EMA
IT & DATA MANAGEMENT RESEARCH, INDUSTRY ANALYSIS & CONSULTING

Prepared for:

alkira BLUECAT BROADCOM IBM kentik
LiveAction netAlly NETSCOUT NOKIA Progress

Network Management Megatrends 2024:

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

May 2024 EMA Research Report
By **Shamus McGillicuddy**, Vice President of Research
Network Infrastructure and Operations

Table of Contents

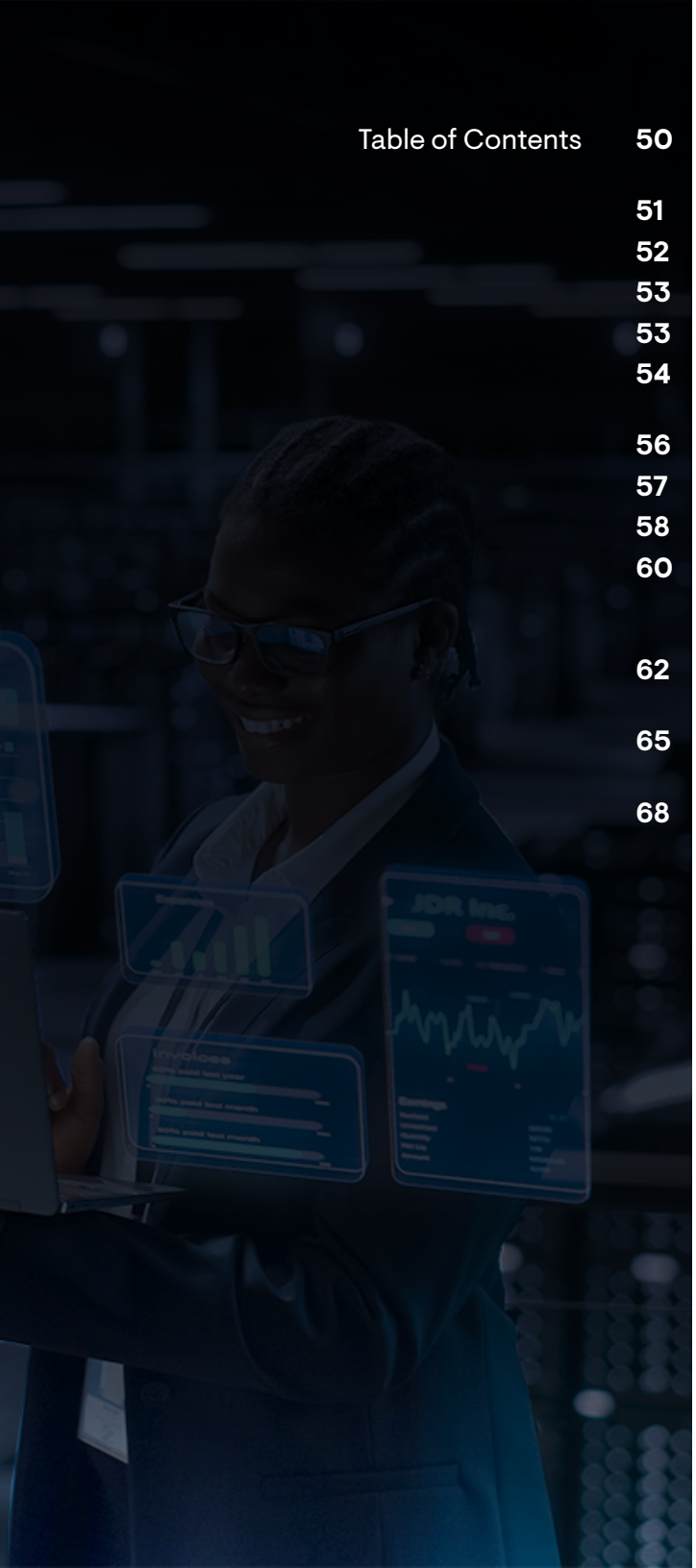


Table of Contents

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.

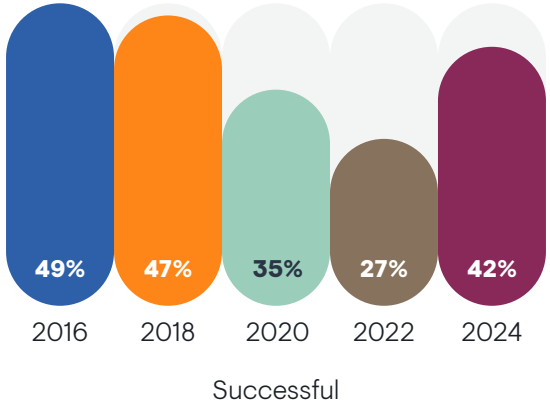
In recent years, EMA observed a concerning negative trend in self-assessments of network operations success. From 2016 to 2022, the percentage of survey respondents who believed their network teams were completely successful with monitoring and managing networks declined from 49% to 27%. EMA attributed 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

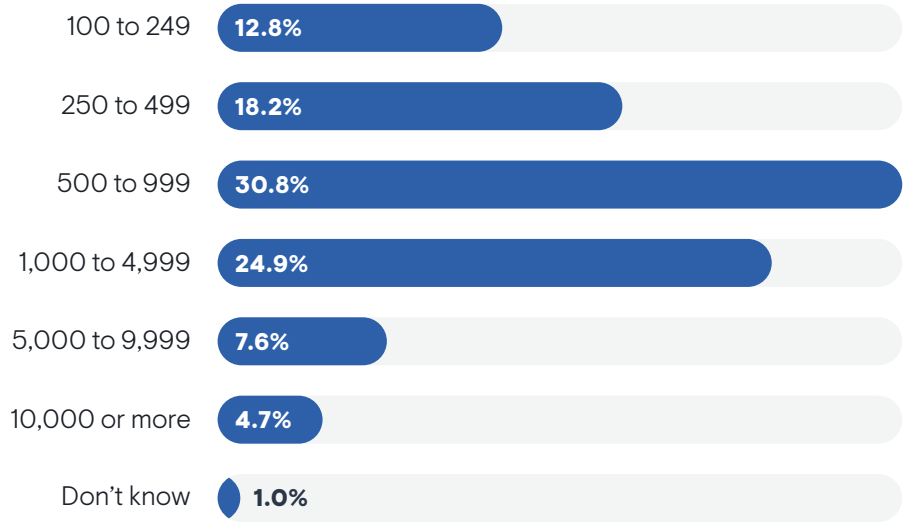
Location

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

To qualify for EMA's survey, respondents had to work for an organization with at least 1,000 employees that earned at minimum $50 million in annual revenue. EMA targeted traditional enterprise IT organizations, so we excluded certain industries, including communication service providers, cloud providers, and providers of IT products and services. Finance/insurance, manufacturing, health care, and retail/wholesale/distribution combined to represent more than half of the respondents in this research.

Figure 3 reveals the size of the networks the participants in this study managed. Respondents had to have at least 100 network devices in their networks. In fact, 37.2% were managing a network with 1,000 devices or more.

FIGURE 3. HOW MANY NETWORK DEVICES DOES YOUR ORGANIZATION CURRENTLY MANAGE, SUCH AS SWITCHES, ROUTERS, SD-WAN APPLIANCES, LOAD BALANCERS, WI-FI ACCESS POINTS, AND NETWORK SECURITY APPLIANCES?



Sample Size = 406

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
- Network pros believe they could eliminate 53% of network outages and performance problems with better network management tools
- 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
- Field operations remain prominent: 60% of network teams send a technician into the field with a portable analysis tool at least three times a month
- 65% of network teams prefer to consume their management tools as a SaaS service
- 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

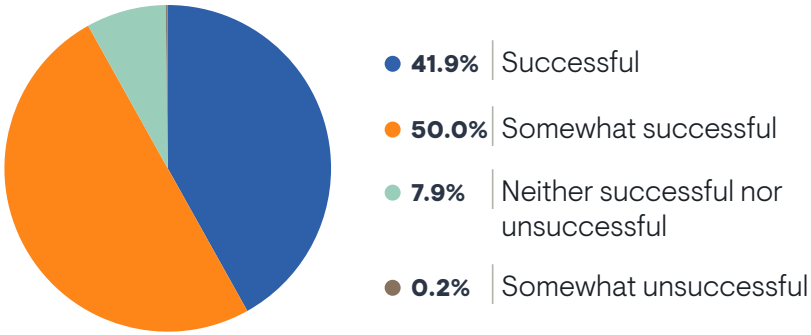
Network Operations Outcomes

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 4** reveals this dynamic.

FIGURE 4. OVER THE PAST YEAR, HOW WOULD YOU RATE THE SUCCESS OF YOUR NETWORK OPERATIONS ORGANIZATION?



"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.

Sample Size = 406

Technical personnel were more enthusiastic about network operations success, which is a reversal of what EMA has seen in the past. Usually, subject matter experts are more pessimistic and IT executives are the optimists. On the flipside, members of network engineering teams and IT service management were also pessimistic about success. Enthusiasm was more prevalent in cloud, DevOps, data center operations, and network operations teams.

"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 that for the size that we are and as many things as we are trying to do, it's pretty decent," said an IT operations manager with a very large government agency. "We're into measuring everything, measuring end-user experience, measuring hops between places. It gets to the point where a decent amount of our traffic is simply from measuring."

Hybrid cloud architecture adds complexity. Companies that have a mix of public cloud and private data center infrastructure are reporting less overall success than organizations that are cloud-only or data center-only.

We found that less successful network operations teams are more likely than others to be strategically driven by three technical initiatives, suggesting that they are extremely difficult to support:

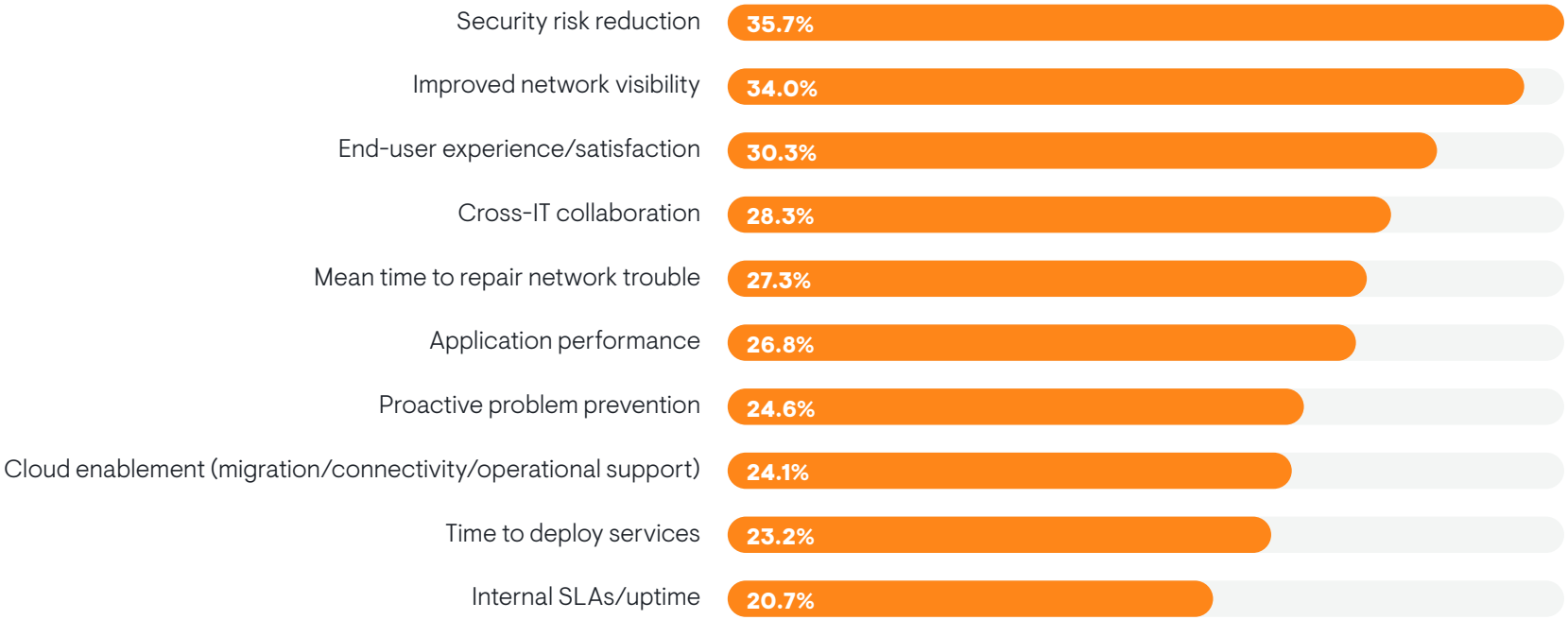
- Cross-domain operations and full-stack observability
- Enterprise AI projects
- Regulatory compliance

Measuring Success

Figure 5 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 5. 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

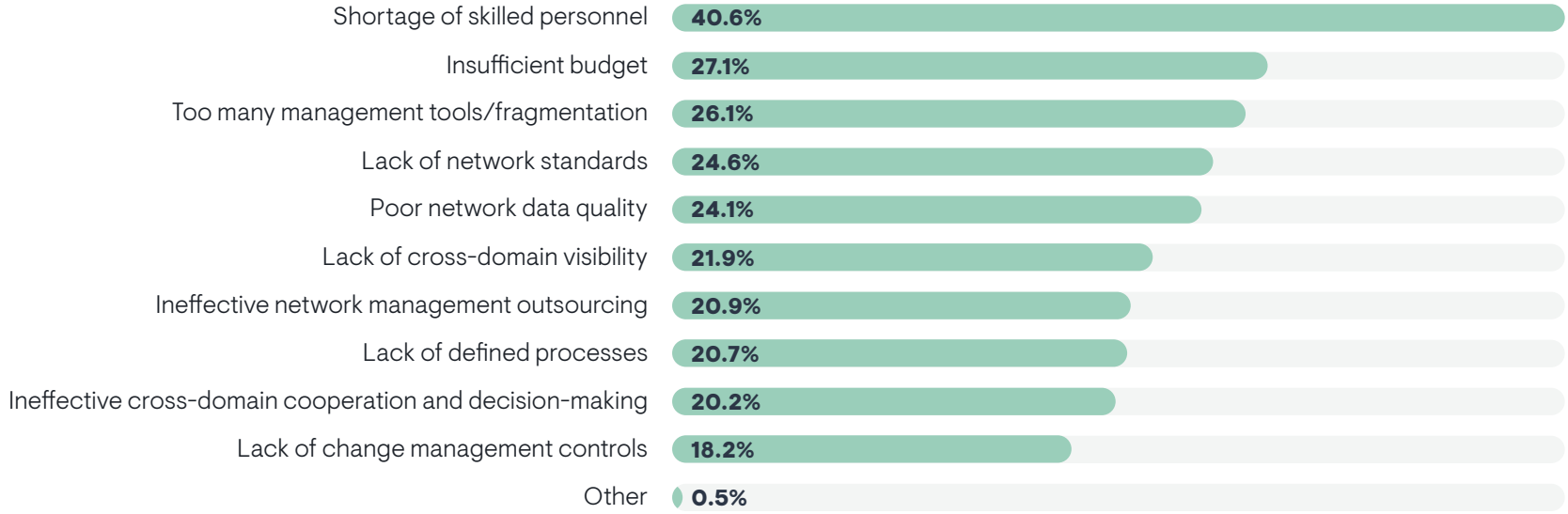
Figure 6 identifies the issues that are challenging network operations success. A shortage of skilled personnel is the main problem by a big margin. In 2022, it was the number-two problem behind network data quality, which dropped to the middle of the pack this time. Respondents who told us that they 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.

"Sometimes, an extra $50,000 in annual spend could make a huge difference, but there isn't always an understanding of that," said a network engineering director for a large insurance company. "I'm good at translating technical stuff into high-level management speak, but even so, there are some investments that makes sense to a network operations person, but they don't make sense to the person who would write the check. IP address management, for example. They told me to just use a spreadsheet without understanding how we do this stuff. So, I took open source software and had one of my guys who is good at programming tweak it. That gets us a solid tool, but a commercial tool would get us from 3.5 out of 5 stars to 5."

FIGURE 6. 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

"Using multiple tools adds to administrative overhead. You might have different inventories in one system versus another," said an IT tools architect at a Fortune 500 media company. "It adds extra costs, too. Users push against consolidation. They have personal favorites. I'm not saying one tool is better than another, but there needs to be a collective decision to select a tool that addresses most of the organization's needs so that we can reduce operational overhead and reduce technical debt. We also have people making decisions like deciding to move everyone into Office 365, which means we have to upgrade our WAN links. So we're struggling with cross-domain decision-making."

Tool fragmentation was a bigger issue for less successful network operations teams. Technical personnel were less concerned with tool bloat than middle management and IT executives. Instead, engineers and other subject matter experts were more challenged by a lack of defined processes and a lack of network standards. Members of DevOps and network operations teams were especially concerned with undefined processes and a lack of standards. A lack of network standards also challenged organizations that rely 100% on the public cloud for hosting applications, which suggests that network standards fell by the wayside as resources migrated from data centers to the cloud.

"People keep adding things to our network, and you need money to expand capacity," said an IT operations manager with a very large government agency. "Then, the government has this thing where they don't like us to have technical debt, but they're not giving us money to buy anything. So we continue to have technical debt."

A network security architect with a Fortune 500 cybersecurity company said things move and change so fast in his company that cross-domain collaboration is breaking down. "Ticket routing has been an issue because we're not sure who is working on what since it all moves so fast. Sometimes, a ticket goes to the wrong place and we have a week or two of delay."

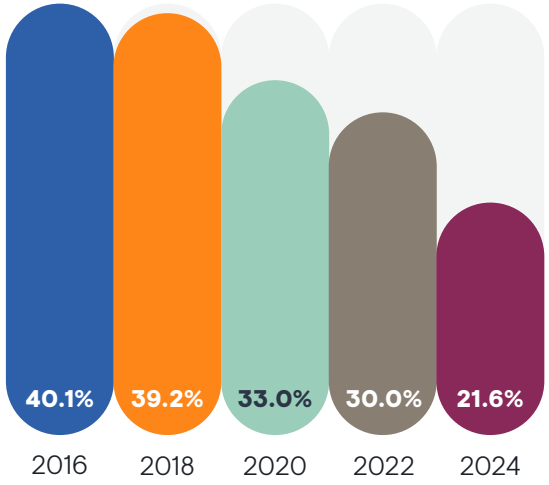
"One of our biggest challenges is understanding the boundaries and the delineation of duties between network operations and network engineering," said a network engineer with a Fortune 500 aerospace and defense company. "Implementing local topologies in the network is an example. That should be engineering, but operations sometimes comes up with things they want to do. And it doesn't meet our standard."

Spotting Trouble

Proactive Detection is Rising

EMA has long asked research participants to estimate how many service problems and outages end users experience and report before network operations can detect them. Over the last eight years, that percentage has declined from 40% to less than 22%, nearly being cut in half, as **Figure 7** reveals. The decline from 2022 to 2024 was especially precipitous, partly explaining why overall network operations success rebounded this year. Reactive troubleshooting is in decline.

FIGURE 7. PLEASE ESTIMATE THE PERCENTAGE OF IT SERVICE ISSUES OR OUTAGES THAT OCCUR IN A TYPICAL MONTH THAT END USERS FIRST RECOGNIZE AND REPORT (AS OPPOSED TO BEING RECOGNIZED FIRST BY YOUR NETWORK OPERATIONS TEAM).



Smaller companies (500 to 2,499 employees) reported a higher rate of reactive troubleshooting. EMA observed that organizations with a higher rate of reactive troubleshooting sent technicians into the field with handheld network testing equipment more often. We'll explore this issue in depth later in this report.

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 8** 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.

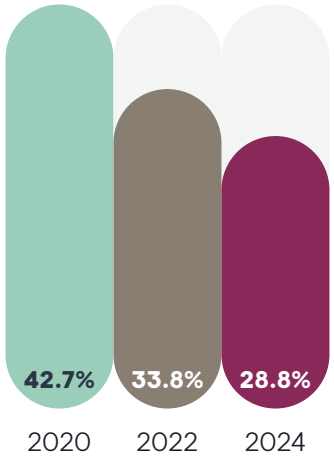
"One of our tools just sends out a lot of white noise, lots of SNMP traps that don't make a lot of sense," said a network engineer with a Fortune 500 aerospace and defense company. "It takes time to tune that."

"A lot of work was done over the last couple years on this," said an IT tools architect at a Fortune 500 media company. "We've been working on alert aggregation, but we still have noise. It's a factor of how much data you want to get out of a system. The more data you get, the more noise increases. We run it through different rule sets to reduce it. We've seen almost a 99% noise reduction in the NOC, partially through human-built rules and through machine learning and AIOps."

Multi-cloud enterprises reported less noise, especially those with four or more providers. Organizations that host at least some applications and data in private infrastructure (data centers or colocation providers) also reported better alerting.

"We have refined and refined and refined it over a period of years," said a network engineering director for a large insurance company. "Now, if we receive an alert, it is something that we should pay attention to. Several years back, it was extremely noisy and alert exhaustion was a real problem."

FIGURE 8. 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

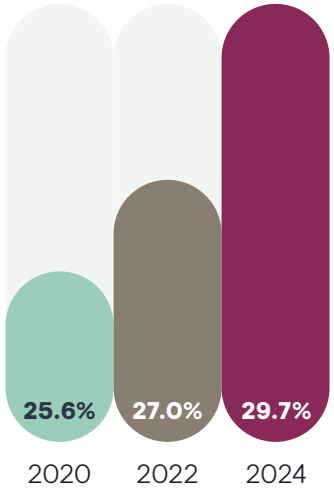
In 2020, EMA began asking Megatrends respondents to estimate the percentage of their network problems that is attributable to a manual administrative error, like a bad configuration change. **Figure 9** reveals that rates of error-driven trouble have been climbing over the last four years, from less than 26% in 2020 to nearly 30% in 2024.

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.

Counterintuitively, more successful network operations teams reported a higher rate of manual errors. This suggests that some network teams have devoted significant resources to improving their ability to detect bad changes and resolve them. While an effective approach to identifying bad changes may make them feel successful, EMA would argue that they would be better off devoting resources to preemptively eliminating bad changes altogether.

FIGURE 9. WHAT PERCENTAGE OF YOUR NETWORK-RELATED PROBLEMS IS CAUSED BY MANUAL ADMINISTRATIVE ERRORS (BAD CONFIGURATION CHANGE, ETC.)?



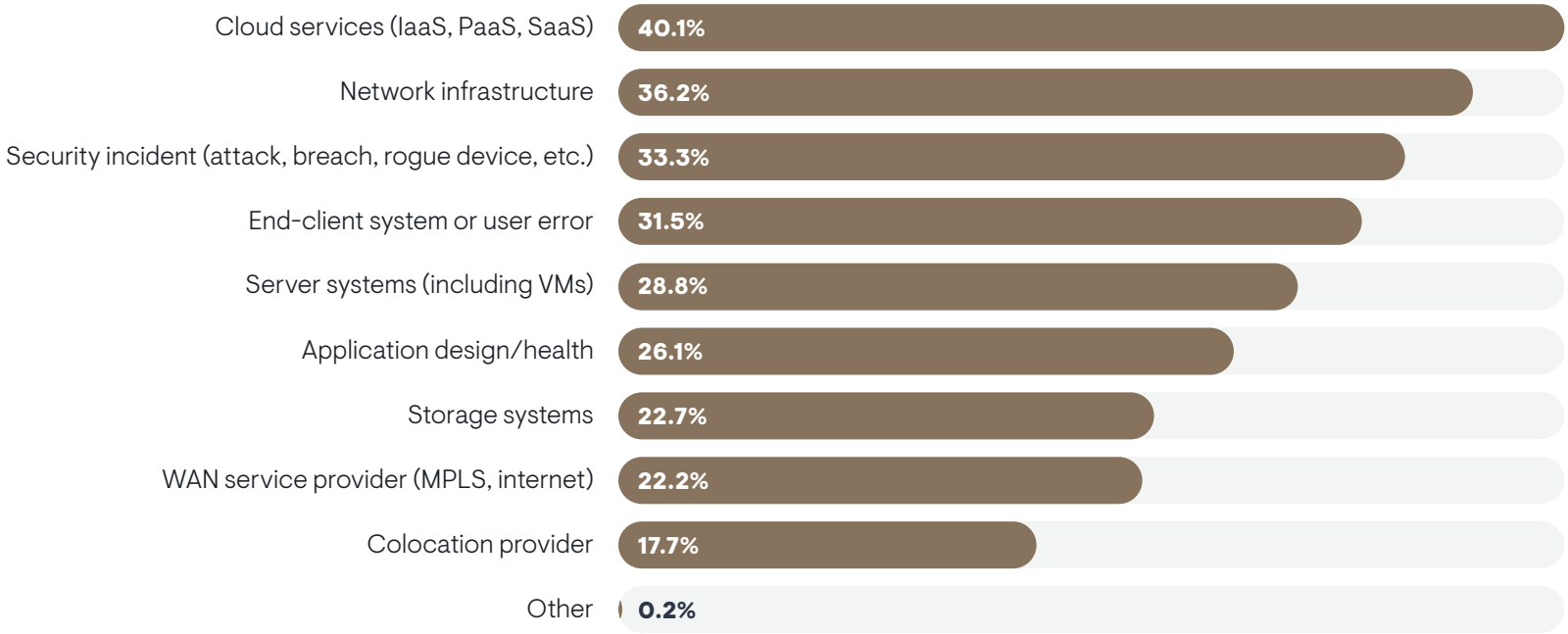
Root Cause Domains of War Room Events

Complex IT service problems often require collaboration across different groups of specialists who work together to isolate and analyze a problem and formulate a resolution. IT organizations often refer to this gathering of subject matter experts as a war room.

Figure 10 reveals the root cause domains of war room activity that pulled in the network team. Cloud services are the biggest culprit, suggesting all of IT operations, not just the networking group, is struggling to optimize cloud observability. SASE also appears to cause trouble here, since organizations that have completed a SASE implementation were more likely to identify the cloud as a problem domain.

Network infrastructure, security incidents, and end-user errors or user device problems were the top secondary root cause domains. Networks are causing more complex service issues in enterprises that have a hybrid cloud environment, using a mix of private infrastructure and public cloud services. WAN providers are a bigger source of trouble for organizations that are cloud-only.

FIGURE 10. THINK ABOUT THE LAST THREE DIFFICULT IT SERVICE PERFORMANCE ISSUES THAT REQUIRED YOUR NETWORKING TEAM TO COLLABORATE WITH OTHER GROUPS. WHICH OF THE FOLLOWING TURNED OUT TO BE THE PRIMARY ROOT CAUSE(S)?



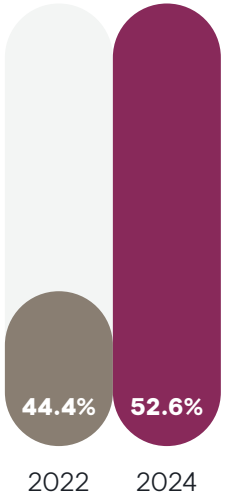
Sample Size = 406, Valid Cases = 406, Total Mentions = 1,051

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 11** 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.

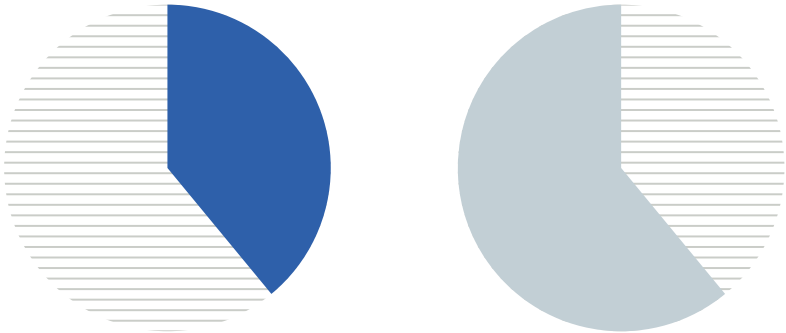
FIGURE 11. WHAT PERCENTAGE OF YOUR NETWORK-RELATED PROBLEMS DO YOU THINK WOULD BE PREVENTABLE WITH BETTER NETWORK MANAGEMENT TOOLS?



Troubleshooting IT Services

Troubleshooting is the true cost center of network operations. When a network problem occurs, networking pros often drop whatever they're doing to fix the issue. Thus, troubleshooting prevents network teams from delivering added value to the business through the execution of strategic projects. **Figure 12** reveals that 39% of a network professional's day is spent on troubleshooting in the average company.

FIGURE 12. IN YOUR ORGANIZATION, WHAT PERCENTAGE OF THE TYPICAL NETWORK OPERATIONS PROFESSIONAL'S DAY IS SPENT TROUBLESHOOTING NETWORK PROBLEMS?



39.0% Network troubleshooting

61.0% All other tasks

Network teams spend more time on troubleshooting in multi-cloud enterprises, suggesting that multi-cloud networks are adding operational complexity.

Network Operations Strategy

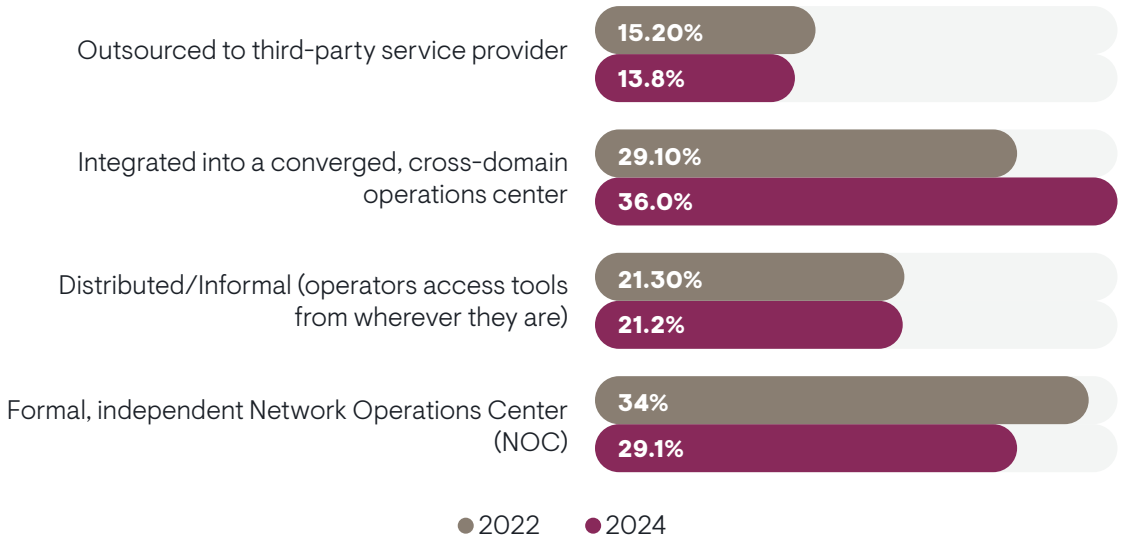
Organizing the Network Operations Function

Figure 13 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."

People who worked in a network engineering or network operations team reported the use of a NOC more often, while people who worked in DevOps or a CIO's suite were more likely to perceive a cross-domain approach. Expanding the borders of digital infrastructure had some bearing on strategy. Organizations that have supplemented on-premises data center infrastructure with infrastructure deployed in a colocation data center provider were more likely to use a cross-domain operations center. Those that hadn't ventured into colocation environments were more likely to have a traditional NOC.

FIGURE 13. WHICH OF THE FOLLOWING BEST DESCRIBES THE WAY IN WHICH YOUR ORGANIZATION PRIMARILY CONDUCTS NETWORK MONITORING AND MANAGEMENT?

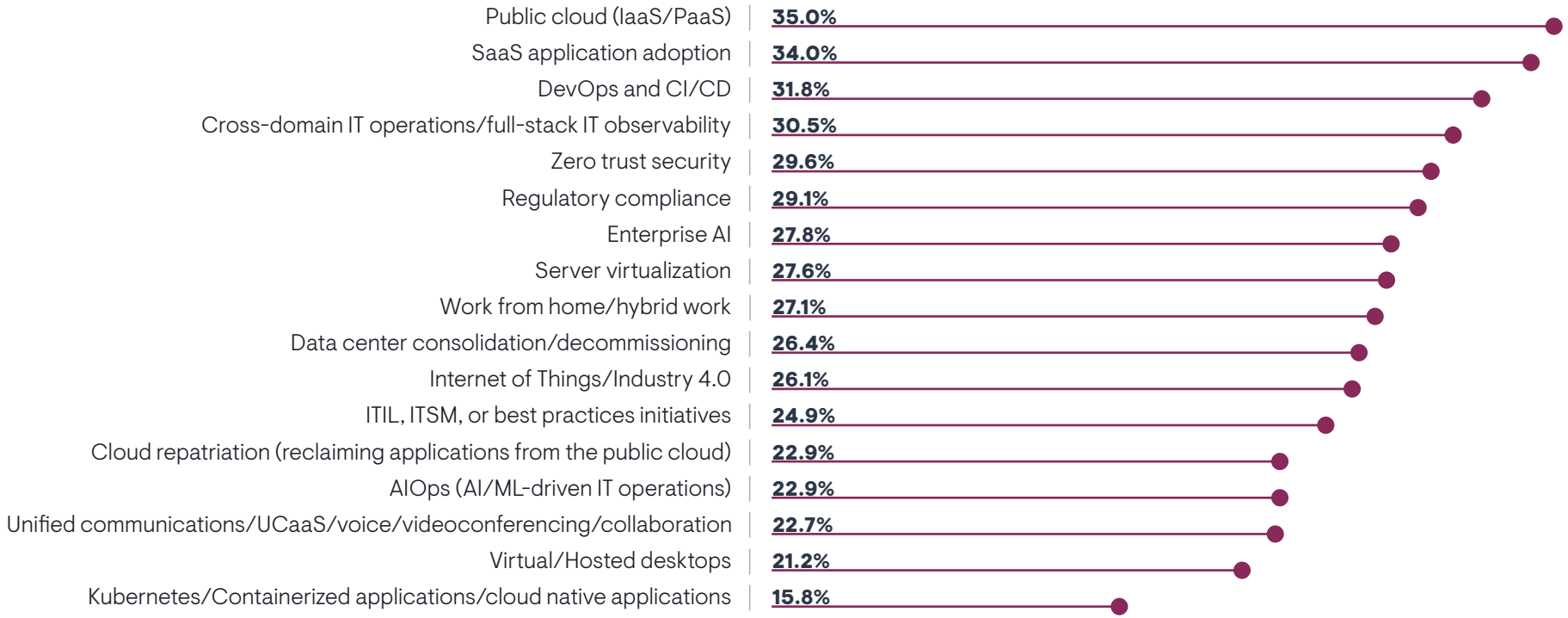


Technical Initiatives that Shape Network Operations

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 14 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 14. 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

EMA made some changes to this question's multiple choice options this year, which may have changed the top three. For instance, we elaborated on "cloud native application platforms" by renaming it "Kubernetes/containerized applications/cloud native applications." This topic dropped from second to last between 2022 and 2024. Meanwhile, we changed "DevOps" to "DevOps and CI/CD," and this initiative rose from eighth to third. This suggests that CI/CD practices are impacting network operations strategies.

Cross-domain IT operations/full-stack observability was also a major driver this year, further reinforcing that network teams are trying to align with cloud and DevOps teams.

Finally, zero trust security is rising in importance. It was the fifth most influential initiative this year compared to thirteenth in 2022. EMA believes zero trust concepts are propagating throughout enterprises and network teams are key players in enablement.

IT executives tended to select more responses to this question, revealing a broader perspective on how network operations are tied to technical initiatives. They were more likely to select public cloud, SaaS, zero trust security, hybrid work, UC and collaboration, and AIOps.

Respondents who work for multi-cloud enterprises were more likely to report AIOps, cloud repatriation, and data center consolidation/decommissioning as influential. Single-cloud organizations were more likely to report ITIL/ITSM as a driver.

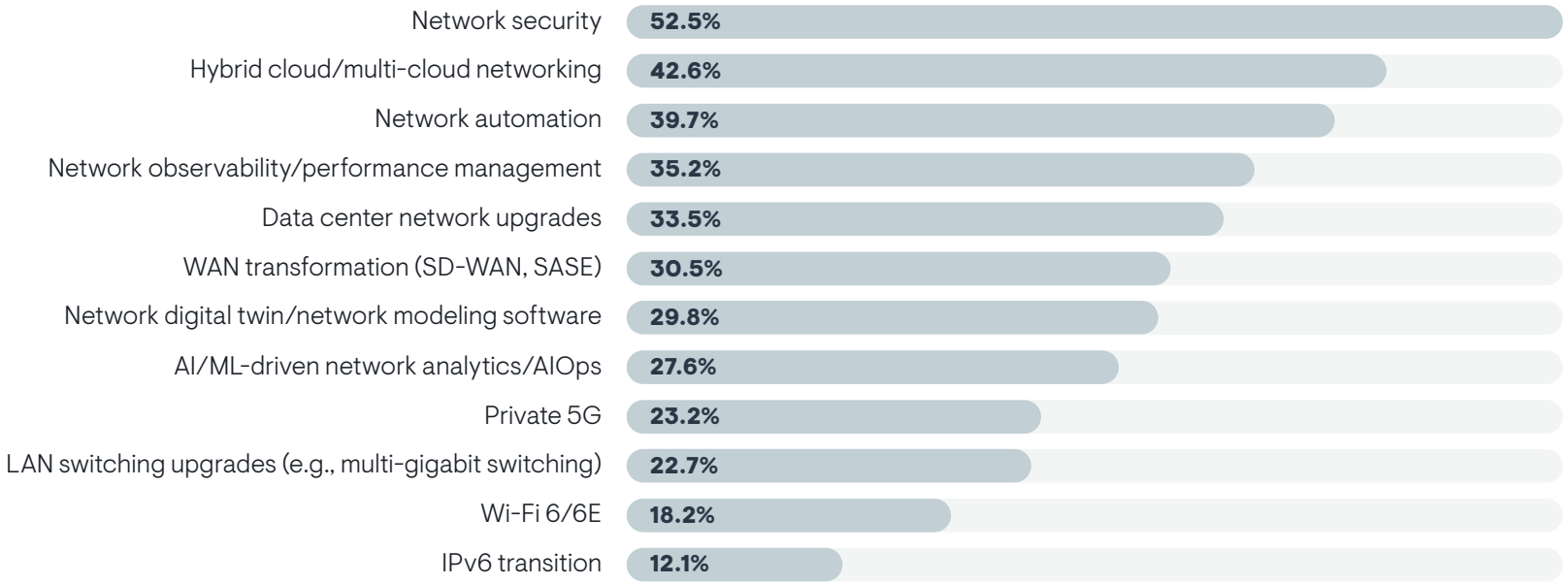
Network Technology Investments and Projects that Shape Operational Priorities

Figure 15 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 15. WHICH OF THE FOLLOWING NETWORKING TECHNOLOGY INITIATIVES/INVESTMENTS ARE HIGH PRIORITIES FOR YOUR ORGANIZATION TODAY?



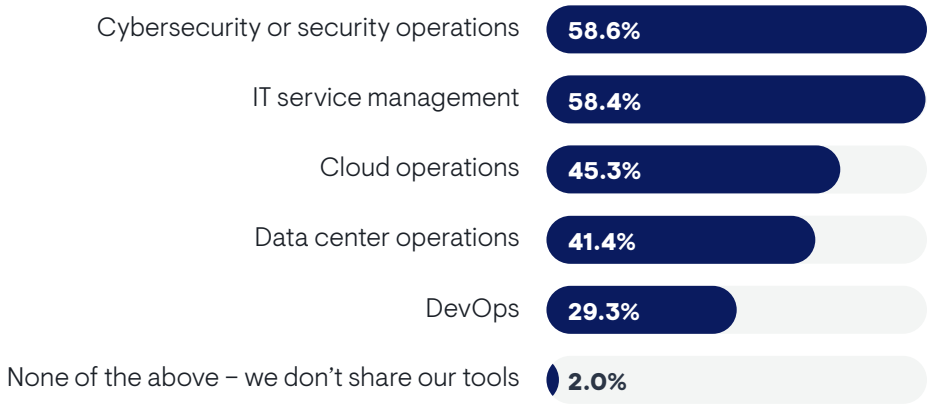
Sample Size = 406

Breaking Down Silos by Sharing Tools

While many organizations in this research have established cross-domain operations centers, network management tools remain highly specialized and require users to have significant networking expertise. Thus, networking pros often limit or curate access to such tools from other parts of the organization. **Figure 16** shows the extent to which these other groups are using network management tools. Most network teams give both the cybersecurity team and the IT service management group access to their tools. However, actual technical personnel (admins, engineers, architects) were less likely to report allowing such access. Executives and middle managers were more likely to perceive this.

Most network teams give both the cybersecurity team and the IT service management group access to their tools.

FIGURE 16. DOES YOUR NETWORK TEAM ALLOW PEOPLE FROM ANY OF THE FOLLOWING GROUPS TO USE ITS NETWORK MANAGEMENT TOOLS?



Sample Size = 406, Valid Cases = 406, Total Mentions = 954

In multi-cloud enterprises, network teams were more likely to share tools with the IT service management group. Organizations that host applications and data both in private data centers and the public cloud were more likely to share network management tools with the security group, which suggests that the security risks of hybrid cloud architecture drive a need for such tool sharing.

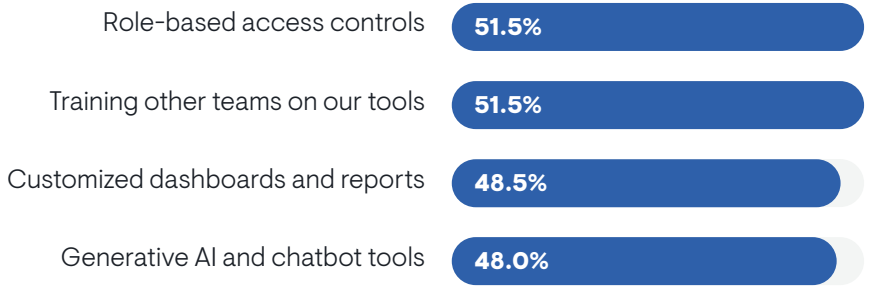
Network teams were less likely to share their tools with cloud operations, data center operations, and DevOps teams. However, data center operations teams in large enterprises (10,000 or more employees) tended to have access to these tools.

Enabling Tool Sharing

Figure 17 reveals how network teams facilitate sharing their tools. More than half are using role-based access controls and taking time to train other teams on their tools. Training is a preference of more successful network operations teams.

Many also build customized dashboards and reports. Others adopt generative AI tools that enable other teams to prompt a tool for information via natural language. Members of network operations teams were more likely to perceive the use of custom dashboards and reports.

FIGURE 17. HOW DOES YOUR NETWORK TEAM ENABLE PEOPLE FROM OTHER GROUPS TO USE NETWORK MANAGEMENT TOOLS?



Sample Size = 398, Valid Cases = 398, Total Mentions = 794

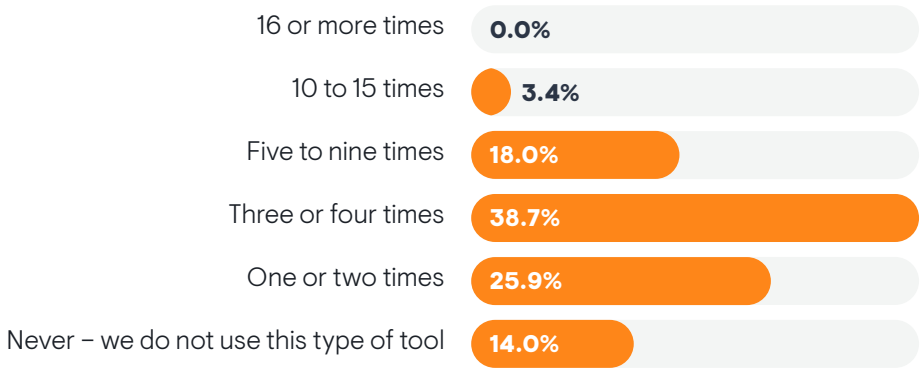
Field Ops: Troubleshooting and Validating Physical Networks

While much of this report explores how network teams operate their network from a central location (a desk) using network management and monitoring tools, field operations are also essential. Since the beginning of the digital era, technicians and engineers have ventured from their desks to physically analyze the network using portable tools. This section explores how network teams are handling the time-honored tradition of going out into the field.

Frequency of Trips to the Field

Figure 18 reveals that 86% of network teams send people into the field to assess and analyze networks. The typical team sends people into the field one to four times per month. A fair number send people into the field five to nine times per month. It's rare for an organization to do more than that. Technical personnel perceive more frequent trips than middle managers and executives. Small and midsized enterprises (500 to 9,999 employees) tend to send people into the field one to four times a month. Larger companies are all over the place, with 22% never sending people into the field and 29% sending people into the field 5 to 15 times a month.

FIGURE 18. IN A GIVEN MONTH, HOW OFTEN DOES A MEMBER OF YOUR NETWORK TEAM HAVE TO GO INTO THE FIELD WITH A HANDHELD NETWORK TROUBLESHOOTING/ANALYSIS TOOL OR LAPTOP/MOBILE DEVICE WITH NETWORK TROUBLESHOOTING SOFTWARE?



"In my experience, it's usually outside consultants who do this," said a network security architect with a Fortune 500 cybersecurity company. "I've been a consultant and that's what I did, going to every floor in every building with a Wi-Fi analyzer."

EMA found that successful network operations teams dispatch field technicians more often. On the other hand, our analysis indicated that organizations with a reactive posture to network problems tend to dispatch field technicians more often. Engagement with private 5G wireless networks and LAN switch upgrades correlate with more frequent trips into the field.

Organizations that send technicians into the field most often tend to want monitoring tools that automate the process of escalating issues to subject matter experts. This kind of automation can accelerate the mean time to response by field technicians.

Network teams that make frequent trips into the field are more likely to struggle with:

- Complex service problems that storage systems, application issues, or security incidents cause
- A lack of defined network operations processes
- A lack of network standards
- Ineffective cross-domain cooperation
- Bad network data

Network teams that send technicians into the field frequently also tend to report:

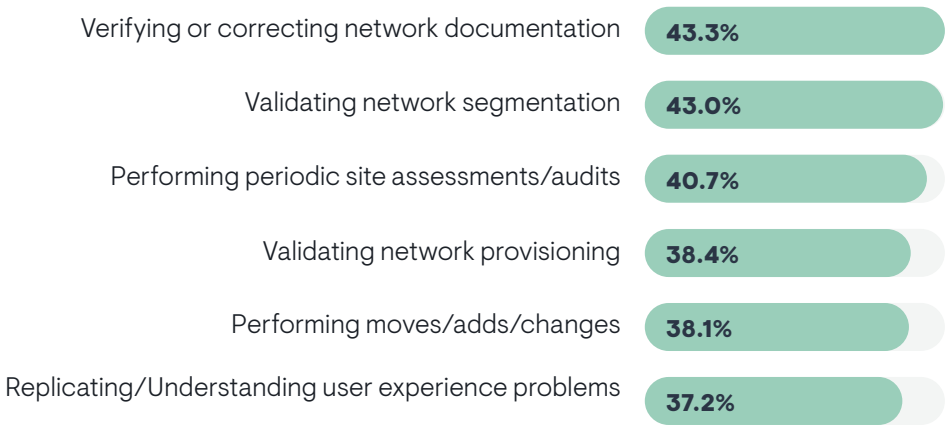
- Network teams spend more of their workday on troubleshooting
- Manual administrative errors, like a bad config change, cause a higher percentage of network trouble

The next section will reveal that many trips into the field are aimed at correcting some of these issues proactively.

Typical Field Ops Activity

Figure 19 reveals what technicians are doing when they leave their desk with network testing gear. There is not one activity that truly stands out from the rest, but the most common missions are aimed at validation rather than troubleshooting. The top two responses were network documentation verification and network segmentation validation. Periodic site assessments or audits were also common. Middle managers reported this latter use case more often than technical personnel.

FIGURE 19. WHEN YOUR NETWORK TEAM MEMBERS TAKE A HANDHELD NETWORK TROUBLESHOOTING/ANALYSIS TOOL OR LAPTOP/MOBILE DEVICE INTO THE FIELD, WHAT ARE THEY TYPICALLY DOING?



The stereotypical troubleshooting process of trying to replicate or understand user experience problems was the least reported activity.

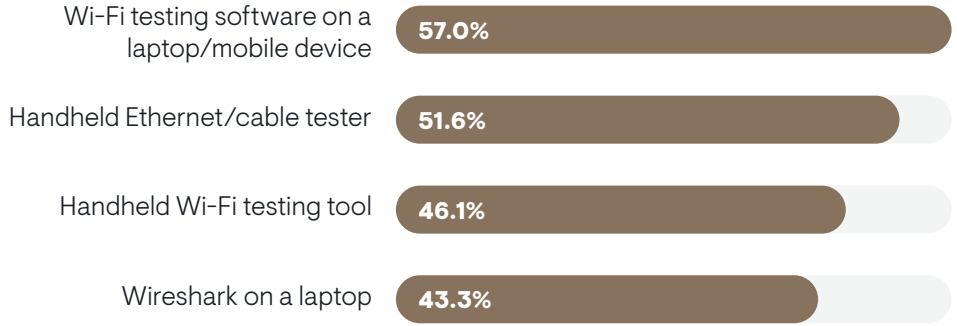
"We send people out on rare occasions," said a network engineer with a Fortune 500 aerospace and defense company. "We had a subsidiary that was compromised and was being hacked repeatedly. So, we did a remote audit and when the time came, we sent people to sites to do onsite analysis of security. We found a lot of open SSIDs that were being advertised without even a captive portal. One person went around with a handheld [Wi-Fi analyzer] and others were using a free utility on smartphones."

Sample Size = 349, Valid Cases = 349, Total Mentions = 840

Portable Tools Used for Field Ops

Figure 20 reveals what network technicians carry with them when they go into the field. The most common tool is Wi-Fi testing software on a laptop or mobile device. This one of the cheapest tools if it's open source or freeware, and it's also a tool choice that correlates with less successful network operations teams, suggesting that they are better off using a commercial handheld Wi-Fi tester.

FIGURE 20. WHAT KINDS OF PORTABLE NETWORK TROUBLESHOOTING/ANALYSIS TOOLS DOES YOUR ORGANIZATION USE?



Most organizations also have handheld Ethernet or cable testing devices, which are useful for isolating and analyzing physical problems on a wired network. Handheld Wi-Fi testing tools are a little less popular.

The other cheap option, Wireshark on a laptop, is the least popular. It's also the option that requires the most skill, which many field technicians often lack. Dedicated handheld devices tend to automate analysis more than Wireshark. Members of network engineering and IT architecture groups, which to have higher-skilled personnel, perceived more usage of Wireshark.

Sample Size = 349, Valid Cases = 349, Total Mentions = 691

Network Operations Toolsets

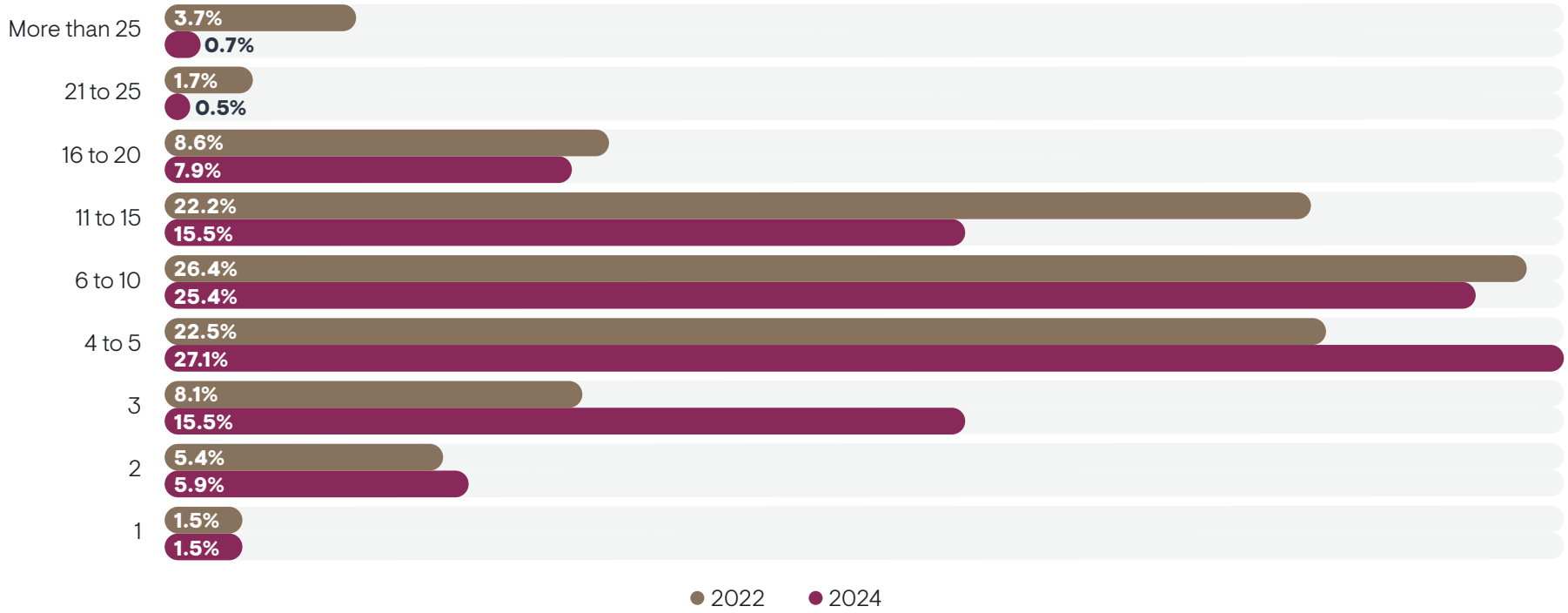
Toolset Sprawl Remains the Norm

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



Sample Size: 2024=406, 2022=409

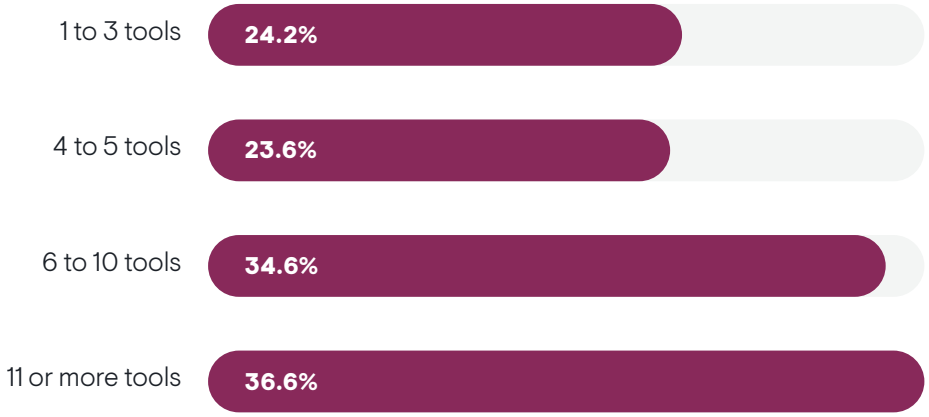
EMA found that the larger a company is in terms of employee count, the more tools they use to manage their networks. We also found that use of multiple cloud providers correlated with a larger toolset, suggesting that network teams are adopting tools specific to individual cloud providers to address operational gaps. IT organizations with a network operations strategy that is influenced by investments in network performance management solutions reported smaller toolsets, suggesting that they were consolidating tools through such investments. On the other hand, network operations strategies influenced by investments in digital network twin technology reported larger toolsets, suggesting that such tools are typically standalone solutions that add to a tool count.

SASE adoption correlated with a larger toolset, especially if network teams were struggling with managing security policies and controls in a SASE solution.

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 22** demonstrates that manual administrative errors that lead to network downtime or performance issues are more common with larger toolsets. **Figure 23** 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.

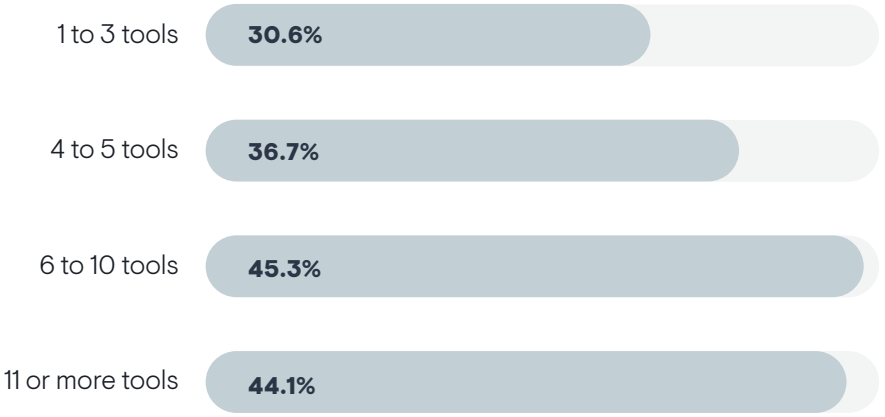
Larger toolsets are introducing operational complexity that makes tools less effective and networking personnel less efficient.

FIGURE 22. PERCENTAGE OF NETWORK-RELATED PROBLEMS CAUSED BY MANUAL ADMINISTRATIVE ERRORS, BY NUMBER OF TOOLS IN THE NETWORK OPERATIONS TOOLSET



Sample Size = 406

FIGURE 23. 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 24** 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.

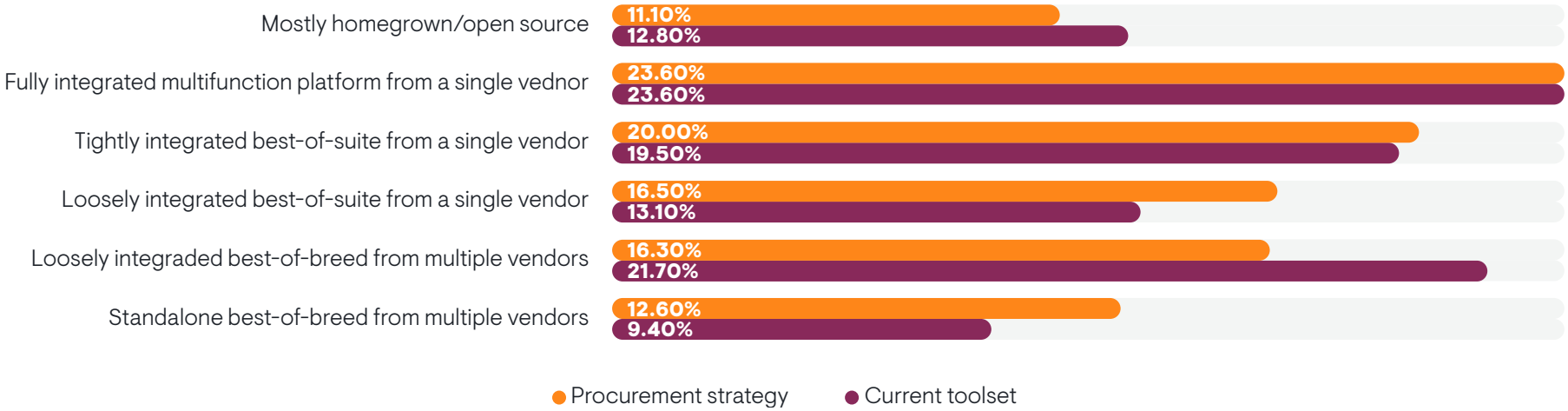
Roughly 20% have a tightly integrated suite from a single vendor and will stay that way. These organizations typically use a suite from a tool vendor that grew its capabilities through acquisitions of complementary vendors.

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.

"We have a next-generation transformation project around network performance management, particularly around SNMP and NetFlow data," said an IT tools architect at a Fortune 500 media company. "We had three tools across those two things and we're trying to consolidate to a multifunction tool."

FIGURE 24. 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

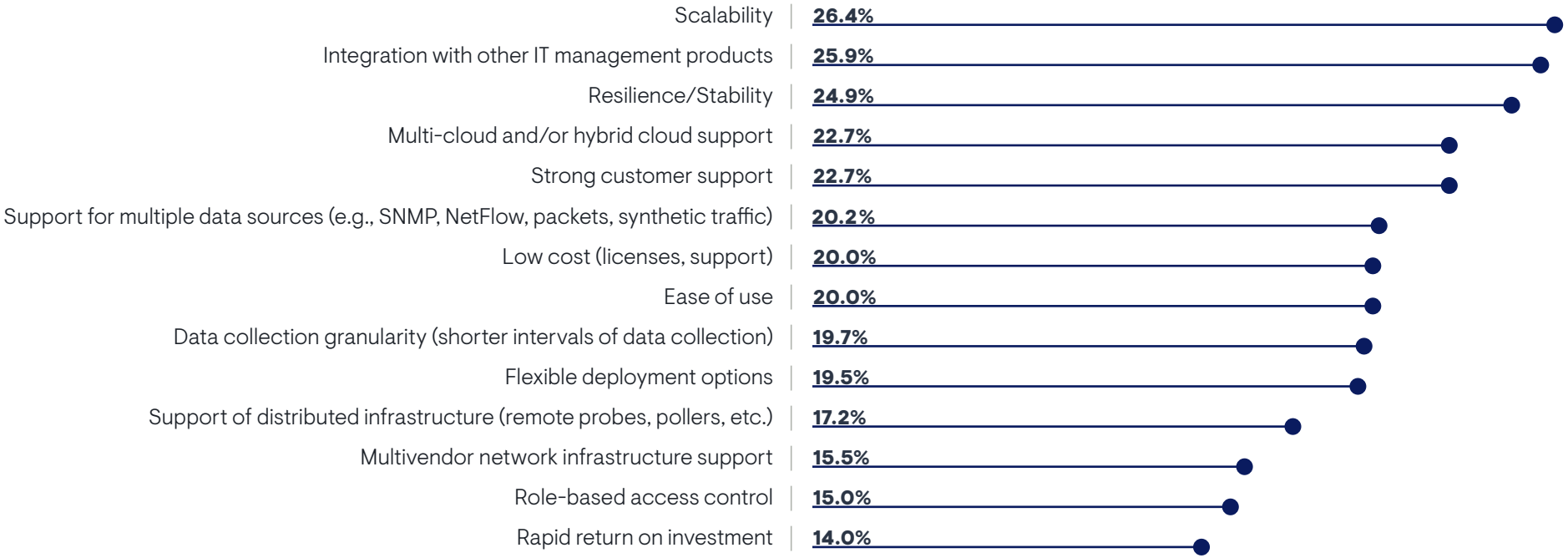
Platform and Business Requirements

Figure 25 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.

"Tools are expensive," said an IT operations manager with a very large government agency. "Also, the problem with us is always scalability. There's a lot of overhead involved in getting timely information on a very large network. When you have 300,000 Cisco devices set to report warnings via syslog if something bad is happening, your tools are going to get inundated with data."

FIGURE 25. WHAT ARE YOUR ORGANIZATION'S TOP BUSINESS AND PLATFORM REQUIREMENTS FOR NETWORK MANAGEMENT PRODUCTS?



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

"A big one is scale," said a network engineering director for a large insurance company. "When my company first started doing mergers and acquisitions, we had ten locations. All that had to be factored in was, 'Is this new acquisition overlapping with the IP address scheme in those ten locations?' Now, we're at 250 locations and it's hard to account for things."

Support of multiple networking vendors was a low overall priority for respondents, but successful network operations teams singled it out as a top requirement. Members of network engineering teams also prioritized multi-vendor support. Technical personnel (admins, engineers, architects) were more likely to select role-based access control and support for multiple data sources.

"I need tools that can accept more than one [vendor]," said a network security architect at a Fortune 500 cybersecurity company. "I see tools that can support Cisco SD-WAN, but not Versa. We need both. I also have concerns about tools that are too antiquated, like Java-based tools. I have a preference for tools that were born in the cloud."

Feature Requirements

Figure 26 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.

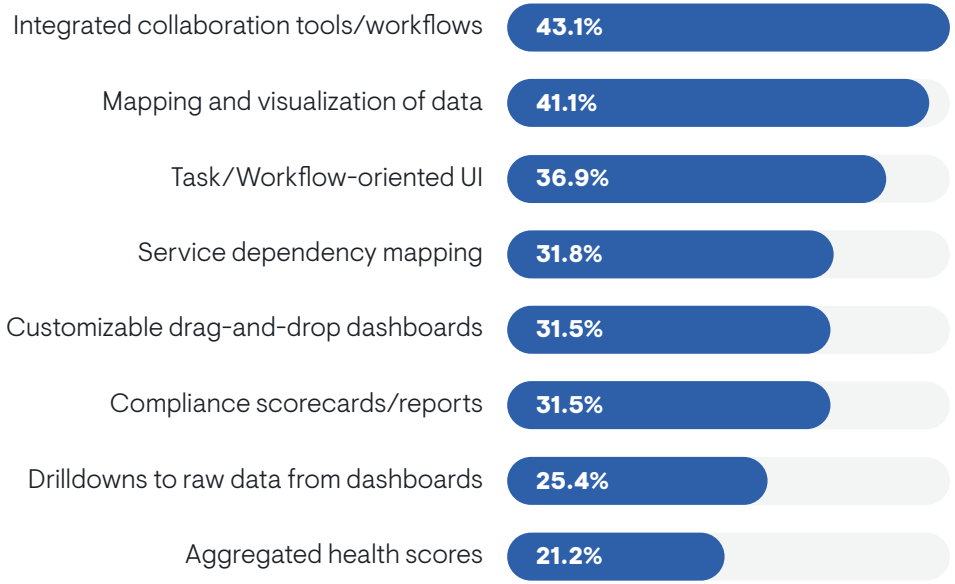
"The graphical information I can get out of my SNMP-based tools is fantastic. I like being able to get lots of charts and real-time data on utilization, latency, packet loss," said a network engineer with a Fortune 500 aerospace and defense company.

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.

"The info needs to be readily accessible and we need to be able to go from a high level to a deep, deep level," said a network engineering director for a large insurance company. "It needs to capture enough data and present it in a solid way, with a summary that we can drill into if needed."

FIGURE 26. WHICH OF THE FOLLOWING GENERAL NETWORK MANAGEMENT TOOL FEATURES ARE MOST IMPORTANT AND USEFUL?



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

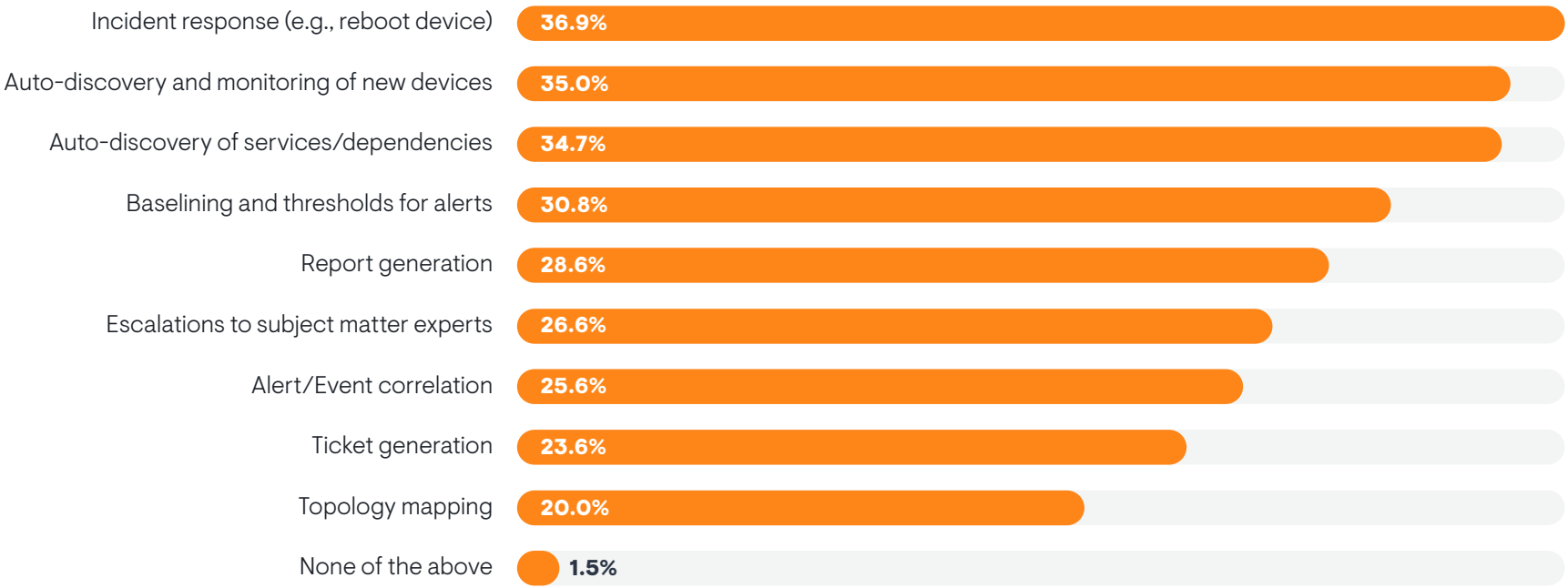
Tool Automation Requirements

Figure 27 reveals what aspects of network monitoring tools IT organizations need to automate to improve operational efficiency. Incident response is the top priority. These are typically automated actions triggered by an event detected by a tool. Some tools offer out-of-the-box runbooks for enabling this kind of automation. In other cases, network teams will write and maintain a library of homegrown scripts that are triggered by a tool.

The other two top priorities are more oriented toward ensuring that a tool is monitoring everything, specifically through auto-discovery and monitoring of new devices and auto-discovery of services and dependencies. This ensures that a tool can monitor and report on everything that is important to network operations.

Secondarily, IT organizations want tools that can automatically baseline the network and generate reports. Report generation and baselining were more important to smaller enterprises. Baselining was also important to multi-cloud enterprises.

FIGURE 27. WHAT ASPECTS OF YOUR NETWORK MONITORING TOOLS DO YOU AUTOMATE OR NEED TO AUTOMATE TO IMPROVE OPERATIONAL EFFICIENCY?



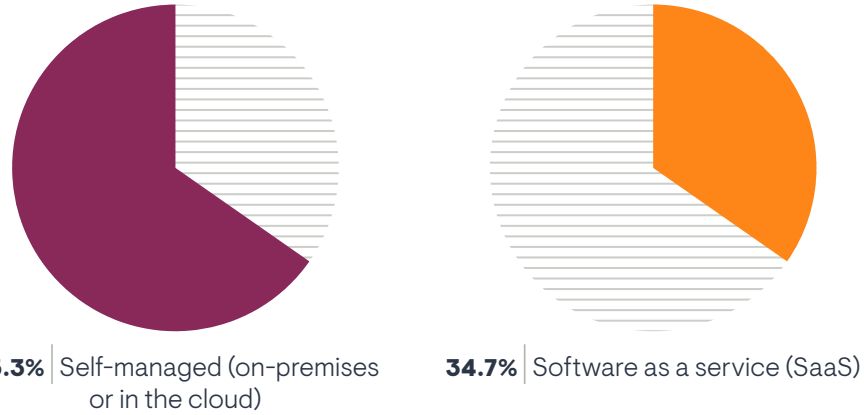
Sample Size = 406, Valid Cases = 406, Total Mentions = 1,069

Tool Consumption Models

SaaS-Delivered Tools are Now the Standard

More than 65% of network teams now prefer to consume their management tools as a SaaS offering, as **Figure 28** reveals. EMA research has observed a steady shift toward this preference over the last eight years. Self-managed tool deployments (typically deployed on-premises) were the preferred consumption model for many years, but those days are over. However, interest is softer in large enterprises (10,000 or more employees), where 48% still prefer a self-managed tool. Also, members of IT architecture and network engineering teams were more likely to prefer a self-managed tool.

FIGURE 28. WHAT IS YOUR PREFERRED DEPLOYMENT MODEL FOR NETWORK MANAGEMENT TOOLS?



"Most of our tools are on-premises," said an IT tools architect at a Fortune 500 media company. "It comes down to organizational requirements, budgets, and cyber constraints. One time, I was looking at a new tool and saw that it costs the same on-premises and in the cloud, so why pay for it on-premises, since I have to pay for compute resources on top of it? But then cybersecurity told me it's a no-no. They are heavily against polling from outside our network."

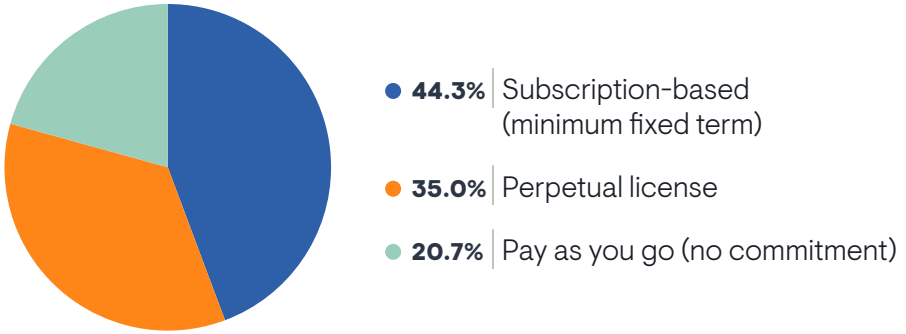
Sample Size = 406

"It has to be deployable in the cloud at least, either as a SaaS app directly from the vendor or through an IaaS provider," said a network engineering director for a large insurance company. "Nobody is in the business building data centers anymore. We want to ship tools offsite one way or another."

Perpetual Licenses are History

With the shift to SaaS tools, licensing preferences also changed. Perpetual licenses were the standard when tools were self-managed and deployed on-premises. **Figure 29** reveals that subscription licenses are now the more popular option. A smaller number of companies are seeking pay-as-you-go licensing, which is essentially a subscription without a minimum term. Tools vendors rarely offer this option. DevOps professionals were more likely to seek pay-as-you-go licensing.

FIGURE 29. WHAT IS YOUR PREFERRED LICENSING MODEL FOR NETWORK MANAGEMENT TOOLS?



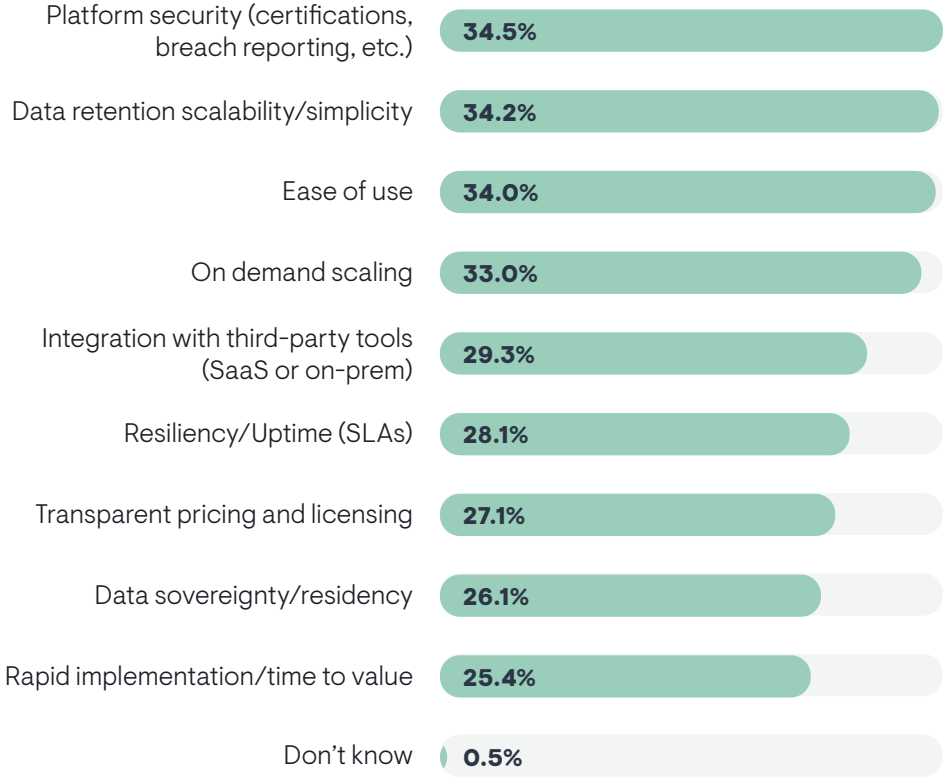
Midsized enterprises (2,500 to 9,999 employees) were the most interested in subscription-based tools. Larger enterprises, with their affinity for self-managed tools, often still prefer a perpetual license.

Sample Size = 406

The Appeal of SaaS-Delivered Tools

Figure 30 reveals that IT organizations perceive four chief benefits from a SaaS tool: platform security, data retention, ease of use, and on-demand scaling. Ease of use appeals more to large enterprises (10,000 or more employees). Multi-cloud enterprises were more likely to select on-demand scaling, as were organizations that struggle to hire networking personnel.

FIGURE 30. WHAT ARE THE MOST APPEALING ASPECTS OF USING A SAAS-BASED NETWORK MANAGEMENT TOOL?



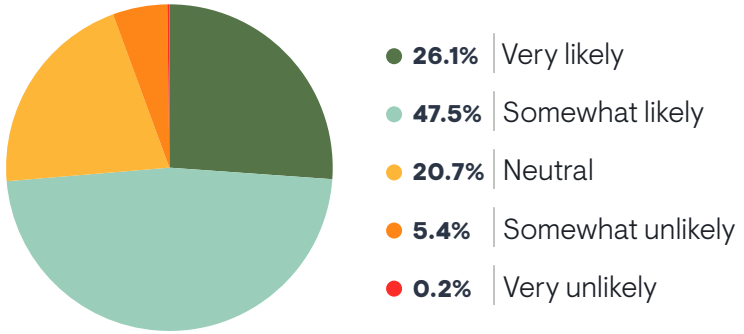
Sample Size = 406, Valid Cases = 406, Total Mentions = 1,105

Members of network engineering teams were more likely to cite data sovereignty and ease of use. IT tool engineering teams had a strong affinity for transparent pricing.

Replacing Incumbent Tools

Figure 31 reveals that nearly 84% 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 31. 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

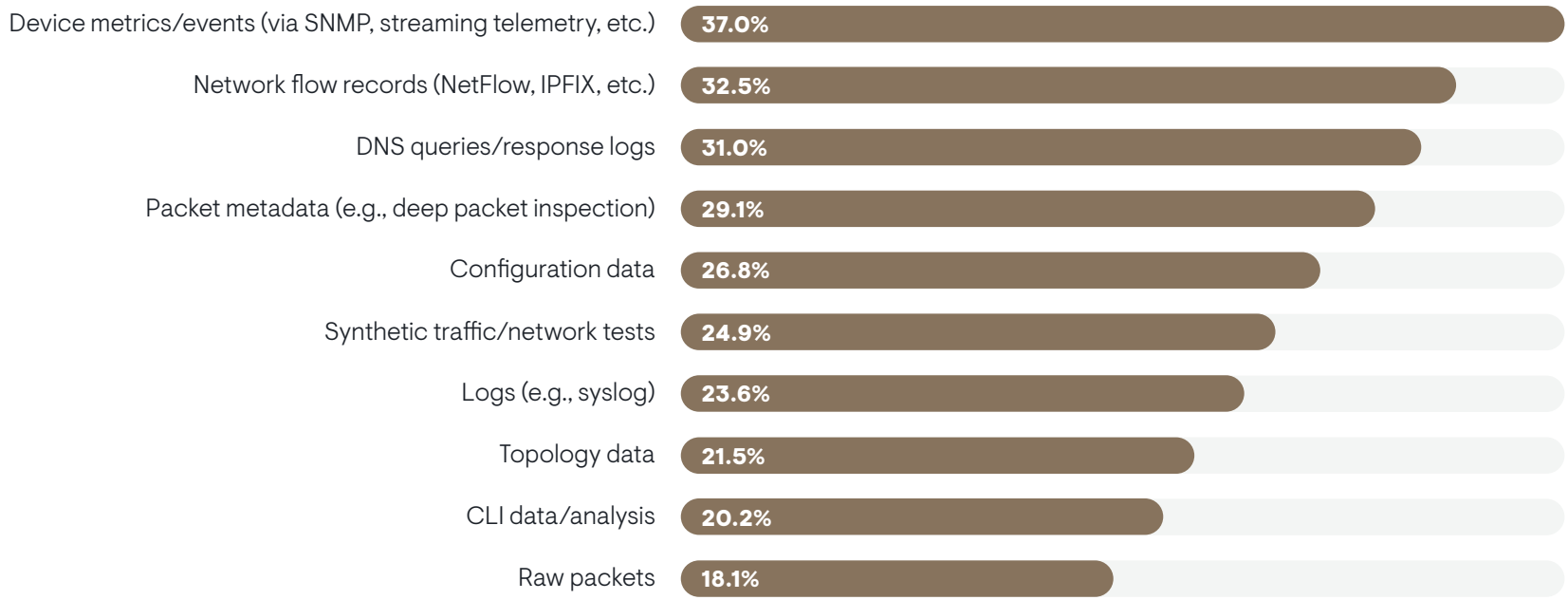
Network Data Requirements

Critical Monitoring and Troubleshooting Data

Figure 32 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 32. 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.

Interest is Strong

Figure 33 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.

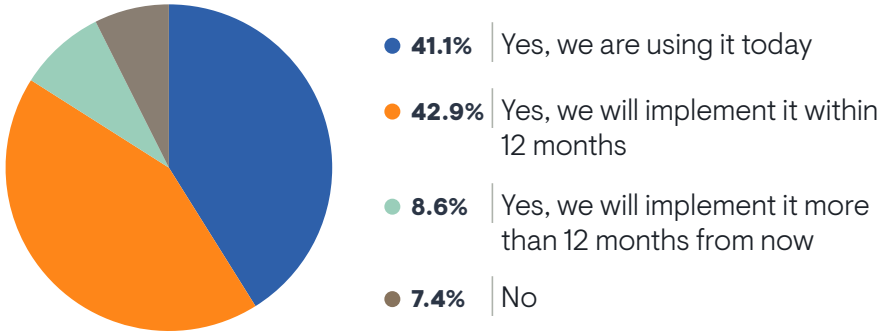
Nearly 92% of IT organizations are interested in using streaming telemetry and 41% claim they are already using it.

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.

"We're not looking at it right now," said a network engineer with a Fortune 500 aerospace and defense company. "But SNMP is facing death because of security vulnerabilities and other things. Right now, I'm trying to grasp the concepts."

Adoption is lower in organizations that struggle to hire networking personnel, suggesting that a lack of expertise holds them back from experimenting with the emerging technology.

FIGURE 33. 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 34** 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 34. 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

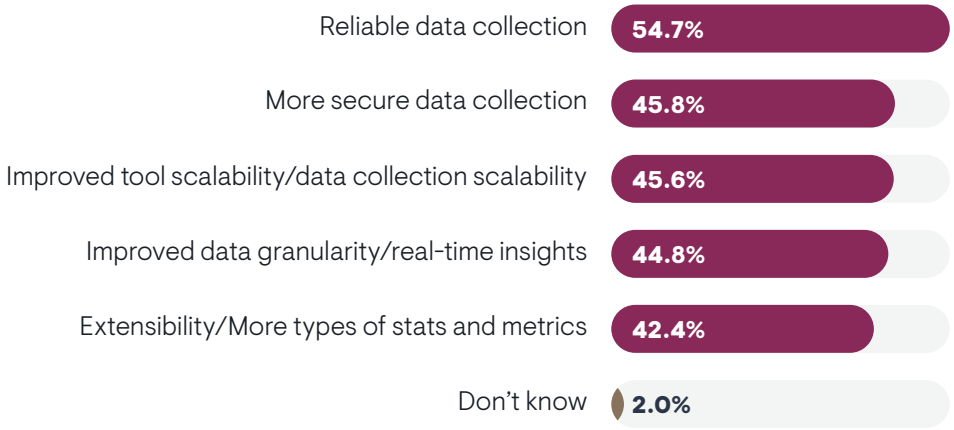
26.3% Required – we want to remove SNMP from our network

Sample Size = 376

Potential Benefits

Figure 35 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 35. 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

Adoption Roadblocks

Figure 36 explores why mainstream adoption of streaming telemetry hasn't arrived. The three biggest speedbumps are security risk, skills gaps, and complexity of extracting data from platforms. Skills gaps and security risks were the top two challenges in 2022. The third leading roadblock in 2022 was unclear business value, an issue that dropped to the bottom of the list this year. Thus, two years of investigation have helped network teams identify the potential business value of streaming telemetry, but other issues are still holding them back.

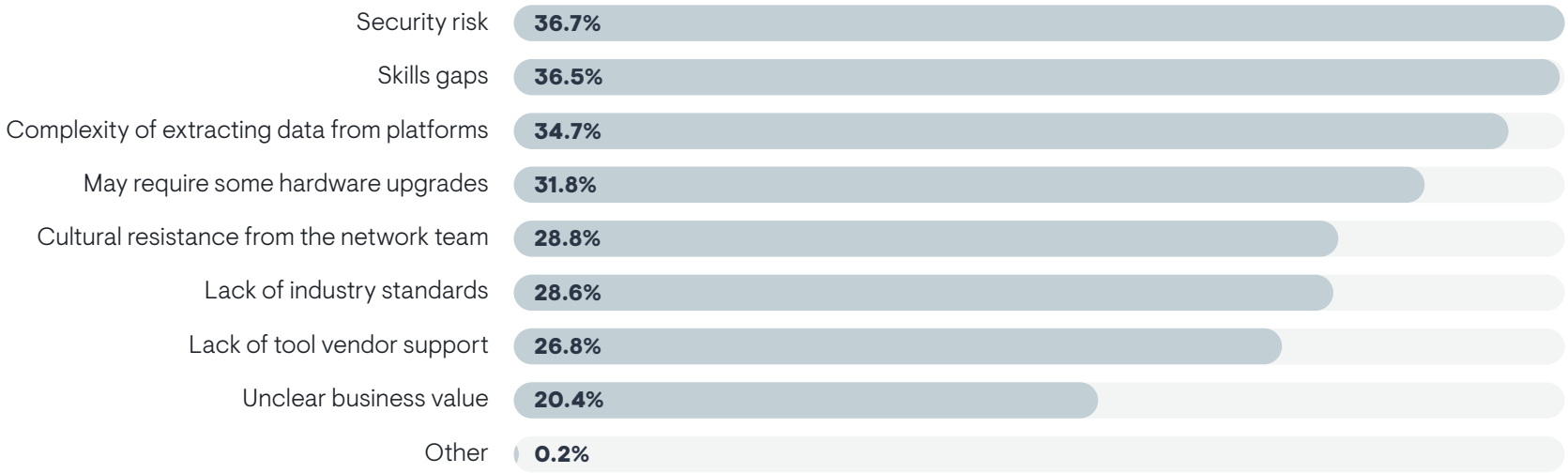
Technical personnel (admins, engineers, architects) were more likely to cite a lack of industry standards as a major issue. Members of network engineering and IT tool engineering teams were particularly concerned with this problem. Cloud teams were more likely to complain about the complexity of extracting data and cultural resistance.

"I don't see it as available in a highly scalable manner," said an IT tools architect at a Fortune 500 media company. "We are using it a little, but it's not fully supported. SNMP has been around for multiple decades. Its standards are fully documented and understood. With streaming telemetry, it's all over the place, with vendor-specific formats, different protocols, different data models. It's not standardized. I'd like to see vendors use the same standard across the board, but I haven't seen that yet."

"You need to have the proper tools to do it," said an IT operations manager with a very large government agency. "Then, you have to ask if streaming is actually any better than SNMP and whether your routers and switches support streaming enough to the point where it makes sense to use it."

"It sounds really interesting, but I haven't found anyone who can fully operate with our networking vendor at this point," said a network engineering director for a large insurance company.

FIGURE 36. WHAT ARE THE PRIMARY BARRIERS TO ADOPTION OF STREAMING NETWORK TELEMETRY?



Sample Size = 406, Valid Cases = 406, Total Mentions = 993

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

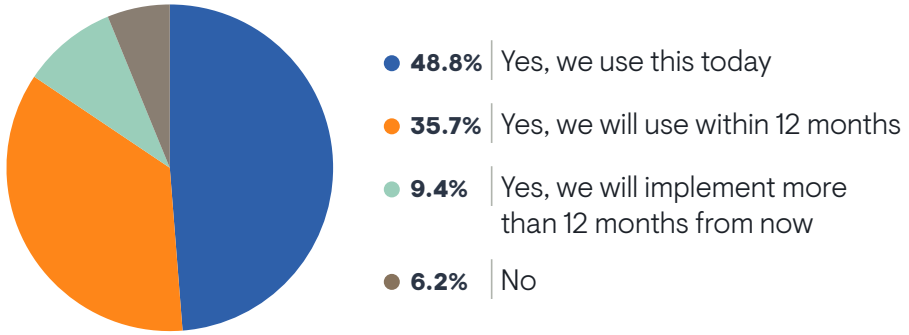
Figure 37 reveals that nearly 49% of organizations are using a synthetic network monitoring tool today. In 2022, adoption was at 48%. Only 6% have no current plans to adopt synthetic monitoring solutions. Successful network operations teams were more likely (62%) to use it today.

"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."

Technical personnel were more aware of current adoption, which makes sense, since they are more likely to understand the nuanced differences between synthetic traffic and other types of network data that network operations teams use. Multi-cloud enterprises reported higher adoption. Organizations that have implemented SASE technology are also more likely to have these tools.

Organizations that struggle to hire networking personnel were less likely to use the technology today, suggesting they lack internal resources to onboard such a tool.

FIGURE 37. 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 38** 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."

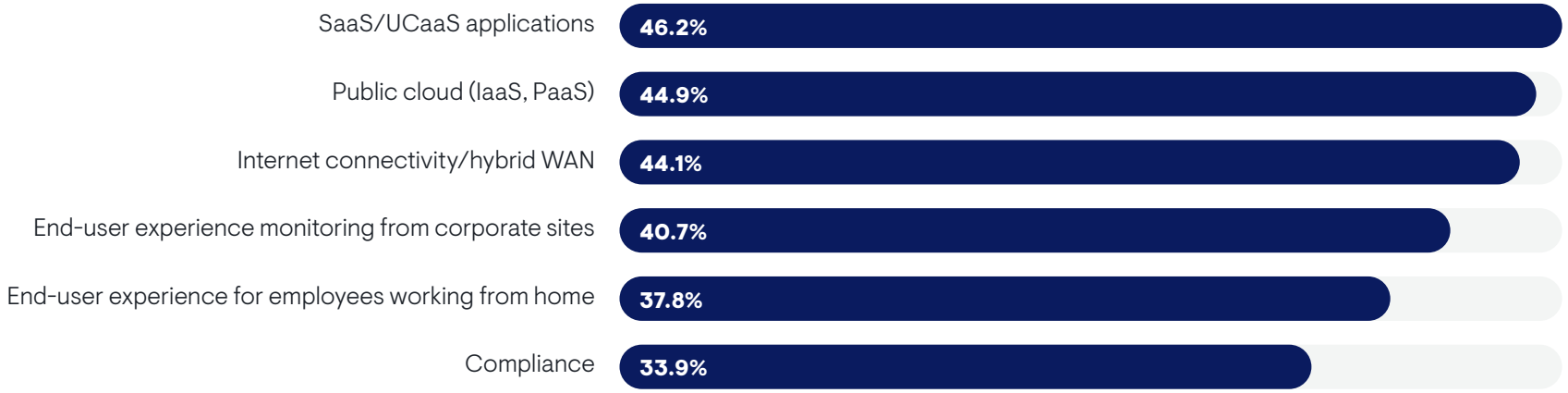
End-user experience from corporate sites and remote workers' home offices are secondary use cases. Multi-cloud enterprises were more likely to cite internet connectivity as a driver, while organizations that use only one cloud provider were more focused on end-user experience from corporate sites. Organizations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

"We want to make sure that people in branch offices are fully secure, but also that their experience going to apps in the cloud are good. They should be going directly to the internet from the branch office and not be backhauled through a centralized data center, so additional monitoring is needed," said an IT tools architect at a Fortune 500 media company. "We have agents performing tests from offices to SaaS apps to underhand that apps are reachable, but are also responding in a reasonable amount of time."

"We have 20,000 client devices on our network and a large percentage of traffic is voice-related. We use synthetic monitoring to quickly drill down into what the source of an issue is with calls," said a network engineering director for a large insurance company. "It's very handy on the voice side. It's also handy for determining where a fault is. It's not just about ruling out the network. It can help us find things that fall into the cracks, for finding the root cause of issues when you don't control everything from point A to point B."

"We like its ability to peel apart different layers," said a network engineer with a Fortune 500 aerospace and defense company. "Network operations, network engineering, and cybersecurity are interested in it for in-depth analysis of performance. And the cyber group was interested in using it to track unauthorized communications or connections."

FIGURE 38. WHICH OF THE FOLLOWING ARE DRIVING YOUR NETWORKING TEAM'S INTEREST IN SYNTHETIC NETWORK MONITORING?

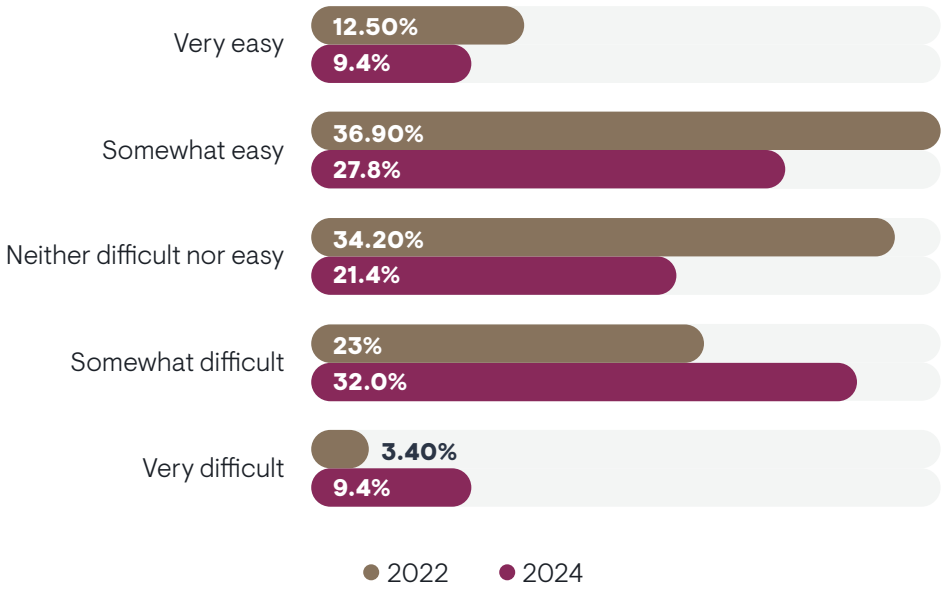


Sample Size = 381, Valid Cases = 381, Total Mentions = 943

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



"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."

Sample Size: 2024=406, 2022=409

"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.

"For us, hiring new talent has gotten easier over the last couple years with layoffs from big tech," said an IT tools architect at a Fortune 500 media company. "It helped us hire people."

"We had a special pay bonus for security people because we were really struggling to hire and retain them. Then that was expanded to everyone," said an IT operations manager with a very large government agency. "So, hiring networking people is not too bad."

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

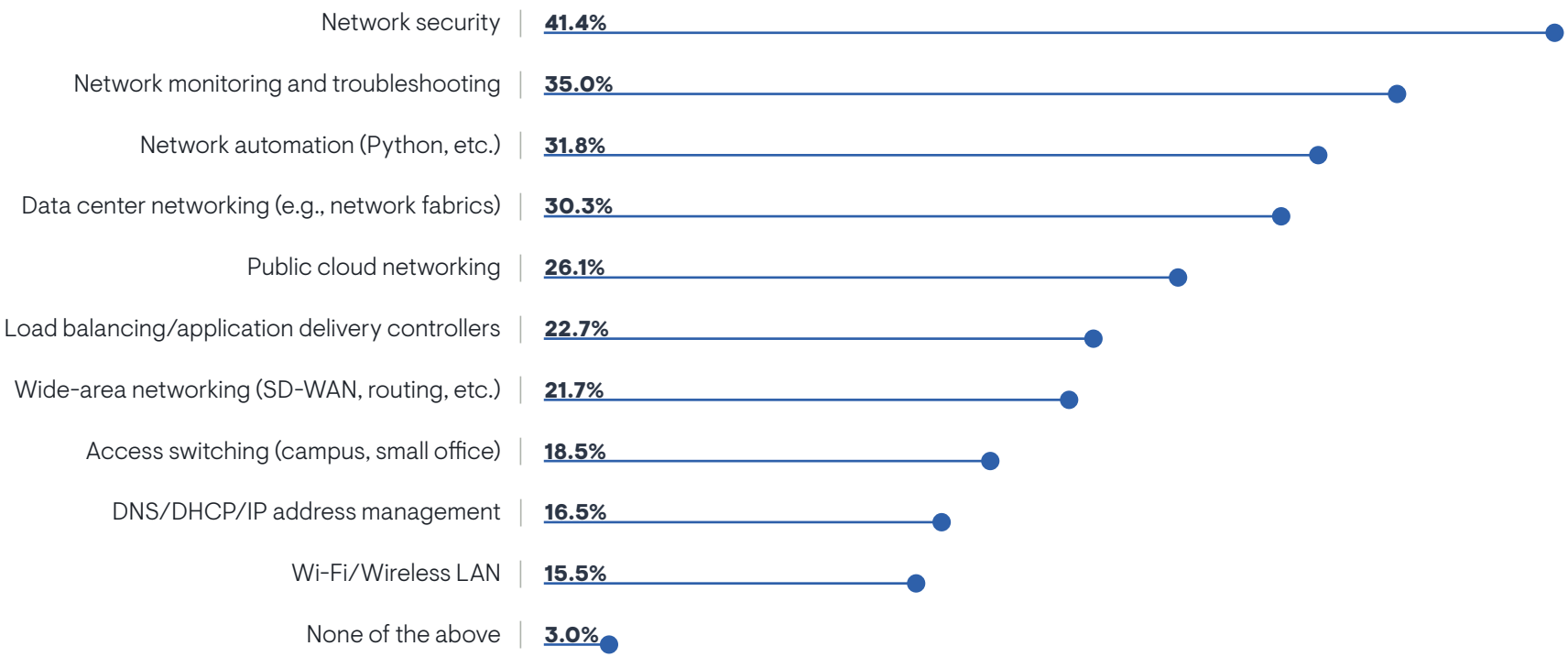
Technical Skills that are Scarce

Figure 40 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 40. 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

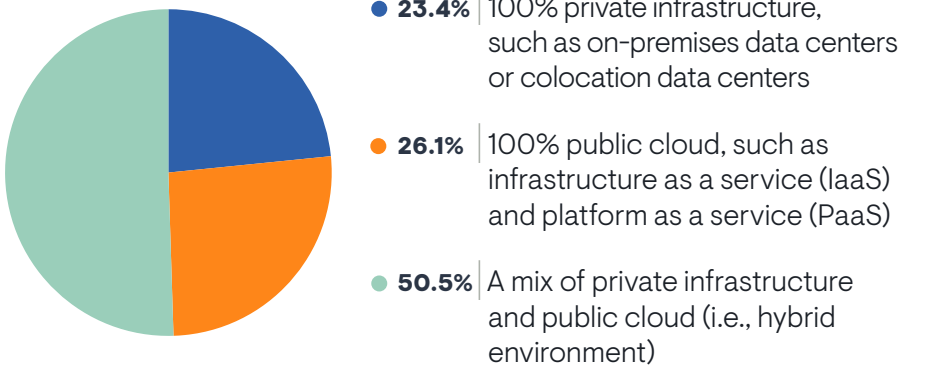
Megatrend #2:
Adapting Network Operations to the Cloud

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



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.

Sample Size = 406

EMA observed that certain network operations drivers correlated with the various approaches to infrastructure explored here.

A 100% public cloud strategy correlated with:

- ITIL/ITSM best practices initiatives
- Data center consolidation/decommissioning
- AIOps
- DevOps and CI/CD
- •Pv6 transition
- Digital network twin/network modeling software

A 100% data center strategy correlated with:

- Server virtualization
- Cloud repatriation
- SaaS application adoption
- Cross-domain operations
- DevOps and CI/CD
- Data center network upgrades
- Network automation

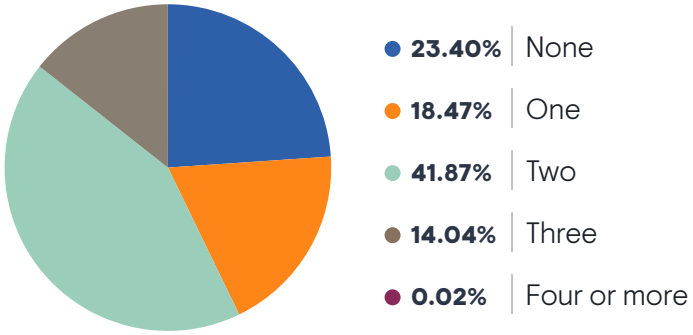
A hybrid cloud approach correlated with:

- Kubernetes/Cloud native applications
- WAN transformation
- Data center network upgrades
- AI/ML-driven network analytics
- Network observability
- Hybrid and multi-cloud networking technology

Multi-Cloud Adoption

Figure 42 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 42. NUMBER OF CLOUD PROVIDERS USED



On-Premises versus Colocation Data Centers

Figure 43 identifies the nature of data centers the 300 organizations in this survey who have private infrastructure used. Nearly 44% rely on only on-premises data centers and more than 16% rely only on colocation providers. The rest use both.

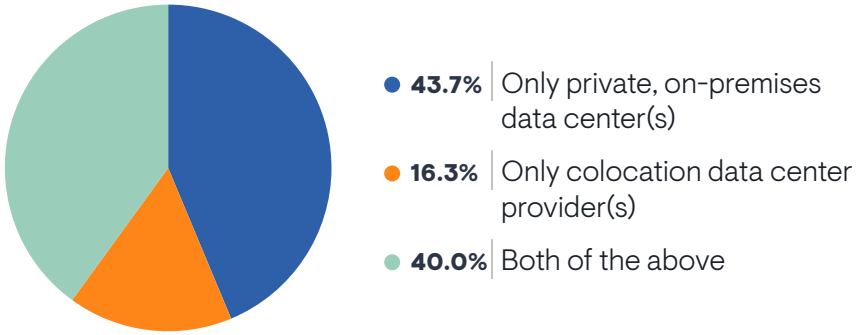
"We have many colocation points of presence because we are a media company and we are using many clouds. We use colos as entry points into the network," said an IT tools architect at a Fortune 500 media company.

Technical personnel were less aware of colocation use, while middle managers and IT executives were more aware. Organizations that reported no public cloud use were more likely to have only on-premises data centers. Organizations that are in the cloud were very likely to use both on-premises and colocation data centers. Finally, successful network operations correlated more with on-premises data centers than colocation data centers, suggesting that full control of data center infrastructure and facilities is a potential best practice.

EMA asked respondents why their organizations were using colocation providers. Their top five drivers were:

1. Reducing or eliminating on-premises data center footprint (49%)
2. Disaster recovery and resiliency (46%)
3. Deploying applications and data closer to users (44%)
4. Skills gaps (43%)
5. Cloud repatriation (40%)

FIGURE 43. PRIVATE INFRASTRUCTURE: ON-PREMISES DATA CENTERS VERSUS COLOCATION PROVIDERS



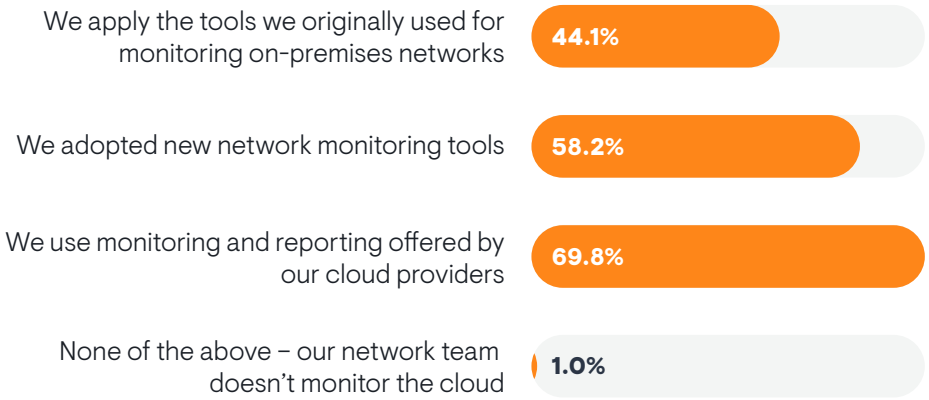
Sample Size = 300

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 44** 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 44. 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.

"We use Azure's monitoring tools. They are adequate. Maybe not as up to speed as our tools, which we would use if the infrastructure were in my own data center. They could be better, but they meet the minimum standard that I set," said a network engineering director for a large insurance company.

Large enterprises (10,000 or more employees) were less likely to use native monitoring capabilities that cloud providers offer. Instead, they had a greater affinity for new and incumbent third-party monitoring tools. Members of network operations teams were more likely to report use of incumbent on-premises tools, while the CIO's suite and DevOps perceived more frequent adoption of new tools.

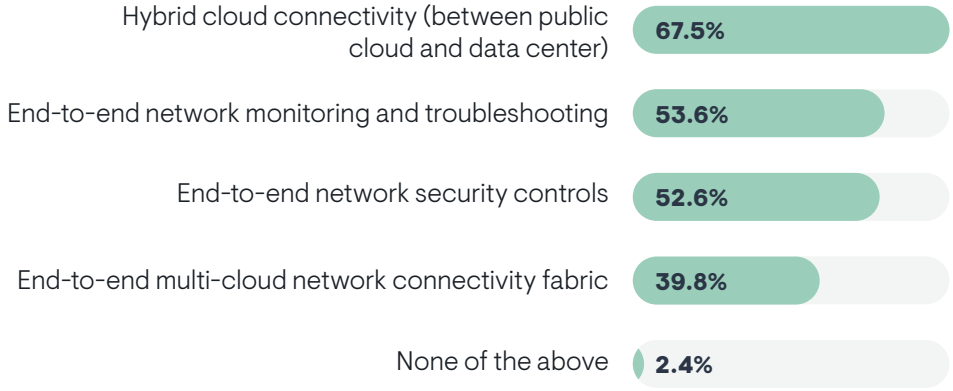
Engagement with Hybrid Multi-Cloud Networking Solutions

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 45 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 45. 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.

"We've been doing more virtual SD-WAN appliances in the cloud and going over the internet with IPsec tunnels, both between clouds and between data centers and the cloud," said a network security architect with a Fortune 500 cybersecurity company. "On the monitoring side, we've been relying on logs. But there's not tools that are designed to give us visibility across different clouds."

"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."

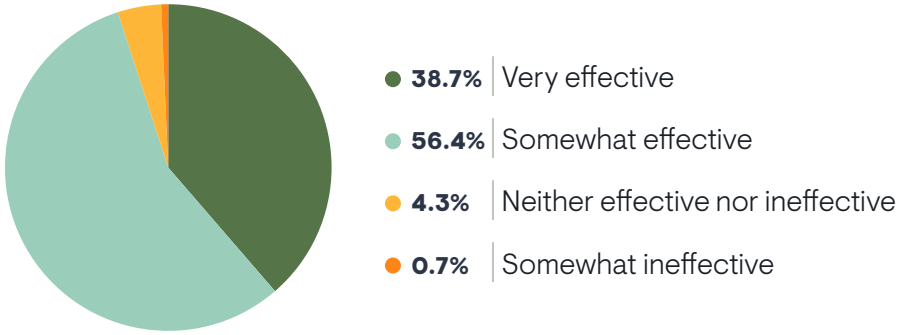
"Multi-cloud networking is in progress right now," said a network engineer with a Fortune 500 aerospace and defense company.

"I am continuously having to find virtual pieces of network hardware that can interoperate between multiple cloud providers," said a network engineering director for a large insurance company. "I deploy virtual appliances across the big three cloud providers to create an overlay using SD-WAN and firewalls."

Outcomes with Hybrid and Multi-Cloud Networking

Figure 46 reveals how effective respondents believe their organizations are in their efforts to implement hybrid and multi-cloud network infrastructure and operations. Overall, 39% believe they are completely effective, while 56% see some room for improvement. Less than 1% believe they are actually failing.

FIGURE 46. HOW EFFECTIVE ARE YOUR EFFORTS TO MANAGE NETWORKING AND SECURITY ACROSS THESE HYBRID CLOUD AND/OR MULTI-CLOUD ENVIRONMENTS?



Sample Size = 282

Members of cloud engineering and operations teams were more optimistic about hybrid and multi-cloud networking. Members of network engineering, IT architecture, DevOps, IT service management, and IT tool engineering teams and the CIO's suite were all feeling less optimistic. Also, organizations that were struggling to hire networking talent tended to report less effectiveness with cloud networking.

Traditional network monitoring tools show promise here. Organizations that monitor cloud networks with their incumbent on-premises network monitoring tools reported more success with hybrid multi-cloud networking than organizations that monitor with tools and reporting that individual cloud providers offer.

Megatrend #3:
SASE Introduces Operational Challenges

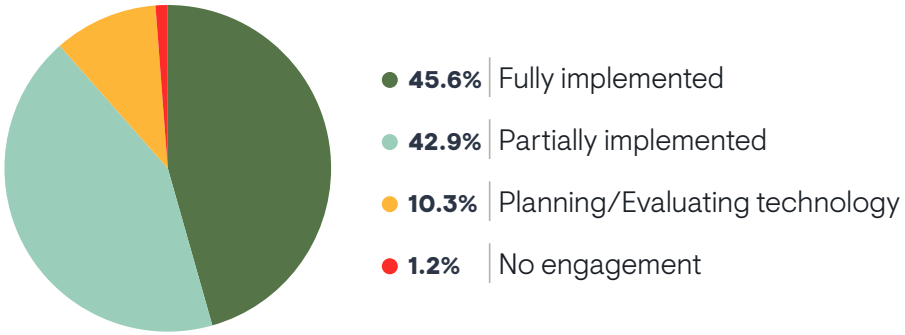
SASE is the next wave of wide-area network (WAN) transformation. SASE is an architecture that integrates SD-WAN with cloud-delivered security services, such as firewalls, secure web gateways, cloud application security brokers, and zero trust network access. EMA research previously established that 99% 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 47 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 47. WHAT IS THE STATUS OF YOUR ORGANIZATION'S ENGAGEMENT WITH SASE?



Sample Size = 406

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. Moreover, companies that had completed a SASE project were more likely to be doing the following with their hybrid and multi-cloud networks, and they were more likely to report success with such efforts:

- Hybrid cloud connectivity
- End-to-end network security across clouds
- End-to-end multi-cloud connectivity fabrics

SASE adoption also correlated with the following:

- Lack of difficulty in hiring network personnel
- Investments in network automation
- Investments in digital network twin technology
- Efforts to monitor the performance of SaaS applications
- A strategic focus on AIOps and unified communications and collaboration solutions

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

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 48** 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

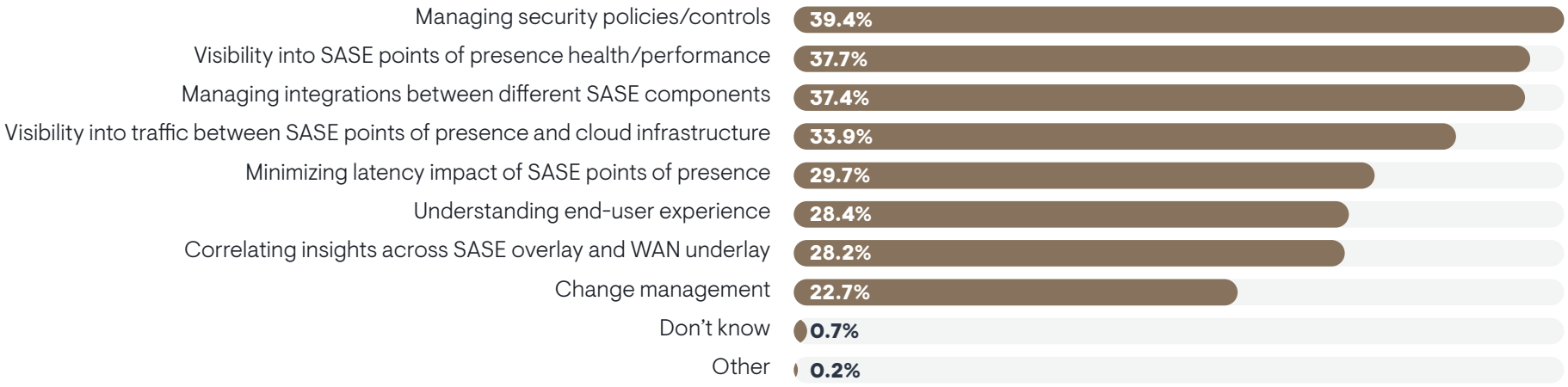
"Things have changed drastically since we implemented SASE," said a network security architect with a Fortune 500 cybersecurity company. "Users are proxied through these policy nodes [SASE PoPs] and that makes troubleshooting a little different. It's hard because we're not looking at things from the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

IT executives were more concerned about managing security policies and controls than more technical personnel. Concerns about observability of SASE points of presence were higher among multi-cloud organizations. Multi-cloud organizations were also more likely to struggle with change management and correlating insights across SASE overlays and WAN underlays.

The prevalence of issues with integrating SASE components is not surprising given that our previous research on WAN transformation revealed that many organizations adopt a multi-vendor approach to SASE, which poses a risk of integration complexity. Even some single-vendor solutions require integrations because many vendors have established a SASE solution through mergers and acquisitions.

FIGURE 48. WHAT DO YOU FIND MOST CHALLENGING ABOUT MANAGING AND MONITORING SASE TECHNOLOGY?

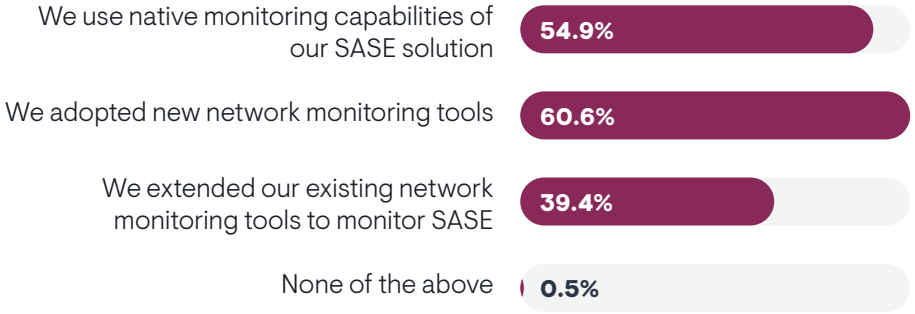


Sample Size = 401, Valid Cases = 401, Total Mentions = 1,036

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



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.

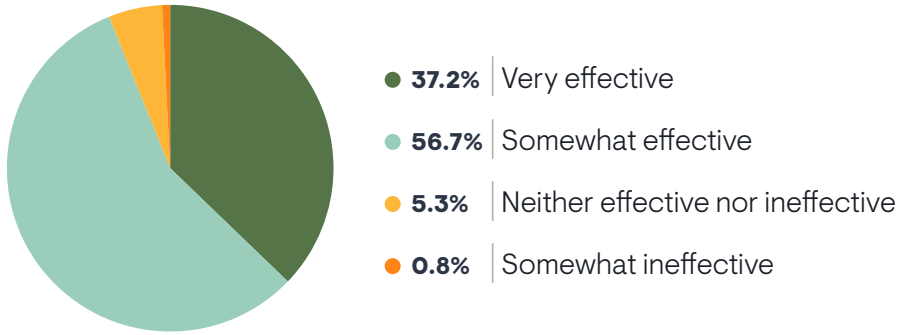
"We're running all these different kinds of network tests, trying to run some kind of simulated traffic to find out if we're using the right paths," said an IT tools architect at a Fortune 500 media company. "We have to run them frequently to get a baseline of environments. That takes time and investment. 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."

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

Effectiveness of Observability

Figure 50 shows that 37% of respondents believe their efforts to monitor SASE architecture are completely successful. Most see some room for improvement, but less than 1% describe their approach as ineffective. Respondents who reported that they use native SASE monitoring capabilities reported the most success with SASE observability.

FIGURE 50. HOW EFFECTIVE ARE YOUR EFFORTS TO MONITOR YOUR SASE ARCHITECTURE?



Organizations that struggle to hire networking personnel reported less effective SASE visibility. Members of network engineering, cloud, network operations, and IT service management groups were more optimistic than the IT architecture group.

Sample Size = 358

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 51** indicates. Earlier in this report, we also found that such technology is a high priority for 28% of organizations.

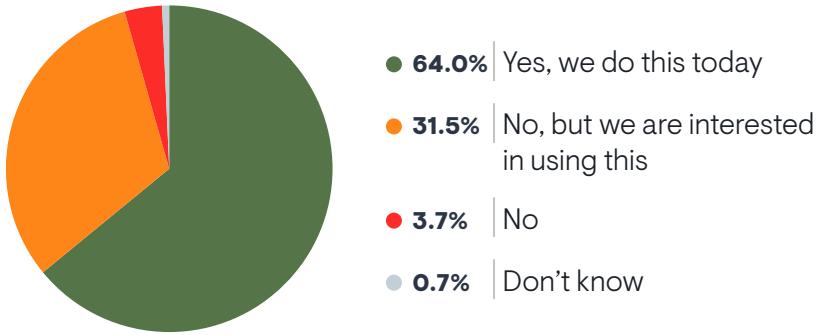
"We're always open to looking for how AI can help us, but it feels more and more like a buzzword right now," said an IT tools architect at a Fortune 500 media company. "It's like if you don't have AI in your slide decks and marketing, you're not there."

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.

"From what I've seen, [AI] just gets in the way," said a network engineer with a Fortune 500 aerospace and defense company. "I haven't seen anything that can save me a large amount of time or present data to me in a way that would be more accurate than me doing it manually. I'm open to it, but I just haven't been impressed."

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 51. 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

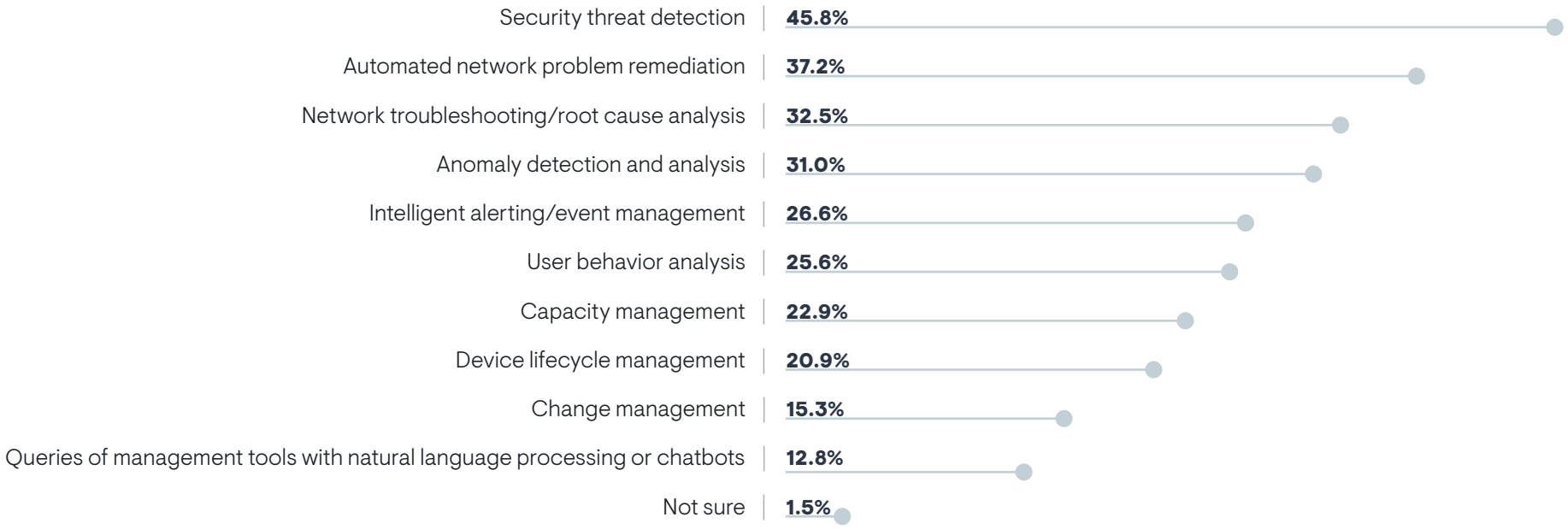
Security threat detection is the most interesting use case for AI/ML-driven network management today, as shown in **Figure 52**. IT executives were the most engaged with this use case.

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.

"Automated actions are fraught with peril," said an IT operations manager with a very large government agency. "If we don't write the rules exactly right, it will just shut everything down. You want to constrain what AI can do."

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



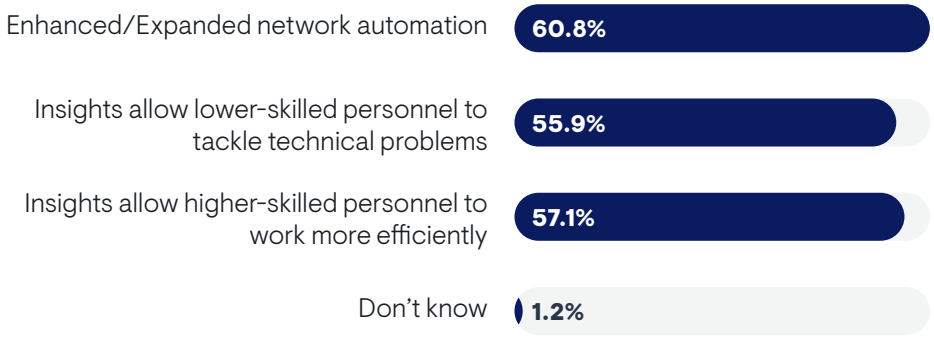
Sample Size = 406

AI/ML Impact on Network Operations

EMA asked respondents to reveal how they think AI/ML technology will enhance network operations. **Figure 53** 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 53. 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.

Case Study: Industrial Services Company Assures ERP User Experience During Cloud Migration with NETSCOUT

Cloud Migration Challenges

A large industrial services company depended heavily on its field service employees in regional offices to support the logistics for and execution of services, pickups, receiving, and deliveries at customer locations. The company's enterprise resource planning (ERP) application was essential to organizing several aspects of these field services, including service scheduling, customer order processing, materials receiving, shipping, and finance.

The company launched an application consolidation and modernization project to dispense with several data center-based management information system (MIS)/ERP software applications. As the company began a migration of its MIS/ERP software application to the Amazon Web Services (AWS), cloud performance issues emerged.

NETSCOUT Identifies Issues

The IT team responded first by conducting an audit of user experience and performance for the legacy ERP application with the NETSCOUT nGenius Enterprise Performance Management solution, which it previously used for monitoring network, application, and user experience performance. The audit provided user experience and performance metrics throughout the ERP migration in both the legacy data center and cloud environments. The analysis showed that field office employees using local ERP servers for regular barcode reading and printing services historically had a response time of around one second.

The company's new ERP system was hosted in AWS public cloud. The weekend following the cloud migration of the ERP solution, field office employees complained of slowdowns reaching over five seconds. Customer order completion and employee productivity were impacted by this five-fold increase in ERP response times to issue and print bar code assignments.

The IT team executed a process-driven approach to the ERP migration with nGenius® Enterprise Performance Management.

- In the **Pre-Migration Phase**, the team used InfiniStreamNG packet monitoring in the legacy data center to assess performance response time for the current ERP application and identify historical utilization patterns. They used these insights to develop an evidence-based migration plan.
- During the **Migration Phase**, the IT teams collaborated on the implementation of the ERP application in AWS cloud along with NETSCOUT vSTREAMs for packet-based performance analysis in the virtualized environment. They analyzed smart data in nGeniusONE to validate decisions and deployment choices.
- In the **Post-Migration Phase**, the IT team was able to monitor the new application on the first day of production, which made troubleshooting the problems reported in those early days swift and effective.

The dashboard views in nGeniusONE showed emerging degradations in the ERP application. Troubleshooting workflows identified two issues with the cloud-based ERP servers that led to intermittent increased response times. The IT team shared this detailed evidence with AWS, which worked collaboratively with them to address the server performance and improve responsiveness to the remote locations.

A Successful ERP Migration

User complaints after an application migration are commonplace. The IT team's decision to benchmark performance of the legacy application and deploy monitoring to validate deployment decisions enabled it to optimize the migration and monitor and troubleshoot the new cloud ERP application efficiently.

Case Study: FIS Extends Visibility Beyond Network Edge With AppNeta by Broadcom

IT Operations Adapt to Evolving Networks

The IT operations teams inside leading financial technology (FinTech) provider FIS faced multiple challenges while trying to meet the key objectives of a company that provides solutions to 95% of the world's leading banks.

FinTech Requires Network Performance and Availability

FIS' services and customers are highly reliant upon IT infrastructure and reliable network connectivity. Ensuring optimal network performance is the foundation of the company's ability to deliver solutions and support customers' critical services.

"If a network device takes a hit, hundreds of apps and all the users relying on those apps can be affected," said a senior systems engineer.

Adapting to Changing Networks

Both FIS and its customers have grown increasingly reliant on cloud services, which means they're also increasingly reliant upon cloud providers' networks. Plus, with rising acceptance of remote and hybrid work, users now access resources via a diverse set of networks, including local Wi-Fi and third-party ISPs.

The user experience is highly contingent upon networks that reside outside the traditional borders of the enterprise network. Traditionally, end users accessed applications via stable, dependable corporate networks. Suddenly, those stable environments ceased to exist.

The Requirement: Visibility Inside and Outside the Data Center

"In recent years, we've been contending with an ever-expanding spiderweb of networking," the systems engineer explained. "Where communications used to be contained within a data center, the user experience continues to depend on networks and environments outside of the data center. To be able to continue to deliver 24/7 availability to clients, we have to be able to successfully monitor those domains as well."

The IT operations organization needed end-to-end visibility across these diverse networks. When issues arose, the team needs to quickly pinpoint exactly where along the network path the issue is occurring, whether it's within the FIS network or networks that ISPs, cloud providers, or other third parties manage.

Solution: Expanding Engagement with Broadcom

For several years, the team has been using on Broadcom solutions to support and optimize its IT service management.

"We've had a long and successful relationship with Broadcom," the systems engineer stated.

Over time, they've continued to expand their usage of DX NetOps by Broadcom. Today, they're using the solution to monitor fault, performance, and flow of their traditional and software-defined networking architectures. In addition, with the changing nature of their modern networks, they've had to transform the way they've done monitoring.

"We still have a lot of clients and networks on-premises, but we've had to extend monitoring to cloud services, including public cloud environments and our own private cloud services," the systems engineer revealed. "This has had a significant impact on our strategies and approaches for monitoring."

To meet this demand, FIS' IT operations group added AppNeta by Broadcom to its Broadcom toolset.

"We've recently purchased AppNeta by Broadcom, which is an excellent complement to the other Broadcom solutions we have," the systems engineer explained. "AppNeta enables us to look at the network path overall. When users encounter latency or connectivity issues, AppNeta enables us to quickly pinpoint which domain is responsible."

AppNeta Use Case Example: Tracing an Application Issue to a Data Center Network Device

AppNeta helped IT operations pinpoint a problem with an application delivered from a data center. Users were experiencing timeouts, latency, and connectivity issues. Various IT groups investigated the issue.

"We had bridge calls, so-called 'war rooms,' set up with various teams trying to diagnose the issue," the systems engineer explained. "If you don't have the right monitoring in place, these efforts can be chaotic, and mean time to resolution (MTTR) and mean time to innocence (MTTI) keep expanding."

Through AppNeta, the team was immediately able to pinpoint the cause of the issue to a network device. The device itself was failing to write errors to logs, which meant an operator accessing the device via command line execution would not have spotted the issue.

"It turns out a process was hanging," said the systems engineer. "We were able to detect the cause of the issue and point the vendor directly to what was happening. This substantially reduced resolution time for the vendor—and meant that the issue duration was kept to a minimum."

Overall Results

Faster MTTR and MTTI

With Broadcom solutions, IT teams can correlate individual device performance and end-to-end managed and unmanaged network path health. Now, they can pinpoint the root cause of any degradation that affects the user experience, whether it arises in managed or unmanaged networks. This enables network operations to identify and resolve any network issue much faster. In fact, with Broadcom solutions, the team was able to speed triage by up to 95%.

Improved Customer Satisfaction

AppNeta's active network testing of new service offerings enables FIS to validate every hop in the network path, from client to application, helping deliver optimized service levels. Improved triage and troubleshooting times ensure high availability of network services, which protects the company's reputation and continues to build loyalty with their customer base.

"Along with the evolution of our networks, we're transforming monitoring and continuing to ensure our services are available for customers 24/7," said the systems engineer.

Enhanced SLA Compliance

In the past, IT operations groups sometimes missed service-level agreements (SLAs).

"With Broadcom solutions, our team is better equipped to meet or beat our SLAs," the systems engineer explained. "This means we can avoid the financial penalties and poor customer experiences associated with SLA breaches."

Case Study: Box Achieves Google Cloud Migration Success with Kentik

Box, a leading provider of cloud-based content management solutions, used the Kentik Network Observability Platform for years to optimize its network infrastructure and enhance business performance. Box initially engaged with Kentik to monitor its on-premises infrastructure. However, when Box decided to expand network resources to Google Cloud, it looked to Kentik to help inventory on-premises resources and monitor a complex cloud migration.

Kentik's platform enabled Box to overcome network challenges, improve visibility, and empower its network team's successful migration of resources from its on-premises infrastructure to Google Cloud on a very short deadline.

The Migration Challenge

Box needed visibility into on-premises infrastructure throughout the migration process to ensure a successful implementation. The Box networking team decided to apply its existing Kentik solution.

"We love the dashboards and the custom alerts we get with Kentik. Adding another network monitoring platform would have made our jobs so much more difficult. With Kentik, we are confident that we have the visibility we need to take action to ensure our network is performing optimally," said Louis Bolanos, staff cloud network engineer.

That visibility enabled Box to discover lingering dependencies between cloud and on-premises services, helping to ensure an exceptional experience for customers.

Box's existing on-premises infrastructure still needed maintenance throughout the migration. Google's native cloud tools lack comprehensive visibility into network traffic, especially between on-premises and cloud and within container workloads. Monitoring and maintaining on-premises, cloud, and Kubernetes networks simultaneously without additional headcount would challenge this migration. Additionally, Box's network team knew it needed to pinpoint latency issues, bandwidth utilization, and hair-pinning between on-premises and cloud services.

Meeting security and compliance requirements was also an important consideration. Box needed to ensure stringent security measures were in place to protect sensitive customer data and comply with industry regulations while maintaining its high standard of seamless content collaboration and data sharing.

The network team realized that cloud costs could quickly spiral out of control without visibility into inter- and intra-cloud traffic flows. They needed to identify inter-region traffic volumes to perform cost attribution easily, even down to the level of Kubernetes clusters.

Kentik Enables Cloud Migration

Box turned to Kentik to help expedite and troubleshoot its migration to Google Cloud.

Kentik's advanced analytics and real-time traffic monitoring provide Box with deep visibility into its hybrid network infrastructure. Network behavior within and between container workloads, particularly Kubernetes, was also critical to the Box networking team.

Kentik Cloud allowed the networking team to analyze traffic patterns, identify bottlenecks and hotspots, and optimize network performance.

"Visibility into cloud-deployed Kubernetes clusters in Kentik is super clear and makes troubleshooting so much easier," Bolanos said.

Kentik's intelligent anomaly detection enabled Box to promptly identify and respond to unusual network behavior. Real-time alerts empowered the IT teams to proactively prevent potential service disruptions.

Kentik's security analytics capabilities allowed Box to monitor network traffic for potential security threats. With Kentik Protect, the team can easily monitor the network for malicious or anomalous activity.

The scalability and flexibility of Kentik's cloud-native architecture seamlessly integrated with Box's existing infrastructure and allowed the networking team to empower other stakeholders during the migration.

"We were able to provide custom migration dashboards for internal service owners, giving them the ability to observe traffic declines on services that were being sunset and discover misconfigured services routing calls to the wrong locations."

Kentik provided the visibility needed to ensure traffic flowing to, from, and within Google Cloud was optimized for performance and cost.

Ongoing Cloud Networking Success

Kentik played a critical role in helping the Box network team transition to Google Cloud. "Kentik saved us time and gave us full confidence that we'd be aware of and be able to respond to any cloud or on-prem network issues on a timely basis," Bolanos said.

With Kentik, Box could inventory and track migration progress efficiently, collaborate without pivot fatigue, and monitor/validate the performance of Box services during migration.

"The network diversifying into various flavors of virtualization on top of cloud migrations drove us to look at various aspects of network performance in different tools," Bolanos said. "Kentik's Google Cloud and Kubernetes observability allowed us to investigate traffic on Google Cloud VMs and Kubernetes clusters, including the separation of workload namespace to help simplify our suite of tools used for reporting and troubleshooting."

Kentik was instrumental in Box understanding and tracking traffic patterns between on-premises and public cloud-hosted services.

The Kentik Network Observability Platform helped Box achieve the visibility and responsiveness native tools couldn't provide while migrating to Google Cloud. Box can rely on Kentik when they need to introduce or extend to a cloud network, perform cloud migrations, or maintain hybrid cloud networks. "To save time and costs and improve the performance of hybrid networks, there's no need to retool if you use Kentik," said Bolanos.

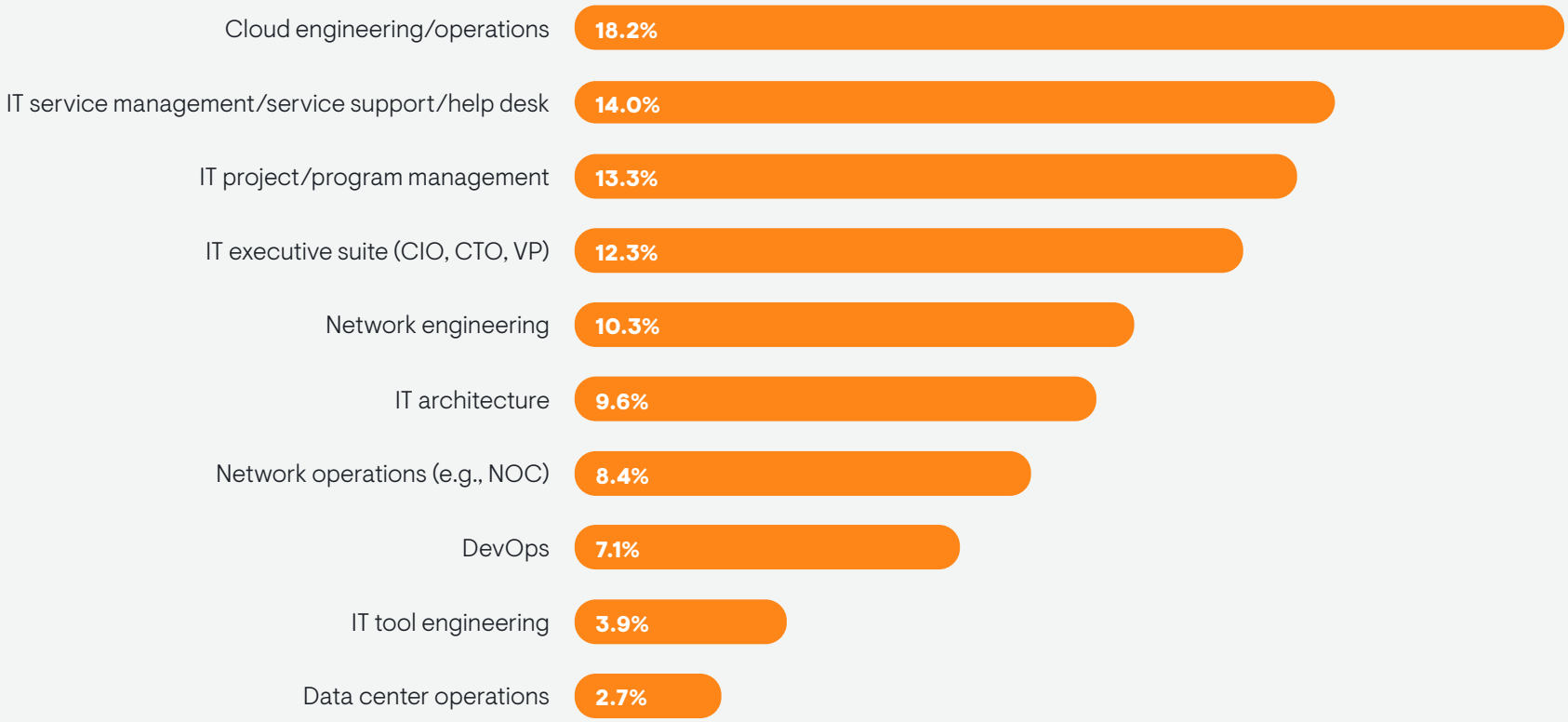
Implementing Kentik's network-agnostic advanced analytics and real-time monitoring capabilities enabled Box to optimize network performance, ensure data security, and improve overall operational efficiency.

Demographics

FIGURE 54. JOB TITLES OF RESPONDENTS

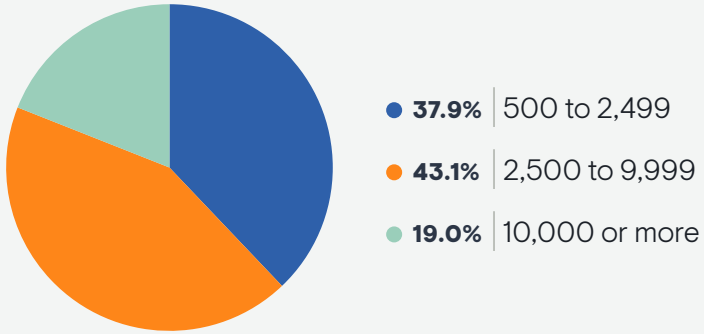
Sample Size = 406

FIGURE 55. IT GROUPS AFFILIATED WITH RESPONDENTS



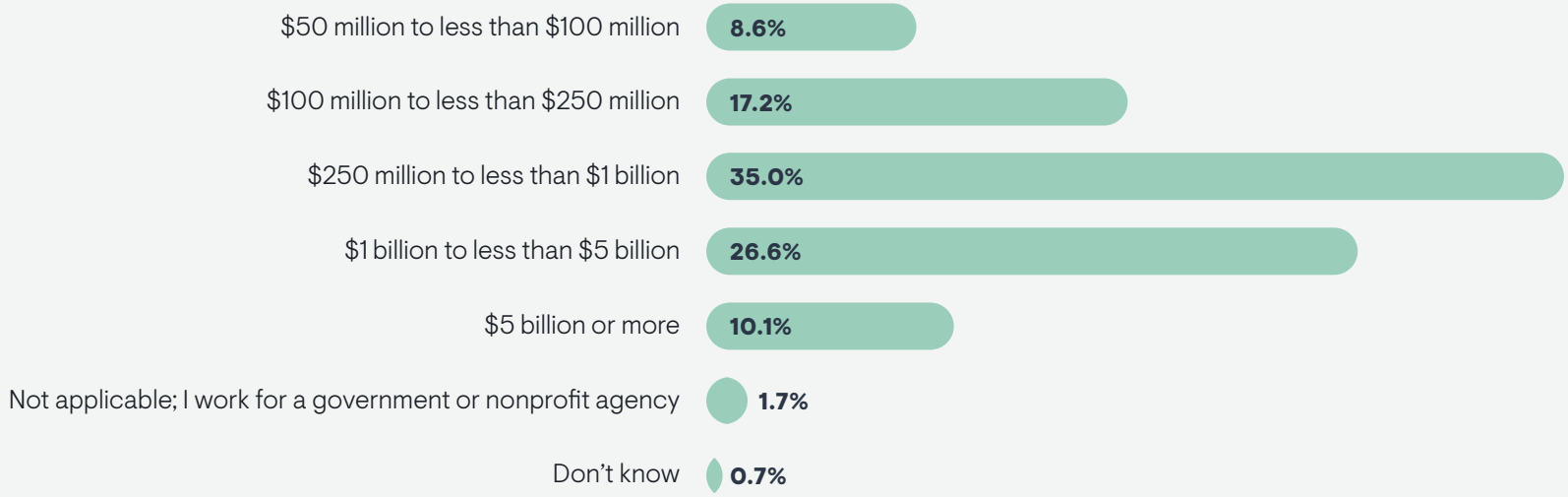
Sample Size = 406

FIGURE 56. SIZE BY EMPLOYEES OF RESPONDENT COMPANIES



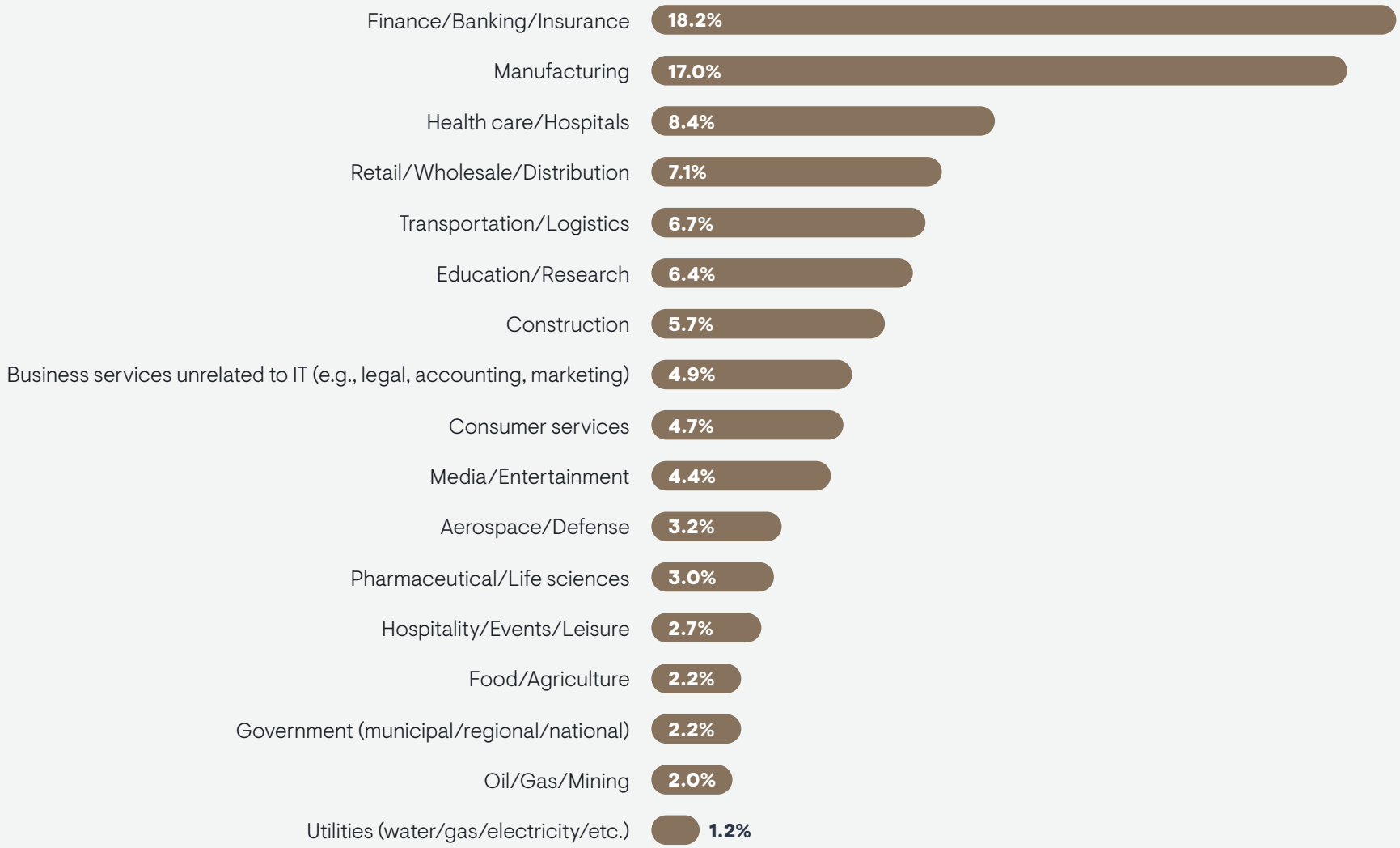
Sample Size = 406

FIGURE 57. ANNUAL REVENUE OF RESPONDENT COMPANIES



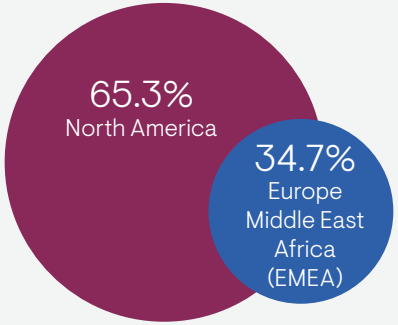
Sample Size = 406

FIGURE 58. INDUSTRIES REPRESENTED BY RESPONDENTS



Sample Size = 406

FIGURE 59. LOCATION OF RESPONDENTS



Sample Size = 406

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**.

This report, in whole or in part, may not be duplicated, reproduced, stored in a retrieval system or retransmitted without prior written permission of Enterprise Management Associates, Inc. All opinions and estimates herein constitute our judgement as of this date and are subject to change without notice. Product names mentioned herein may be trademarks and/or registered trademarks of their respective companies. "EMA" and "Enterprise Management Associates" are trademarks of Enterprise Management Associates, Inc. in the United States and other countries.

©2024 Enterprise Management Associates, Inc. All Rights Reserved. EMA™, ENTERPRISE MANAGEMENT ASSOCIATES®, and the mobius symbol are registered trademarks or common law trademarks of Enterprise Management Associates, Inc.

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

4407.050724