**

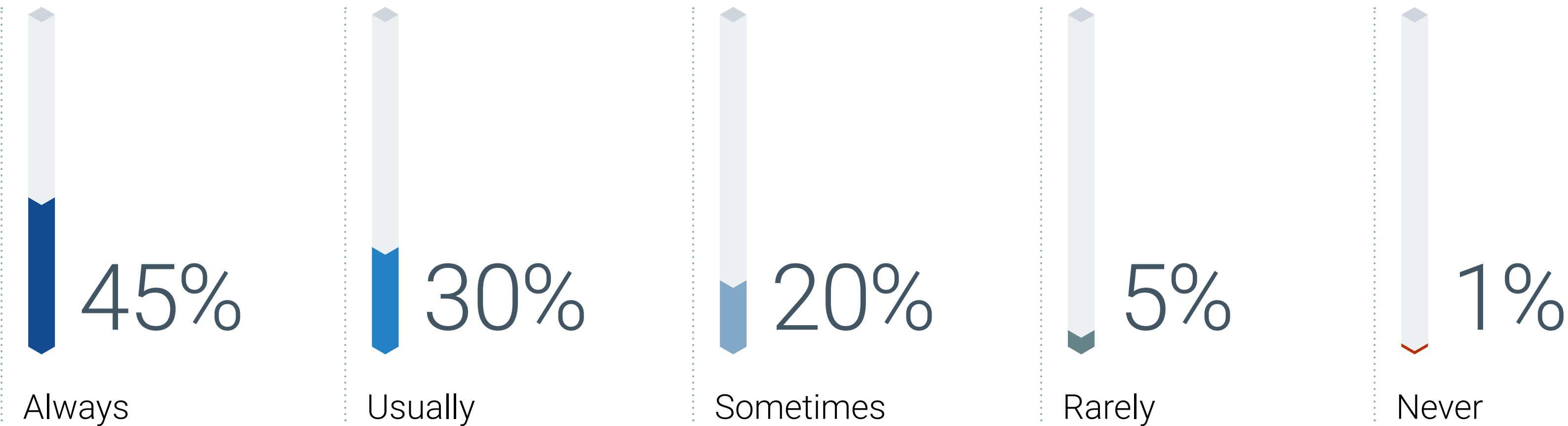
Get to the Root of the Problem With RCA

RCA is a technique used to uncover the fundamental reasons behind an observed or experienced incident.

AI-powered RCA can isolate underlying causes of performance issues automatically in a highly efficient and proactive manner, often triggering alerts when discovered.

Yet less than half of all respondents (45%) expressed assuredness of their ability to always conduct a thorough RCA if necessary.

The majority of organizations are unable to always provide RCA.



45%
of respondents
expressed
**assuredness of
their ability to
always conduct
a thorough RCA
if necessary.**

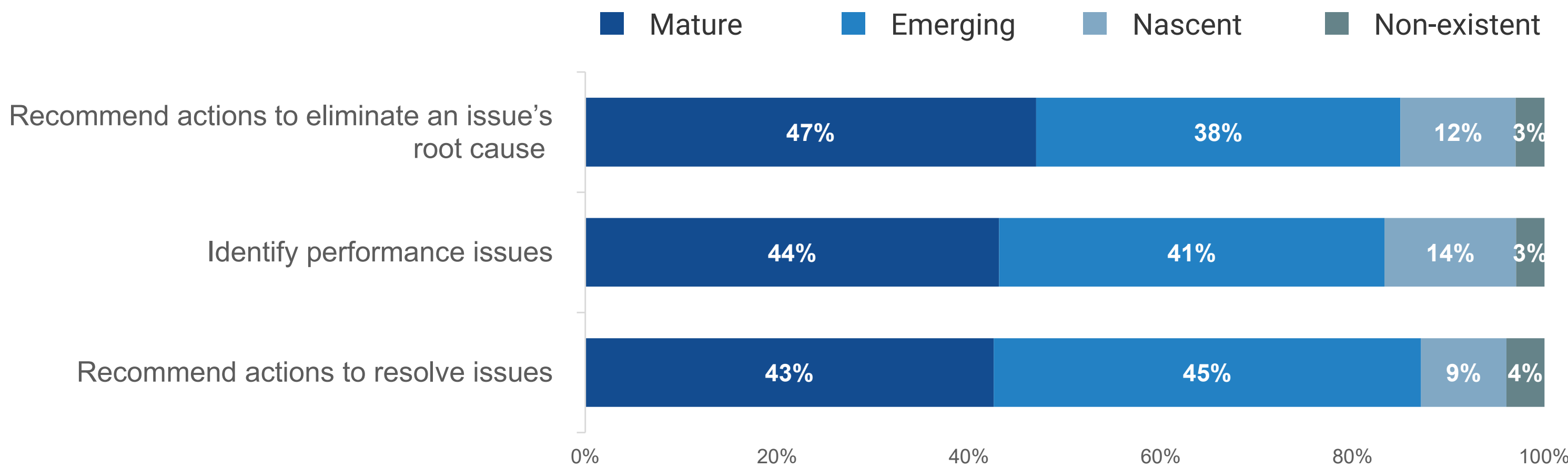
DEM Solutions Are Better Able to Maximize Observability With AI-Based RCA

Organizations identified their DEM solution’s ability to leverage AI/ML capabilities, based on their own assessment, as being mature, emerging, nascent, or non-existent (as well as not knowing).

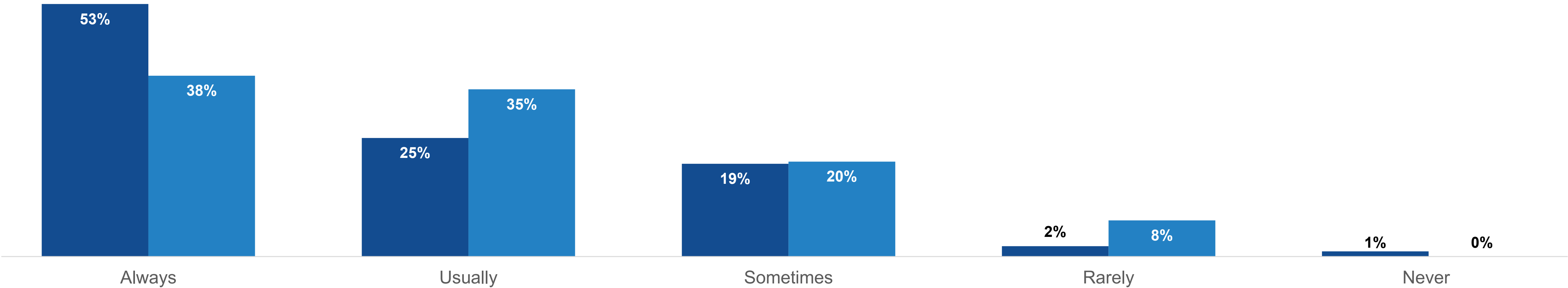
47% of organizations reported that their DEM solution is mature when it comes to leveraging AI/ML to recommend actions to eliminate an issue’s root cause.

Moreover, those organizations saying their DEM solutions have mature AI capabilities were 40% more likely to report being always able to conduct a thorough RCA when incidents occur.

Organizations that have DEM solutions with mature AI are more likely to enjoy RCA.



When incidents occur, mature organizations are 40% more likely to be always able to conduct a thorough RCA.



ROI in Dem Solutions Is Illustrated by Strong Key Performance Indicators

Organizations have seen improvements around several network monitoring key performance indicators, many of which greatly support zero trust initiatives. The top three areas where respondents saw either game-changing or significant improvements were the following:



1. Improved end-user productivity (65%).



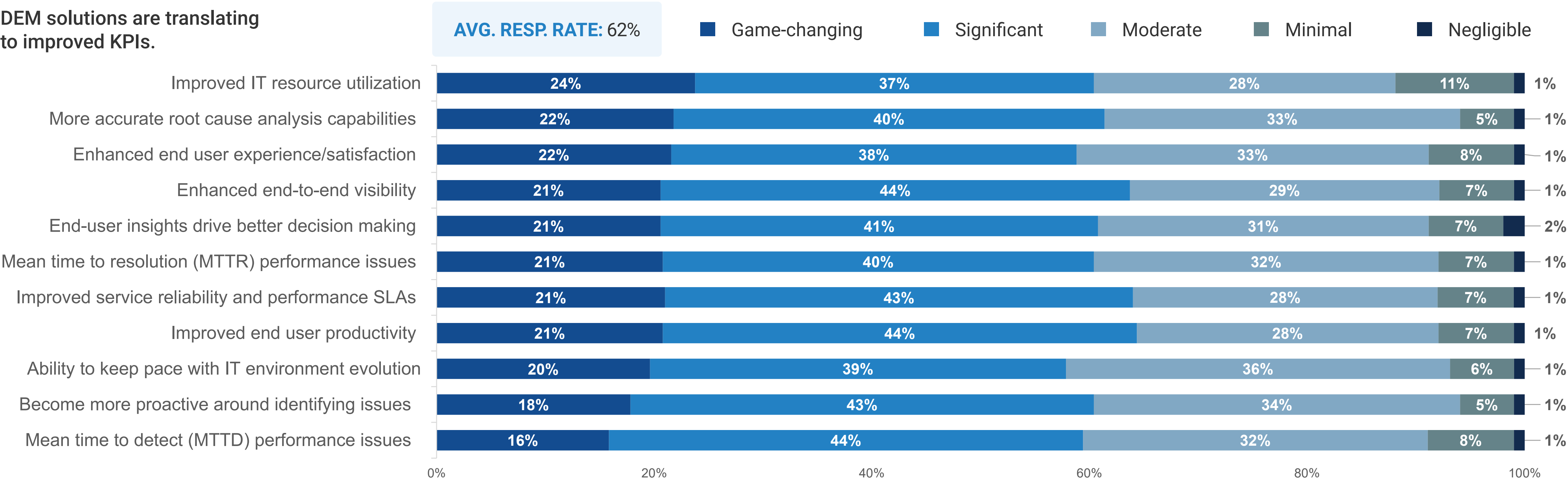
2. Enhanced end-to-end visibility (65%).



3. Improved service reliability and performance SLAs (64%).

Overall, 62% of respondents in aggregate experienced significant improvements across all KPIs.

DEM solutions are translating to improved KPIs.

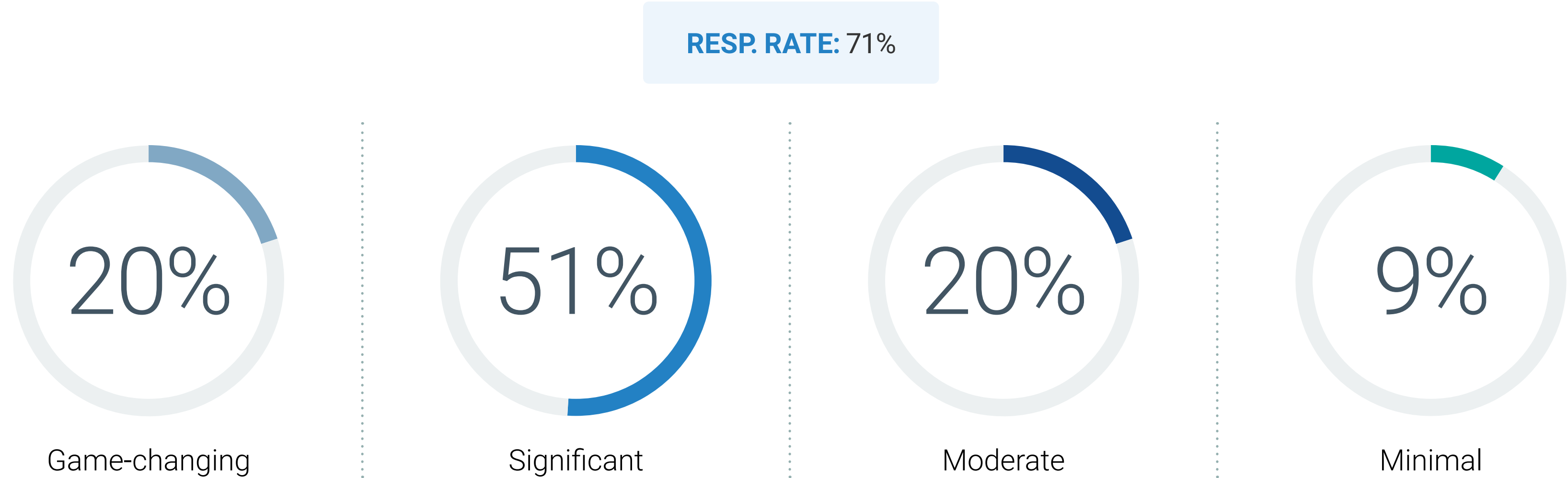


DEM Solutions That Leverage AI Improve End-to-end Visibility and Are Vital to Network Monitoring Success

Using DEM solutions with artificial intelligence capabilities offers several KPI benefits. For example, 71% of respondents with AI-based anomaly detection and recommendations have seen game-changing or significant improvements in their end-to-end visibility.

AI enhances user data collection and boosts network monitoring by analyzing network activity and application data from user interactions. Faster anomaly detection, root cause analysis, and automated responses improve digital experience monitoring, enhancing end-to-end visibility.

DEM solutions improve end-to-end visibility.



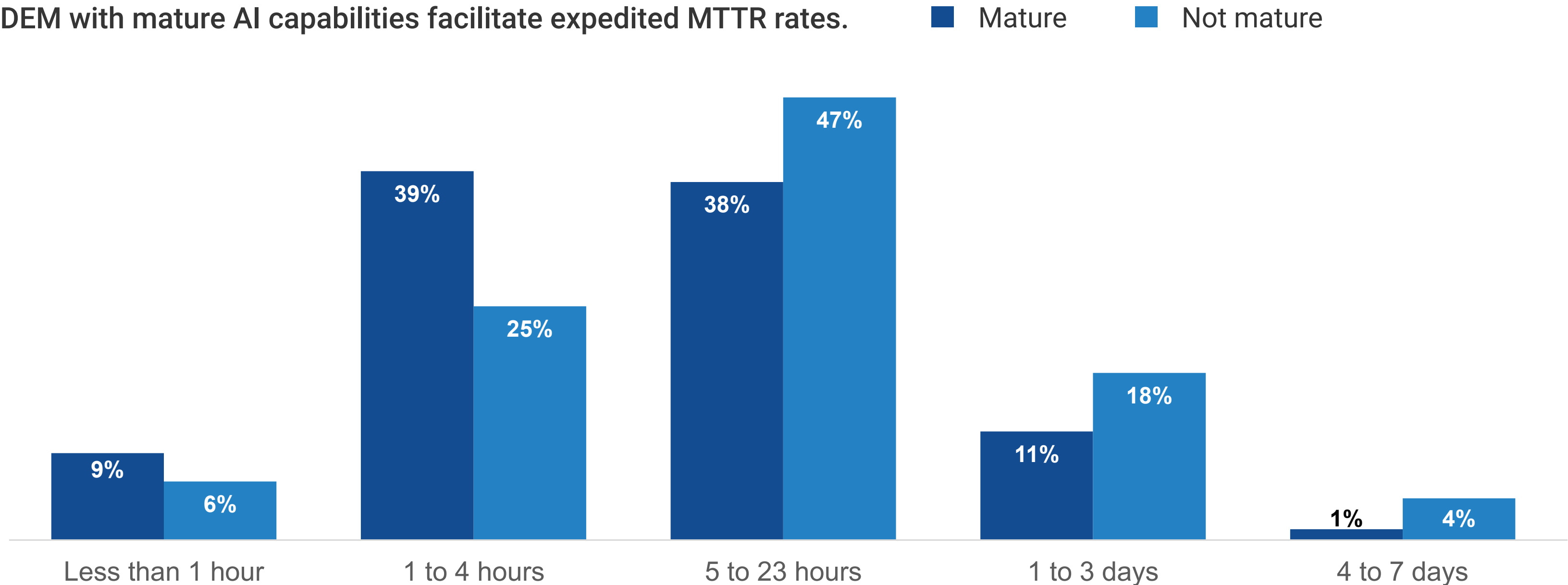
“71% of respondents with AI-based anomaly detection and recommendations have seen **game-changing or significant improvements in their end-to-end visibility.**”

“When incidents and issues do arise, organizations leveraging DEM solutions with more mature AI capabilities were **55% more likely to enjoy an MTTR under a maximum of four hours, compared to those with less-mature AI.**”

AI Capabilities in DEM Can Also Help Reduce MTTR

When AI maturity in organizations’ DEM solutions were evaluated, 47% had RCA capabilities. These RCA capabilities greatly support and expedite resolution to uncovered incidents.

When incidents and issues do arise, organizations leveraging DEM solutions with more mature AI capabilities were 55% more likely to enjoy an MTTR under a maximum of four hours, compared to those with less-mature AI.



Conclusion

There is a clearly demonstrated enterprise-wide need for organizations to adopt zero trust initiatives to mitigate potential threats across the digital landscape. The effectiveness of zero trust is heavily reliant on the quality of the insights provided across the assortment of applications, tools, and services utilized for network monitoring. However, it is evident that DEM solutions can, and do, support zero trust initiatives.

DEM solutions have the ability to improve end-user productivity, enhance end-to-end visibility, and improve service reliability, among many other benefits. Leveraging DEM solutions that feature AI and RCA capabilities only further enhances an organization’s network monitoring experience and potential to maximize the effectiveness of their zero trust initiatives.

About Zscaler

Zscaler (NASDAQ: ZS) accelerates digital transformation so that customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange™ protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SASE–based Zero Trust Exchange is the world’s largest inline cloud security platform.

[LEARN MORE](#)



RESEARCH METHODOLOGY
AND DEMOGRAPHICS

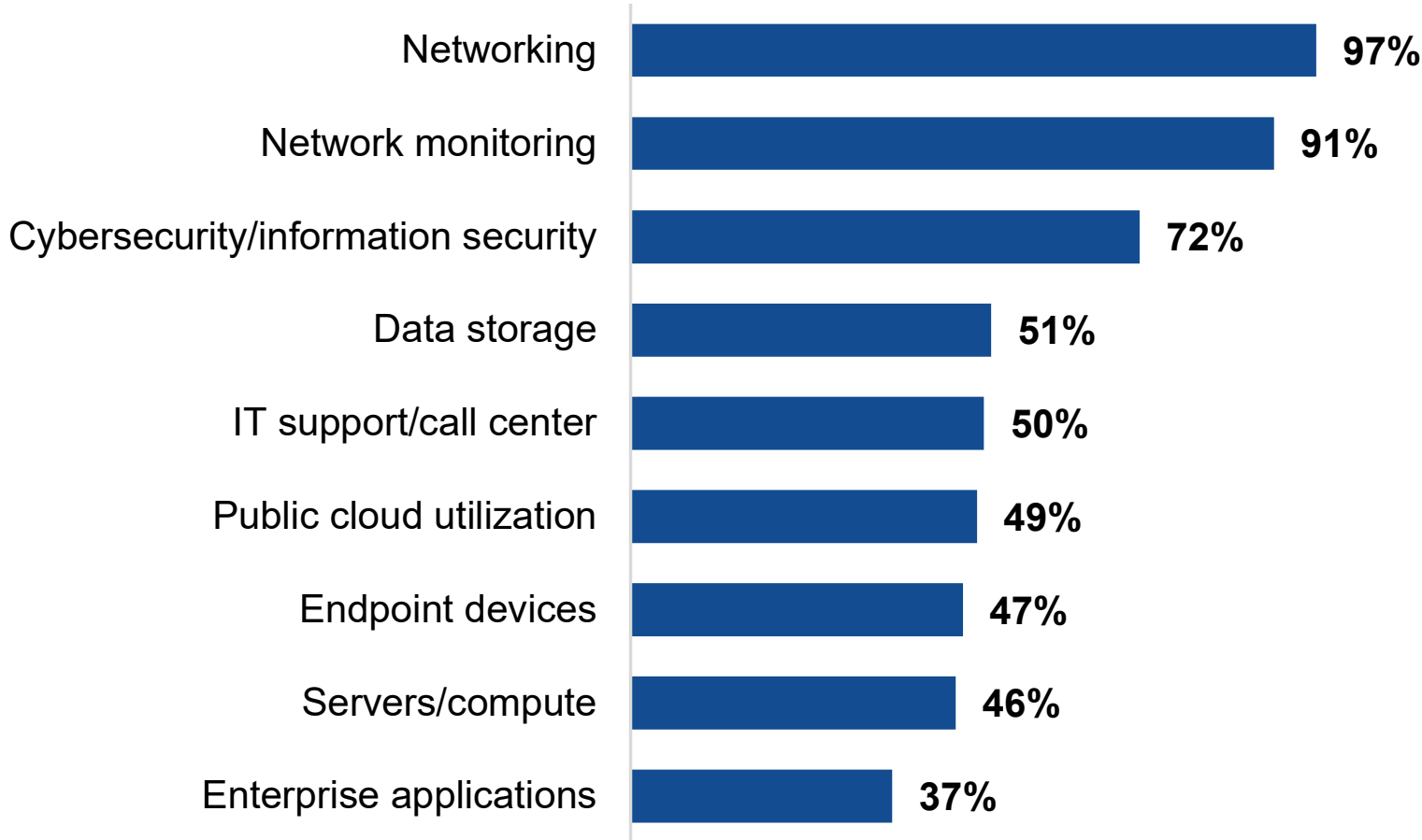
This study—fielded between February 9, 2024 and February 18, 2024—included IT and network professionals involved with their organization’s digital experience monitoring technologies and needs. The respondents in the study were employed at organizations with 5,000+ employees located in the U.S. and Canada that had an annual revenue of \$500M+.

After applying data quality control best practices and screening the remaining completed responses (on several criteria) for data integrity, a final sample of 200 respondents remained. All respondents were provided an incentive to complete the survey in the form of cash awards and/or cash equivalents.

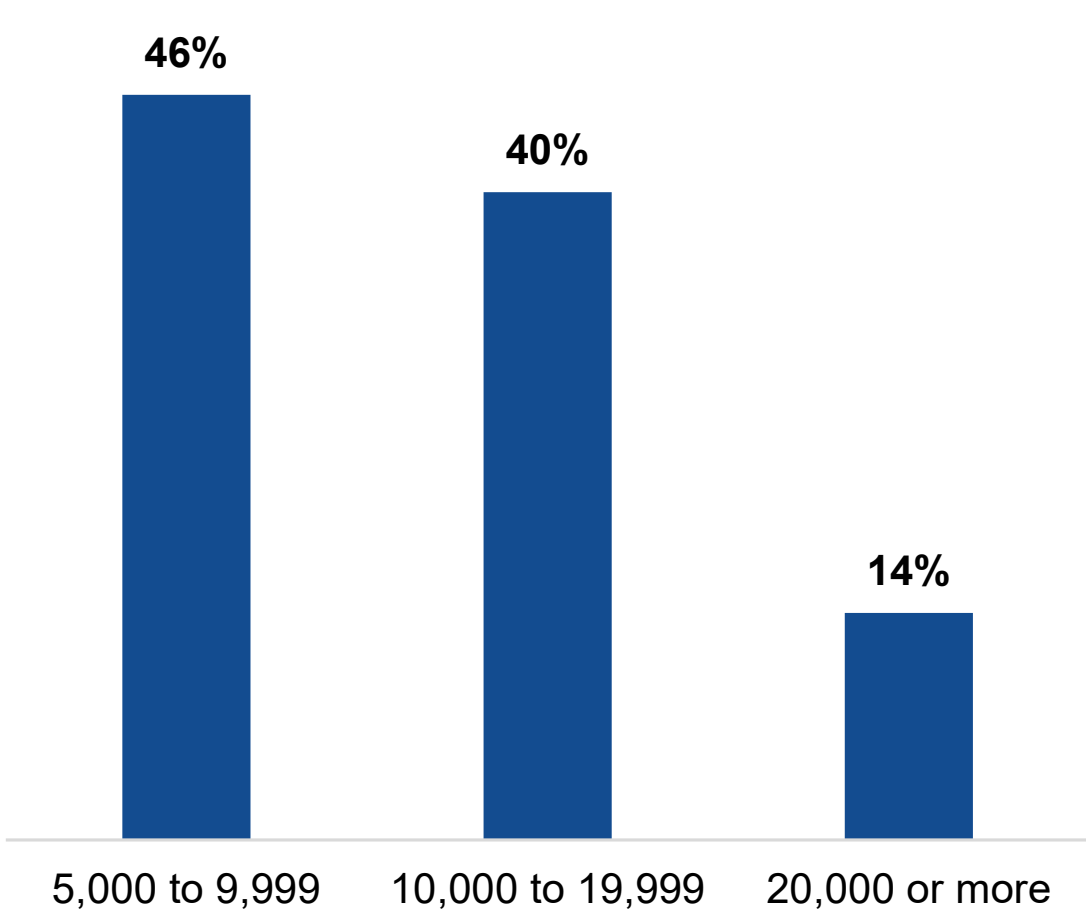
Survey confidence level is 95% with a margin of error was +/-6.9%

Note: Totals in figures and tables throughout this report may not add up to 100% due to rounding.

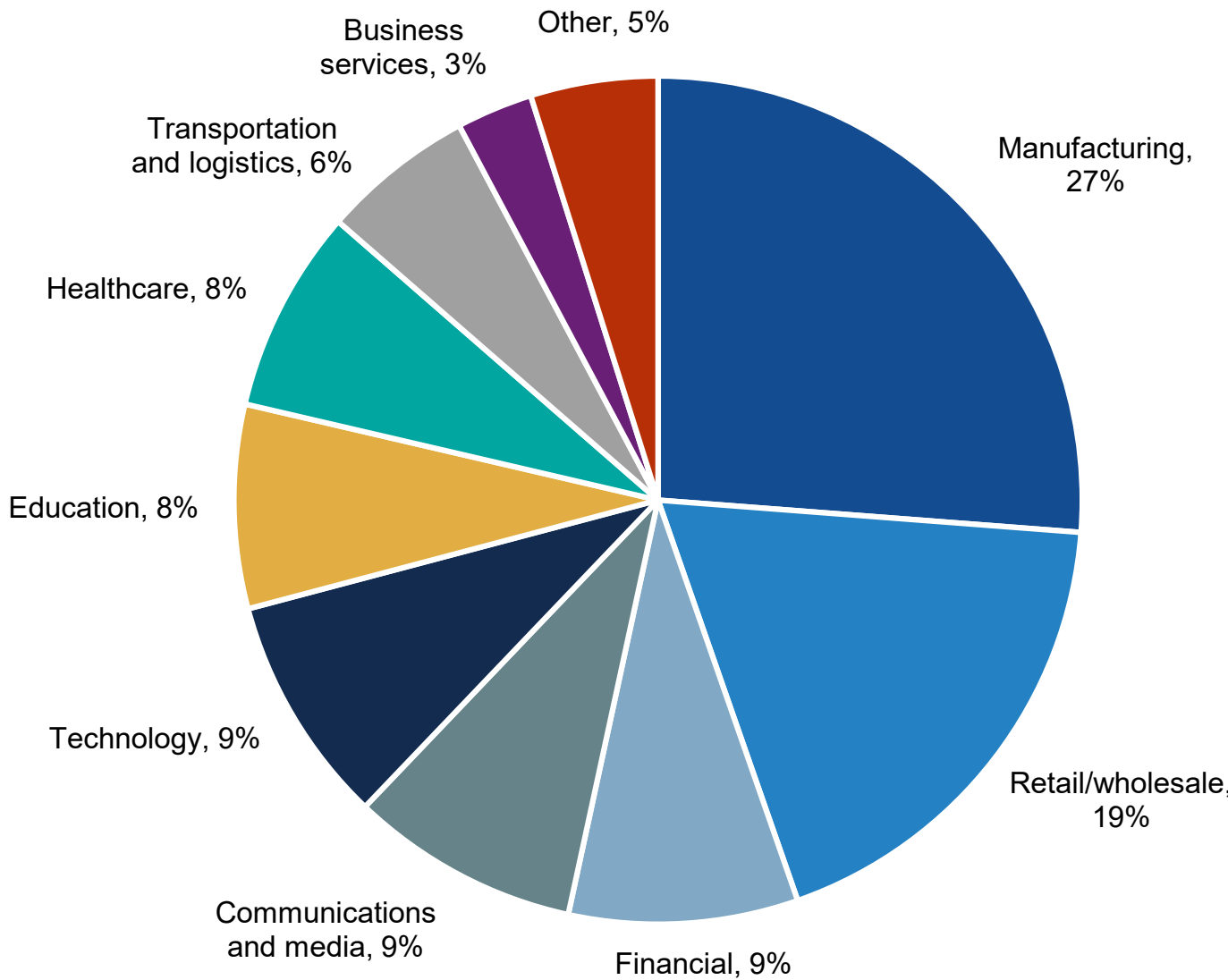
Respondents by areas of IT involvement.



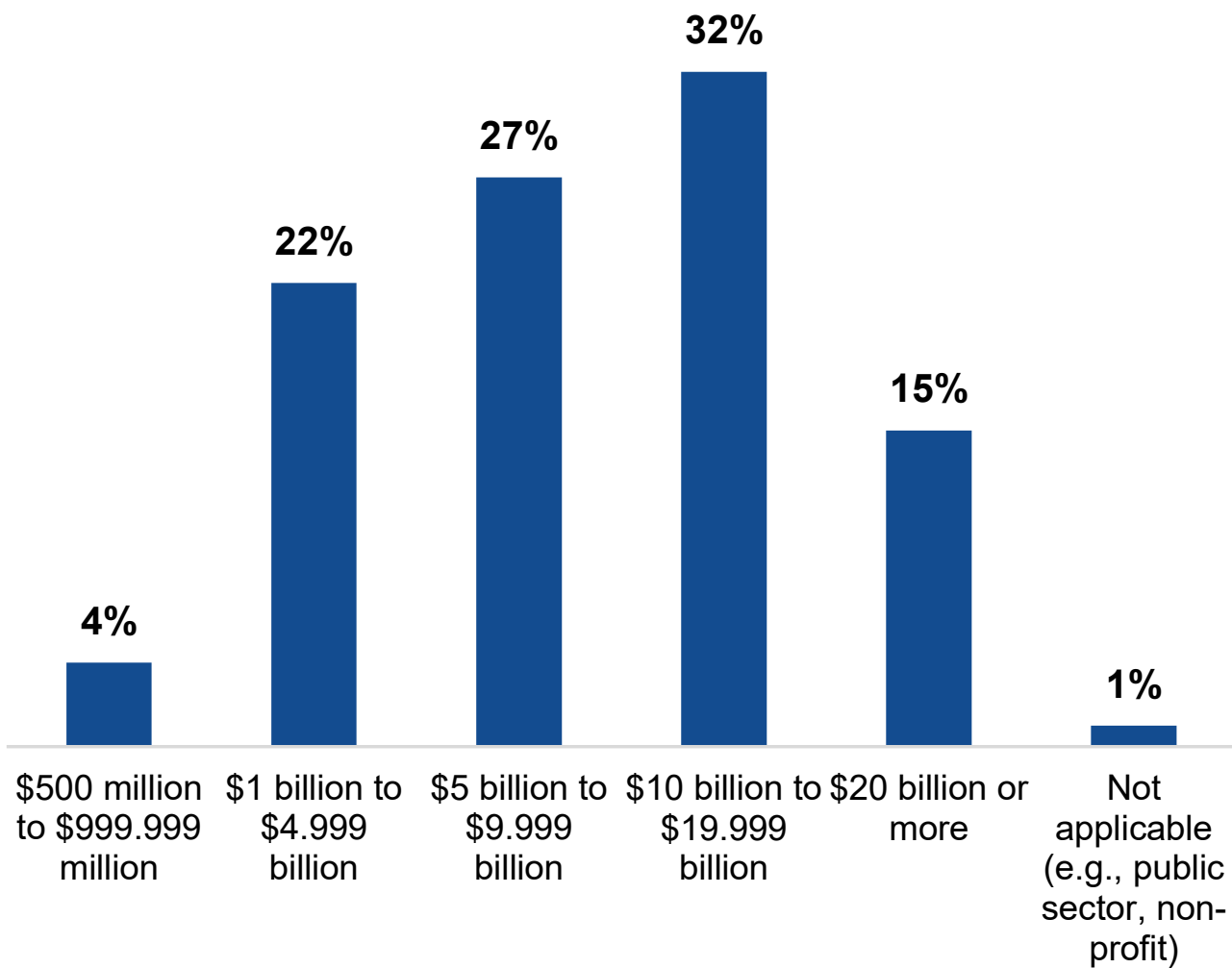
Respondents by number of employees.



Respondents by Industry vertical.



Respondents by their organization’s annual revenue (\$US)?



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.

© 2024 TechTarget, Inc. All Rights Reserved.