EMA
IT & DATA MANAGEMENT RESEARCH, INDUSTRY ANALYSIS & CONSULTING

Prepared for:

Progress®

Network Management Megatrends 2024:

Skills Gaps, Hybrid and Multi-Cloud, SASE, and AI-Driven Operations

May 2024 EMA Research Report Summary

By **Shamus McGillicuddy**, Vice President of Research
Network Infrastructure and Operations

Table of Contents

1 Introduction
3 Research Methodology
4 Key Findings
6 Network Operations Outcomes
7 Network Operations Success
7 Grading Themselves
8 Measuring Success
9 Operational Challenges
10 Alert Noise is Increasing
10 Sources of Trouble
10 Manual Errors
11 The Opportunity for Better Tools
12 Network Operations Strategy
13 Organizing the Network Operations Function
14 Technical Initiatives that Shape Network Operations
15 Network Technology Investments and Projects that Shape Operational Priorities
16 Network Operations Toolsets
17 Toolset Sprawl Remains the Norm
19 Striving for an Integrated Toolset
20 Network Tool Requirements
20 Platform and Business Requirements
21 Feature Requirements
21 Replacing Incumbent Tools
23 Network Data Requirements
24 Critical Monitoring and Troubleshooting Data
25 Streaming Telemetry
25 Interest is Strong
26 Adoption is Mostly Experimental
26 Potential Benefits
27 Synthetic Network Traffic
27 Adoption is High
28 Drivers of Interest
29 Megatrend #1: Hiring Networking Personnel is Getting Harder
31 Technical Skills that are Scarce
32 Megatrend #2: Adapting Network Operations to the Cloud
33 Cloud versus Data Center
33 Multi-Cloud Adoption
34 Cloud Network Monitoring
35 Engagement with Hybrid Multi-Cloud Networking Solutions
36 Megatrend #3: SASE Introduces Operational Challenges
37 SASE Adoption
38 Operational Pain with SASE
39 SASE Observability
40 Megatrend #4: AI/ML-Driven Network Management is Mainstream
42 AI/ML Network Management Use Cases
43 AI/ML Impact on Network Operations
44 Conclusion

Introduction

Enterprise Management Associates' (EMA) Network Management Megatrends research has been the industry benchmark of enterprise network operations tools and practices since it was first published in 2008. This biennial research surveys hundreds of IT professionals about their approach to managing, monitoring, and troubleshooting their networks. It also examines the business and technology trends that are shaping network operations strategy.

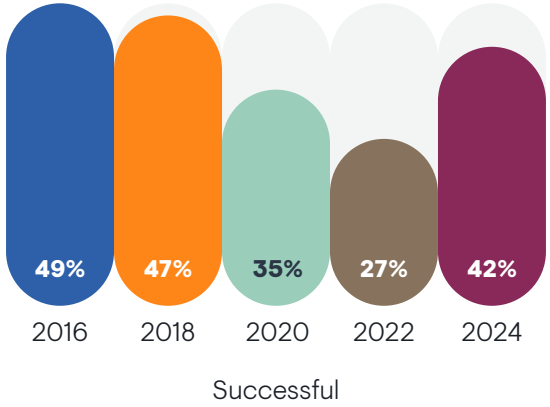
In recent years, EMA observed a concerning negative trend in self-assessments of network operations success. From 2016 to 2022, the percentage of survey respondents who believed their network teams were completely successful with monitoring and managing networks declined from 49% to 27%. EMA attributed this downward trend to a variety of disruptors, including the rise of hybrid multi-cloud architecture, SaaS application adoption, cloud native applications, and WAN transformation with software-defined WAN (SD-WAN) and secure access service edge (SASE). Also, the 2022 research found that many enterprises were struggling to hire networking personnel, and we assumed that this was impacting success.

Our 2024 survey revealed a network operations rebound, as **Figure 1** details. This year, 42% of respondents claimed their network operations group was fully successful. What accounts for this change in fortunes? Time will tell. This year's results could be a fluke. However, there are several other dynamics at play.

This research found that adoption of artificial intelligence (AI) tools for network management has grown, and adoption correlated with success. Also, network teams have had more time to adjust their strategic focus on major disruptors, like multi-cloud, SaaS applications, and SASE. Network toolsets are clearly evolving to support these changes. Just four years ago, our research found that the cloud remained an afterthought even though it had turned the world of IT operations upside down.

As always, EMA's Network Management Megatrends research explores what network teams can do to improve their chance of success.

FIGURE 1. HOW WOULD YOU RATE THE SUCCESS OF YOUR NETWORK OPERATIONS ORGANIZATION OVER THE PAST YEAR?



Research Methodology

EMA surveyed 406 IT professionals for this research. Our goal was to survey personnel responsible for network management or knowledgeable about how their companies manage their networks. To qualify for this survey, respondents had to be engaged with their company's networks in one of three ways:

1. Networking was a significant focus of their overall responsibilities as an IT professional (48%)
2. Networking was the sole focus of their role as an IT professional (33%)
3. They provided executive leadership to teams responsible for networking (19%)

Figure 2 reveals the demographic overview of respondents. They hailed from North America and Europe and worked in a variety of roles, from highly technical to executive level. Survey participants worked within a variety of groups in their IT organizations, including cloud engineering, IT service management, project management, network engineering, IT architecture, and network operations.

FIGURE 2. DEMOGRAPHIC OVERVIEW

Job titles

- **49.3%** Technical personnel
- **36.2%** IT middle management
- **14.5%** IT executives

IT groups/departments

- **18.2%** Cloud engineering/operations
- **14.0%** IT service management/service support
- **13.3%** IT project management
- **10.3%** Network engineering
- **9.6%** IT architecture
- **8.4%** Network operations
- **7.1%** DevOps
- **3.9%** IT tool engineering
- **2.7%** Data center operations

Top industries

- **18.2%** Finance/Insurance
- **17.0%** Manufacturing
- **8.4%** Health care
- **7.1%** Retail/Wholesale/Distribution
- **6.7%** Transportation
- **6.4%** Education/Research
- **5.7%** Construction
- **4.9%** Business services unrelated to IT

Company size (employees)

- **37.9%** 500 to 2,499
- **43.1%** 2,500 to 9,999
- **19.0%** 10,000 or more

Annual revenue

- **25.8%** $50 million to less than $250 million
- **35%** $250 million to less than $1 billion
- **36.7%** $1 billion or more
- **2.4%** Unknown/not applicable

Location

- **65.3%** North America
- **43.7%** Europe

Key Findings

- 42% of network operations groups are fully successful today, up from 27% in 2022
- Today's network teams are most challenged by shortages of skilled personnel, budget shortfalls, and large, fragmented toolsets
- Public cloud migration, SaaS application adoption, and DevOps and CI/CD frameworks are the initiatives most responsible for driving network operations strategy today
- Network security, hybrid/multi-cloud networking, and network automation are the top investment priorities for network teams
- Network management toolsets consolidated recently, but the typical team still has anywhere from 3 to 15 tools
- 74% of network teams are thinking about replacing a network management tool
- Only 9% of IT groups find it very easy to hire skilled networking personnel
- 93% of IT organizations are using or planning to use a synthetic network monitoring tool, primarily to improve observability of SaaS applications, public cloud infrastructure, and internet-based WAN connectivity
- 56% of network teams are supporting a multi-cloud environment
- 40% of network teams that are supporting hybrid or multi-cloud networks are adopting end-to-end multi-cloud networking fabrics
- 46% of network teams have fully implemented a SASE solution
- Network teams are finding it difficult to manage SASE security policies and controls, monitor the health and performance of SASE points of presence, and integrate the components of a SASE architecture
- 64% of network teams have adopted AI features their network management tools offer, primarily to improve security threat detection, automate network problem remediation, and improve network troubleshooting processes

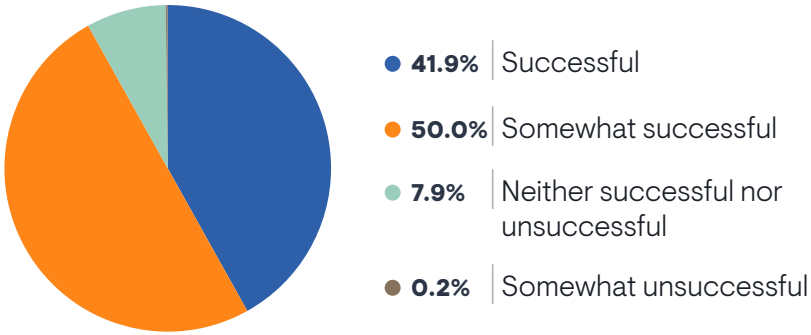
Network Operations Outcomes

Network Operations Success

Grading Themselves

Network operations success rebounded this year after several years of decline. Over the years, EMA has found that IT professionals rarely give themselves a failing grade on this question. Most respondents either select "somewhat successful" or "successful." The former represents network teams that see room for improvement, so we focus our analysis on the differences between the latter and the former. **Figure 3** reveals this dynamic.

FIGURE 3. OVER THE PAST YEAR, HOW WOULD YOU RATE THE SUCCESS OF YOUR NETWORK OPERATIONS ORGANIZATION?



Sample Size = 406

"I would say that overall, network operations on my team are very solid," said a network engineering director for a large insurance company. "I'm the team lead, and I'm able to guide them and help them stay away from common pitfalls."

"I think we're doing a decent job, given that complexity has increased as our workforce has gotten more hybrid," said an IT tools architect with a Fortune 500 media company.

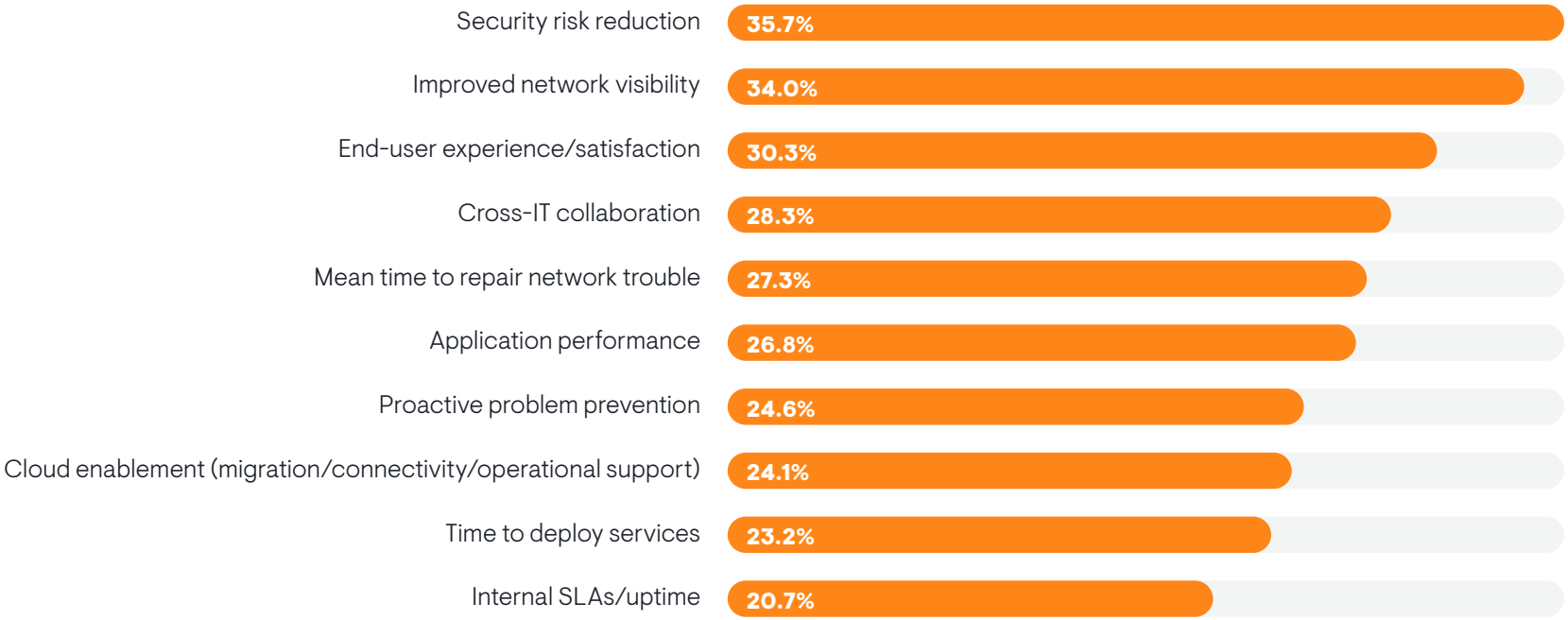
"I think we're doing a decent job, given that complexity has increased as our workforce has gotten more hybrid," said an IT tools architect with a Fortune 500 media company.

Measuring Success

Figure 4 reveals how organizations measure network operations success. The top criteria are security risk reduction and improved network visibility. These were also the top criteria in 2022. Mean time to repair (MTTR) network trouble was the number-three response in 2022, but it dropped to fifth this year, suggesting that other measures like end-user satisfaction and cross-domain collaboration are rising in importance, especially end-user satisfaction, which was sixth in 2022. Larger enterprises (10,000 or more employees) were more likely to still rely on MTTR as a measure of success.

Time to deploy new services is a minor criterion, but successful network operations teams were more likely to be measured against it. Organizations that report fewer problems with hiring were more likely to measure their success against proactive problem prevention and application performance.

FIGURE 4. WHICH OF THE FOLLOWING CONCEPTS ARE MOST IMPORTANT FOR MEASURING THE SUCCESS OF THE NETWORK MANAGEMENT TEAM?



Sample Size = 406, Valid Cases = 406, Total Mentions = 1,117

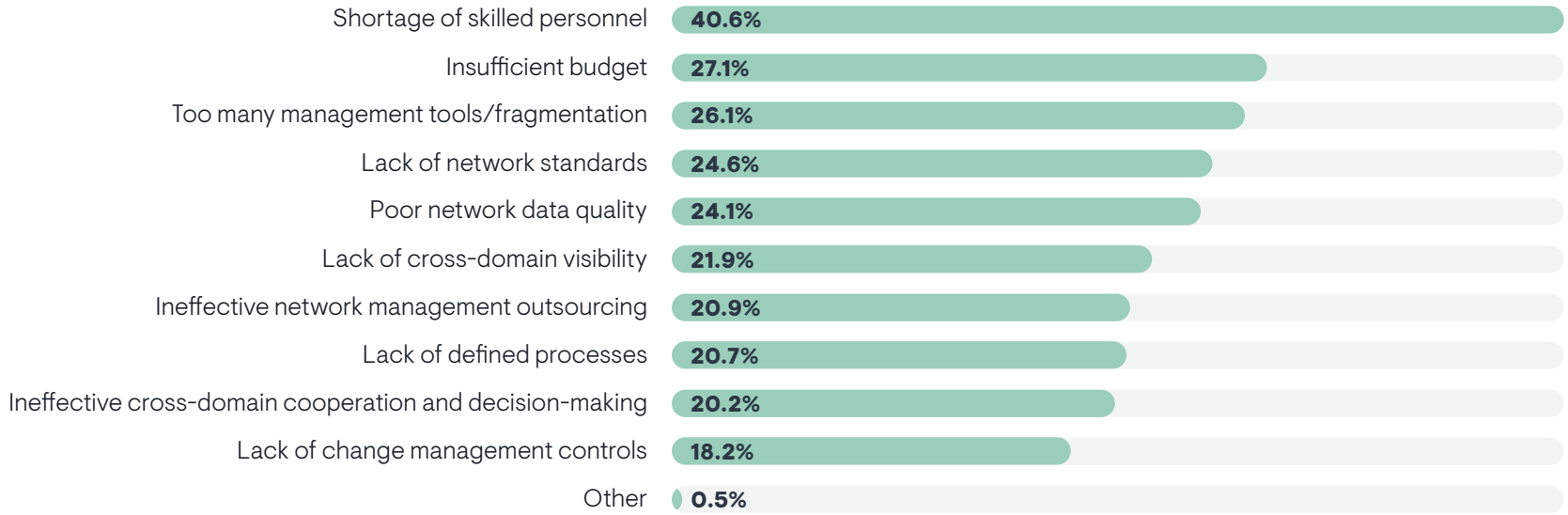
Operational Challenges

Figure 5 identifies the issues that are challenging network operations success. A shortage of skilled personnel is the main problem by a big margin. In 2022, it was the number-two problem behind network data quality, which dropped to the middle of the pack this time. Respondents who told us that they are struggling significantly with hiring networking personnel reported less network operations success. Later in this report, we'll explore labor issues in depth.

Although data quality has become a less urgent challenge, one network engineer at a Fortune 500 aerospace and defense company indicated that he has a significant challenge. "Sometimes the polling data that the tool gets can differ from what's actually on the device itself. I tell people not to capture data in a tool and send it up the chain immediately. You need to recheck in command line to verify it. We have to question the data before we act."

Budget shortfalls, tool fragmentation and sprawl, and a lack of network standards are the other leading operational challenges this year.

FIGURE 5. WHICH OF THE FOLLOWING ARE THE BIGGEST CHALLENGES TO SUCCESS FOR NETWORK OPERATIONS IN YOUR ORGANIZATION?



Sample Size = 406, Valid Cases = 406, Total Mentions = 995

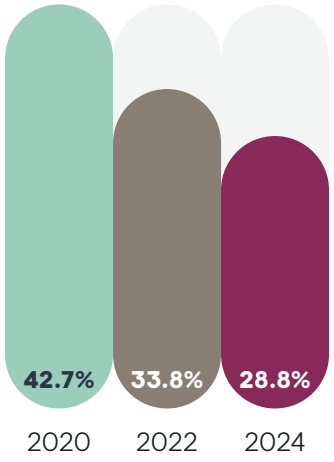
Alert Noise is Increasing

While proactive problem detection is improving, alert management is getting worse. Since 2020, EMA has asked respondents to estimate what percentage of the alerts their network management tools are producing is indicative of a problem that must be fixed. In other words, how may alerts are actionable as opposed to noise? **Figure 6** reveals that nearly 43% of network alerts were actionable in 2020, and today, fewer than 29% are actionable. Technical personnel (admins, engineers, architects) reported a lower rate of actionable alarms, which is concerning given that they are the ones most often tasked with responding to alerts and thus have the most accurate picture of this issue.

Nearly 43% of network alerts were actionable in 2020, and today, fewer than 29% are actionable.

"One of our tools just sends out a lot of white noise, lots of SNMP traps that don't make a lot of sense," said a network engineer with a Fortune 500 aerospace and defense company. "It takes time to tune that."

FIGURE 6. WHAT PERCENTAGE OF THE ALERTS YOUR NETWORK MONITORING TOOLS PRODUCE IS INDICATIVE OF A REAL PROBLEM THAT MUST BE FIXED?



Sources of Trouble

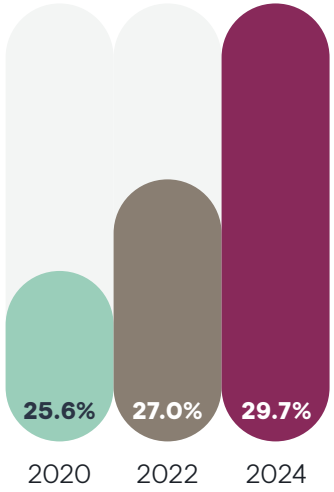
Manual Errors

In 2020, EMA began asking Megatrends respondents to estimate the percentage of their network problems that is attributable to a manual administrative error, like a bad configuration change. **Figure 7** reveals that rates of error-driven trouble have been climbing over the last four years, from less than 26% in 2020 to nearly 30% in 2024.

Manual errors were more common in smaller enterprises (500 to 2,499 employees). Organizations that have a hybrid cloud environment reported lower rates of error-driven trouble than organizations that are 100% in the cloud and organizations that are 100% relying on private data centers.

Rates of error-driven trouble have been climbing over the last four years, from less than 26% in 2020 to nearly 30% in 2024.

FIGURE 7. WHAT PERCENTAGE OF YOUR NETWORK-RELATED PROBLEMS IS CAUSED BY MANUAL ADMINISTRATIVE ERRORS (BAD CONFIGURATION CHANGE, ETC.)?

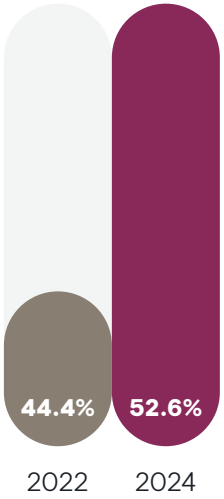


IT professionals believe that better network management tools could prevent or eliminate nearly 53% of their network problems.

The Opportunity for Better Tools

Network teams are increasingly recognizing that that they need to improve their tools. **Figure 8** reveals that IT professionals believe that better network management tools could prevent or eliminate nearly 53% of their network problems. The chart also shows that the impact of bad tools may be getting worse. Just two years ago, our research showed a smaller opportunity of just 44% of problems.

FIGURE 8. WHAT PERCENTAGE OF YOUR NETWORK-RELATED PROBLEMS DO YOU THINK WOULD BE PREVENTABLE WITH BETTER NETWORK MANAGEMENT TOOLS?



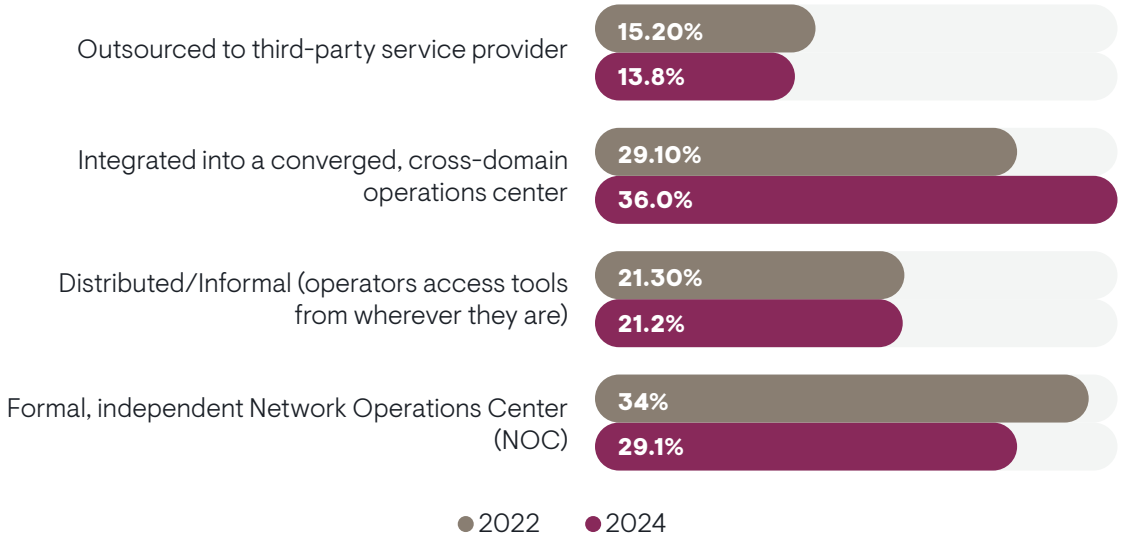
Network Operations Strategy

Organizing the Network Operations Function

Figure 9 details how enterprises are organizing the people who are responsible for managing and monitoring their networks. Things have changed since we last examined this issue in 2022. We see a significant decline in the traditional, standalone network operations center (NOC) in favor of a converged, cross-domain operations center where specialists from different technology silos work together to monitor and troubleshoot infrastructure and applications. Meanwhile, the small number that outsource network operations to a third party decreased very slightly, while those that take a distributed, informal approach remained unchanged.

"It's less formal [than a NOC] here, and it's segmented according to area," said a network security architect at a Fortune 500 cybersecurity company. "By area, I mean AWS cloud or Azure cloud. And we have the traditional on-premises people who also deal with SD-WAN. They have some SD-WAN exposure into the cloud, so there is some segmentation there. Once traffic goes deeper into the cloud, they hand it off to another group."

FIGURE 9. WHICH OF THE FOLLOWING BEST DESCRIBES THE WAY IN WHICH YOUR ORGANIZATION PRIMARILY CONDUCTS NETWORK MONITORING AND MANAGEMENT?

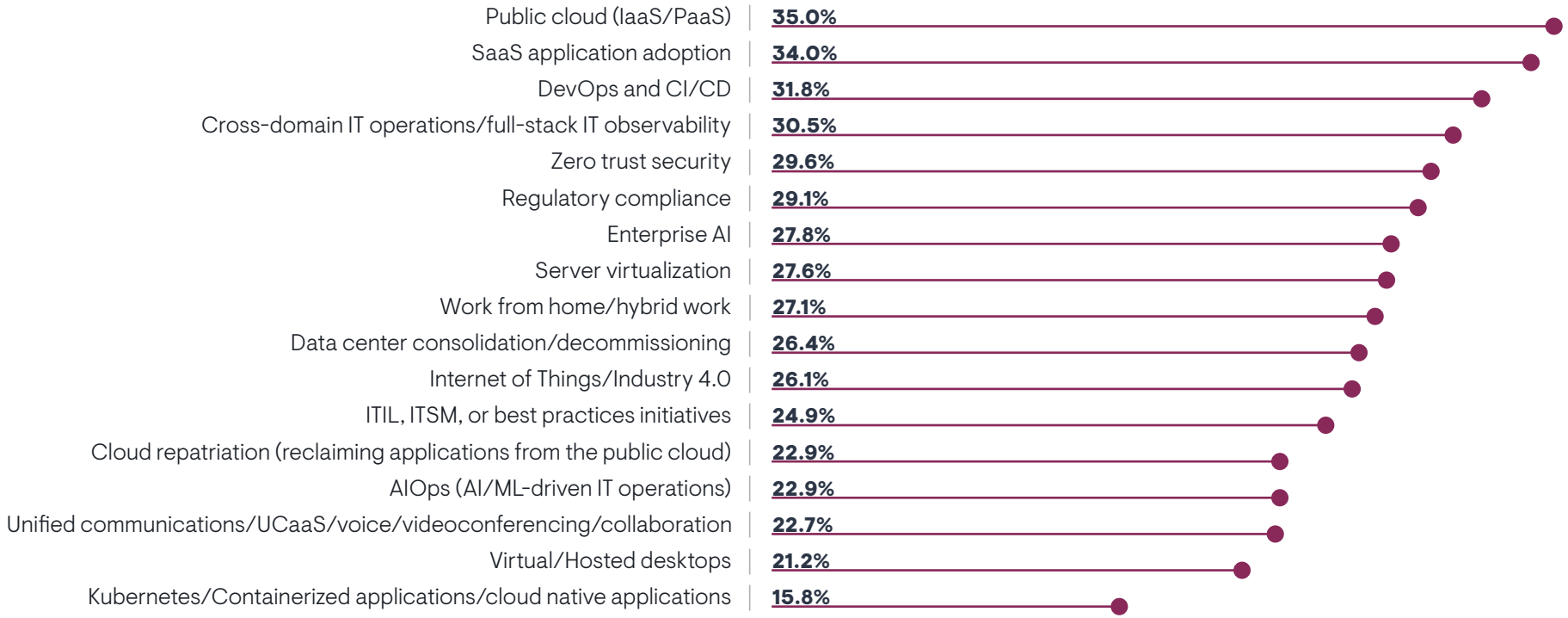


Technical Initiatives that Shape Network Operations

Since 2008, EMA's Network Management Megatrends research has asked respondents to identify the technical initiatives that are most responsible for driving their current priorities for managing and monitoring their networks. From 2008 to 2020, the top response to that question was always server virtualization. This reflected the major disruption that hypervisor technology introduced to data center networks, with a massive increase in east-west traffic, increased portability of workloads, and decreased visibility into traffic between virtual servers. Network teams devoted significant resources to evolving their network to support new traffic patterns and updating their tools to improve observability. In 2022, server virtualization dropped from the top of the list, replaced by a new top three of public cloud adoption, cloud native application platforms, and SaaS application adoption.

Figure 10 reveals a continuation of this trend. This year, cloud, SaaS, DevOps, and CI/CD are the top drivers of networking strategy, suggesting a tight alignment of network infrastructure and operations teams with the groups responsible for modernizing application infrastructure and operations.

FIGURE 10. WHICH OF THE FOLLOWING IT INITIATIVES ARE DRIVING YOUR ORGANIZATION'S CURRENT PRIORITIES IN MONITORING/MANAGING NETWORKS?



Sample Size = 406, Valid Cases = 406, Total Mentions = 1,848

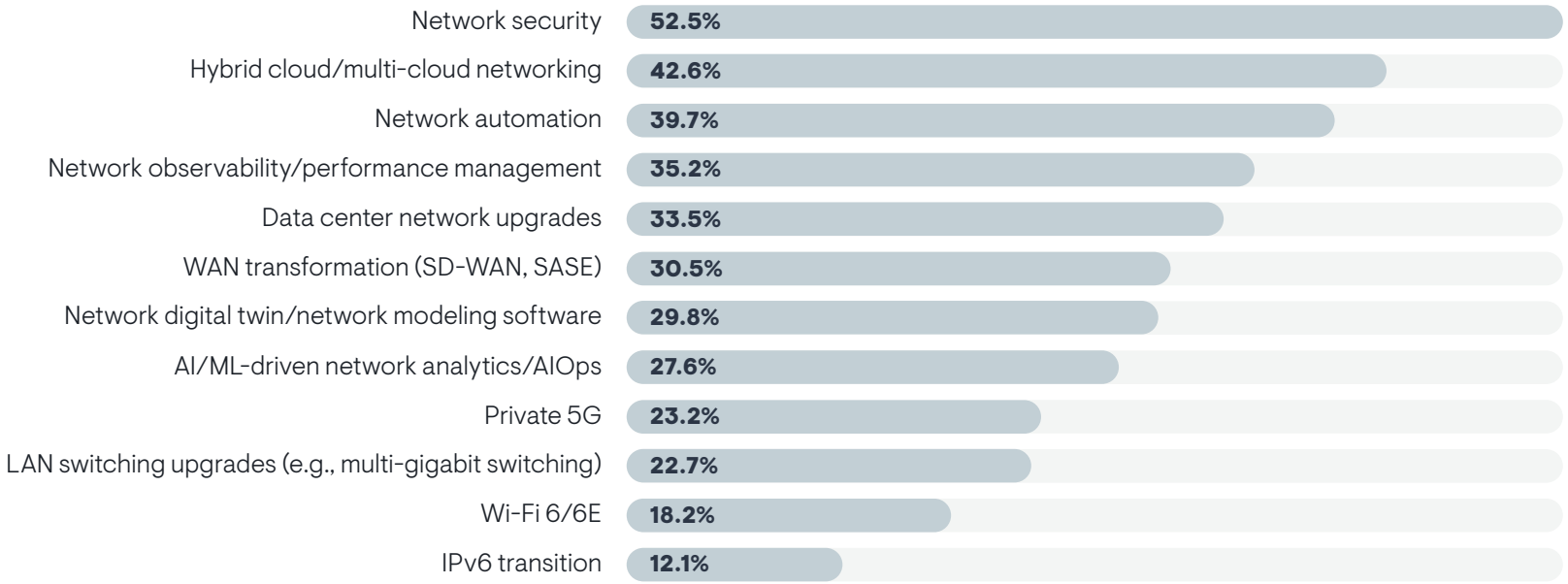
Network Technology Investments and Projects that Shape Operational Priorities

Figure 11 reveals the networking technology initiatives and investments that are high priorities for organizations today. Network security is the major priority, as it was in previous iterations of this report. Network security was a bigger priority for the most successful network operations groups represented in this research. Hybrid/multi-cloud networking technology and network automation were the chief secondary priorities.

Overall, the positions of responses on this chart are largely unchanged from 2022, with a couple of exceptions. WAN transformation dropped from third in 2022 to sixth this year. Private 5G advanced from eleventh in 2022 to ninth this year. Digital twin/network modeling software was added as a response option in 2024 and emerged as a tertiary priority overall.

Digital network twin software and IPv6 were more popular influences among organizations that host 100% of their applications in the public cloud. Organizations that maintain a mix of data centers and public cloud for application infrastructure were more likely to select network observability, network security, and hybrid multi-cloud networking. Enterprises that use multiple public cloud providers had a greater affinity for digital network twins, WAN transformation, AI/ML-driven networking, data center network upgrades, and network security.

FIGURE 11. WHICH OF THE FOLLOWING NETWORKING TECHNOLOGY INITIATIVES/INVESTMENTS ARE HIGH PRIORITIES FOR YOUR ORGANIZATION TODAY?



Sample Size = 406

Network Operations Toolsets

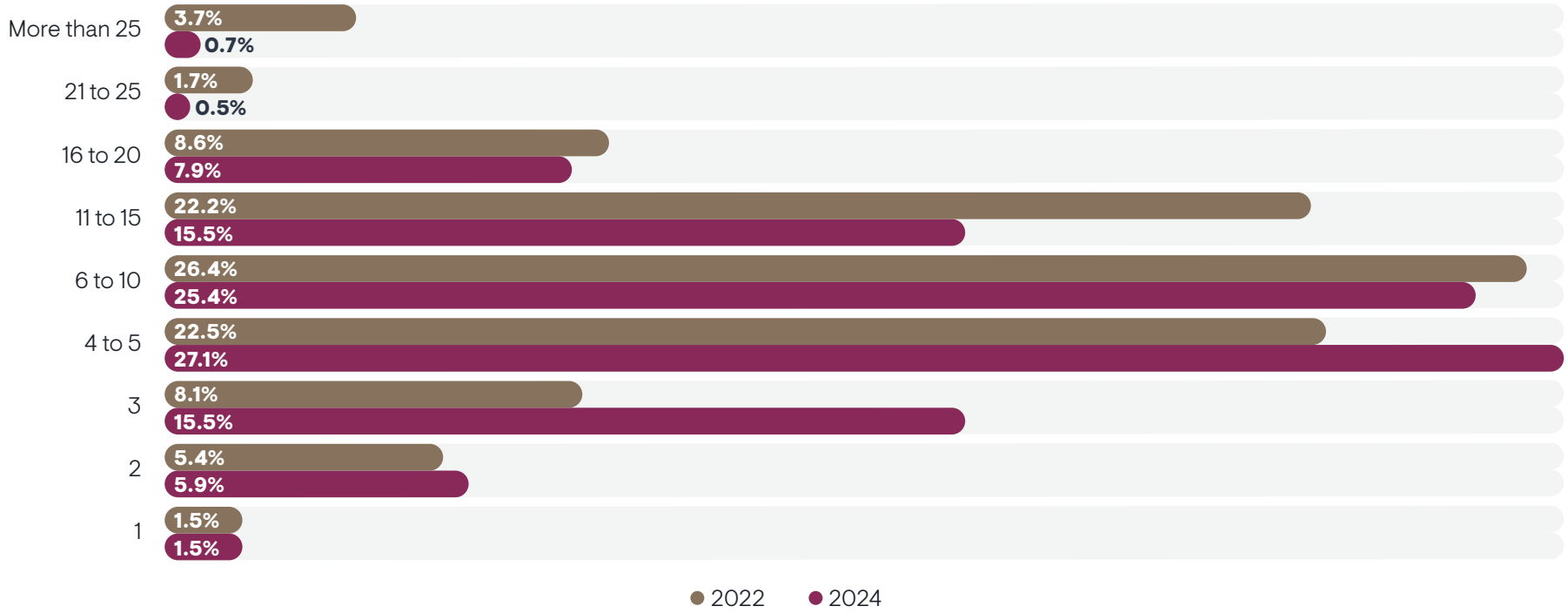
Toolset Sprawl Remains the Norm

Despite the ready availability of unified, multifunction network management platforms from vendors, IT organizations tend to have a multi-tool approach to network operations. EMA's Megatrends report always asks participants to identify how many tools they use to manage, monitor, and troubleshoot their networks, and the typical response ranges from 4 to 15 tools. This year, we see evidence of tool consolidation. **Figure 12** reveals that from 2022 to 2024, the number of network teams that use three to five tools grew significantly, while the number who use 11 or more decreased significantly. Despite this consolidation, multi-tool network operation remains the norm.

"We use many tools, but not to the depth and breadth that we should," said an IT tools architect at a Fortune 500 media company. "Before I started here, there were seven or eight tools in the network operations space. We're consolidating right now."

"There really is no unified toolset that applies to all the network hardware we encounter," said a network engineering director for a large insurance company.

FIGURE 12. IN TOTAL, ABOUT HOW MANY TOOLS DOES THE NETWORK OPERATIONS TEAM USE FOR NETWORK MONITORING AND TROUBLESHOOTING?



Sample Size: 2024=406, 2022=409

Larger toolsets are introducing operational complexity that makes tools less effective and networking personnel less efficient.

Tool sprawl has a mixed impact on overall network operations success. For instance, organizations with larger toolsets were enjoying more success, but there are red flags. **Figure 13** demonstrates that manual administrative errors that lead to network downtime or performance issues are more common with larger toolsets. **Figure 14** shows that networking professionals spend a larger portion of their workday troubleshooting the network if they have a larger toolset. The combination of these two findings suggests that larger toolsets are introducing operational complexity that makes tools less effective and networking personnel less efficient.

FIGURE 13. PERCENTAGE OF NETWORK-RELATED PROBLEMS CAUSED BY MANUAL ADMINISTRATIVE ERRORS, BY NUMBER OF TOOLS IN THE NETWORK OPERATIONS TOOLSET

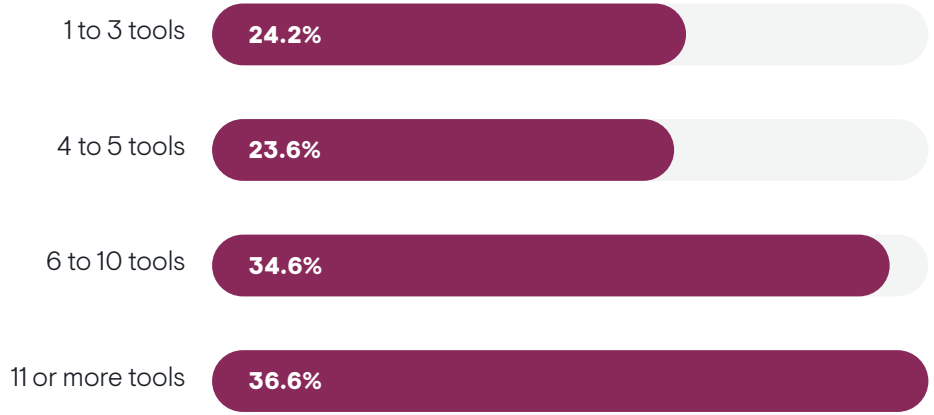
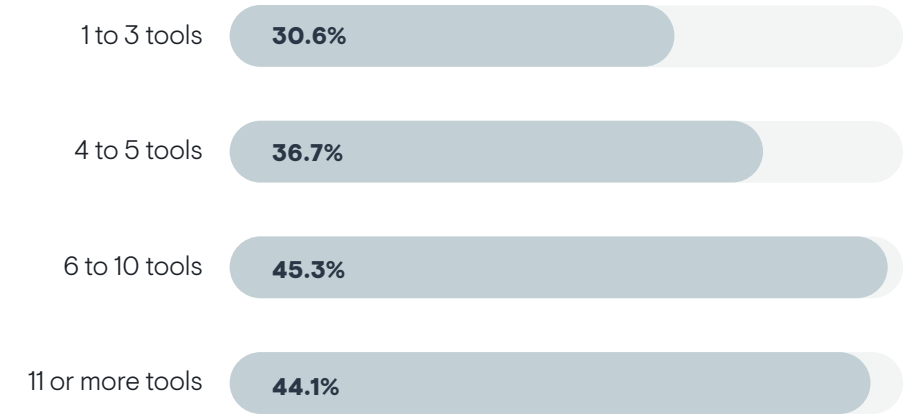


FIGURE 14. PERCENTAGE OF THE TYPICAL NETWORK OPERATIONS PROFESSIONAL'S DAY SPENT ON TROUBLESHOOTING NETWORK PROBLEMS, BY NUMBER OF TOOLS IN THE NETWORK OPERATIONS TOOLSET



Sample Size = 406

Striving for an Integrated Toolset

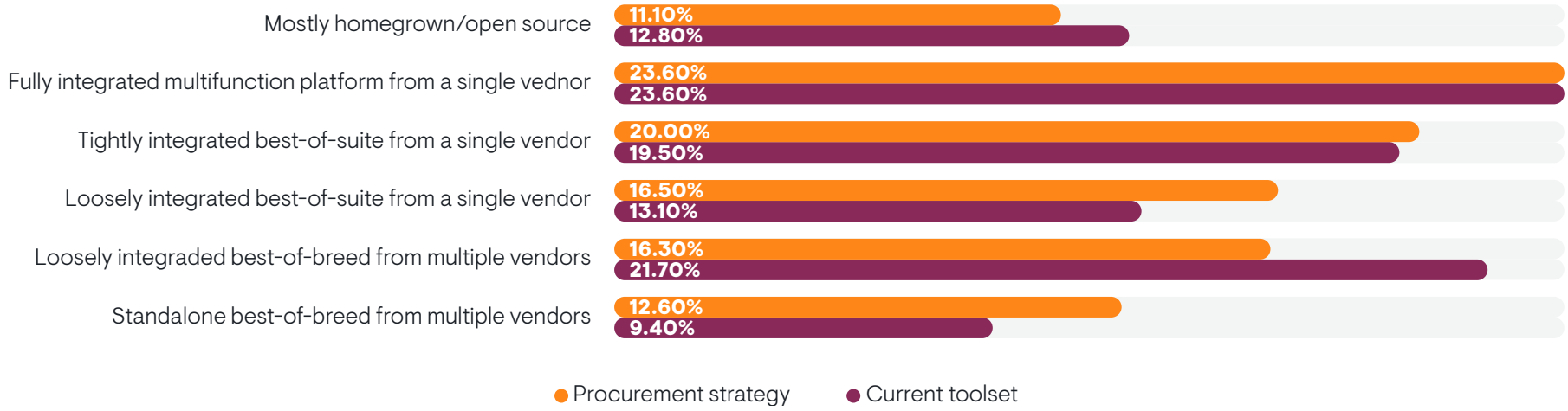
Given that nearly every IT organization relies on multiple tools to manage their networks, integration becomes a critical consideration. With an integrated toolset, network teams can reduce workflow complexity and share data across tools to strive for the mythical "single pane of glass" view of their networks. **Figure 15** reveals where organizations are with these efforts. It charts how well integrated toolsets generally are today and the procurement strategy that organizations pursue to enable this integration. First, it shows that nearly 24% of organizations have a fully integrated, multifunction network management platform from a single vendor and will continue to make that their procurement priority. Based on our interactions with IT operations personnel, we believe most of these organizations have tools from other vendors, but the unified platform dominates their overall network operations processes.

Roughly 20% have a tightly integrated suite from a single vendor and will stay that way. These organizations typically use a suite from a tool vendor that grew its capabilities through acquisitions of complementary vendors.

The chart also reveals that many have a loosely integrated best-of-breed toolset from multiple vendors, and they anticipate moving away from this approach by implementing to a loosely integrated suite from a single vendor or moving toward a standalone, multi-vendor approach.

Less successful network operations teams tend to focus their tool procurement strategies on loosely integrated single-vendor suites or unintegrated multi-vendor toolsets. On the other hand, more successful network operations teams were more likely to use homegrown and open source or fully integrated multifunction platforms.

FIGURE 15. WHICH OF THE FOLLOWING IS YOUR ORGANIZATION'S OFFICIAL STRATEGY WHEN ACQUIRING AND DEPLOYING NETWORK MONITORING AND MANAGEMENT TOOLS AND WHICH REFLECT THE CURRENT REALITY OF YOUR TOOLSET?



Sample Size = 406

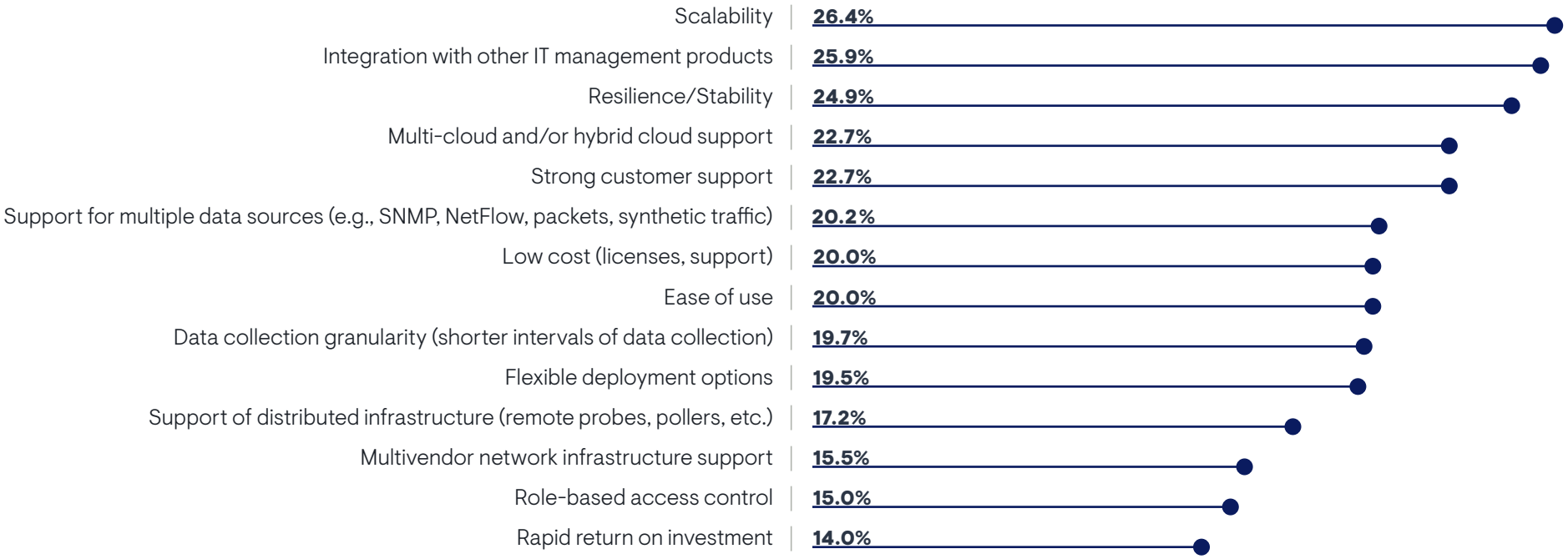
Network Tool Requirements

Platform and Business Requirements

Figure 16 examines what IT organizations look for from network management tools in terms of general platform characteristics and vendor capabilities. The three big priorities are scalability, integrations, and resilience. In other words, network teams need tools that are always on, can handle any size of network, and can integrate with other IT operations management systems.

Multi-cloud and hybrid cloud support and strong customer support are the top secondary requirements. Also, organizations that use multiple cloud providers were more likely to select low-cost tools and tool support of multiple data sources.

FIGURE 16. WHAT ARE YOUR ORGANIZATION'S TOP BUSINESS AND PLATFORM REQUIREMENTS FOR NETWORK MANAGEMENT PRODUCTS?

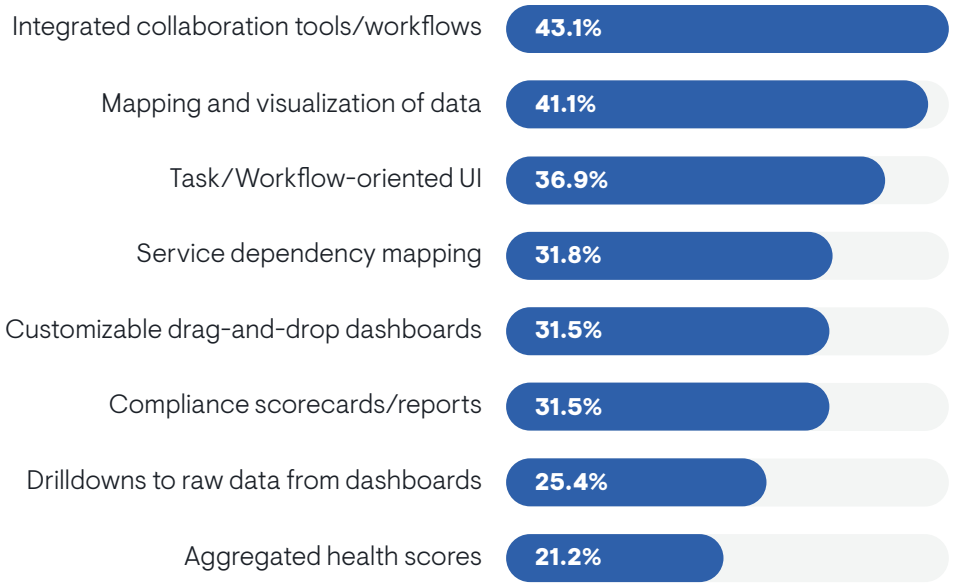


Sample Size = 406, Valid Cases = 406, Total Mentions = 1,151

Feature Requirements

Figure 17 identifies the general features that network teams find most important in a network management tool. Integrated collaboration tools/workflows and mapping and visualization of data are the most critical capabilities.

FIGURE 17. WHICH OF THE FOLLOWING GENERAL NETWORK MANAGEMENT TOOL FEATURES ARE MOST IMPORTANT AND USEFUL?



Sample Size = 406, Valid Cases = 406, Total Mentions = 1,066

"The graphical information I can get out of my SNMP-based tools is fantastic. I like being able to get lots of charts and real-time data on utilization, latency, packet loss," said a network engineer with a Fortune 500 aerospace and defense company.

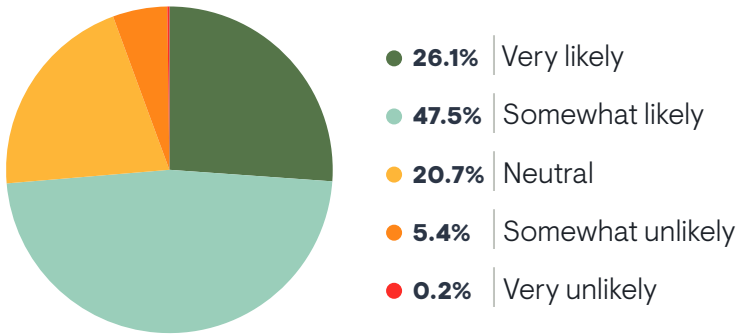
User interfaces oriented around network management tasks and workflows are the chief secondary requirement of tools. Rather than presenting monitoring data in a variety of charts and reports, tools can integrate workflows into their dashboards that enable capacity planning and troubleshooting, for instance. Organizations that struggle to hire networking personnel were more likely to seek tools with workflow-oriented UIs and integrated collaboration capabilities.

Service dependency mapping and aggregated health scores were moderate-to-low priorities overall, but multi-cloud enterprises were more interested in such features. Technical personnel were also more interested in aggregated health scores than IT executives and middle management, and members of the network engineering team were especially interested. Drilldowns to raw monitoring data were low priorities, but more important to network engineering and cloud engineering teams.

Replacing Incumbent Tools

Figure 18 reveals that nearly 74% of IT organizations are at least somewhat likely to replace a network management tool over the next two years. IT professionals whose roles are 100% focused on networking were the most open to changing tools. IT generalists and executives were less open. Smaller companies were more open to change.

FIGURE 18. HOW LIKELY IS YOUR ORGANIZATION TO REPLACE A NETWORK MANAGEMENT TOOL OVER THE NEXT TWO YEARS?



Sample Size = 406

"In general, my organization is pretty open to changing tools," said an IT tools architect at a Fortune 500 media company. "But the more complex your organization is, the more complex it is to replace a tool. We have many different teams and business units, but we are open to trying something new to try to solve problems better."

"We are open to new tools," said a network engineer with a Fortune 500 aerospace and defense company. "It would come down to depth of functionality, the [network] manufacturers that it supports, and cost."

Organizations that measure network operations success by their ability to proactively prevent problems were also more willing to make a change, which indicates that their existing toolsets aren't necessarily supporting that goal. Adoption of SASE and multi-cloud networking solutions also correlated with interest in tool replacement, which aligns with EMA's view that cloud and SASE disrupt network observability and management.

Network teams were more open to switching tools if they were:

- Struggling with a lack of defined processes
- Experiencing a high number of network outages that manual administrative errors cause
- Spending too much time on network troubleshooting
- Struggling to correlate SASE overlay and WAN underlay performance
- Lacking visibility into SASE points of presence

"We don't keep anything that is crap," said an IT operations manager with a very large government agency. "I don't think anyone is tied to their existing tools. If a new tool comes along that is better or cheaper, we'll consider it."

Organizations that are open to swapping out tools were more likely to tell EMA that they need tools that offer:

- An ability to collect and analyze multiple classes of network data (e.g., SNMP, network flows, etc.)
- Aggregated network health scores
- Auto-discovery of services and dependencies
- Automatic topology mapping
- Service dependency mapping
- Streaming telemetry support
- Synthetic network traffic monitoring, particularly for hybrid WAN performance and end-user experience insights

Openness to tool replacement also correlated with interest in applying AI and ML technology to network management. These were the use cases they found most compelling for AI:

- Intelligent alerting/event management
- Change management
- Capacity management
- Conversational tool queries via a chatbot

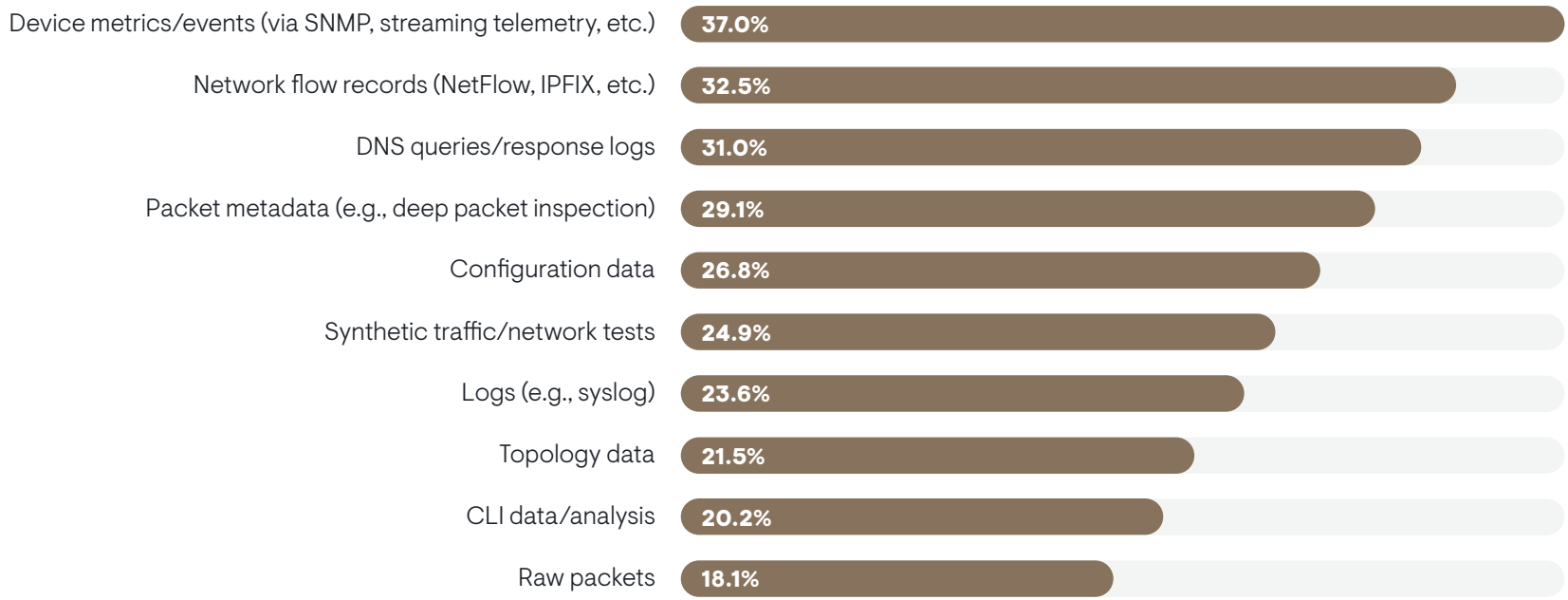
Network Data Requirements

Critical Monitoring and Troubleshooting Data

Figure 19 reveals the data that IT organizations consider most essential to network monitoring and troubleshooting. Device metrics and events collected via SNMP, APIs, or streaming telemetry are the most critical, followed by network flow records, DNS data, and packet metadata (typically generated by DPI-based network monitoring tools or network packet brokers).

Less successful network operations groups cited logs as a critical source of data. Logs were also more important to large enterprises (10,000 or more employees). Raw packets were a very low priority, but members of network engineering teams (the group most likely to have personnel who can analyze this data) marked it as a high priority. Raw packets were also important to respondents who host their applications and data only in data centers rather than the cloud. This makes sense, since raw packets are more difficult to collect in cloud environments.

FIGURE 19. WHICH OF THE FOLLOWING DATA SOURCES DOES YOUR ORGANIZATION MOST RELY UPON FOR MONITORING AND TROUBLESHOOTING ITS NETWORK?



Sample Size = 381, Valid Cases = 381, Total Mentions = 1,009

Streaming Telemetry

Streaming network telemetry is a relatively new method for collecting metrics and events from infrastructure that promises to be a potential replacement for Simple Network Management Protocol (SNMP). SNMP has long been the standard for collecting this data. It uses a pull method for metric collection, polling devices at regular intervals. SNMP also has a "trap" capability in which network engineers can configure devices to send event information in certain conditions.

Streaming telemetry is a push method for data collection. Monitoring tools subscribe to telemetry streams from network devices that support the technology. Thus, devices send telemetry when conditions change rather than when data is requested. Streaming telemetry offers efficiency and granularity.

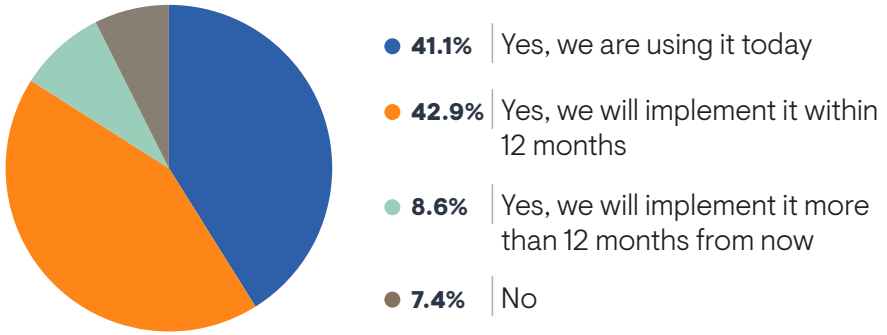
Nearly 92% of IT organizations are interested in using streaming telemetry and 41% claim they are already using it.

Interest is Strong

Figure 20 reveals that nearly 92% of IT organizations are interested in using streaming telemetry and 41% claim they are already using it. Successful network operations teams (57%) are more likely to use it today. The 2022 edition of this research found that 43% were using it. Thus, adoption hasn't progressed over the last two years.

Reports of current adoption are highest among DevOps and cloud teams where streaming telemetry is more mature, thanks to the OpenTelemetry standard that many DevOps-oriented application observability solutions support. Adoption is also higher among multi-cloud enterprises. Larger companies (10,000 or more employees) were less interested in it.

FIGURE 20. IS YOUR ORGANIZATION INTERESTED IN USING STREAMING NETWORK TELEMETRY?



Sample Size = 406

Adoption is Mostly Experimental

EMA asked respondents who were using or planning to use streaming telemetry why they were implementing the technology. **Figure 21** reveals that nearly 74% are experimenting with it, trying to understand its value. Only 26% are trying to adopt it as a primary method for collecting network data and hoping to eliminate SNMP from the network. These numbers are nearly identical to our findings in 2022. Members of IT architecture and IT service management teams were more likely to pursue an SNMP replacement, while cloud teams were still in an experimental phase.

FIGURE 21. WHICH OF THE FOLLOWING DESCRIBES WHY YOU ARE INTERESTED IN USING STREAMING TELEMETRY?

73.7% Nice to have – we want to try it and understand its value

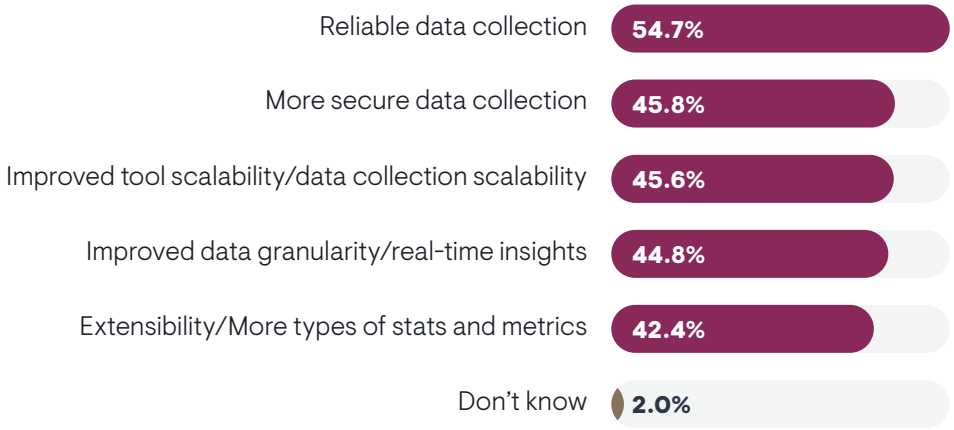
26.3% Required – we want to remove SNMP from our network

Sample Size = 376

Potential Benefits

Figure 22 identifies why network teams are looking at streaming telemetry. They perceive reliable data collection as the biggest opportunity. They believe a streaming option is less prone to data collection challenges than SNMP, which can experience polling errors.

FIGURE 22. REGARDLESS OF YOUR PLANS FOR USING IT, WHAT DO YOU THINK IS MOST VALUABLE ABOUT STREAMING NETWORK TELEMETRY?



Data granularity and data extensibility were secondary benefits, but successful network operations teams were more likely to cite them as top opportunities. Granularity, extensibility, and improved tool scalability were more interesting to multi-cloud enterprises. Members of network engineering teams were also enthusiastic about data granularity.

"Streaming telemetry offers high-resolution data sent in a way that isn't doable with SNMP," said an IT tools architect at a Fortune 500 media company. "It's also intelligent. You can have it push data when certain changes are detected."

Sample Size = 406, Valid Cases = 406, Total Mentions = 955

Synthetic Network Traffic

Synthetic network traffic monitoring tools have emerged as useful solutions for understanding network performance in hybrid infrastructure environments where IT organizations don't have administrative control of all aspects of digital architecture, such as internet-based WAN connectivity, SaaS applications, and public cloud services. Synthetic traffic can observe performance conditions by measuring loss, latency, and jitter on a hop-by-hop and end-to-end basis. Some synthetic monitoring tools will provide deeper visibility with additional capabilities, such as simulated application transactions.

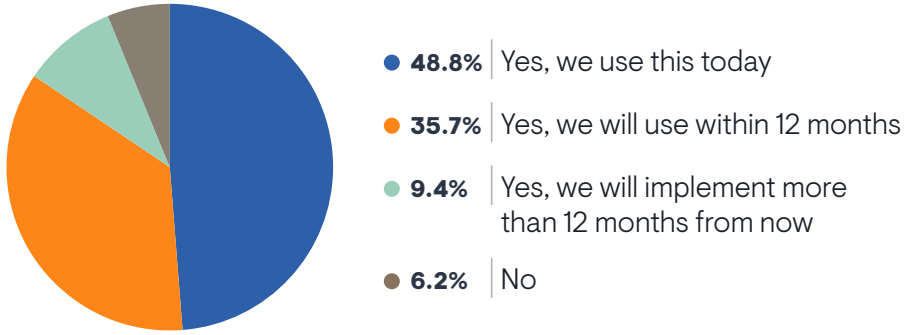
49% of organizations are using a synthetic network monitoring tool today.

Adoption is High

Figure 23 reveals that nearly 49% of organizations are using a synthetic network monitoring tool today. In 2022, adoption was at 48%. Only 6% have no current plans to adopt synthetic monitoring solutions. Successful network operations teams were more likely (62%) to use it today.

"We were looking at it and decided not to do it because it is too cost-prohibitive," said a network engineer with a Fortune 500 aerospace and defense company. "We're going to come back next year and look at it again."

FIGURE 23. IS YOUR NETWORKING TEAM INTERESTED IN USING MONITORING TOOLS THAT GENERATE AND ANALYZE SYNTHETIC NETWORK TRAFFIC?



Sample Size = 406

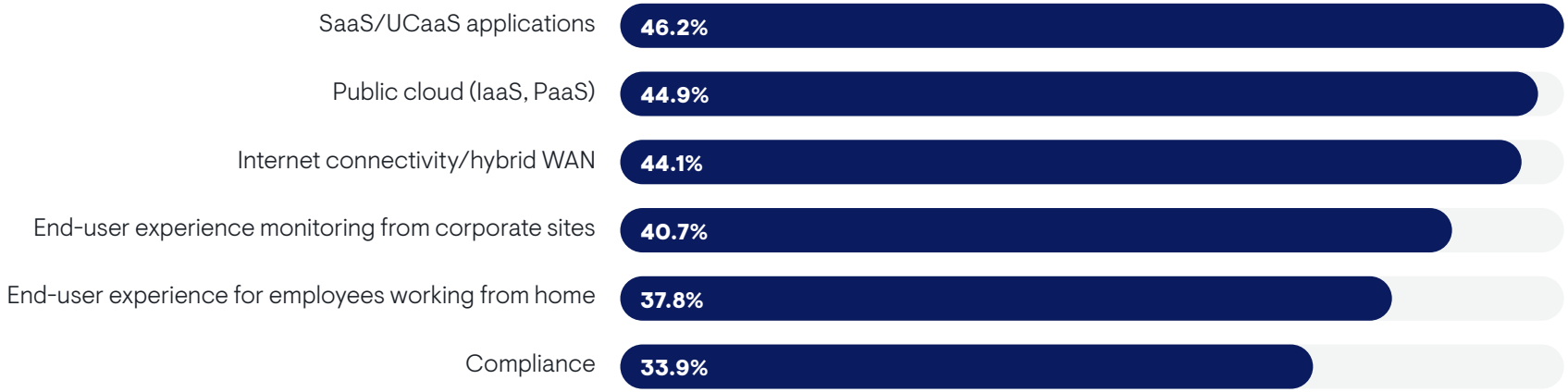
Drivers of Interest

Network teams are using synthetic network monitoring primarily for observability of SaaS applications, public cloud services, and internet-based WAN connectivity, as **Figure 24** details. Successful network operations teams revealed internet observability as their primary driver.

"Basically, we're trying to figure out what's talking to what and how often," said an IT operations manager with a very large government agency. "It shows us how the network flows and does discovery to a certain extent."

End-user experience from corporate sites and remote workers' home offices are secondary use cases. Multi-cloud enterprises were more likely to cite internet connectivity as a driver, while organizations that use only one cloud provider were more focused on end-user experience from corporate sites. Organizations that had fully implemented a SASE solution were more likely to cite end-user experience from both corporate sites and remote workers' homes as drivers.

FIGURE 24. WHICH OF THE FOLLOWING ARE DRIVING YOUR NETWORKING TEAM'S INTEREST IN SYNTHETIC NETWORK MONITORING?

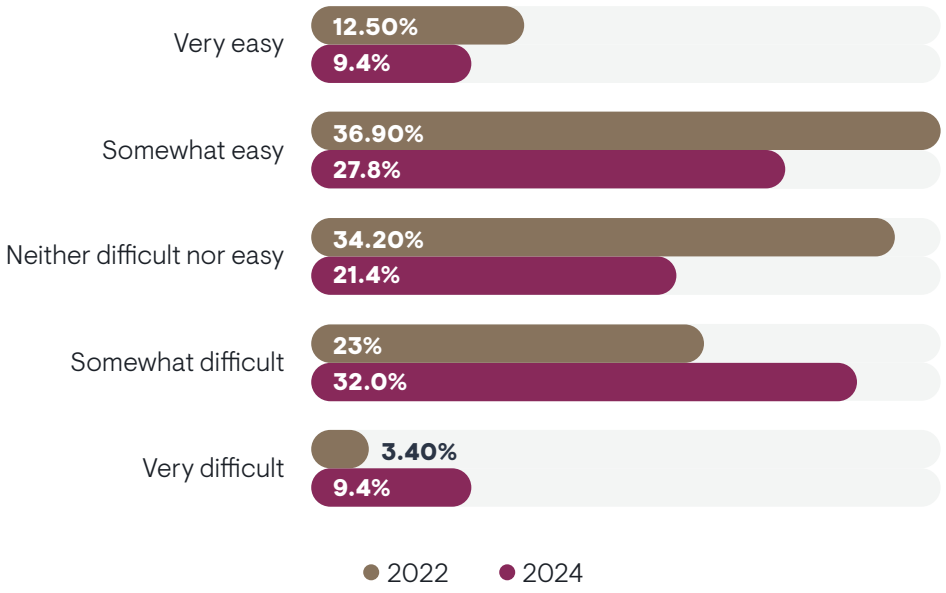


Sample Size = 381, Valid Cases = 381, Total Mentions = 943

Megatrend #1:
Hiring Networking Personnel is Getting Harder

In the 2022 version of this report, EMA asked respondents whether their IT organizations found it easy or difficult to hire and retain personnel with networking expertise. This year, we repeated the question. **Figure 25** reveals a worsening trend. In 2022, only 26% believed that it was somewhat to very difficult to hire networking pros. This year, that number rose to 41%.

FIGURE 25. DOES YOUR ORGANIZATION FIND IT DIFFICULT OR EASY TO FIND, HIRE, AND RETAIN PERSONNEL WITH NETWORK TECHNOLOGY EXPERTISE?



Sample Size: 2024=406, 2022=409

"I've been surprised with the high quality of the talent pool and how diverse it is," said a network engineer with a Fortune 500 aerospace and defense company. "But it seems like a hot job market and a lot of people have declined our offers because of pay. We've been underbidding salaries. One guy declined on the day he was supposed to start because he had a better offer."

"I feel pretty good about hiring," said a network engineering director for a large insurance company. "If someone were to leave, I feel like I have a solid personal network for hiring a replacement. I also have a network of recruiters that I've worked with."

The largest companies in EMA's survey (10,000 or more employees) reported the most trouble with hiring, with 52% reporting that it was somewhat to very difficult. Multi-cloud enterprises also struggled with hiring. Our analysis of the data reveals that difficulty with hiring networking experts correlated strongly with less overall network operations success.

Difficulty with hiring networking experts correlated strongly with less overall network operations success.

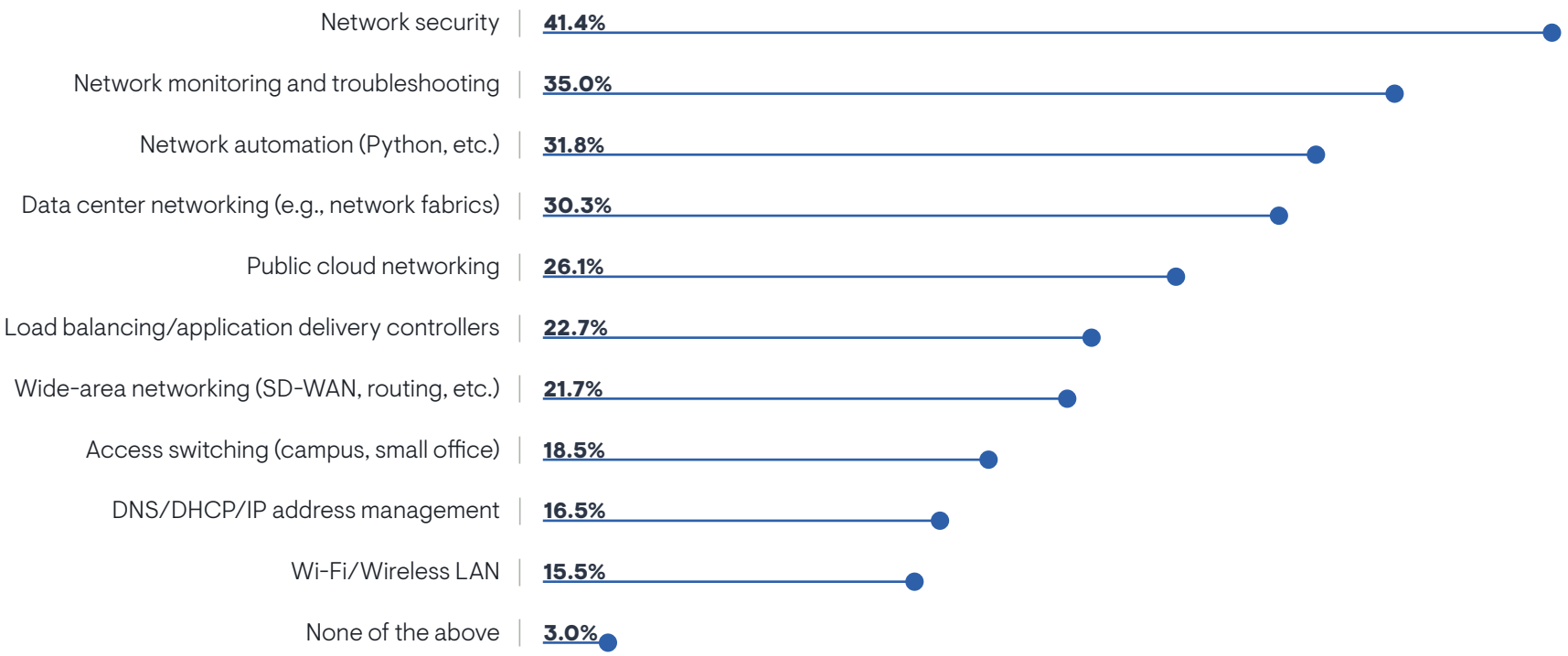
Technical Skills that are Scarce

Figure 26 reveals the skills that IT organizations struggle to find in new hires. Network security know-how is the scarcest and it can make or break an organization. Respondents who reported problems with hiring network security experts also reported less success with network operations.

"Network security is hard to hire for," said an IT operations manager with a very large government agency. "Those people tend to be mercenaries."

Network monitoring and troubleshooting, network automation, and data center networking are secondarily hard to find. Members of network engineering, DevOps, and IT tool engineering teams were more likely to perceive problems with finding network automation experts. Small and midsized enterprises (fewer than 10,000 employees) reported more difficulty with finding data center networking experts.

FIGURE 26. WHICH OF THE FOLLOWING NETWORKING SKILLS ARE THE MOST DIFFICULT FOR YOUR ORGANIZATION TO FIND IN NEW HIRES?



Sample Size = 406, Valid Cases = 406, Total Mentions = 1,065

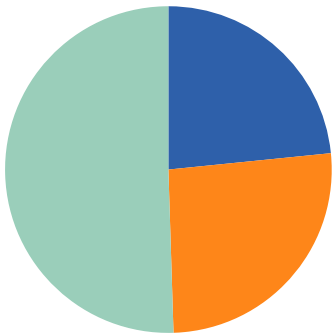
Megatrend #2:
Adapting Network Operations to the Cloud

EMA research has consistently found that the migration of applications and data to public cloud providers has significantly disrupted network operations by reducing the network team's visibility into and control over networks. This section explores the issue in detail.

Cloud versus Data Center

Figure 27 reveals how many enterprises have moved into the public cloud. Only 23% rely exclusively on private infrastructure, such as on-premises or colocation data centers. Slightly more are 100% reliant on the public cloud, while more than half use both. Large enterprises (10,000 or more employees) were the least likely to be exclusively in the cloud. Instead, they tended to rely on a mix of data centers and cloud services.

FIGURE 27. WHICH OF THE FOLLOWING BEST DESCRIBES THE INFRASTRUCTURE THAT HOSTS YOUR ORGANIZATION'S APPLICATIONS AND DATA?



- **23.4%** 100% private infrastructure, such as on-premises data centers or colocation data centers
- **26.1%** 100% public cloud, such as infrastructure as a service (IaaS) and platform as a service (PaaS)
- **50.5%** A mix of private infrastructure and public cloud (i.e., hybrid environment)

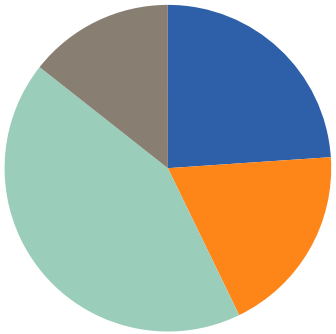
Sample Size = 406

Network operations success correlated more with exclusive use of private infrastructure or exclusive use of cloud services. Less successful organizations tended to use a mix of both. This pattern reflects the fact that hybrid infrastructure is inherently more complex than using a homogeneous approach to infrastructure.

Multi-Cloud Adoption

Figure 28 reveals how many organizations are using more than one cloud provider, which adds operational complexity and drives a need for multi-cloud networking solutions. More than 56% of companies have multi-cloud environments and typically two or three different cloud providers. Only nine respondents claimed to have three or more.

FIGURE 28. NUMBER OF CLOUD PROVIDERS USED



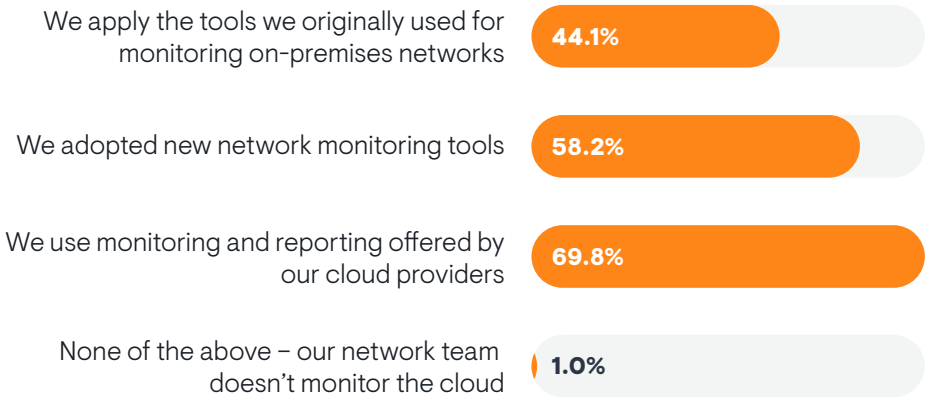
- **23.40%** None
- **18.47%** One
- **41.87%** Two
- **14.04%** Three
- **0.02%** Four or more

Cloud Network Monitoring

99% of network teams within enterprises that use the cloud are monitoring and troubleshooting cloud networks.

In the early days of public cloud services, network operations professionals often told EMA that they did not try to manage cloud networks. Their monitoring tools could not collect telemetry from the cloud and cloud teams often discouraged network teams from touching the cloud at all, viewing them as dinosaurs that would only get in the way. More recently, things changed. **Figure 29** reveals that among enterprises that use public cloud services, 99% of network teams within enterprises that use the cloud are monitoring and troubleshooting cloud networks.

FIGURE 29. WHAT DOES YOUR NETWORK TEAM USE TO MONITOR AND TROUBLESHOOT NETWORK ISSUES IN THE PUBLIC CLOUD?



Sample Size = 311, Valid Cases = 311, Total Mentions = 538

The most popular approach to cloud network monitoring is the use of the tools and reporting that individual cloud providers offer natively. In multi-cloud environments this is less ideal, given that they will struggle to get an end-to-end view of multi-cloud network performance. In fact, respondents from multi-cloud enterprises were more likely to select all three options in the chart, including the use of new tools and the use of incumbent tools that were originally designed to monitor on-premises networks.

"I see a lack of holistic visibility in the cloud," said a network security architect at a Fortune 500 cybersecurity company. "It's hard to have a single pane of glass when you're looking at various systems."

Among new monitoring systems, EMA finds that many enterprises have adopted synthetic network monitoring tools, which are often capable of revealing loss, latency, and jitter across multiple hops within a cloud provider's environment. Meanwhile, among those that apply on-premises tools, many network teams have started collecting cloud metrics with their SNMP-based monitoring tools and passive traffic monitoring tools.

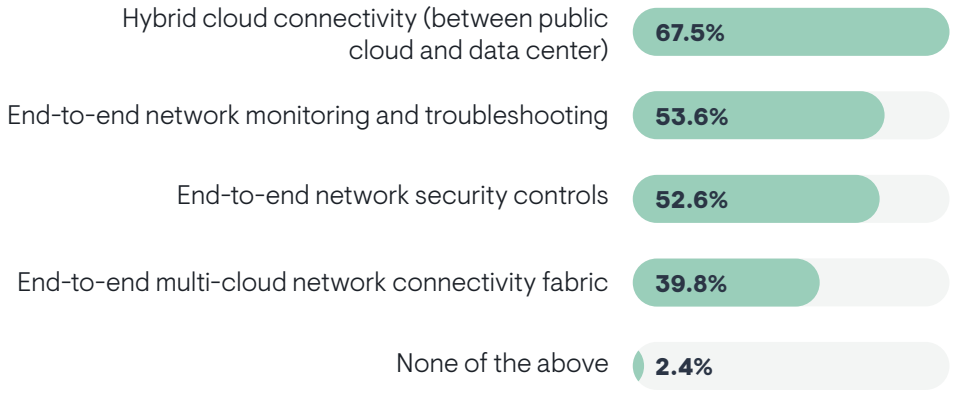
Engagement with Hybrid Multi-Cloud Networking Solutions

Overall, 289 participants in this research reported having at least one of the following environments:

- A combination of private infrastructure (e.g., data centers) and public cloud
- Multiple public cloud providers

Figure 30 reveals the kinds of steps these organizations are taking to standardize network infrastructure and operations across these hybrid and multi-cloud architectures. First, nearly 68% are trying to establish hybrid cloud connectivity between public and private infrastructure. Interest in hybrid cloud connectivity was higher among multi-cloud enterprises, suggesting that many multi-cloud architectures rely on private infrastructure to anchor their overall digital environment.

FIGURE 30. IS YOUR ORGANIZATION TRYING TO DO ANY OF THE FOLLOWING ACROSS YOUR HYBRID AND/OR MULTI-CLOUD ENVIRONMENT?



Sample Size = 289, Valid Cases = 289, Total Mentions = 624

More than half of them are also trying to establish end-to-end network monitoring and troubleshooting and end-to-end network security controls. Organizations that are more successful with network operations had a stronger affinity for end-to-end monitoring.

Many are also trying to implement an end-to-end multi-cloud network connectivity fabric. Members of IT architecture groups were especially interested in establishing such a fabric.

"Multi-cloud networking is in progress right now," said a network engineer with a Fortune 500 aerospace and defense company. "We want to home VPN users and VPN resources out of regional sites rather than just East Coast and West Coast. I think we're going to have application replication across AWS and Azure on a regional basis."

"Multi-cloud networking is in progress right now," said a network engineer with a Fortune 500 aerospace and defense company.

Megatrend #3:
SASE Introduces Operational Challenges

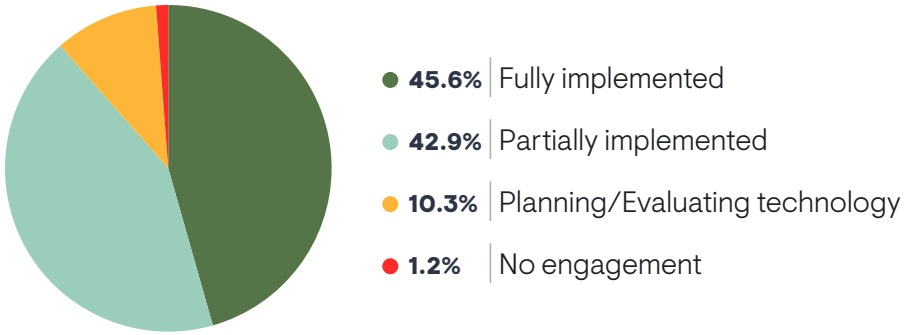
SASE is the next wave of wide-area network (WAN) transformation. SASE is an architecture that integrates SD-WAN with cloud-delivered security services, such as firewalls, secure web gateways, cloud application security brokers, and zero trust network access. EMA research previously established that 99% of enterprises are engaged with SD-WAN today and that many are now evolving that SD-WAN implementation into a SASE architecture.[1]

Nearly 46% of organizations in this research have a fully implemented SASE solution.

SASE Adoption

Figure 31 reveals that nearly 46% of organizations in this research have a fully implemented SASE solution. Only 1% have no plans to adopt SASE. Organizations that report network operations success were more likely to have completed an implementation.

FIGURE 31. WHAT IS THE STATUS OF YOUR ORGANIZATION'S ENGAGEMENT WITH SASE?



Multi-cloud appears to spur SASE adoption. Respondents who reported that their companies hosted 100% of applications in the public cloud were also more likely to be using SASE today. However, organizations that were using only a single cloud provider were less advanced with SASE.

[1] EMA, "WAN Transformation with SD-WAN: Establishing a Mature Foundation for SASE Success," April 2023.

Sample Size = 406

Operational Pain with SASE

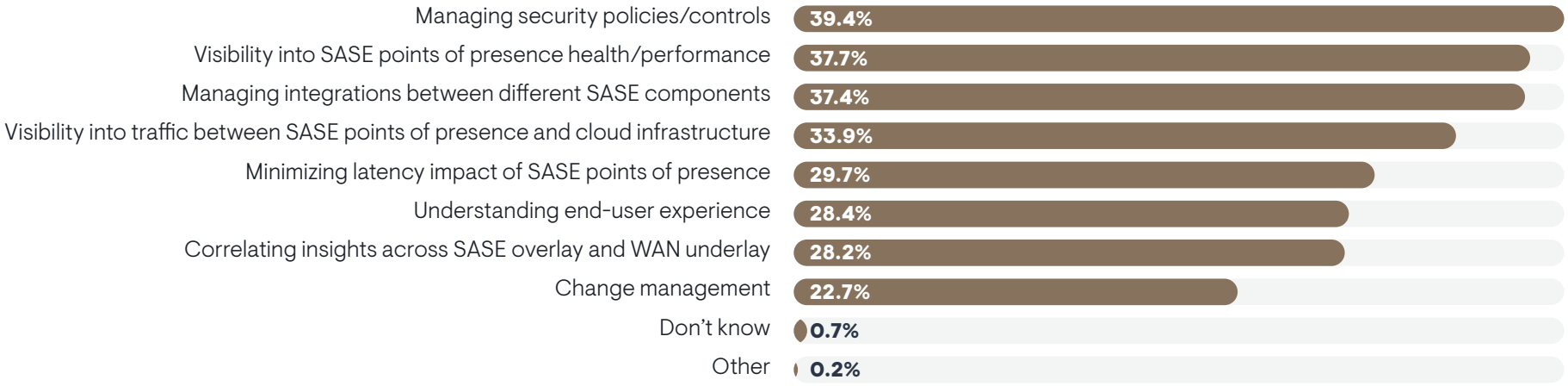
EMA research last year found that only 11% of enterprises believe the transition from SD-WAN to SASE is very easy. **Figure 32** explores the kinds of operational issues that organizations in this research have had with SASE. There are three primary challenges:

1. Managing security policies and controls
2. Visibility into SASE points of presence health and performance
3. Managing integrations between different SASE components

"Things have changed drastically since we implemented SASE," said a network security architect with a Fortune 500 cybersecurity company. "Users are proxied through these policy nodes [SASE PoPs] and that makes troubleshooting a little different. It's hard because we're not looking at things from the laptop to the application. It's really about looking at things from the SASE node to wherever your user is going."

Visibility into traffic between SASE points of presence and cloud infrastructure is prominent in part due to the fact that such traffic is encrypted, which exacerbates this issue. Organizations that struggle to hire skilled networking personnel were more likely to complain about this visibility, as well as challenges with managing security policies and controls.

FIGURE 32. WHAT DO YOU FIND MOST CHALLENGING ABOUT MANAGING AND MONITORING SASE TECHNOLOGY?

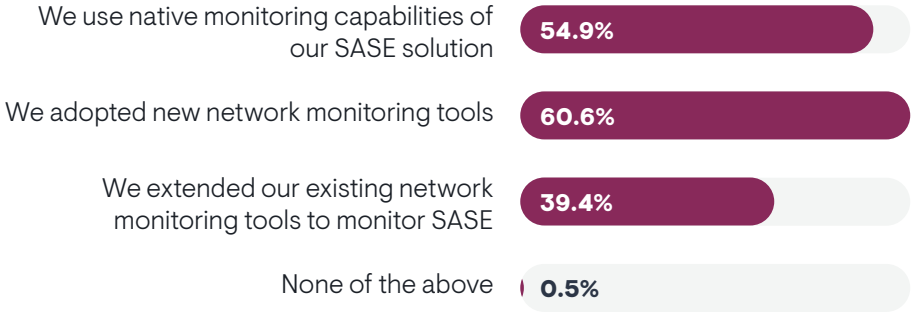


Sample Size = 401, Valid Cases = 401, Total Mentions = 1,036

SASE Observability

SASE solutions typically offer native observability capabilities for monitoring and troubleshooting. However, many IT organizations lean on third-party tools for SASE observability. **Figure 33** shows that only 55% are using or planning to use native SASE monitoring capabilities. However, those who do use native SASE monitoring tools are more likely to report complete success with overall network operations.

FIGURE 33. HOW DOES YOUR ORGANIZATION MONITOR OR PLAN TO MONITOR THE HEALTH AND PERFORMANCE OF ITS SASE SOLUTION?



Sample Size = 401, Valid Cases = 401, Total Mentions = 623

Nearly 61% will adopt new network monitoring tools to address SASE visibility. More than 39% will extend their existing tools. Technical personnel were less likely to perceive plans to extend incumbent tools to SASE monitoring. Respondents who reported that their SASE implementations are complete were more likely to select all three options on this chart.

"We're running all these different kinds of network tests, trying to run some kind of simulated traffic to find out if we're using the right paths," said an IT tools architect at a Fortune 500 media company. "We have to run them frequently to get a baseline of environments. That takes time and investment. I'm not concerned that we can't do it. It's more about having the right focus and setting it up. It's a complex deployment."

Megatrend #4:
AI/ML-Driven Network Management is Mainstream

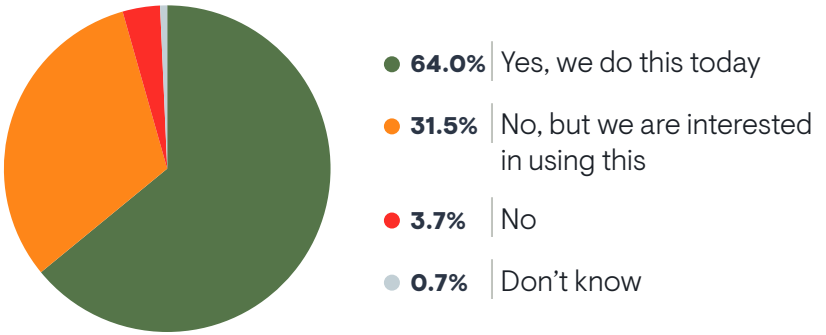
64% of IT organizations have adopted AI/ML-driven network management already.

Network infrastructure vendors and network management vendors are increasingly investing in artificial intelligence and machine learning (AI/ML) technology to enhance and automate their solutions. EMA research found strong interest in applying AI/ML to network management for several years now. This year's Megatrends research found that 64% of IT organizations have adopted AI/ML-driven network management already, as **Figure 34** indicates. Earlier in this report, we also found that such technology is a high priority for 28% of organizations.

Successful network operations teams are more likely to use it today. AI/ML users also reported more effective monitoring of cloud networks and SASE solutions. Smaller companies (fewer than 10,000 employees) are moving more quickly, as are multi-cloud enterprises.

AI/ML appears to make network management tools stickier in an organization. Respondents who use it today are less open to replacing their tools with new solutions.

FIGURE 34. DOES YOUR ORGANIZATION USE ANY AI/ML-BASED FEATURES DELIVERED BY YOUR NETWORK MANAGEMENT AND NETWORK INFRASTRUCTURE VENDORS?



Sample Size = 406

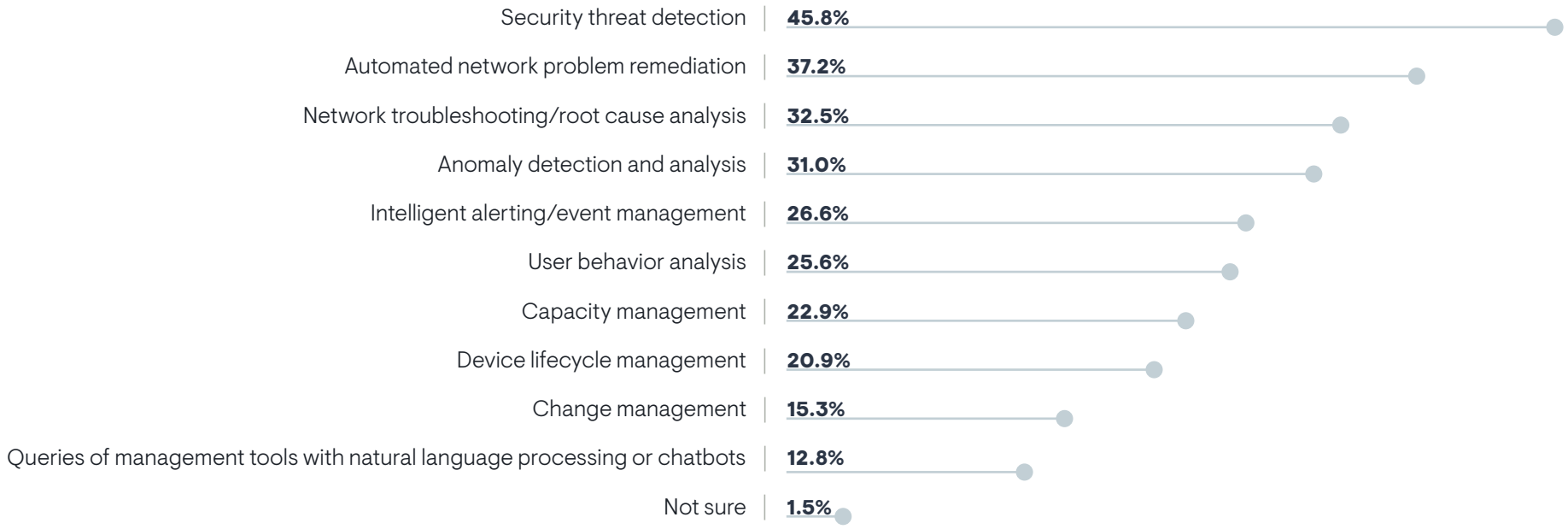
AI/ML Network Management Use Cases

Security threat detection is the most interesting use case for AI/ML-driven network management today, as shown in **Figure 35**. IT executives were the most engaged with this use case.

Many are also interested in automated network problem remediation, automated network troubleshooting, and anomaly detection and analysis. Smaller companies (500 to fewer than 2,499 employees) expressed the most interest in auto-remediation of network issues. Capacity management was a lower priority, but network engineering teams in the survey selected it as a top use case.

"Our primary use case for AI is event and noise reduction," said an IT tools architect at a Fortune 500 media company. "We've been using human-built rules to reduce millions of alerts by 90%. Getting to 95% or 99% is very hard. By applying machine learning to it, we see examples in which our system will learn and identify patterns and use those to correlate data sets. We keep maturing the model and we are getting it from 95% to 99%."

FIGURE 35. TO WHICH GENERAL NETWORK MANAGEMENT TASKS DO YOU MOST WANT TO APPLY AI/ML?



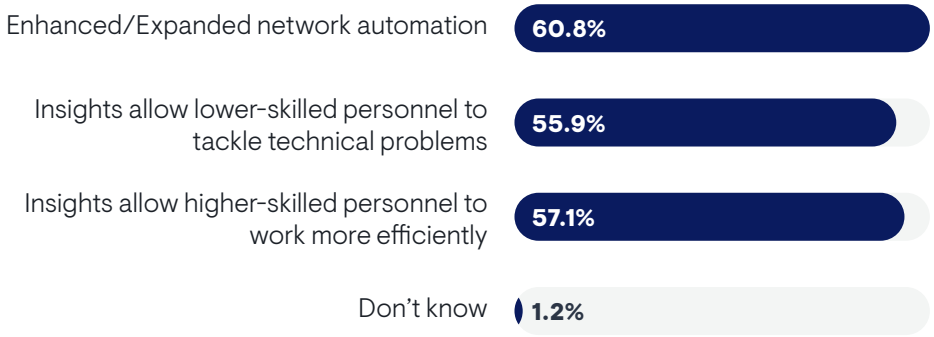
Sample Size = 406

AI/ML Impact on Network Operations

EMA asked respondents to reveal how they think AI/ML technology will enhance network operations. **Figure 36** reveals that nearly 61% believe it will enhance or expand network automation. More than 57% believe it will allow higher-skilled networking personnel to work more efficiently. IT executives especially believe this is an opportunity. Multi-cloud enterprises especially recognize this opportunity.

Nearly 56% believe AI will allow lower-skilled personnel to tackle technical problems that they previously couldn't. This benefit correlated directly with network operations success. Also, organizations that report fewer challenges with hiring skilled networking personnel were more likely to recognize this benefit. EMA suspects that use of AI/ML for this purpose is reducing their need to hire skilled personnel, which allows them to avoid the hiring challenges that other organizations are encountering.

FIGURE 36. HOW MIGHT THE APPLICATION OF AI/ML TECHNOLOGY TO NETWORK MANAGEMENT IMPROVE THE WAY THAT YOUR NETWORK TEAM WORKS?



Sample Size = 406, Valid Cases = 406, Total Mentions = 711

Conclusion

After years of decline, network operations teams have turned things around and found a way to improve success. Even more encouraging, much of the enthusiasm is coming from the trenches. It's the network admins, engineers, and architects who told EMA that things have improved.

It is hard to say definitively what is driving this rebound. Some of the underlying problems remain. Network management toolsets remain bloated, fragmented, and noisy. IT organizations are struggling more than ever to hire skilled network engineers and architects.

However, we see some common patterns. Successful network teams are:

- Replacing ineffective network management tools
- Adopting synthetic network monitoring to improve observability, especially internet visibility
- Focusing on improving network security at all stages of network operations
- Embracing AI and ML technology to optimize tools, automate operations, and enable lower-skilled personnel to take on more responsibility
- Modernizing their networks with SASE and multi-cloud networking solutions

Network teams appear more aligned with current technology priorities today than they have been in the past. Before 2022, the cloud was an afterthought for networking teams. Now, it's their core priority. They are aligning with public cloud, SaaS applications, and DevOps and CI/CD paradigms.

EMA hopes that network operations success continues to rebound from the declines we observed over the last several years. We also hope this report offers some guidance to IT leaders on how to make that happen.

About Enterprise Management Associates, Inc.

Founded in 1996, Enterprise Management Associates (EMA) is a leading IT analyst research firm that specializes in going "beyond the surface" to provide deep insight across the full spectrum of IT management technologies. EMA analysts leverage a unique combination of practical experience, insight into industry best practices, and in-depth knowledge of current and planned vendor solutions to help its clients achieve their goals. Learn more about EMA research, analysis, and consulting services at **www.enterprisemanagement.com** or follow EMA on **X** or **LinkedIn**.

2770 Arapahoe Road, Ste 132 - 544, Lafayette, CO 80026 +1 303.543.9500 www.enterprisemanagement.com

4407.052024