VIAVI

16TH ANNUAL 2024/25

State of the Network Study

Discover How Transitioning to Observability Drives Success in Managing and Protecting Hybrid Network Environments

Enterprise Strategy Group™
by TechTarget

VIAVI delivers unmatched network performance and security solutions, providing comprehensive visibility and proactive management of performance issues and cybersecurity threats. By transforming complex data into actionable insights, VIAVI helps organizations secure and optimize their digital environments. The Observer Platform offers end-to-end monitoring, advanced threat forensics, and scalable solutions, ensuring seamless application delivery and robust security. This unified approach enhances network reliability and security, driving optimal performance and protection in the digital landscape.

Contents

Executive Summary

TechTarget's Enterprise Strategy Group proudly presents the findings of the 16th Edition 2024/25 State of the Network study, commissioned by VIAVI Solutions. The study provides insights into, and analysis of, the ever-evolving challenges that network managers face, driven by the proliferation of cloud-native applications and increasingly complex infrastructures, it evaluates the strategic innovations that help to answer the call. There were 754 networking and security professionals surveyed across multiple industries and spanning 10 countries, including Australia, Brazil, Canada, France, Germany, Mexico, New Zealand, Singapore, the United Kingdom, and the United States.

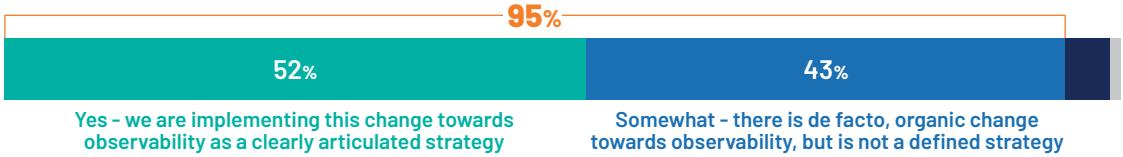
The objective of this ongoing research is to examine the evolution of network performance and security tools over the past 16 years, as well as to assess their impact on the operational and security posture of enterprise organizations. The first national State of the Network study was conducted in 2007 by VIAVI Solutions' predecessor Network Instruments, and this latest edition expands its reach globally.

52% of respondents have a clearly articulated observability strategy.

43% are transitioning to observability in an ad hoc manner.

FROM MONITORING TO OBSERVABILITY

Organizations are adopting an observability strategy. This year's focus is on key trends and transformative practices that network and security professionals must adopt to be effective in a continuously changing digital environment. As part of deep exploration into the evolution of network and security management, the shift from traditional monitoring to advanced observability is rigorously covered. This transition is pivotal, as it enhances the ability to not only predict and respond to network issues but also to understand their impacts on business outcomes. Organizations that have embraced formal observability strategies are shown to gain significant advantages, including enhanced operational insight, better problem resolution, and increased agility. These benefits are vital for organizations that aim to maintain competitive advantages and ensure high levels of user satisfaction.



See full analysis of Figure 2 on page 11

TRIMMING THE MONITORING TOOLCHEST

58% reduction in average MTTR for respondents with 10 or fewer monitoring tools than those with 11 or more tools.

One attractive area explored is the ongoing proliferation of monitoring tools across network environments. Organizations continue to grapple with the choice between maintaining a diverse array of specialized monitoring tools versus consolidating into fewer, more comprehensive solutions. The findings clearly demonstrate that a higher number of tools tends to complicate visibility and reduce operational efficiency. It examines these challenges but also discusses the potential benefits of tool consolidation, which include streamlined operations, reduced costs, and improved response times. The insights provided can guide organizations in making informed decisions that enhance network management capabilities and operational resilience.

VAULTING THE HYBRID HURDLES

Packet and flow data remain critical in hybrid cloud environments. Hybrid, multi-cloud infrastructures are the new normal and are challenging network managers trying to establish comprehensive visibility. Packet and flow data capture remain critical for managing these environments but must be adapted for optimal effectiveness. Surprisingly, only 20% of organizations have collaborative approaches for cloud-based application monitoring, with larger organizations more reliant on cloud service providers (CSPs). This presents both a challenge and an opportunity for network managers to leverage network data for reducing mean time to detect (MTTD) and mean time to repair (MTTR) by fostering cross-team collaboration. Despite progress, visibility challenges persist, particularly in public cloud environments, where 80% of respondents report high difficulty. Effective observability strategies are essential as data sets become more diverse, emphasizing the need for diligent network monitoring strategies to achieve desired levels of visibility.

CONTINUOUS THREAT EXPOSURE MANAGEMENT

A unified approach to security. Another significant development is the convergence of observability and security practices, leading to improved continuous threat exposure management (CTEM). According to our findings, a substantial **88% of organizations recognize the urgent need to enhance their threat management capabilities**, with CTEM emerging as a critical strategy in response to this demand.

The integration of threat exposure management with attack surface management across hybrid environments is particularly relevant today, as organizations face an increased attack surface due to the proliferation of multi-cloud services and remote work arrangements. Other cybersecurity challenges highlighted by respondents include the predominance of regulatory compliance at the expense of best practice implementation; cybersecurity teams being too "incident-focused," which impedes overall posture improvements; the overwhelming volume of security alerts; and insufficient vulnerability assessment capabilities. These challenges underscore the necessity for a strategic shift toward more integrated and proactive security management practices.

88% of organizations believe that improving threat management capabilities is either important or critical.

In response to these complexities, the case for CTEM is compelling. The research shows that while many organizations currently deploy a variety of tools and practices to manage threats, the scale and sophistication of threat landscapes are making these traditional methods increasingly untenable. By integrating observability with security practices, organizations can significantly improve their threat detection capabilities and overall security posture. CTEM leverages this convergence to offer a systematic approach for evaluating and prioritizing risks, enabling organizations to allocate resources more effectively and focus on the most significant threats. This not only enhances security but also optimizes the use of organizational resources. The adoption of CTEM is gaining traction, ranking third among approaches currently embraced by respondents. This suggests a shift toward more strategic, prioritized, and continuous threat management processes, reflecting a critical evolution in the approach to cybersecurity in contemporary network environments.

Key Findings

In this section of the study, we dive into the current state of network and the management technologies used to operate and secure them.

The research behind it was designed to examine monitoring tools in play, the strategic shift from monitoring to observability, challenges created by today's predominantly hybrid infrastructures, and the rapidly rising need to bring together network and security monitoring to address a constantly changing threat landscape. Network and security managers should use these findings to inform their technology choices, work process and practices, and strategy for supporting and securing enterprise networks.

We organized the reporting according to the following key themes based on our findings:

Benefits of a Network Observability Strategy

Those embracing network observability practices were 3.5x more likely to see significant reductions in mean time to detect (MTTD) as a result, as well as other compelling organizational and operational advantages.

Clear Case for Tools Consolidation

Most organizations will readily admit that they have too many tools, and it makes a difference in efficiency. Those with 10 solutions or fewer reported 58% shorter average mean time to repair (MTTR) than those with 11 or more solutions.

Monitoring in Hybrid Cloud Environments

Those operating in hybrid infrastructures are continuing to find strong values in the traditional monitoring techniques of packet capture (97%) and flow data capture (77%).

Converging Observability and Security for Improved Threat Exposure Management

Continuous Threat Exposure Management (CTEM) is emerging as an answer for the 88% of organizations reporting an important or critical need to improve their threat management capabilities.

To Monitor Is Good; To Observe Divine

Monitoring has long been a fundamental practice, but the complexity of today's applications and infrastructure has pushed the industry toward a more advanced set of goals and strategies known as *observability*. While monitoring and observability are related, observability extends beyond it by integrating telemetry, enriching data with context, and facilitating recommended actions.

THE PATH TO NETWORK OBSERVABILITY

In the networking sector, applying observability involves collecting and correlating multiple network data sets; enriching them with business and technical context; and applying advanced analytics to recognize potential issues, enable automated alerting, and trigger corrective actions.

This research revealed key drivers for making the transition to network observability, including improved visibility, reduced MTTR, more comprehensive insights, and a shift toward more predictive and proactive management practices. All these factors should be considered as valid and potentially beneficial outcomes when making the transition to observability.

WHAT IS OBSERVABILITY?

The ability to measure internal states of a system by examining its outputs. For IT, that means bringing together instrumentation, data correlation, AIOps, and incident response.

Network observability provides deep insights into network behavior, performance, and health by collecting, analyzing, and presenting data, enabling administrators to understand and manage the network in real time.

True network observability embraces and leverages all network data sets, including flow data, packet data, and metrics.

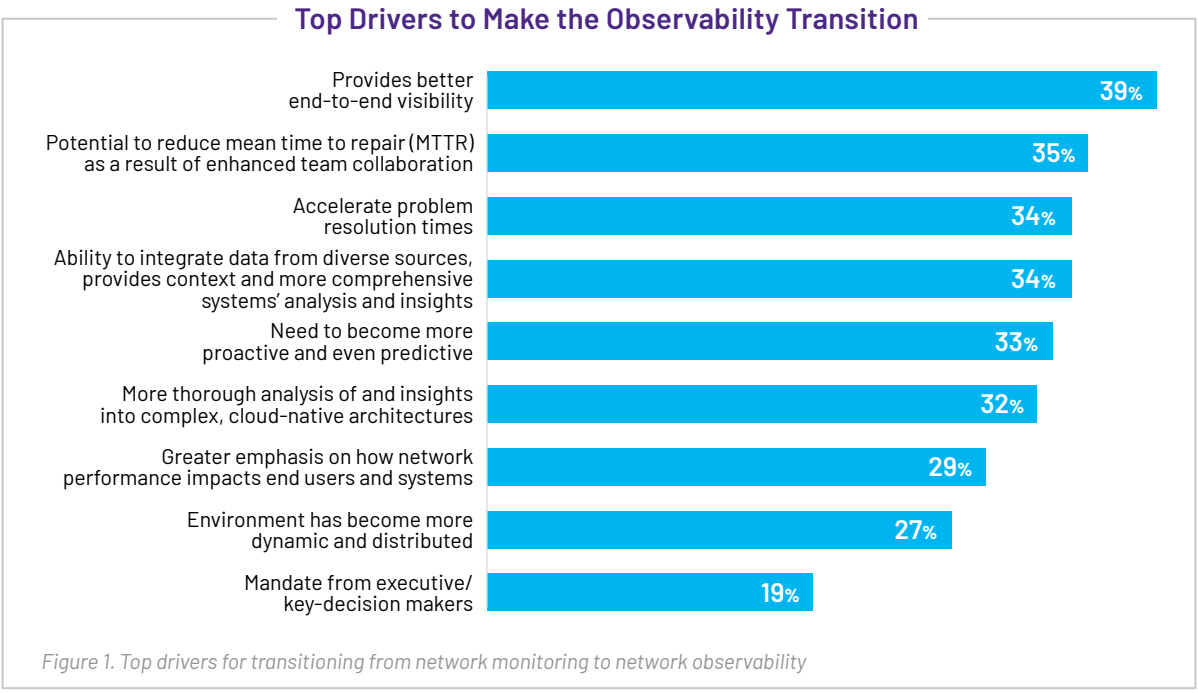


Figure 1. Top drivers for transitioning from network monitoring to network observability

TEAMS ARE MAKING THE MOVE TO NETWORK OBSERVABILITY

To better address the challenges around comprehensive visibility and monitoring of complex environments, as well as analysis of performance, 95% of all organizations are now implementing an actual or de facto transition to more comprehensive network observability strategies.

The monitoring tools market itself is shifting toward observability, led in part by increasingly sophisticated offerings by the vendor community. Adopting these new offerings will help teams make progress, but a clearly articulated strategy is worth developing, as it is key to establishing cross-domain outcome objectives that pay the largest operational dividends.

COMPLEXITY DRIVES THE TRANSITION

Those with 11 or more monitoring solutions in place were 42% more likely to have an articulated strategy for transitioning to network observability.

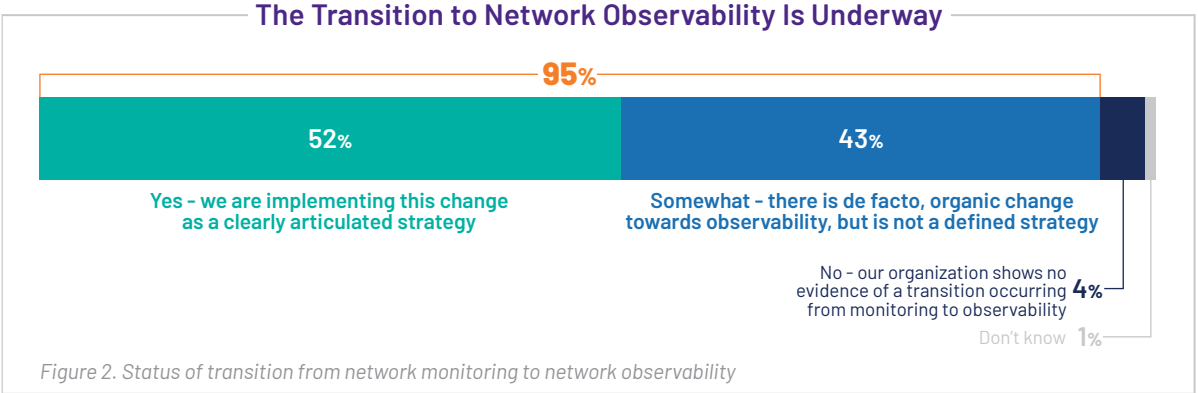


Figure 2. Status of transition from network monitoring to network observability

BONUS PAYOFF: THE SURPRISE BENEFITS OF OBSERVABILITY

While the move to observability brings advantages in terms of tackling technical and organizational challenges around network monitoring, there can be direct benefits as well in other operational areas.

78% of respondents saw significant improvements in the ability to secure their environments and boosting productivity with observability

Among those implementing observability, 78% saw significant improvements in securing environments, boosting product team efficiency, and ensuring compliance. Security advantages stem from increased visibility and asset discoverability, which enhance the organization's posture by identifying potential threats and vulnerabilities more effectively. Additionally, observability frees up product and service teams to innovate faster and advance other critical initiatives, resulting in more efficient operations. These unanticipated benefits reflect the leverage that network observability can provide for making measurable progress toward higher-level business goals, such as improving overall security and achieving better top-line results.

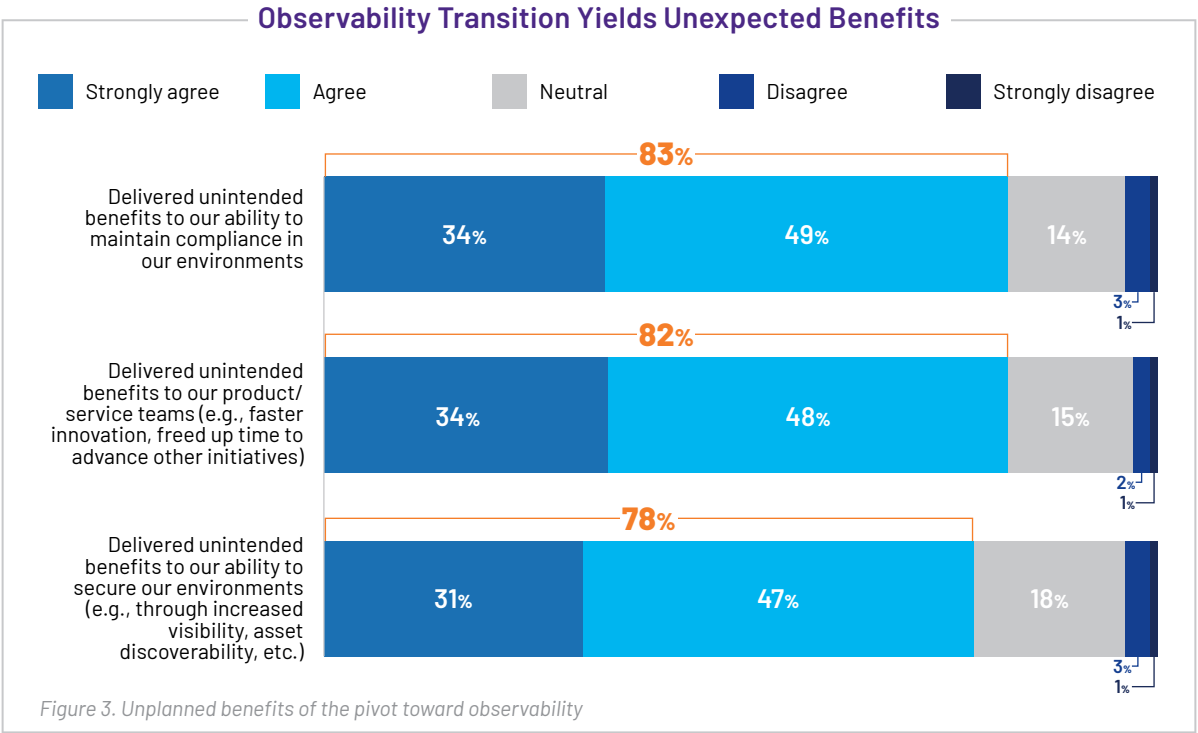


Figure 3. Unplanned benefits of the pivot toward observability

ENHANCING OPERATIONAL EFFICIENCY THROUGH NETWORK OBSERVABILITY

Organizations that have a clearly articulated network observability strategy are 3.5 times more likely to experience a substantial reduction in their MTTD rates over the past year, as compared with those without such a strategy.

This is further evidence that observability not only enhances cross-functional operations but also directly improves operational efficiency. Substantial reduction of MTTD translates into faster incident response times, less downtime, and overall improved business continuity.

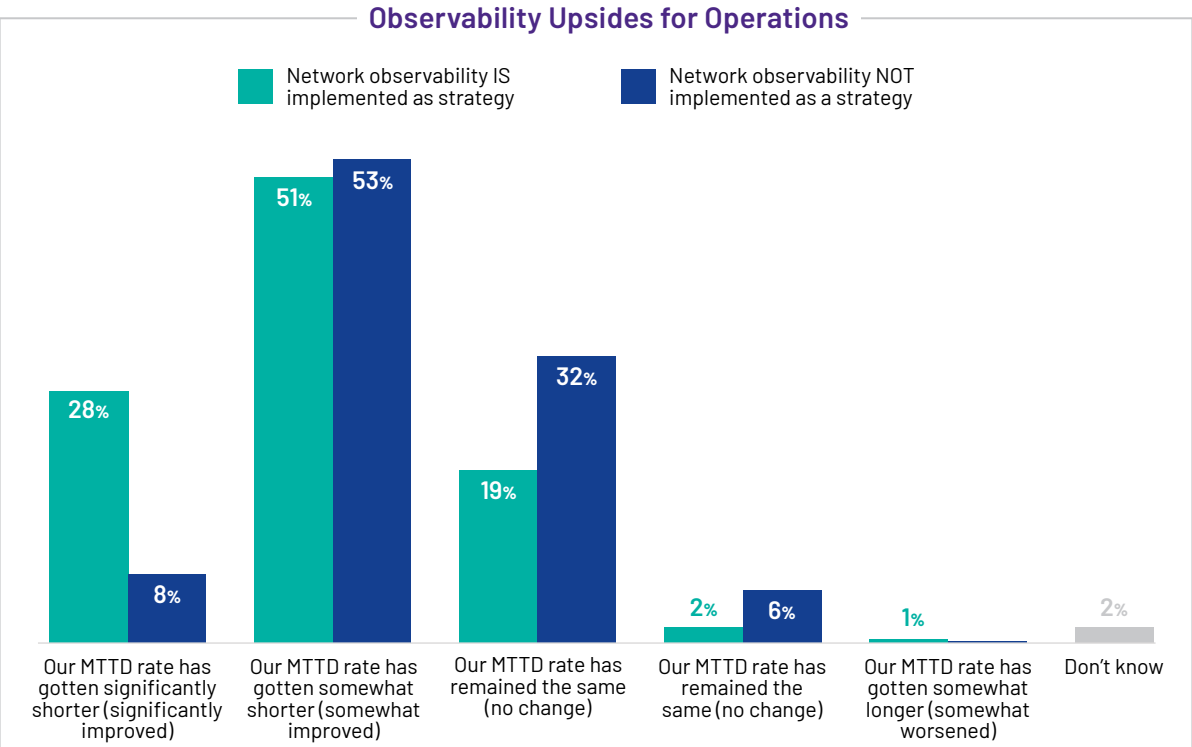
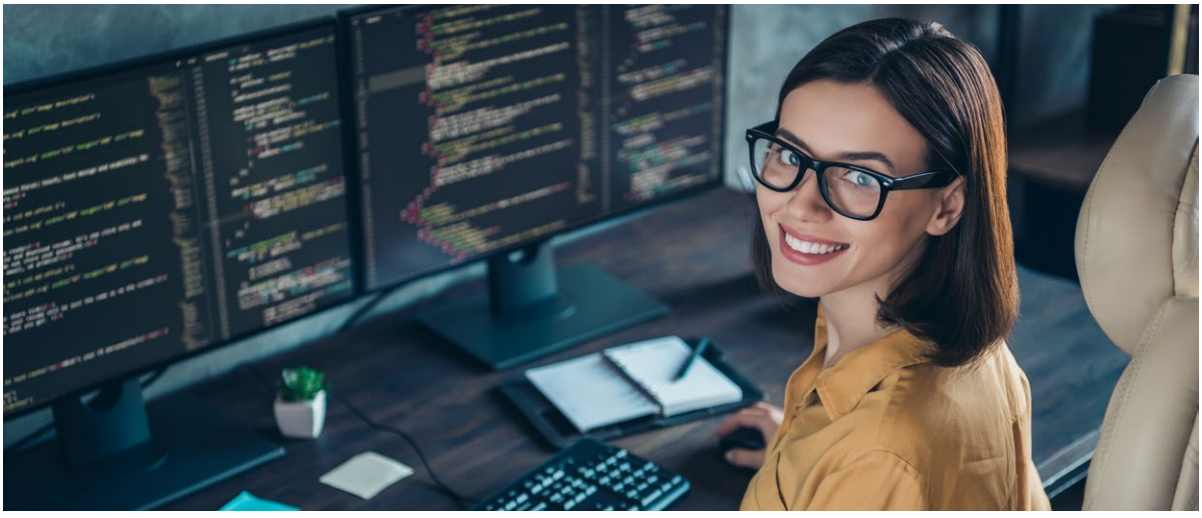


Figure 4. Changes in ability to detect disruptive incidents in the past year. Grouped by observability strategy.

These results underscore that observability is a critical component in modern network management strategies and can deliver multiple positive outcomes to businesses, while supporting the push toward more predictive and proactive operational practices.

Organizations with an observability strategy were 3.5x more likely to see a significant reduction in MTTD.



Trimming the Monitoring Toolchest: Why Less Is More

It's no secret that enterprise organizations have a lot of monitoring tools. Some have so many they need dedicated roles just to keep up with tool sourcing and maintenance. It's necessary to have at least some mix of tools to adequately cover the many inter-related technologies that comprise today's IT infrastructure. But having too many tools can lead to serious inefficiencies in daily work process, as time and resources must be designated toward deciding which tool to use or which data set to believe.

THE ONGOING CHALLENGES OF HIGH TOOL COUNTS

How many monitoring tools are necessary, and how many is too many? This study found that 65% of respondents are using 7 or more monitoring tools, with 38% using 11 or more and the overall average at nearly 10 monitoring tools.

High tool counts can result from a mix of vendor-specific and multi-vendor suppliers, inorganic organizational growth, or having multiple overlapping, siloed business unit teams. Having a lot of monitoring tools can have benefits, such as greater detailed visibility across distributed, heterogeneous infrastructures, but it can also bring disadvantages, such as data and workflow complexity and a higher total cost of ownership.

Having 11 or more monitoring tools collecting data across their networks is the reality for a large slice of study respondents, and, as will become clear in this study, there is ample reason to focus on how to consolidate.

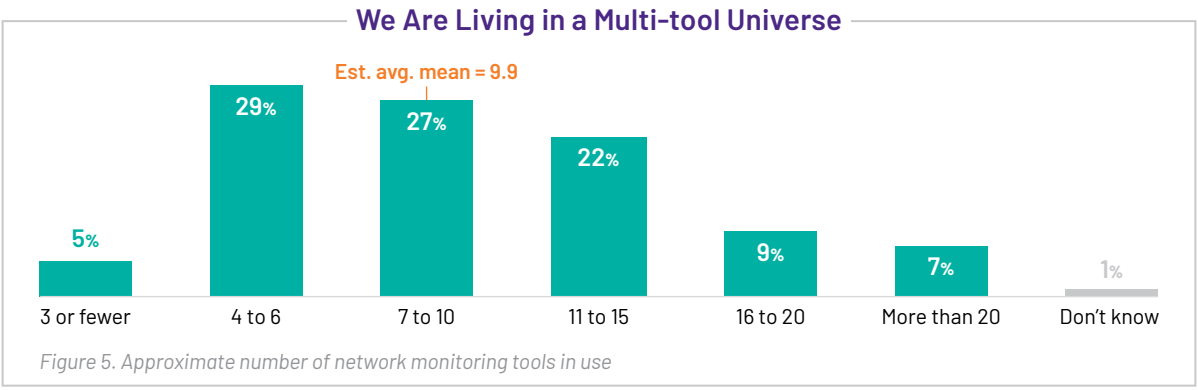


Figure 5. Approximate number of network monitoring tools in use

WHICH TOOLS ARE IN USE?

What drives monitoring tool counts? First off, there are many special types and uses of monitoring tools, commonly divided by infrastructure layer or functional objectives.

Of the seven major monitoring tool categories, all were in use by the vast majority of respondents. 82% reported using network performance monitoring (NPM), and 78% reported using security event and information management (SIEM) tools. Even the least common tools, asset/inventory management (58%) and log management (56%), are more likely in use than not.

Given the findings that the average organization has 10 solutions in place, most organizations have more than one solution in place within at least a few of these categories.

While all the tool types represented here are provided by specialized vendors focused on an individual type of monitoring, there are opportunities for consolidation: Vendors can provide more than one type of security tool within a single solution or tightly integrated suite of products that effectively delivers a single solution.

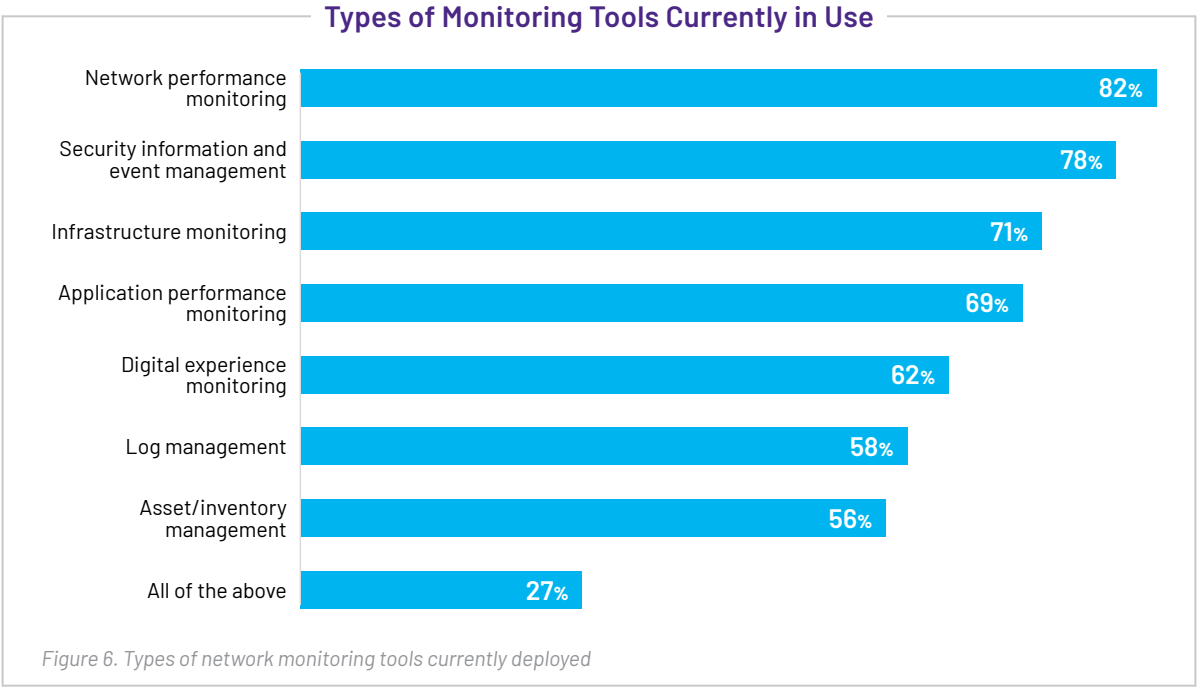


Figure 6. Types of network monitoring tools currently deployed

CURRENT MONITORING CHALLENGES

Organizations face a number of challenges with their monitoring and management strategies, some of which are aggravated and some of which are mitigated by too many tools. While having more tools may improve end-to-end visibility and supports remote workers, it becomes a serious liability for integrating new technologies and services. And those with more than 10 tools were 64% more likely to struggle with comprehensive or automated analysis, such as machine learning (ML) and AIOps.

On balance, the negatives of high tool count outweigh the benefits for most organizations, so reducing tool count must be considered a priority.

TOP 5 CHALLENGES OF MONITORING NETWORK PERFORMANCE

- Complexity in network architecture.
- Difficulty managing the amounts of data flowing through networks.
- Increased adoption of SaaS applications.
- Problems identifying root cause.
- Managing too many disparate performance reports.

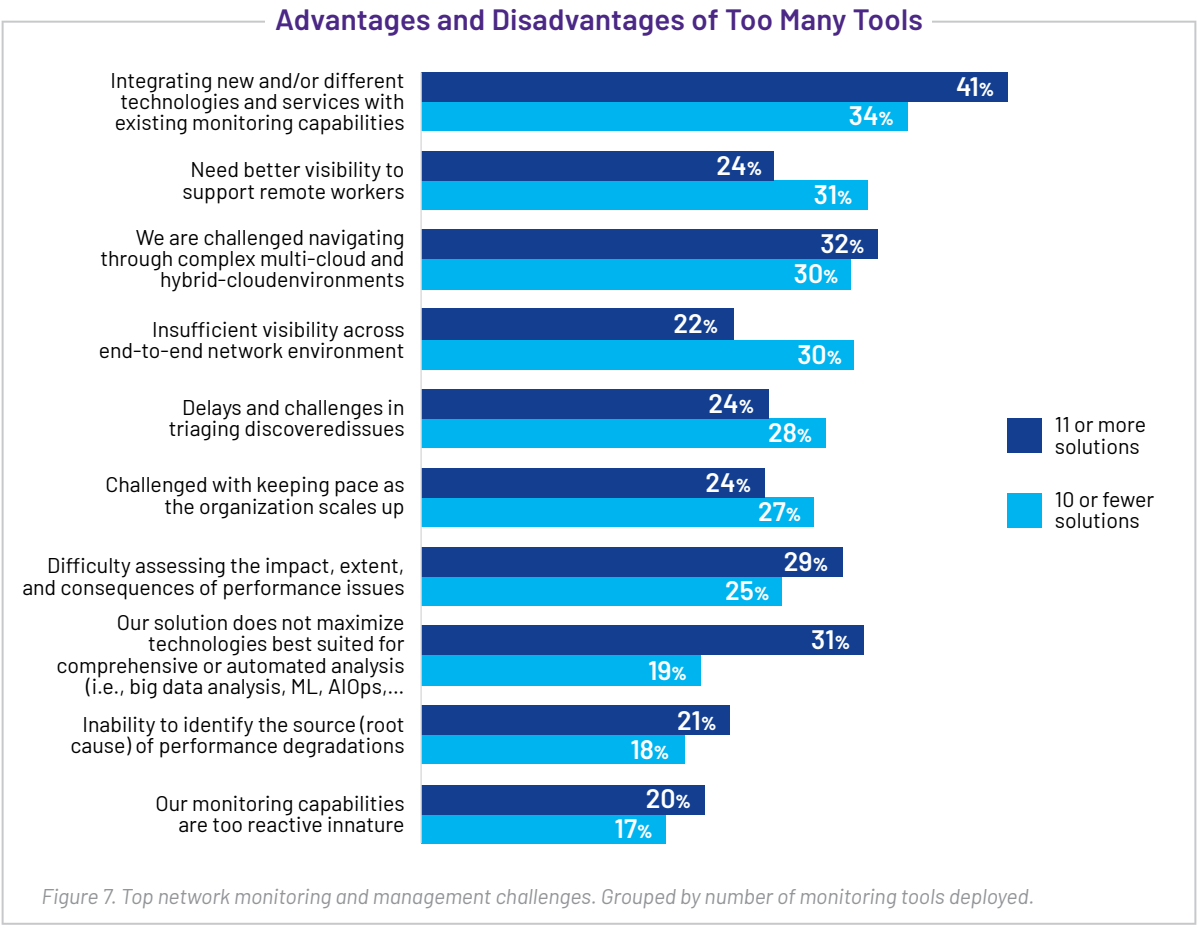


Figure 7. Top network monitoring and management challenges. Grouped by number of monitoring tools deployed.

THE DRIVE TO CONSOLIDATE

Furthering the case for consolidation, there is also direct and compelling evidence related to workflow efficiency. Respondents with 10 or fewer tools saw significantly shorter MTTR than their peers with 11 or more tools, which dropped from an average of 13.7 hours down to an average of 5.7 hours—a nearly 60% reduction!

Consolidation reduces challenges and has direct operational benefits, and a majority of survey respondents are actively seeking to do just that. Organizations should aim to reduce tool count within each functional area or domain and span multiple functional areas whenever and wherever possible.

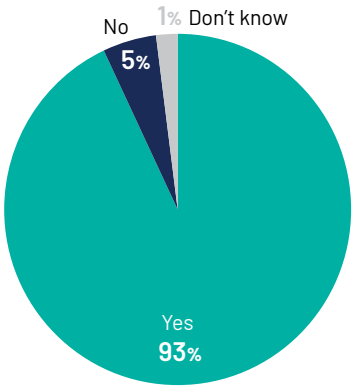


Figure 8. Active intent to consolidate network monitoring and observability vendor tools.

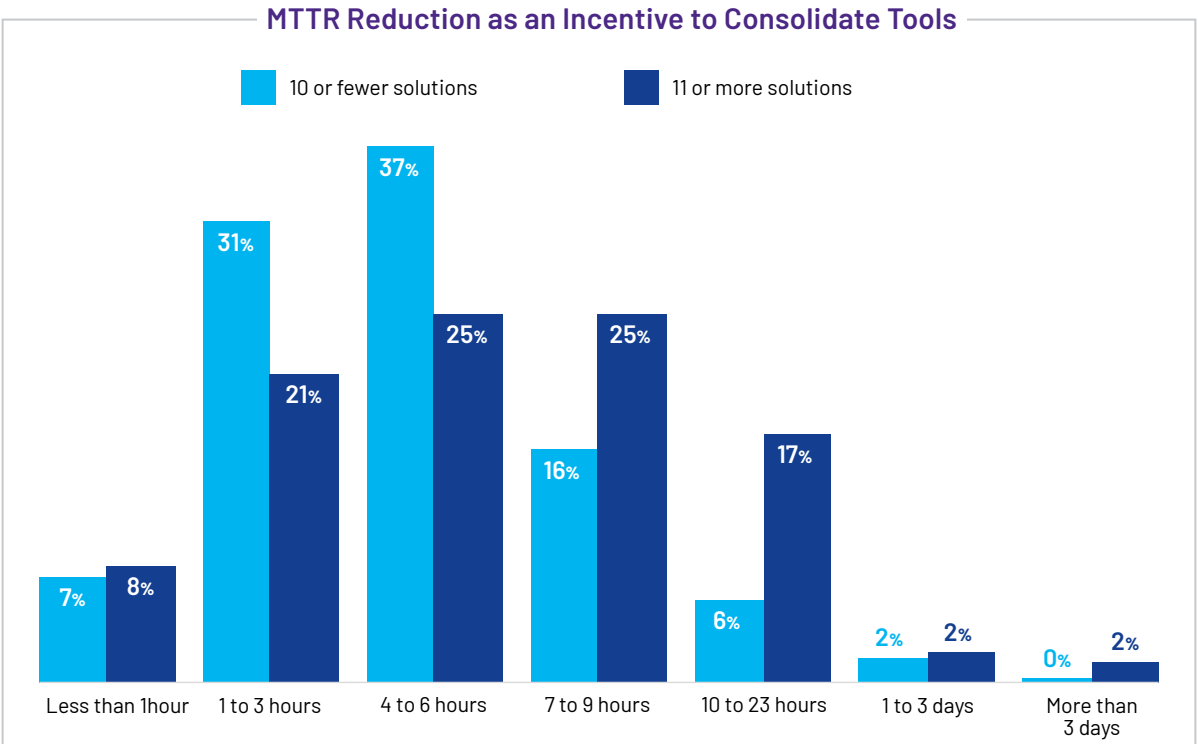


Figure 9. Average MTTR for service-impacting incidents. Grouped by number of monitoring tools deployed.

Vaulting the Hybrid Hurdles

To achieve the operational benefits of observability, it is essential to find an approach that covers all network environments—traditional LAN/WAN as well as cloud. Today's organizations operate in a hybrid, multi-cloud reality, which creates barriers to success that can be both technical and organizational. These barriers must be addressed to capture the promises and rewards of an observability strategy.

ADAPTING TO THE HYBRID REALITY

Hybrid, multi-cloud infrastructures are the new normal, and network managers must find ways to adapt to them. The challenge is to assess whether traditional monitoring technologies are still applicable and how they can be modified to maintain thorough visibility and insights across these complex environments.

According to survey results, two fundamental network monitoring techniques—packet capture and flow data capture—continue to be critical for managing hybrid cloud infrastructures. However, there is a consensus that these and other methods could be further optimized to enhance their effectiveness. The following table highlights the specific data capture methods that need improvement in a hybrid setting.

DATA CAPTURE METHODS THAT NEED IMPROVEMENT IN HYBRID SETTINGS

- NetFlow/IPFIX/Flow logs (cited by 74%)
- Traces (70%)
- Packet data (69%)
- Events (67%)
- Performance/usage metrics (67%)
- Device logs (65%)

Need for Packet Capture and Flow Data Capture Persists for Managing Cloud Environments

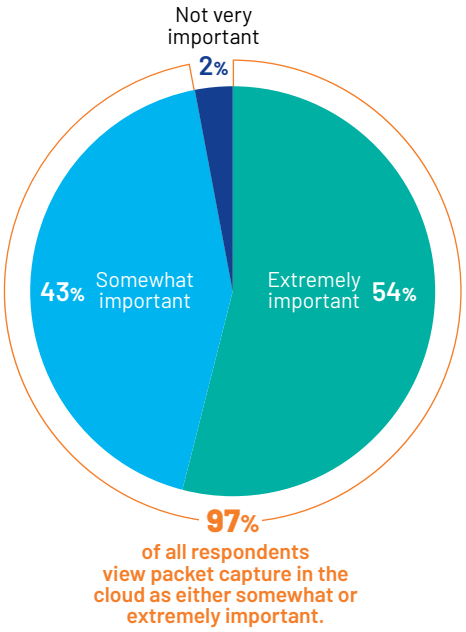


Figure 10. Importance of packet capture in the cloud

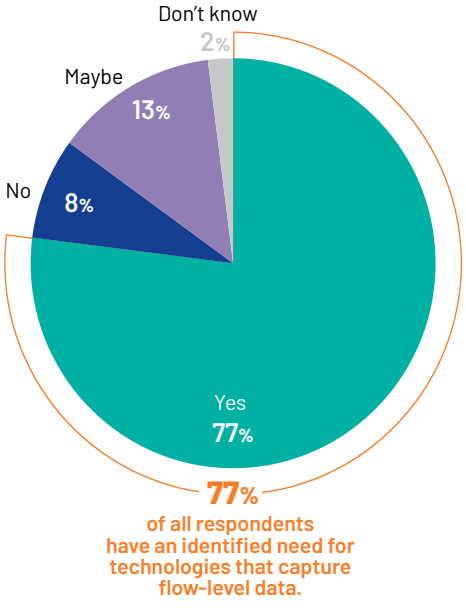


Figure 11. Flow data use cases identified for cloud

THE MANTLE OF RESPONSIBILITY FOR APP PERFORMANCE IN THE CLOUD

Surprisingly, when it comes to responsibility for monitoring and managing performance of applications residing in the cloud, NetOps is the least likely to be cited, and only 20% indicated that there were collaborative approaches in play.

Interestingly, **organizations with 11 or more monitoring solutions were 26% more likely than those with 10 or fewer solutions to rely on CSPs or cloud-focused architects for monitoring and managing performance in the cloud**. This could be because they have more cloud-specific monitoring tools. It could also reveal greater confusion and data overload for this group, leading teams to throw issues to the CSP and cloud teams for lack of a better strategy.

For network managers, this is both a challenge and an opportunity. Network data is powerful for reducing MTTD and MTTR, and it needs to be shared with other teams that might end up holding the bag when application performance issues arise. But networking pros might not be front and center at the time. Observability strategies that drive cross-team collaboration can help open the necessary communications channels to leverage network data.

Cloud Providers and Ops Mostly Held Responsible for App Performance in the Cloud

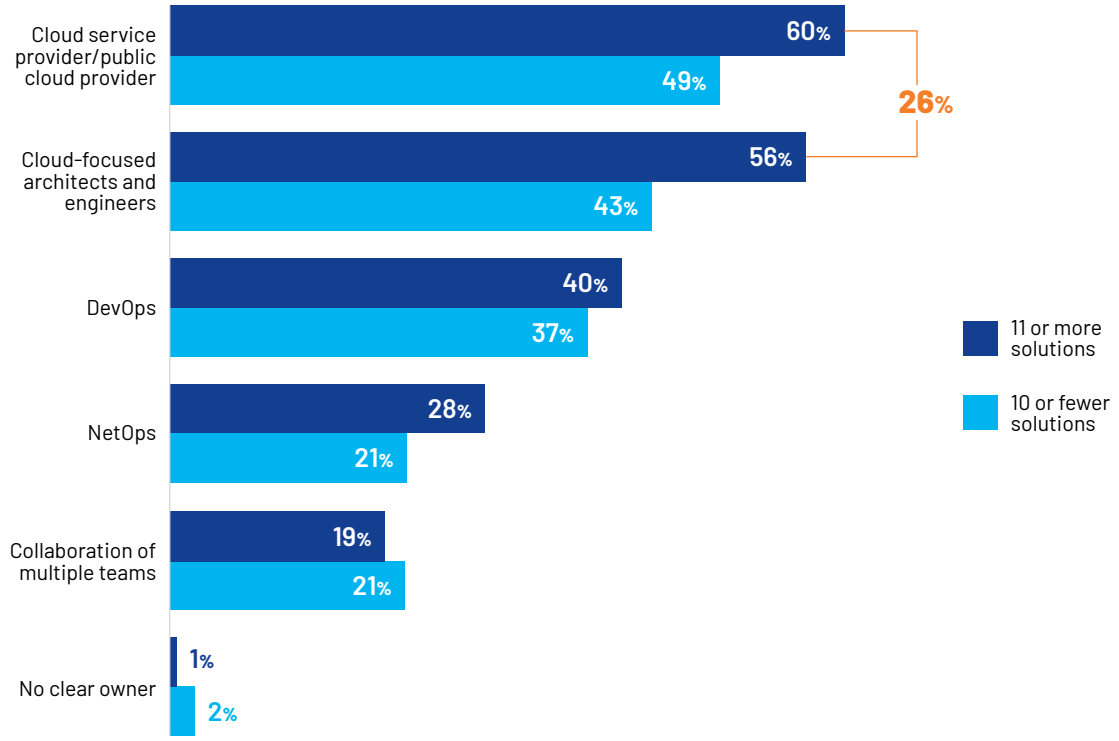
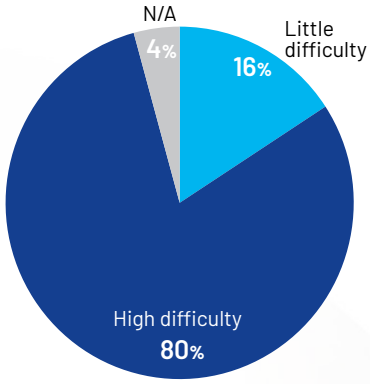


Figure 12. Groups responsible for monitoring and managing performance of applications in the cloud. Grouped by number of monitoring tools deployed.

THE ONGOING VISIBILITY CHALLENGE

Despite steady progress, the public cloud (IaaS) remains high on the list of environments where significant visibility challenges persist. While public cloud isn't unique in this regard, it frequently tops the list of problem areas. Challenges in achieving desired levels of visibility span virtually all networking realms, with 80% of respondents reporting high difficulty in at least one network environment.



Highest reported level of difficulty in visibility across all domains

The benefits of observability compound as data sets become more complete. For network managers, remaining diligent and seeking means to drive visibility into all their network environments is essential. This proactive approach not only mitigates risks but also optimizes performance and efficiency, leading to improved overall network health and business outcomes. Enhanced visibility enables quicker detection and resolution of issues, more effective resource allocation, and better compliance with security standards, in due course contributing to the organization's strategic goals.

Visibility Remains a Challenge in Many Environments

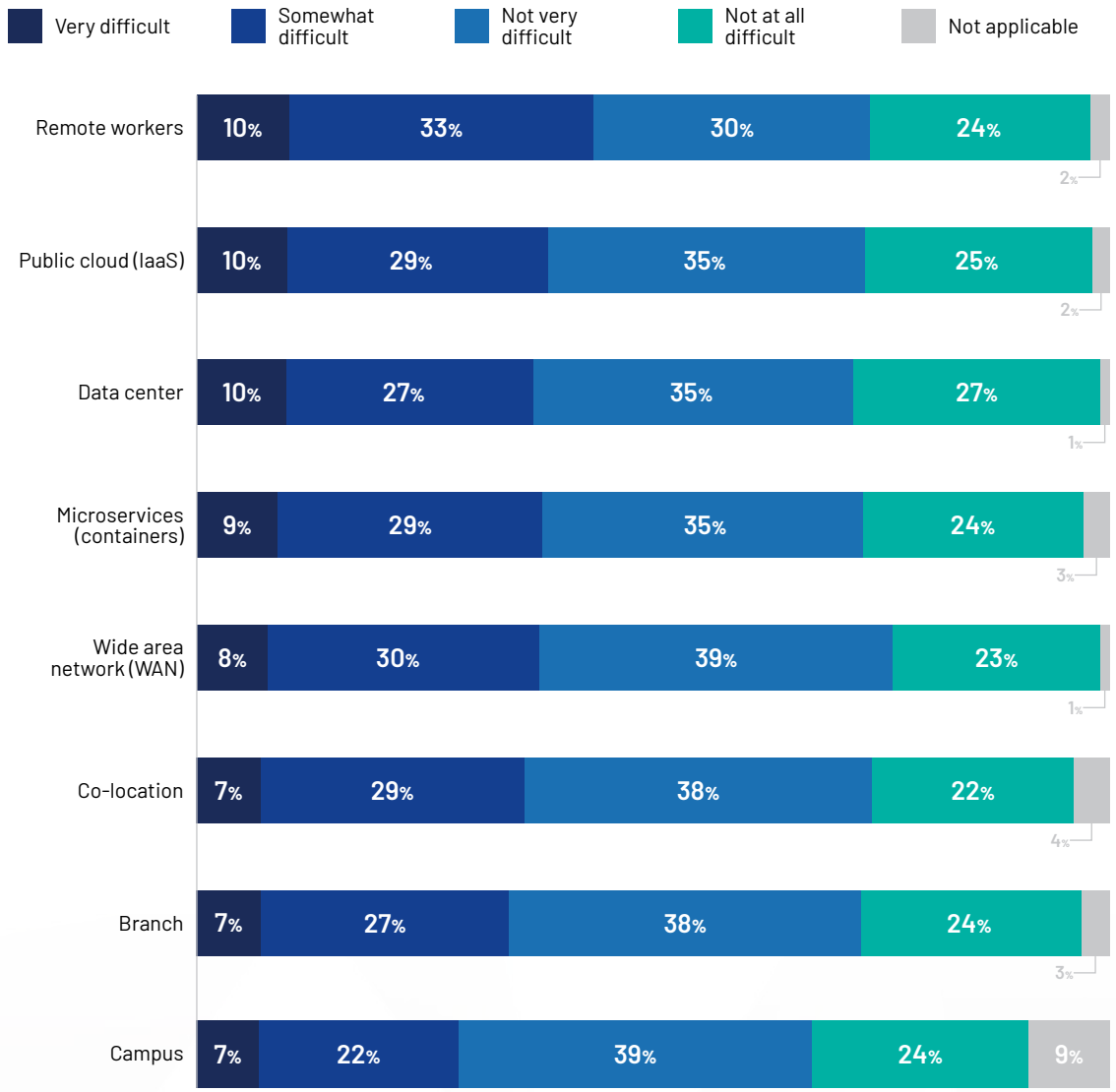


Figure 13. Difficulty achieving desired network visibility across environments

Integrating Threat Exposure and Attack Surface Management Across Hybrid Environments

Transitioning to an observability approach puts organizations in a better position to manage security, in part due to the integration of monitoring data sets and the sharing of insights. Perhaps the most important focal point for such convergence today is better understanding and control of attack surfaces. CTEM has emerged and promises to improve security posture within a constantly changing threat environment. CTEM, as it turns out, relies on many of the same processes and principles as observability, such as integrating multiple data sets, adding context, and applying analytics to identify concerns and trigger responsive actions.

PUTTING SECURITY AND NETWORKING INCIDENTS IN CONTEXT

Good collaboration among teams goes beyond just networking and security. In the end, all teams must find ways to work together because when something goes wrong, the ultimate root cause can literally be anywhere.

With that said, security incidents were cited most often as the incidents organizations' IT teams most frequently work on, with 51% of respondents identifying these as their primary focus. Network infrastructure incidents followed closely at 44%.These statistics highlight the critical areas where IT teams are dedicating their efforts. Organizations need to focus on these two areas to achieve the greatest returns on integrating and advancing monitoring and observability investments, enhancing their ability to detect and respond to threats to minimize downtime and protecting critical assets.

Additionally, organizations should seek a collaborative approach across teams for addressing security and network incidents, fostering more cohesive and efficient incident management which can quickly translate into improved operational resilience and business continuity.

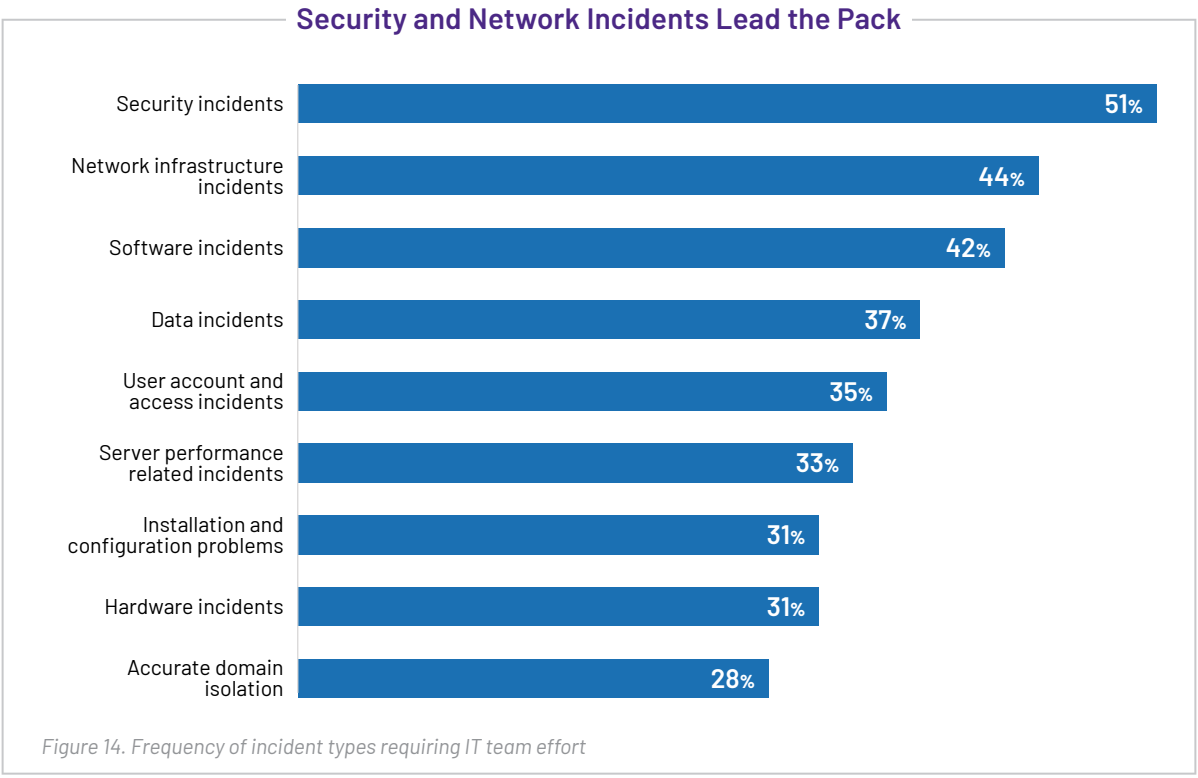


Figure 14. Frequency of incident types requiring IT team effort

THE CONVERGENCE OF OBSERVABILITY AND SECURITY

There have long been close relations between networking and security teams in most organizations. The data sets are similar, though focused on different analyses. When outages, degradations, or traffic anomalies occur, both teams are alerted and generally check in with each other to get an alternative viewpoint.

The industry has been maturing in this regard and is moving broadly toward converging observability and security, recognizing that observability strategies can support security analyses in parallel with operational assessments.

Respondents confirmed the value of network observability, noting improvements in every aspect of network-security collaboration, especially in hybrid, multi-cloud environments. Specifically, 68% of respondents with an observability strategy in place reported enhanced workflows for collaboration processes. Interestingly, even among those without a formal observability strategy, 59% acknowledged improvements in collaboration workflows. Furthermore, 63% of respondents with an observability strategy stated that it increased the frequency of team meetings and collaboration on shared objectives compared to 12 months ago. Additionally, 62% of these respondents highlighted that observability benefits align the tools used across different teams.

The improved tools alignment resulting from observability parallels other findings in this study, where reduction in monitoring tool counts equated to better efficiency and quicker incident response.

TOP FIVE CYBERSECURITY CHALLENGES TODAY, PER PARTICIPANTS IN THIS RESEARCH

- Increased attack surface due to rising multi-cloud services and remote workers.
- Regulatory compliance taking precedence over best practice implementation.
- Cybersecurity teams are too focused on incidents, impeding overall posture improvements.
- Managing the volume of security alerts.
- Insufficient vulnerability assessment capabilities.

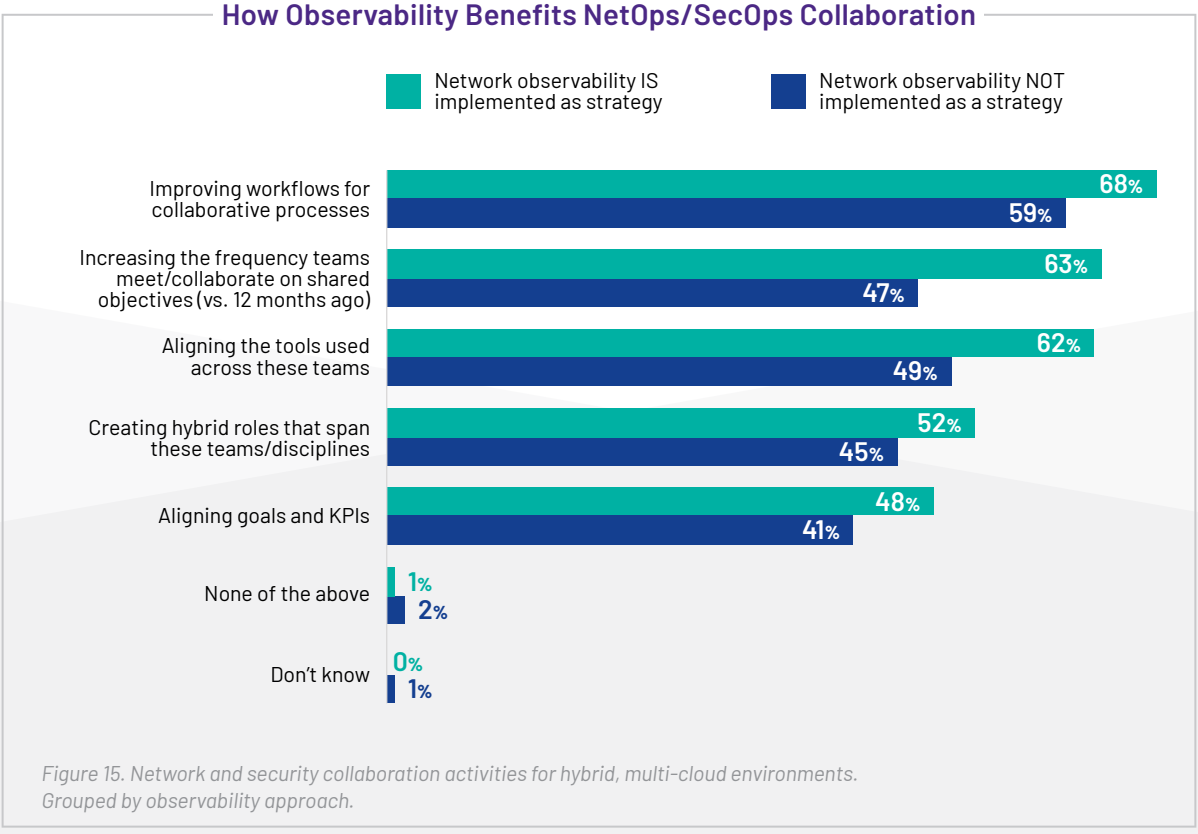


Figure 15. Network and security collaboration activities for hybrid, multi-cloud environments. Grouped by observability approach.

THREAT EXPOSURE MANAGEMENT COMES INTO FOCUS

Securing IT is becoming increasingly complex. Keeping up with a constantly changing landscape of threats, while also managing more complex and distributed architectures, such as hybrid cloud, is a monumental task.

With 88% of all respondents identifying threat exposure management as either important or critical, it is not surprising that **87% anticipate an increase in technology spending to address concerns**.

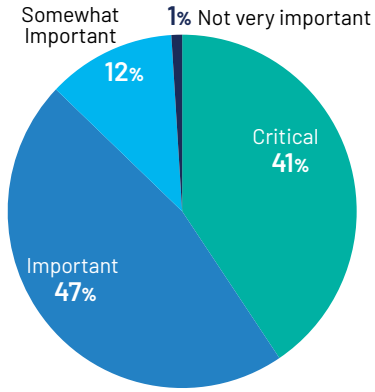


Figure 16. Importance of threat exposure management

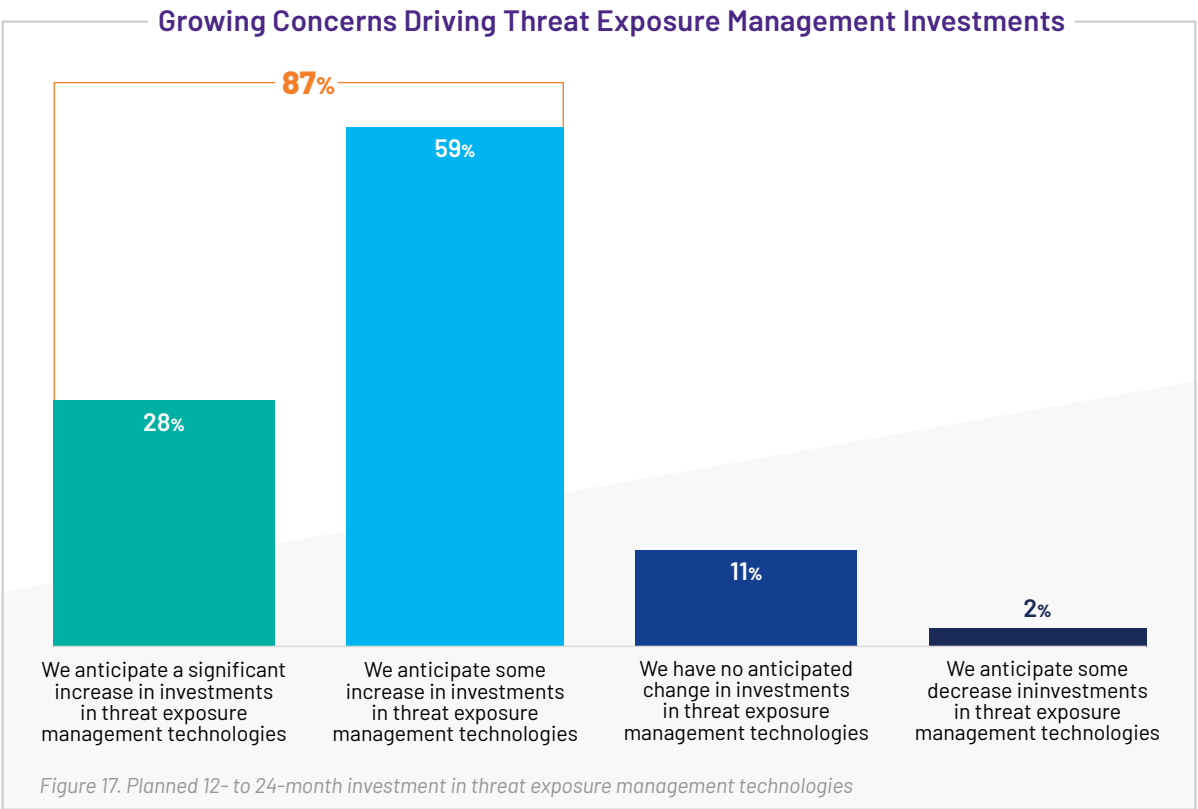


Figure 17. Planned 12- to 24-month investment in threat exposure management technologies

The most commonly identified specific challenge to threat exposure management and attack surface reduction was

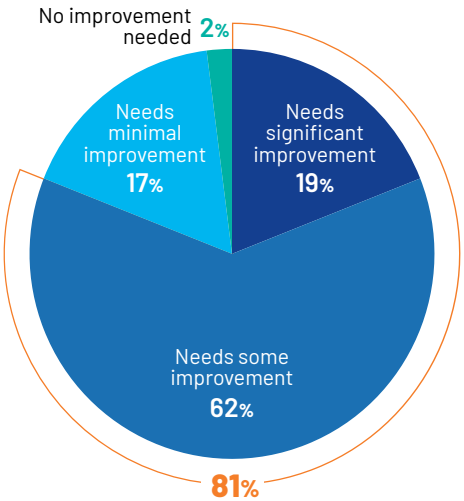
Keeping pace with the volume of evolving bad actors and threats.

SIGNIFICANT WORK REMAINS TO BETTER MANAGE THREAT EXPOSURE

Given the dynamic nature of the threat landscape, the vast majority of respondents (81%) felt that some or significant improvement is needed in their organization's ability to mitigate threats and manage attack surfaces.

Comfort with current security measures plays a big role here. Respondents who feel that security risks were outpacing security measures, were even more compelled to voice a need for some or significant improvements (94%).

As Threats Grow in Sophistication and Frequency, Organizations Recognize the Need for Constant Vigilance



81%

of all respondents felt that some or significant improvement is needed in their organization's ability to mitigate threats and manage attack surfaces

Figure 18. Self-rating of threat mitigation and attack surface management sufficiency over the next 12 months

IMPROVEMENT NEEDS TIED TO CLOUD DATA CAPTURE

Those prioritizing improvements in threat mitigation and attack surface management were much more likely to prioritize network data capture in the cloud, being:

- **2.7x more likely** to consider cloud packet capture as extremely important.
- **7.3x more likely** to have identified a need for cloud flow data capture.

THE CASE FOR CTEM

There are a litany of tools and practices commonly in use to manage threats in today's organizations. The challenge with this is scale. Keeping up with multiple tools, technologies, and practices is daunting.

CTEM takes a systematic approach to evaluating and prioritizing risks, leveraging the convergence of security and observability to improve awareness and deliver more definitive analyses. It's not possible to address every threat, but CTEM helps organizations prioritize and assign resources where they matter the most for the business.

TOP APPROACHES BY ORGANIZATION SIZE

- Large enterprises: Patching, vulnerability assessment.
- Small to medium-sized enterprises: Network segmentation, CTEM.
- Most consistent across size groups: Patching, CTEM.

Our respondents are embracing CTEM, ranking it third on a list of approaches being taken, with 39% of organizations implementing a CTEM program to address threat exposure management. This approach is one of the most consistent responses across organization sizes.

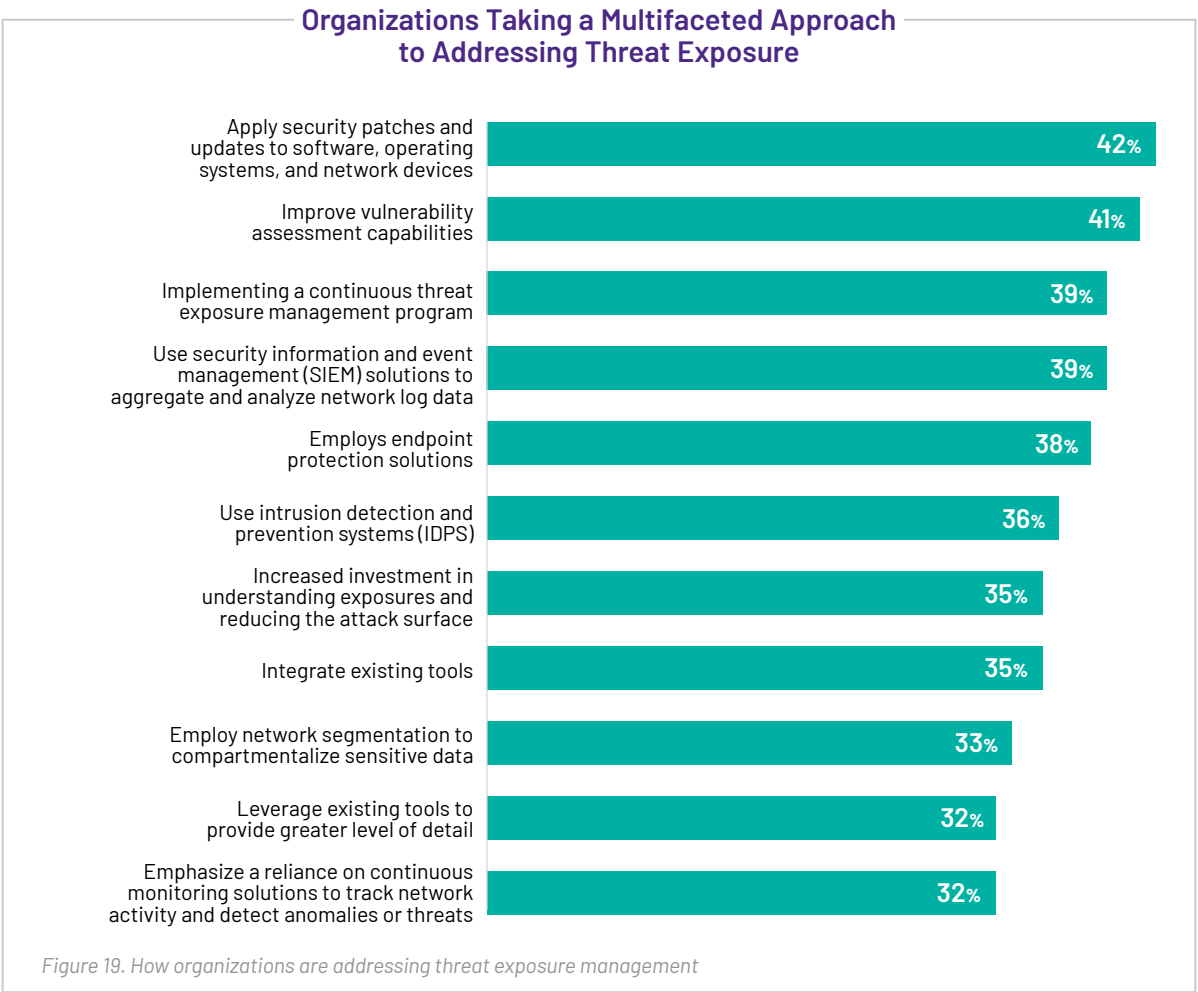


Figure 19. How organizations are addressing threat exposure management

What about other approaches versus CTEM? The top approach cited, by a slim margin, was applying patches and updates to software, operating systems, and network devices. Patching is important, but the process can be time-consuming and reactive, often taking weeks or months to complete. In contrast, CTEM offers a more dynamic and ongoing solution, reducing the window of vulnerability and enhancing overall security posture.

The second most common response was to improve vulnerability assessment capabilities. While also important, traditional vulnerability assessments can fall short by providing only periodic snapshots of an organization's security landscape. CTEM, on the other hand, offers continuous and real-time visibility into threats, enabling more timely and effective responses.

By adopting CTEM, organizations can continuously identify, prioritize, and mitigate vulnerabilities, providing a proactive stance against potential threats. Integrating CTEM with observability strategies ensures that organizations can maintain a comprehensive and up-to-date understanding of their security environment, ultimately leading to more robust and resilient defense mechanisms.

Conclusion

As discovered by VIAVI and Enterprise Strategy Group in 2024, the state of the network is ever more vital to business success, even as it is continuously stretched, evolved, clouded, and threatened. This research indicates that there are strong reasons for pursuing a number of objectives and changes to tool strategies and best practices:

1. **Consolidation of monitoring solutions is a worthwhile effort.** Benefits include more efficient operations, such as a nearly 60% reduction in average MTTR, and improved ability to adapt and integrate into automated analytics systems, which will become even more predominant with the steady influx of AI just ahead, in the immediate future.
2. **Observability strategies throw off multiple benefits.** Besides putting teams on a broader footing for managing complex environments, observability also delivers improved cross-team collaboration and significant operational efficiencies, such as a 3.5x increase in significantly shortened MTTD.
3. **Network monitoring in hybrid environments is still a work in progress.** However, there are some emerging truths, such as the recognition that traditional packet-based and flow-based data sets remain essential for both operational and security monitoring of the cloud.
4. **The convergence of observability and security could not be more necessary than right now.** With attack surfaces growing quickly and the threat landscape always changing, 81% of respondents indicated that improvement in threat mitigation and attack surface management is needed. Bringing network observability data sets together in the service of CTEM will help to turn the tide.

Appendix:

Research Methodology & Respondent Demographics

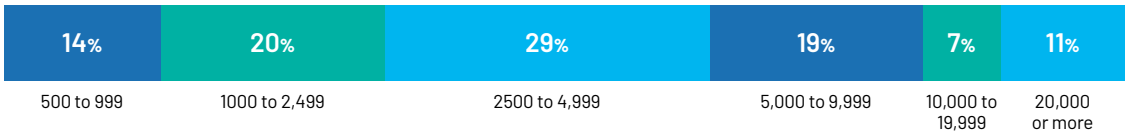
This study—fielded between February 5, 2024, and March 6, 2024—included IT leaders influential in the purchase process for network infrastructure and services at their organization.

Respondents in the study came from organizations designated as Small (500-2,499 employees), Medium (2,500 to 9,999 employees), and Large (10,000+ employees) enterprise organizations. These organizations were based in North America (U.S. and Canada), Western Europe (France, Germany, U.K.), Latin America (Brazil, Mexico) and APAC (ANZ, Singapore).

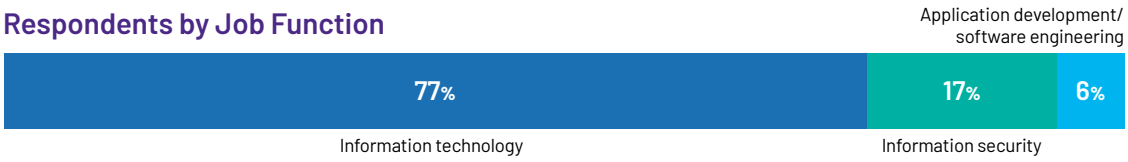
After applying data quality control best practices and screening the remaining completed responses (on several criteria) for data integrity, a final sample of 754 respondents remained. All respondents were provided an incentive to complete the survey in the form of cash awards and/or cash equivalents.

Respondents by Region

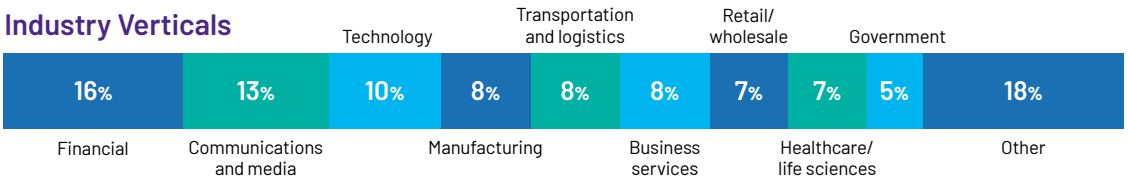
Respondents by Number of Employees



Respondents by Job Function



Industry Verticals



Survey confidence level is 95% with a margin of error of +/-3.5%
Note: Totals in figures and tables throughout this report may not add up to 100% due to rounding.

Areas of IT Technology, Management, and Involvement

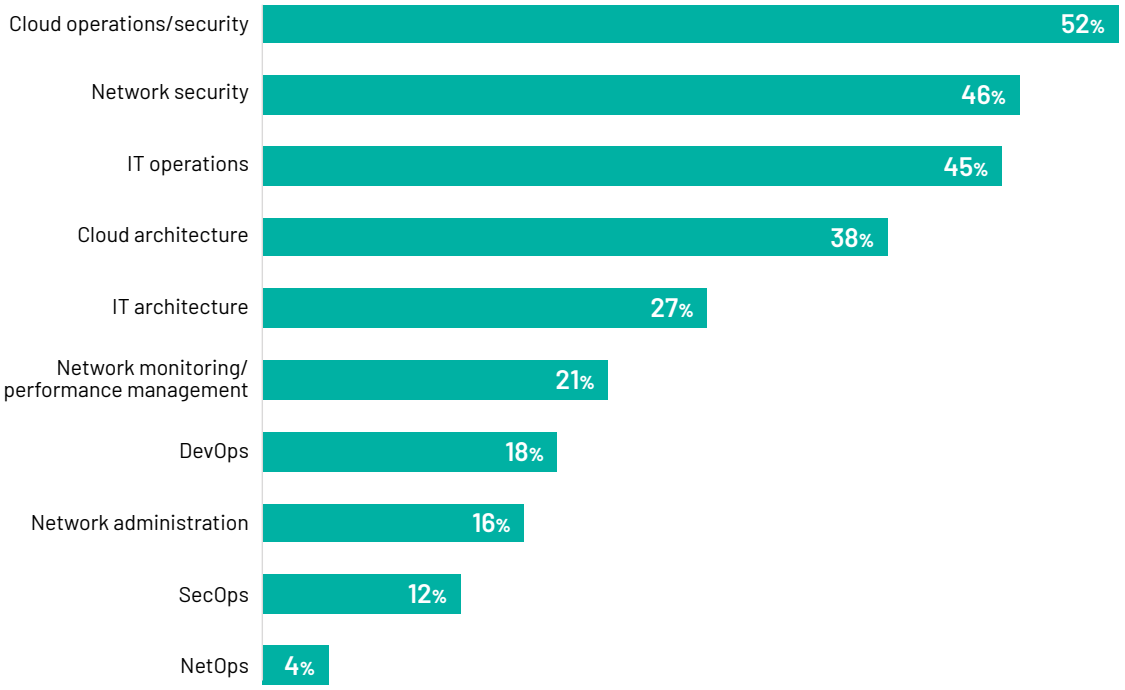


Figure 20. Respondent self-assessments of those technology management areas they were most likely to spend a significant amount of time working on.

Respondents by Job Title/Level

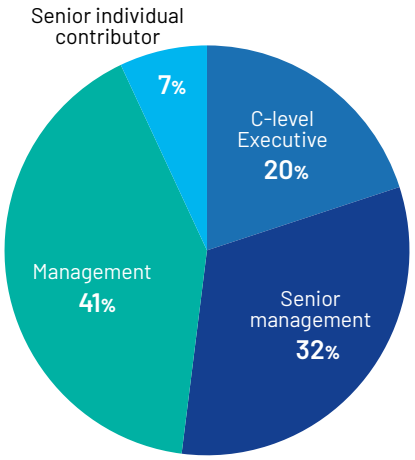


Figure 21. Respondents' level of seniority, classified via job level and/or title.

Respondents by Familiarity With IT, Cybersecurity, and Network Operations

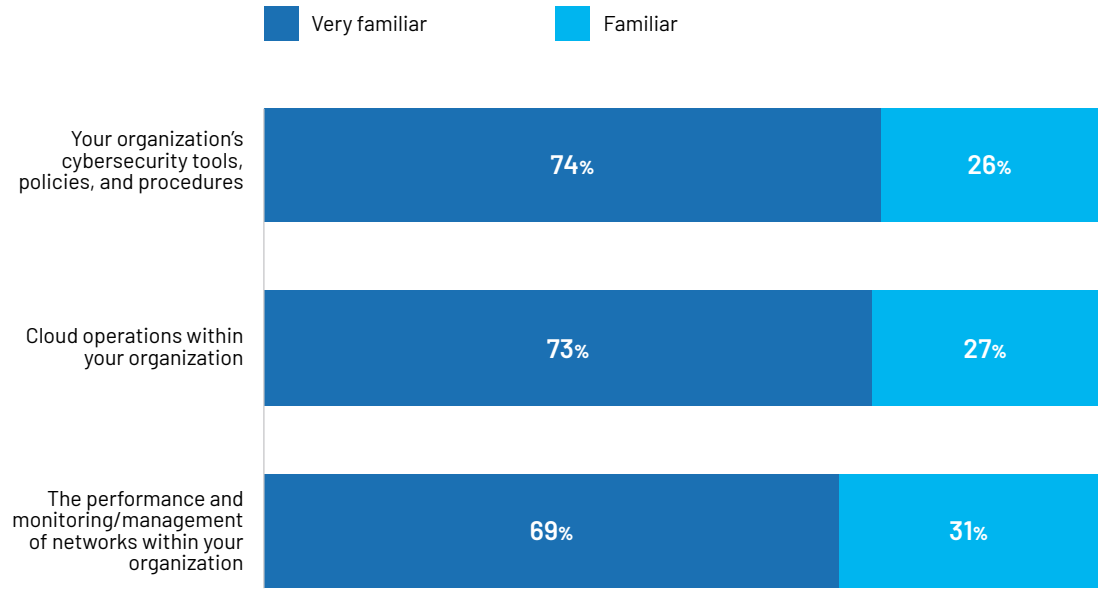


Figure 22. Respondent self-assessments of familiarity with cybersecurity, cloud operations, and performance monitoring/network management.

Respondents by Time Spent Managing Network and Cloud Infrastructure

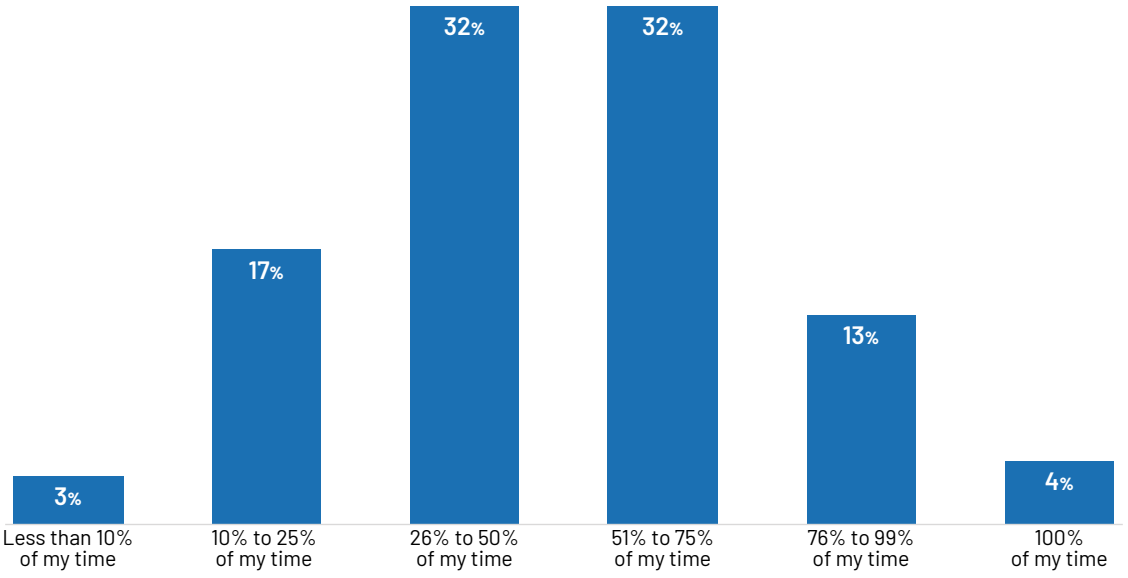


Figure 23. Respondent self-assessments of specific time dedicated to monitoring, managing, troubleshooting, or otherwise ensuring the performance and availability of their organization's network and cloud infrastructure.

Respondents by Age

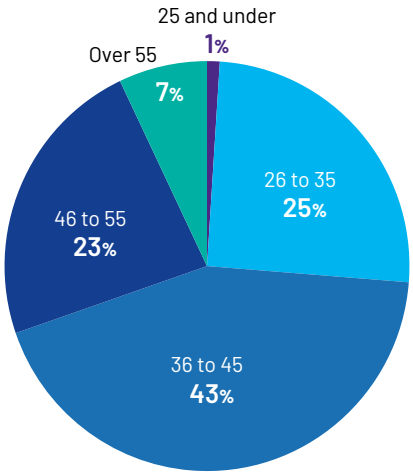


Figure 24. Distribution of all participating survey respondents' ages.

Respondents by Annual Revenue

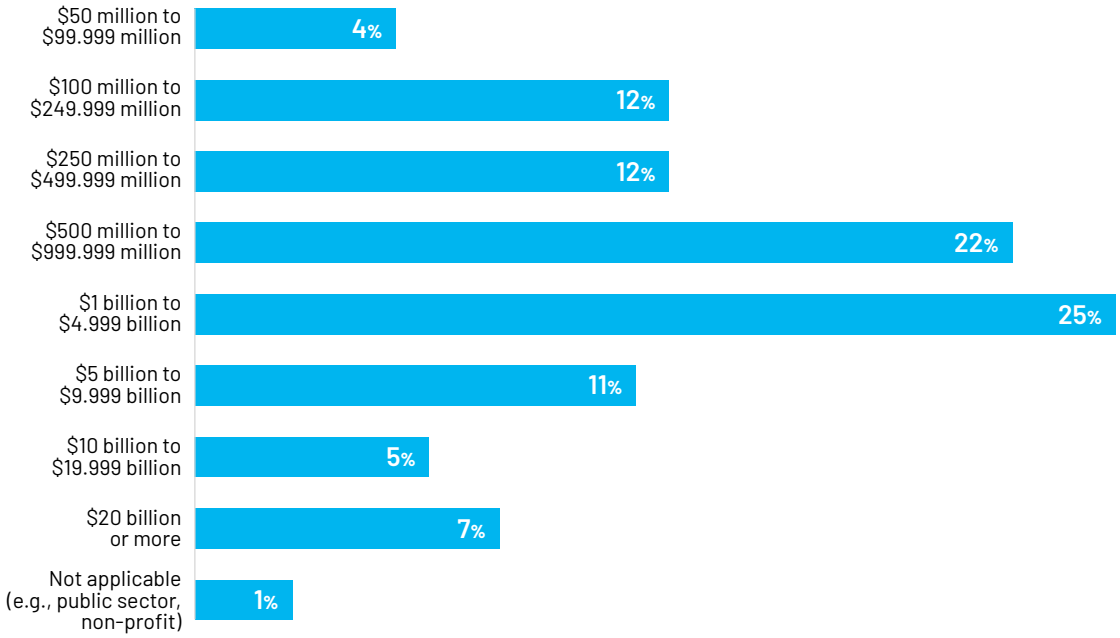


Figure 25. Distribution of the estimated annual revenue of each respondent's organization (reflected in USD).

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. It is a division of TechTarget, Inc. (Nasdaq: TTGT), the global leader in purchase intent-driven marketing and sales services focused on delivering business impact for enterprise technology companies.

VIAVI (NASDAQ: VIAV) is a global provider of network test, monitoring and assurance solutions for telecommunications, cloud, enterprises, first responders, military, aerospace and railway. VIAVI is also a leader in light management technologies for 3D sensing, anti-counterfeiting, consumer electronics, industrial, automotive, government and aerospace applications.

Enterprise Strategy Group™ by TechTarget

sotn24-ec-rpt-nse-ae | 30194142 900 0524