EMA
IT & DATA MANAGEMENT RESEARCH, INDUSTRY ANALYSIS & CONSULTING

Prepared for:

riverbed

Network Observability: Delivering Actionable Insights to Network Operations

October 2022 EMA Research Report

By Shamus McGillicuddy, Vice President of Research and Robert Gates, Senior Analyst

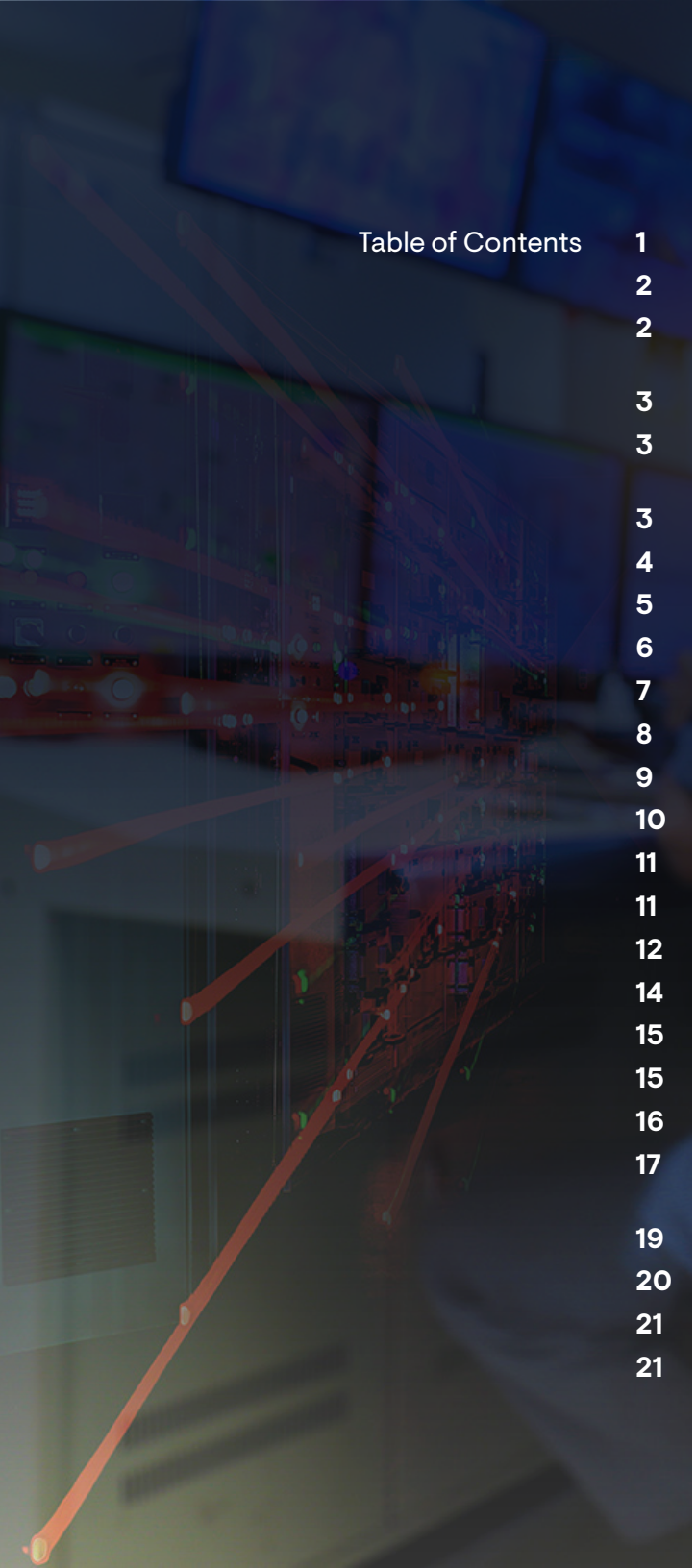


Table of Contents

1 Introduction
2 Network Operations Crossroads
2 Network Management Vendors Embrace Observability
3 Research Goals and Methodology
3 Defining Network Observability and Guiding Industry Innovation
3 Research Methodology
4 Network Snapshots
5 Defining Network Observability
6 The IT Practitioner's View
7 Finding Meaning
8 A Definition of Network Observability
9 The State of Network Operations
10 On Network Tools: "We Could Do Better"
11 The Extent of Global Network Observability
11 Proactive Network Operations
12 Answers and Insights
14 Observability Challenges
15 Alerting
15 Troubleshooting
16 Contextualized Alerts and Events
17 Tools Rarely Deliver Value Immediately Out of the Box
19 Network Observability Requirements
20 Strategic Drivers
21 Monitoring Priorities
21 Cloud
23 Empowering the Entire IT Organization
23 Reduce Escalations by Empowering Admins
24 Tool Democratization Across Silos
26 Network Data Requirements
26 Data Diversity is Critical to Network Observability
27 Volumes of Collected Network Data Exploding
28 Streaming Telemetry is Needed
29 Network Data Lakes are the Future
31 Data Challenges That Must be Addressed
33 Critical Insights
33 Security Insights
34 Observability Features
35 Rethinking Troubleshooting Workflows
36 Intelligent Observability with AIOps
38 Conclusion
40 Appendix: Demographics
46 Case Study: Alaska Federal Credit Union Gains Visibility and Actionable Insights with Alluvio by Riverbed

Introduction

Network Operations Crossroads

The tools that enterprises use to monitor and manage their networks are under a harsh spotlight today. Network operations teams are struggling to maintain visibility in a rapidly changing digital world. In fact, the number of network operations teams that are successful with their overall missions has declined from 47% in 2018 to 27% in 2022, according to EMA's Network Management Megatrends research.[1]

EMA research found that IT organizations are scuffling to hire and retain networking personnel, which leaves them with a dearth of people who know how to effectively use network monitoring tools. They are also challenged by tool sprawl, since network teams use 10, 15, or even 20 tools to monitor and troubleshoot their networks. Furthermore, most enterprises are now multi-cloud and modernizing their digital services with cloud-native application platforms, whereas network operations teams are struggling to maintain operational visibility.

Given all these factors, EMA believes the tools that IT organizations use to monitor and manage network health and performance must evolve.

Network Management Vendors Embrace Observability

Every IT organization maintains several tools for monitoring and troubleshooting networks and analyzing a variety of data to understand where and why network problems are occurring. These tools are also important to network security and capacity management.

Historically, network teams refer to these tools as "network monitoring" or "network performance management." More recently, tool vendors have started using the term "network observability" or a variation, such as "unified observability," to market their solutions. These vendors are borrowing a concept the DevOps industry embraced to describe the tools it uses to monitor dynamic application environments. DevOps defines observability as the process of understanding the internal state of a system by measuring its external outputs. In the context of DevOps, these external outputs are metrics, logs, and traces. However, network teams are dealing with network infrastructure, not applications. Network observability requires its own definition.

After more than one year of conversations with vendors about network observability, EMA has determined that the definition of this novel term is fuzzy at best. However, the emergence of network observability is notable because it signals that vendors are trying to articulate a new wave of innovation in their products.

EMA believes it is critical to define network observability for IT buyers, so they and their vendors can effectively communicate with each other about emerging network operations requirements and the innovations that vendors offer to address those requirements.

The emergence of network observability signals that vendors are trying to articulate a new wave of innovation in their products.

[1] EMA, "Network Management Megatrends 2022: Navigating Multi-Cloud, IoT, and NetDevOps During a Labor Shortage," April 2022.

Research Goals and Methodology

The goal of this market research is to define network observability and to provide a roadmap for IT organizations to navigate the marketing hype surrounding the term.

Defining Network Observability and Guiding Industry Innovation

The goal of this market research is to define network observability and to provide a roadmap for IT organizations to navigate the marketing hype surrounding the term. This research also aims to reveal how network tool vendors should evolve to provide better support to IT organizations. This report will help IT buyers understand what traditional network monitoring and network performance management vendors mean when they use the term network observability. The report should also help vendors establish a product roadmap for so-called network observability solutions.

Research Methodology

This research is based on a market survey of 402 enterprise IT stakeholders who are either responsible for their organizations' network management tools and/or are extensive users of such tools.

The survey participants were a mix of technical personnel, IT middle management, and IT executives. They worked within a variety of functional groups in IT organizations, most often in a network engineering and architecture group, a network operations center, or a CIO's suite.

The enterprises represented in this survey range in size from 500 total employees to 50,000 or more, with annual revenue ranging from $50 million to $5 billion or more. More than one dozen industries participated, with the most numerous being manufacturers, financial and insurance companies, retailers, non-IT professional services firms, healthcare providers, and energy and utility companies. Sixty percent of respondents were in North America and 40% were in Europe.

Full demographic details are revealed in the Appendix.

Additionally, EMA interviewed nine IT professionals one on one, primarily from Fortune 500 companies, to enrich our survey data analysis with qualitative insights. They are quoted anonymously throughout this report.

Network Snapshots

Figures 1 and **2** give readers insight into the size and complexity of the networks represented by the survey participants. Figure 1 details the size of networks by the number of network devices (e.g., switches, routers, firewalls, access points, etc.) that the IT organization is managing. These networks range in size from 150 devices to 10,000 or more devices. The number of devices on a network will impact the requirements that network teams have of their network observability tools, especially around scalability.

Figure 1. Network size (number of network devices under management)

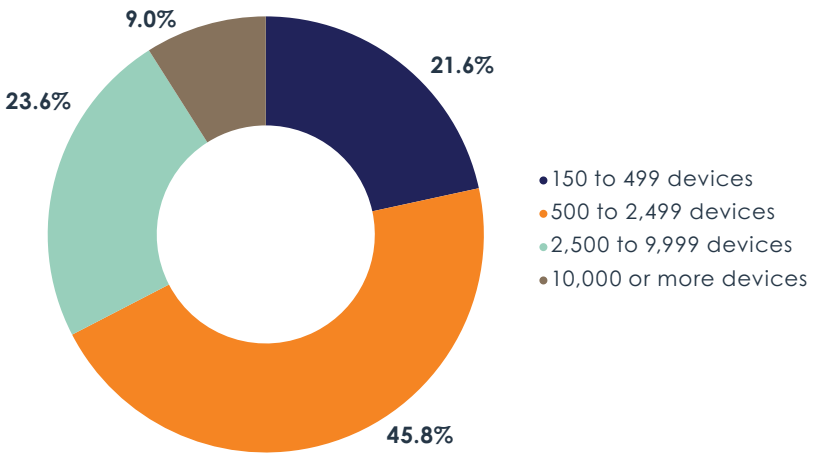
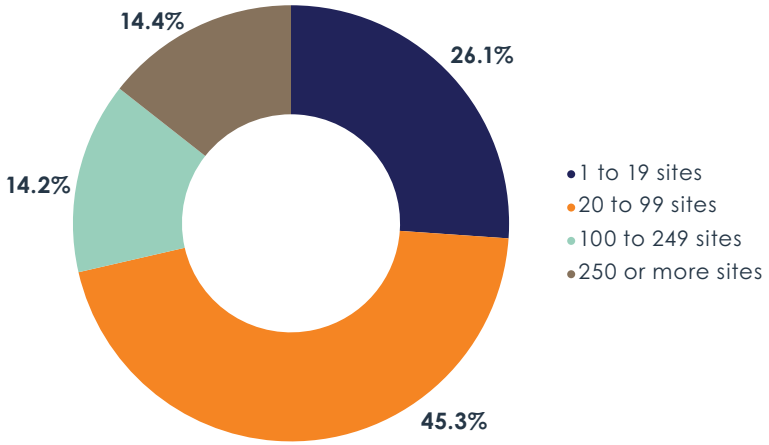


Figure 2 reveals how many corporate sites each company has connected to a wide-area network of the internet, not including home offices. A little more than one quarter have only 1 to 19 sites, while 14% have 250 or more connected sites. Highly distributed enterprises will encounter some complexity in collecting network data and monitoring the end-to-end performance of the network.

Figure 2. Number of sites connected to the network via a wide-area network or the internet



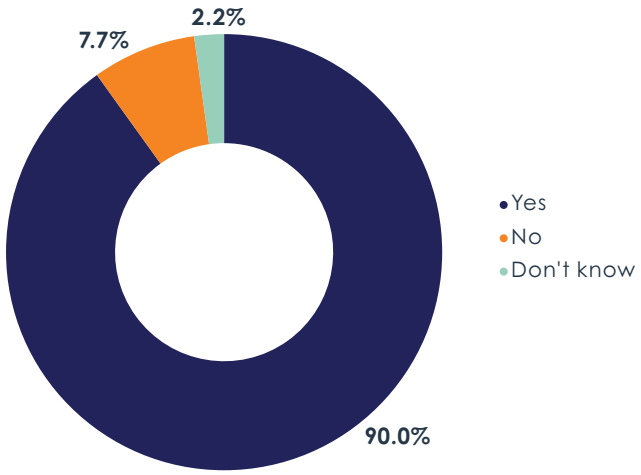
Sample Size = 402

Defining Network Observability

The IT Practitioner's View

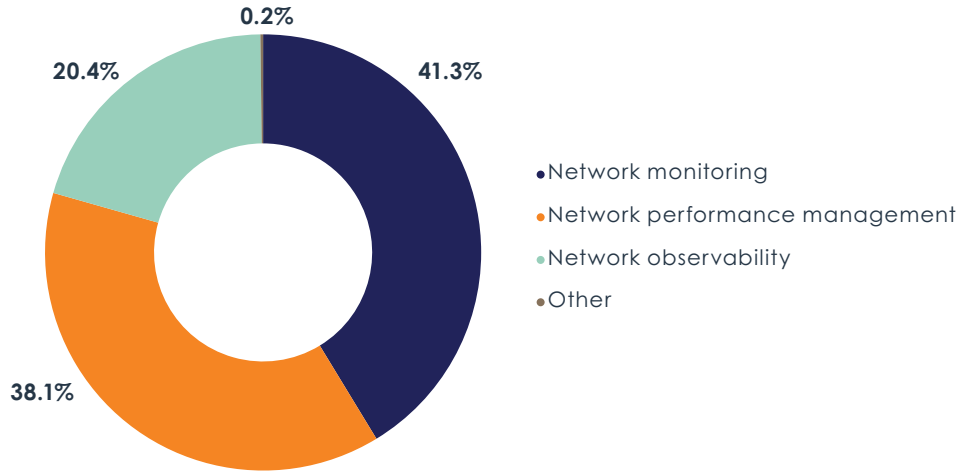
Although network observability is ill-defined, the term is resonating with IT professionals. **Figure 3** reveals that 90% of survey participants believe network observability is a useful term for describing the tools that they use to understand and manage the health and performance of their networks. IT executives were more likely to see the utility of the term while technical personnel, such as engineers and architects, were less likely, suggesting that vendor marketing around network observability has gained more traction in the CIO's suite than among network infrastructure and operations teams.

Figure 3. Do you believe network observability is a useful term for describing the tools you use to understand and manage the health and performance of your network?



Most IT professionals still think that network monitoring or network performance management are better labels for describing their tools, as **Figure 4** reveals. Only 20% prefer to use "network observability" today. One participant selected "other" and typed in "network health management."

Figure 4. Which of the following terms do you prefer when describing the tools your organization uses for monitoring and troubleshooting your network?



People who work in a CIO suite, network engineering, IT architecture, and cybersecurity were all more likely to prefer network observability than were members of a NOC. Note that highly skilled technical personnel who handle complex problems staff network engineering, IT architecture, and cybersecurity, while most NOCs are filled with less experienced technicians who specialize in simple monitoring and triage. EMA suspects that network observability resonates with users who need more advanced capabilities from their tools.

Also, respondents who reported the most success with their network operations tools were more likely than others to embrace the idea of network observability over monitoring and performance management.

Sample Size = 402

Finding Meaning

In one-on-one interviews, IT professionals had mixed opinions on what network observability means.

"For me, it's just another buzzword," said a network engineer at a $14 billion aerospace and defense company. "I'm still for the terms enterprise management or network management."

"I think it's just another catchphrase for network monitoring," said a monitoring engineer at a $15 billion financial services company.

"It's a broadening and deepening of network monitoring," said network engineer at a privately held gaming company. "We've been reasonably good at monitoring the network itself in terms of devices and paths on the network. But we haven't been able to see is what's really going on at an application level and how much network is impacting that."

"It's about getting insights from the network," said a network tools engineer at an $8 billion technology company. "It could mean more of a focus on the business impacts of the network."

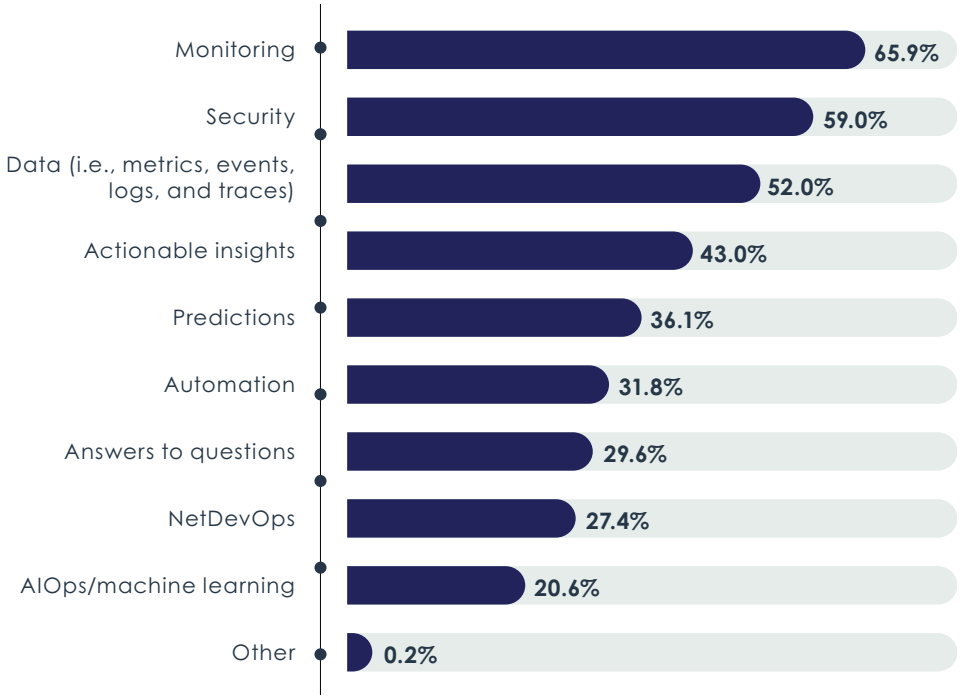
"Network observability is a superset of network monitoring. Monitoring is a subset of observability," said a network operations manager at a $500 million SaaS provider. "I think of monitoring as something that is not 'actioning.' Observability is about integration into event management, turning your observable metrics into something that alerts you or drives an action."

"Theoretically, monitoring is the collection of data, whereas observability is the analysis of that data to tell you if the system is behaving well," said a monitoring architect at a $35 billion media company. "The question is, who does that analysis, a human or the tool? Recently, I've seen tools with which AI and machine learning can enable anomaly detection without any setup of static thresholds."

In most of these interviews, IT professionals recognized network observability as something deeper than network monitoring, moving beyond the collection and presentation of data that most network monitoring tools excel at today. They hinted at a system that turns data into knowledge and actionable insights.

Figure 5 offers more guidance on what network observability means to IT professionals. Most survey respondents associated network observability with "monitoring, "security," and "data."

Figure 5. Words and phrases that research participants most associate with the concept of network observability



Sample Size = 402, Valid Cases = 402, Total Mentions = 1,470

We knew from our interviews that people believe that network observability overlaps significantly with network monitoring. The prominence of security broadens things for us. It's not just about understanding health and performance, but security, too. The popularity of data points to the fact that enterprises are collecting a larger volume and variety of data from their network than ever before. We will explore that issue shortly.

The top secondary selection in Figure 5 is "actionable insights." EMA believes that this is where network observability begins to distinguish itself from network monitoring and network performance management. Generations of network monitoring vendors have spent decades perfecting how they present data so that network engineers can combine data with their own knowledge of their networks to glean insights. EMA argues that network observability represents a step forward into something new. Whether through AI and machine learning, statistical analysis, or other algorithms and correlations, tools must find and present insights so that users can spend less time staring at data and more time acting.

Tools must find and present insights so that users can spend less time staring at data and more time acting.

Organizations that were the most successful with their tools were more likely to select three of the less popular items charted in Figure 5: AIOps, predictions, and NetDevOps. These more successful organizations are pointing to other concepts that should be considered when defining network observability. We already covered AIOps. "Predictions" suggests an interest in preventing problems before they impact the business. "NetDevOps" recalls the DevOps origin of the term observability. It suggests that network teams need to combine their observability efforts with DevOps teams. In fact, previous EMA research found that network and DevOps teams are trying to improve their partnerships. One key area of collaboration that EMA discovered in its research is around monitoring or observability. DevOps teams in particular have told EMA that they want to collaborate on monitoring and observability with network teams.

Members of a cybersecurity or IT security team were more likely to select "answers to questions" and "actionable insights," suggesting these capabilities are important to making network observability solutions relevant to security teams. Organizations with highly distributed networks (large numbers of WAN-connected sites) had an affinity for the word "predictions," suggesting a desire to mitigate complexity with more proactive operations.

A Definition of Network Observability

Given our findings, EMA defines network observability as the following:

A network monitoring system that collects a complete and diverse set of network data to provide deep visibility and actionable insights into the current and future state of a network. Those actionable insights include, but are not limited to, network performance, application performance, network security, and end-user experience.

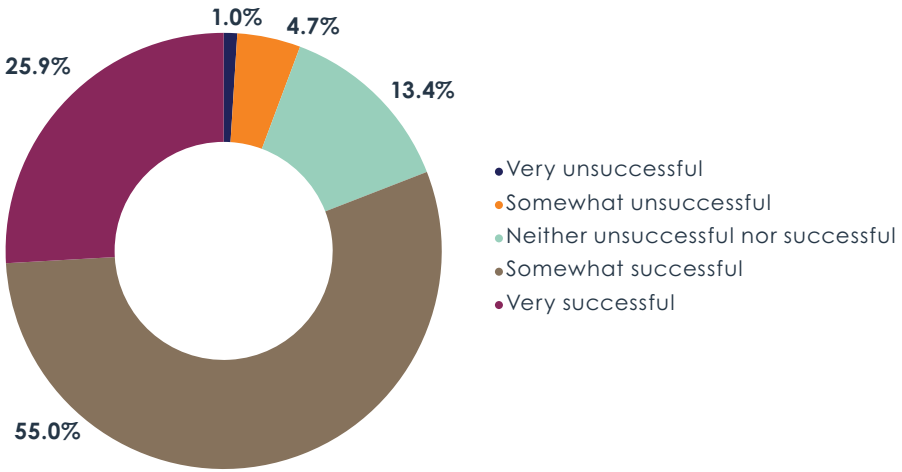
The State of Network Operations

On Network Tools: "We Could Do Better"

Only 25.9% of organizations are fully successful with their use of network monitoring or network observability tools.

This section explores how effectively network operations teams solve problems with the tools they use to monitor and manage their networks. First, **Figure 6** reveals that only 25.9% of organizations are fully successful with their use of network monitoring or network observability tools. A majority describe themselves as somewhat successful, meaning they know they could do better. A network team manager at a $70 billion financial services company offered a classic example of this sentiment: "On a scale of one to ten, I'd say we're at a 7 or 8. There are areas for improvement."

Figure 6. How successful do you think your organization is with its use of network monitoring or network observability tools?



Other interviewees explained why a self-assessment on tooling can be complicated.

"[Our tools] are doing okay, given that we've sunk tens of millions of dollars into them," said an IT operations manager at a very large government agency. "If you're willing to go to all the effort to get all the reporting right, they are fairly effective. The problem is that the larger your enterprise is, the longer it takes to know that something has gone wrong."

"We have certain tools that are fulfilling our needs, particularly newer tools," said a monitoring architect at a $35 billion media company. "There are some legacy tools with pain points that I'm trying to address. About half of my tools are meeting our needs."

"I'm very satisfied with one tool. It's feature-rich. We find that some other tools we use are less effective, with bugs that force us to wonder whether reporting reflects reality," said a network engineer at a $14 billion aerospace and defense company.

"The more time I spend in the industry, the more I feel like we're not getting it quite right," said a network operations manager at a $500 million SaaS provider. "It's a gut feeling. We have gaps for things such as the volume of events occurring on network devices. You can set a myriad of thresholds, but there will always be an edge use case that slips under the radar."

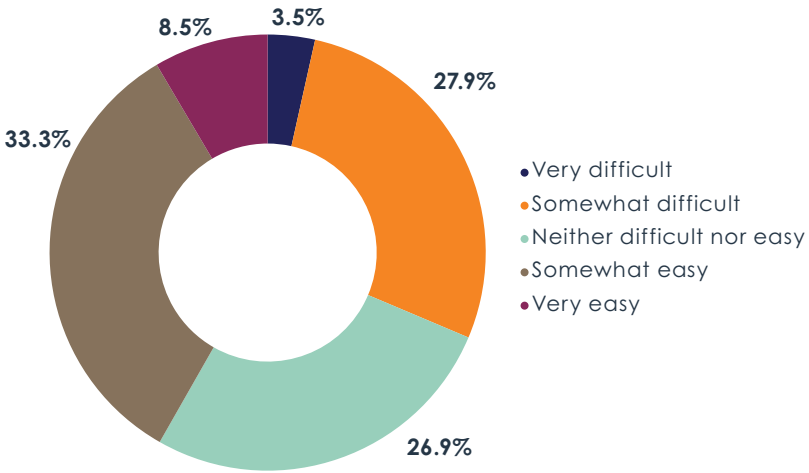
IT executives tended to report more success than middle managers (e.g., IT directors and supervisors), who in turn tended to report more success than technical personnel (e.g., admins, engineers, and architects). It appears that the closer a person is to the tools, the less successful they feel those tools are in serving the business. From a silo perspective, people in the CIO's suite and cybersecurity were the most sanguine about success. Members of network engineering teams, network operations, cloud operations, and IT architecture teams were all more pessimistic.

Sample Size = 402

The Extent of Global Network Observability

We asked participants whether they can get a global view of how their network is operating. **Figure 7** reveals that only 8.5% of organizations consider it very easy to establish this level of network observability. One-third described their view into the global network to be somewhat easy, suggesting that they can get there, but it takes some effort by engineers. More than 31% described this process as at least somewhat difficult. Naturally, respondents who reported the highest level of success with their network tools were the least likely to struggle.

Figure 7. Currently, do you consider it difficult or easy to gain a global view of how your network is operating?

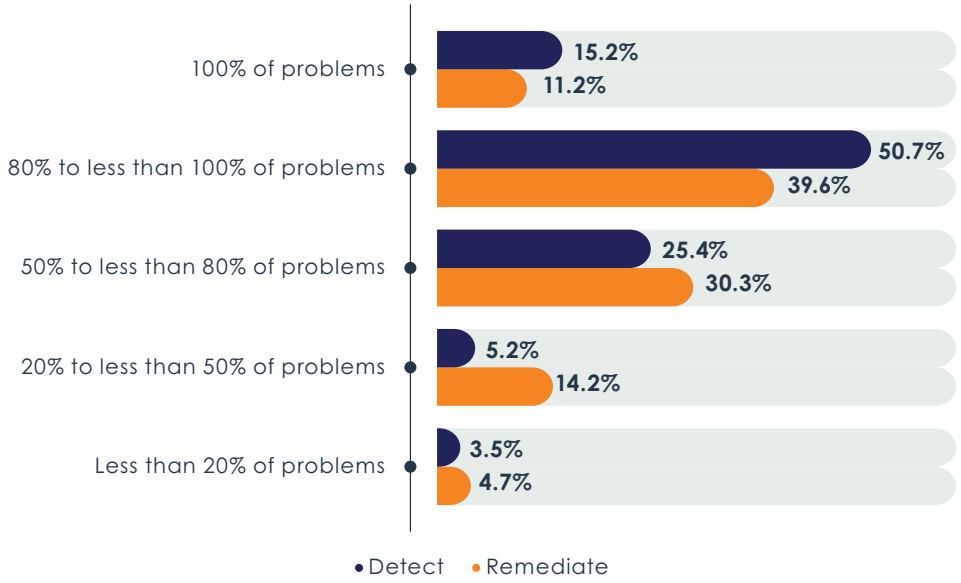


Operators of larger networks were more likely to struggle to get a global view of network operations. Also, members of network engineering, IT governance, and cloud teams were the most likely to report difficulty.

Proactive Network Operations

Figure 8 reveals the extent to which network operations teams can be proactive with network trouble. The majority of such teams are able to proactively detect at least 80% of problems before they impact the business, and about half of them are able to proactively remediate at least 80% of problems.

Figure 8. How often is your network operations team able to detect IT service problems before they impact the business, and how often is the team able to remediate them before they impact the business?



The most successful users of network monitoring and network observability solutions reported a higher rate of proactive operations. Cybersecurity professionals tended to report a higher rate of proactive detection and remediation. Members of network engineering teams were more likely to detect and remediate proactively a lower percentage of issues. Also, IT executives generally painted a rosier picture of proactive operations than technical staff, suggesting an awareness gap in the CIO suite.

Sample Size = 402

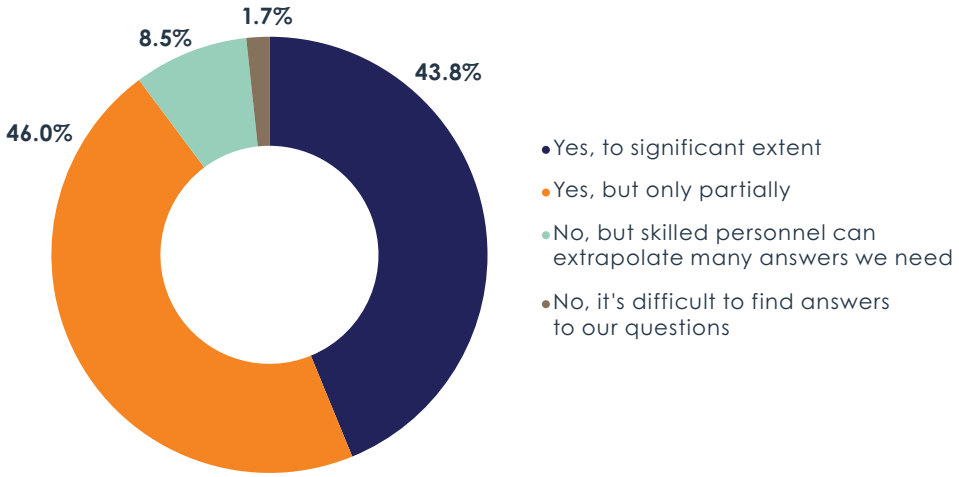
Answers and Insights

Many network operations professionals and network tool vendors have told EMA that network observability solutions should be able to provide easy answers to any questions that an IT professional might have about his or her network. EMA believes this is a fair requirement for a solution that is supposed to provide actionable insights into the state of a network. Thus, we asked research participants if they have a tool that can provide such answers.

Only 43.8% of respondents believe they have a network observability tool that can truly answer any question about the network.

Figure 9 reveals that most network teams do have such a tool, although the ease of getting to those answers varies. Only 43.8% of respondents believe they have a network observability tool that can truly answer any question about the network. Another 46% believe they have limited capabilities, and another 8.5% believe answers require significant extrapolation from data. The most successful users of network observability reported the most advancement in this area.

Figure 9. Do you believe that you have a tool that can answer any question that you might have about your network, such as questions about performance, security, capacity, compliance, and cost?



"You're collecting all this data and you can slice it up in any number of ways," said a network operations manager at a $500 million SaaS provider. "But you're not doing scalable network observability until you get have a system that can send an alert that can immediately say 'X, Y, and Z is happening, go look at it.'"

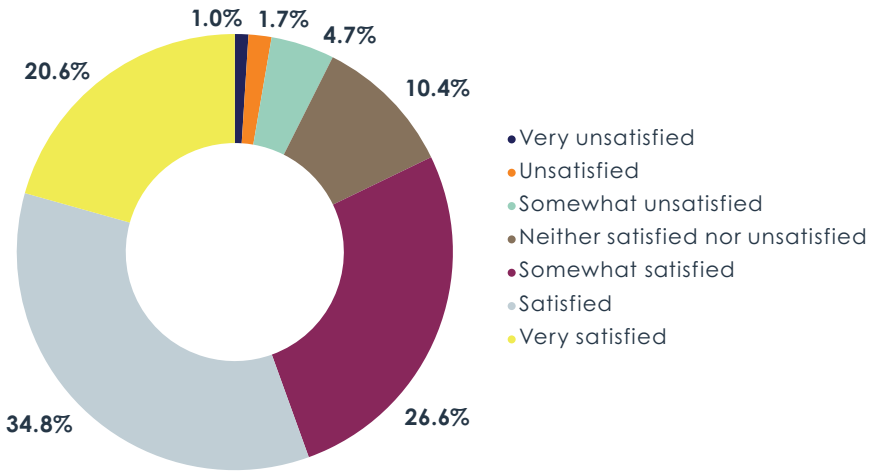
"Until recently, I expected a monitoring tool to know when something is down and when it's up," said a network tools engineer with an $8 billion technology company. "Now it's about, 'How can I proactively use the data to identify ongoing issues and get the insight to fix a problem before it becomes something serious?' Networks are becoming smarter, faster, and more automated. Monitoring has to shift with that."

Sample Size = 402

The approach that an IT organziation takes for tool procurement and implementation has a significant impact on this issue. For instance, this research found that enterprises with dedicated tool team that a focuses exclusively on network management tools are more likely to have tools with a limited ability to answer questions about the network. On the other hand, tool teams that take a cross-domain approach, buying and installing tools for all aspects of IT management, were more likely to provide tools to network operations that can answer questions.

Figure 10 reveals how satisfied IT professionals are with the actionable insights that their tools can provide. While most reported some level of positive feelings, only 20.6% were very satisfied. The rest saw room for improvement. Naturally, overall tool success correlates very strongly with satisfaction. Nearly half of very successful organizations were very satisfied with their actionable insights. IT executives tended to be more satisfied than middle managers and technical personnel. Members of NOC teams were more satisfied than members of the network engineering and security teams.

Figure 10. Satisfaction with the ability of network monitoring or network observability tools to provide actionable insights from network data



Most of the individuals EMA interviewed one on one saw at least some need to improve how their tools provide insights.

"I think most of the time I get what I need, but sometimes, depending on the complexity of the information, I will need to dig in and analyze the data on my own," said a network team manager at a $70 billion financial services company.

"With our tools, you can't take data in its raw form and have it tell you a story," said a network engineer at a $14 billion aerospace and defense company. "You have to dissect the layers of the data. It's a time-consuming process to get the data into a form in which the lightbulb goes on."

"I think [our tools are] good at presenting data to us. I don't know that any platform out there does a good job at providing insights," said a network operations manager at a $500 million SaaS provider.

"We don't have [actionable insights] today," said a NOC analyst at a private communications technology company. "We just see alerts and alarms. Then we have to go deeper. And we have to ask other teams, 'Can you check this out, too, to see if this problem is an actual problem and figure out what's going on?'"

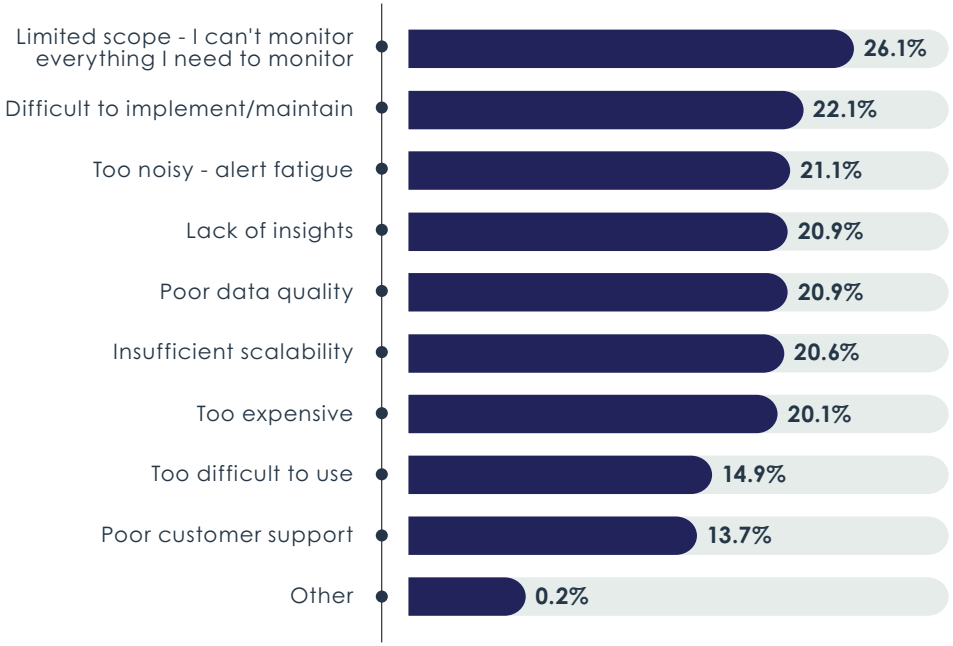
"I think [our tools are] good at presenting data to us. I don't know that any platform out there does a good job at providing insights," said a network operations manager at a $500 million SaaS provider.

Sample Size = 402

Observability Challenges

Figure 11 provides insights into why so few network teams are completely successful with their tools. The number-one issue is scope limitations. There are certain technologies or domains in the network that IT organizations cannot monitor. This issue is driven by the proliferation of disruptive technologies, such as public cloud and software-defined WAN. It's also driven by changes to business operations, such as work-from-anywhere.

Figure 11. Top complaints about network monitoring and network observability tools



Six other issues emerged as significant secondary challenges with tools. Members of IT architecture and IT program management groups were most likely to complain of difficulty with implementing tools. This difficulty was also more prominent among operators of the largest networks in this survey.

Small and medium companies tended to complain more about noisy alerts. Companies that were the least successful with their network monitoring and network observability tools were more likely to struggle with a lack of insights. They were also more likely to complain about poor customer support, which was otherwise the least problematic issue in this survey.

"There are things I'd like the network to tell me, or things I would like to know from the network, but the data and insights are not easily accessible in a practical way," said a network engineer at a privately held gaming company. "If a service is misbehaving or user experience is affected, I want to find out as fast as possible, but that's hard. Sometimes the network knows, but sometimes the network alone can't tell me what's wrong."

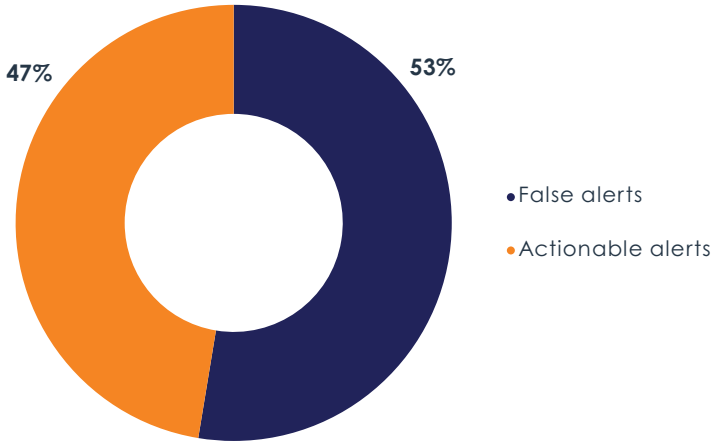
Operators of the smallest networks were more likely to complain about the expensiveness of their tools, although plenty of interviewees from Fortune 500 companies also complained about expense. "Cost is a big factor," said a network tools engineer at an $8 billion technology company. "Tool vendors are going to a subscription model, and that's making things expensive. Everyone we talk to is trying to do a million-dollar deal. They are trying to bundle the solution with so many other things to drive bigger deals. As soon as you go for a tool that is innovative, the price skyrockets."

Sample Size = 402, Valid Cases = 402, Total Mentions = 727

Alerting

Alerting is an essential component of network monitoring and observability tools. In network operations, admins and engineers spend a large percentage of their day responding to and investigating the alerts their tools generate. Unfortunately, alerts tend to be noisy. In their simplest form, tools generate alerts whenever certain conditions on the network change. Vendors and IT organizations devote significant resources to fine-tuning alerts to reduce noise. **Figure 12** reveals that plenty of work remains. Only 47% of alerts that network tools generate are actionable. The majority should be ignored. Unfortunately, it's difficult to know which alerts to ignore without investigating them.

Figure 12. Actionable alerts versus false alerts



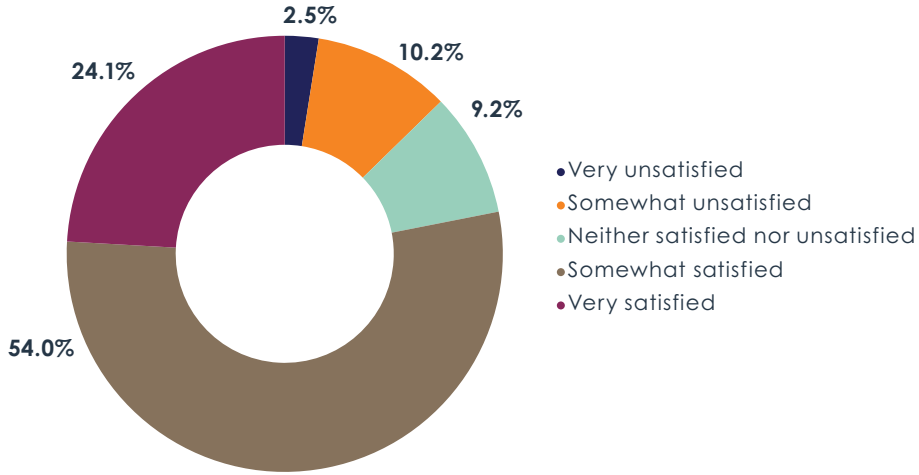
"We don't know which ones to check out, so we have to check all of them to verify that they are false alarms," said a NOC analyst at a private communications technology company.

Research participants who were the most successful with their tools reported a higher rate of actionable alerts. Members of security and NOC teams reported a higher rate of actionable alerts, but members of network engineering teams reported a lower rate.

Troubleshooting

Troubleshooting is one of the most critical processes that network monitoring and network observability tools support. When network teams receive an alert or trouble ticket, they must isolate the source of the problem, understand the root cause, and formulate a fix. In EMA's experience, skilled engineers do a significant amount of manual investigating during troubleshooting. Tools can provide clues, but much of the work is done in so-called wetware. Specific troubleshooting workflows in tools are limited. **Figure 13** supports this anecdotal view. Only 24% of survey respondents were completely satisfied with how their tools support troubleshooting workflows. Very successful users of tools were more likely (44%) to be very satisfied.

Figure 13. Satisfaction with network monitoring or network observability tools' support of troubleshooting workflows



Sample Size = 402

Troubleshooting is an arcane process that requires deep familiarity and trust in monitoring and observability tools. Thus, EMA was not surprised to learn that organizations with dedicated tool teams that select and implement tools for other teams to use tended to have tools with limited troubleshooting support. Respondents were more satisfied with troubleshooting support when they worked in organizations in which network engineering and operations teams select and implement their own tools. We also discovered a satisfaction gap based on job title. IT executives and middle managers were much more satisfied than the technical staff who tend to spend more time actually troubleshooting problems.

Members of the NOC team were more satisfied with troubleshooting support, which is unsurprising since they tend to escalate complex problems to network engineering teams. Members of the network engineering team were less satisfied with troubleshooting support. Troubleshooting satisfaction was also lower among operators of the largest networks, where complexity can make the process more difficult.

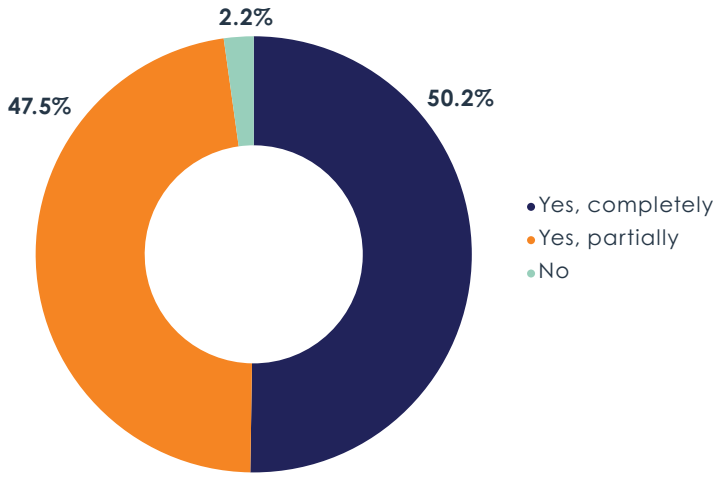
Contextualized Alerts and Events

One key piece of troubleshooting is context. When investing a situation, engineers need reports that can show how various alerts and data fit together. "When I see something is red, I want to be able click the alert and go to what the problem is," said a NOC analyst at a private communications technology company. "Vendors need to make it easier for us to identify what the problem is."

"My biggest pain point is aggregation and correlation," said a monitoring architect at a $35 billion media company. "How can you bring different views from different tools into a single view?"

Most network monitoring and observability tools can provide contextual reporting, but they vary in how completely they can do it. **Figure 14** reveals the extent of that variation. EMA asked survey takers whether they have a tool that can present a report on related events and network changes when they click on an alert in the tool's console. More than 47% say their tools have complete support of this workflow. More than half said they have only partial support.

Figure 14. When you click on an event or alert in your network monitoring or network observability tools, can the tools present a report on other events and network changes related to that event?



"My biggest pain point is aggregation and correlation," said a monitoring architect at a $35 billion media company. "How can you bring different views from different tools into a single view? I need to get alerts into a single pane of glass to find unique situations and conditions as they are happening."

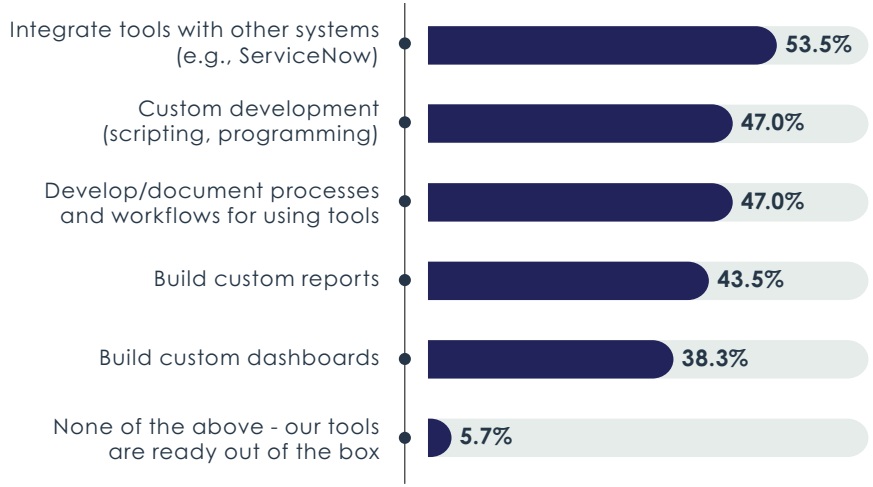
Successful organizations are much more likely to have full support of this contextual reporting. In a rare example of a good knowledge gap between leadership and staff, technical personnel were much more likely than IT executives to report full support in this area. Operators of the largest networks were also more likely to have this capability. Cross-domain tools strategies tend to enable this capability. Tool engineering teams that procure and maintain all IT operations management solutions were more likely to have these capabilities than tool teams that focus solely on network management tools.

Sample Size = 402

Tools Rarely Deliver Value Immediately Out of the Box

For all their rich features and capabilities, network tools require a great deal of customization and tuning before they deliver value. **Figure 15** reveals that only 6% of organizations can get useful insights from their tools without any customization. As tool vendors evolve from network monitoring to network observability, they must find ways to provide actionable insights out of the box. Some customization is inevitable, but IT organizations should expect more of their vendors.

Figure 15. To gain useful insights from network monitoring and network observability tools, IT organizations must customize and optimize tools in the following ways



"When you deploy a monitoring tool, you have to adapt the tool to your environment, train engineers on how to use it, and build processes around the tools," said a network tools engineer with an $8 billion technology company. "We have to do a lot of things for teams to build dashboards, reports, and custom integrations into other tools. Unless you have someone full time to adapt a tool to your network, insights are overlooked or not developed, and that leads to disappointment and management questions about whether they are getting value from an investment."

The integration with other systems is the most common requirement. EMA research often finds that organizations integrate network monitoring and network observability tools with IT service management, IT automation, and security monitoring. IT executives reported integration as a requirement more often than technical personnel. Some integration is always expected. For example, alerts in a network observability tool should open an enriched ticket in an IT service management system. However, the organizations in this research are telling EMA that integration is required for useful insights, suggesting that individual network monitoring tools cannot provide enough value without pulling information with other systems.

Nearly half of organizations also require custom development in the tool, using scripting and coding. The same number must also develop and document processes and workflows for using the tools, suggesting that tools are too difficult for most personnel to use without guidance from highly skilled engineers. A majority of the most successful research participants reported that their organizations develop and document processes and workflows, suggesting this is a best practice for organizations when they run into skills gaps.

A smaller number of network teams spend time building custom reports and dashboards. Less successful organizations were more likely to devote time to building custom reports. Operators of larger and more distributed networks were also more likely to build custom reports.

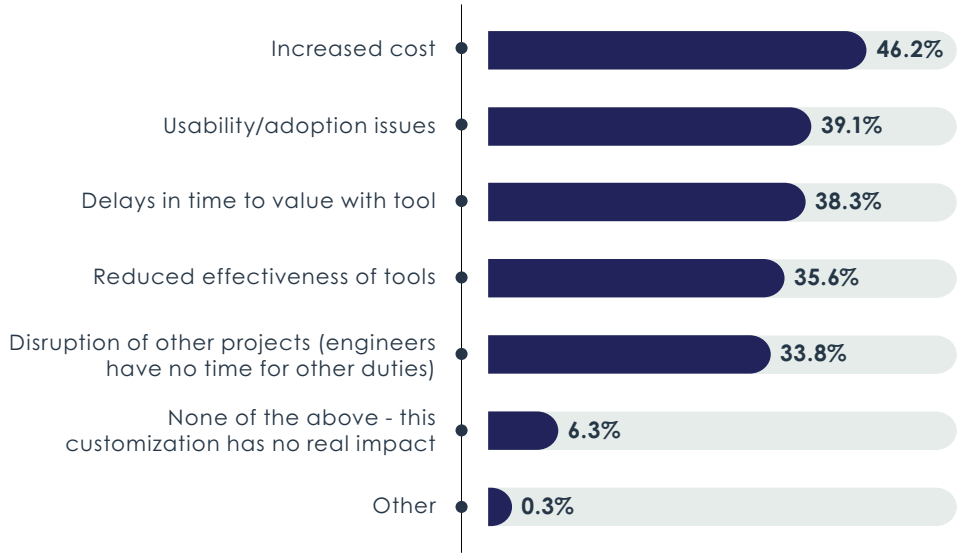
Sample Size = 402, Valid Cases = 402, Total Mentions = 945

This requirement for customization, integration, and documentation can have negative impacts on the value of the tool, as **Figure 16** reveals. Most often, this work drives up costs for an organziation. Cost is especially an issue for IT organizations that lack formal tool engineering teams. When network teams purchase and implement tools on their own, customization is more likely to drive up expenses.

Many organizations also experience problems with usability and adoption of tools. Many reported delays in getting value out of their tools. Delayed value is especially a problem for larger companies and usability is a bigger issue for operators of larger networks.

Some reported that tools are less effective when customization is required. More than one-third reported that this work disrupts other projects, as engineers have no time for other duties. Technical personnel were more likely to report disruption of other projects than IT executives, and members of network engineering teams were especially aware of this issue.

Figure 16. Negative impacts of tool customization



Sample Size = 379, Valid Cases = 379, Total Mentions = 756

Network Observability Requirements

This chapter offers IT decision-makers guidance on what to look for in a next-generation network observability solution. It explores the strategic drivers of tool selection and the solution requirements that network teams have. It also identifies some best practices for network teams to follow.

Strategic Drivers

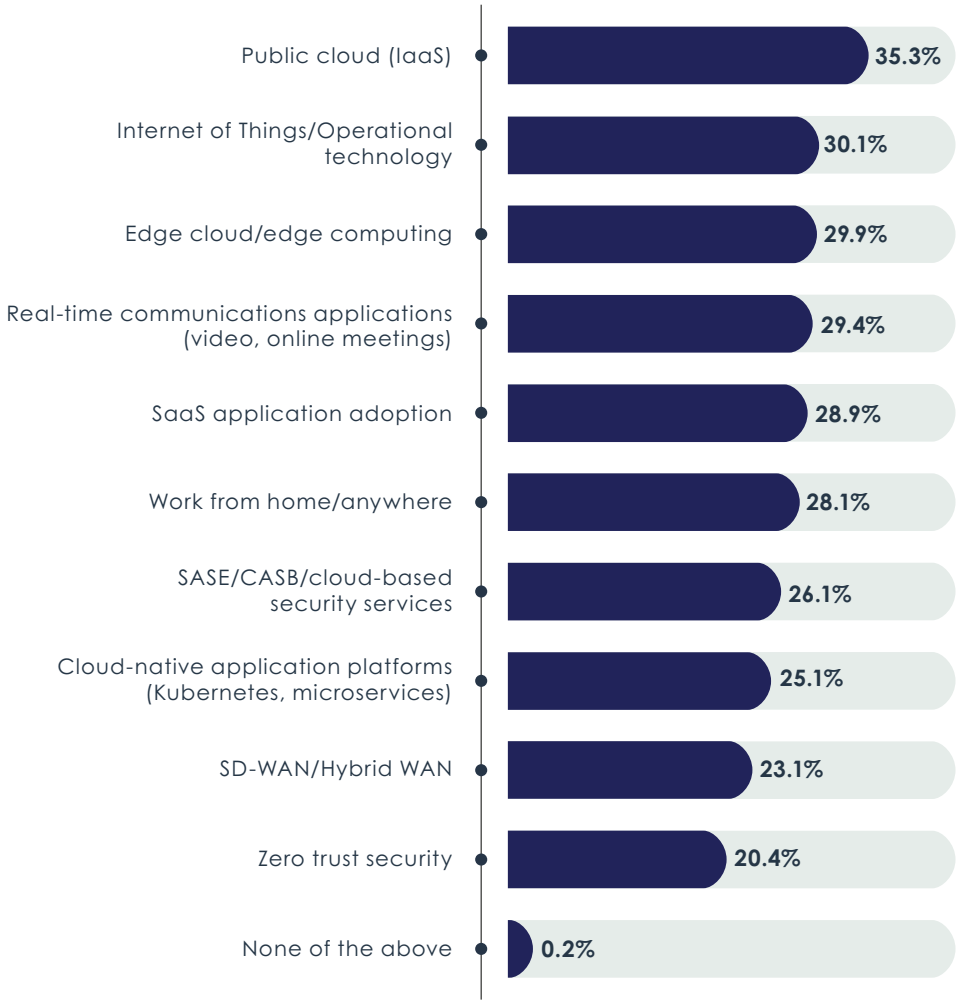
Figure 17 reveals the technologies and trends that are influencing the network management tool decisions that IT organizations make. Public cloud stands alone as the most prominent driver. This finding echoes additional ongoing EMA research, which found that over the last two years, network infrastructure and operations teams set their sights on public cloud and multi-cloud as the preeminent drivers of their strategies. The network engineering team and the CIO's office were more likely to identify the cloud as a driver, but the network operations team was less likely, pointing to a gap in understanding between different factions of the networking organziation.

The Internet of Things, edge cloud, real-time communications applications, SaaS applications, and work-from-home were secondary drivers. Here, EMA observed additional differences of opinion between the NOC and the network engineering team. Network operations was more likely to identify work-from-home and real-time applications as drivers, but the network engineering team was less likely. Instead, network engineering pointed to SaaS applications as a driver.

Cloud-based security (SASE/CASB), cloud-native applications, SD-WAN, and zero trust security were the least influential. However, highly distributed enterprises with large numbers of WAN-connected sites were more likely to select SASE/CASB.

The most successful users of network monitoring and network observability tools were more likely to identify the public cloud, cloud-native application platforms, and SASE/CASB/cloud-based security as drivers. Less successful organizations were more likely to select real-time communications applications and work-from-home as drivers. These differences potentially point to where current networking tools are best positioned to deliver value today.

Figure 17. Technologies and trends are driving new requirements of network monitoring or network observability tools

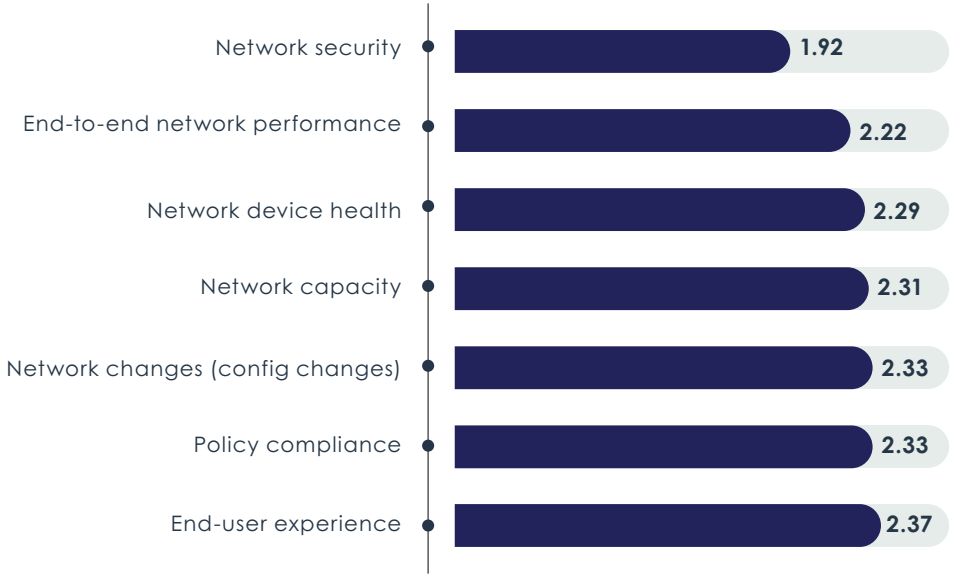


Sample Size = 402, Valid Cases = 402, Total Mentions = 1,112

Monitoring Priorities

EMA asked respondents to rate the priorities of seven aspects of the network that network operations teams might monitor. **Figure 18** reveals a strong focus on network security, followed by end-to-end network performance. Everything else is essentially tied for third. Successful users of tools were more likely to rate all of these as a higher priority, suggesting that it's a best practice to adopt network monitoring and network observability tools that can provide visibility into multiple aspects of network operations.

Figure 18. Mean responses: Monitoring priorities of the network operations team, with 1 being highest priority and 5 being lowest priority

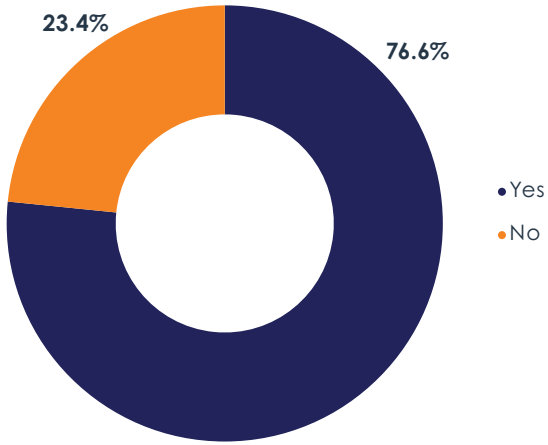


IT executives were more likely than technical personnel to place a higher priority on monitoring end-to-end network performance, policy compliance, end-user experience, and network security. Policy compliance emerged as more important to large enterprises than to small and medium enterprises.

Cloud

The public cloud is the top driver of network monitoring and network observability strategies. **Figure 19** reveals that 77% of network teams are attempting to monitor the cloud with the tools that they use to monitor on-premises networks. Network teams that buy and implement their own tools rather than rely on a dedicated tool engineering team are the most likely to try to extend their tools to the cloud.

Figure 19. Are the tools that your organziation uses to monitor on-premises networks also used to monitor the public cloud?

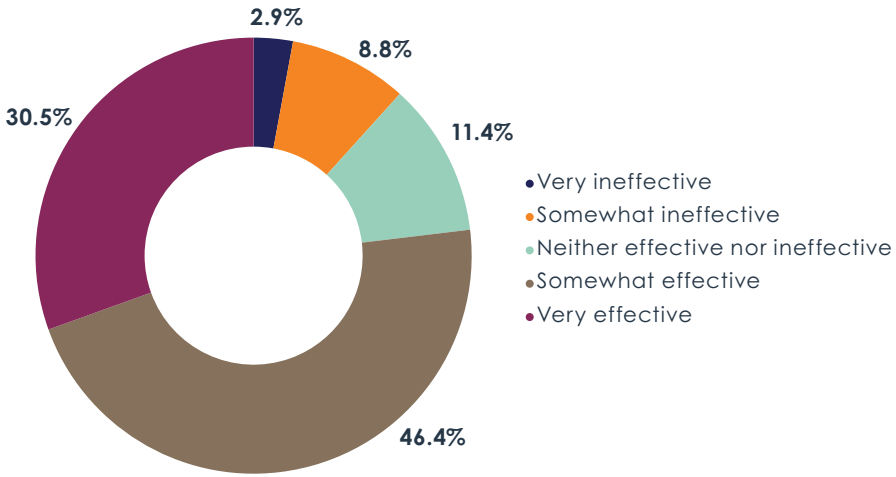


Members of security teams and cloud teams were less likely to report an effort to extend on-premises network tools into the cloud, but people from network engineering and the CIO's office were more likely.

Sample Size = 402

Organizations that reported the highest level of success with their network monitoring and network observability tools were the most likely to extend their tools to the cloud, but **Figure 20** reveals that few network teams are very satisfied with the visibility they're getting in the cloud. Less than one-third of companies have completely effective cloud visibility.

Figure 20. Effectiveness of on-premises network at monitoring the public cloud



"The more we migrate to the cloud, the more it changes how things work and what tools we use," said a monitoring engineer at a $15 billion financial services company. "Some tools are more cloud-friendly and some are more difficult to get to work in the cloud."

"There is a monitoring shortfall in the cloud," said a network engineer at a $15 billion aerospace and defense company. "The data is not as rich as we want it to be."

Effective cloud visibility corelates extremely closely with overall success with network monitoring and network observability tools, suggesting that adapting existing tools to the cloud can make or break network operations. Unfortunately, IT executives were much more enthusiastic about cloud visibility than the technical personnel who are most likely to use the tools. Only 19.5% of technical staff described the cloud visibility as very effective, versus 41.9% of executives. Within technical groups, members of network operations and cybersecurity were more enthusiastic than network engineering, DevOps, and cloud teams.

Sample Size = 308

Empowering the Entire IT Organization

Many network management tools are difficult to use. They offer dashboards that are easy to understand, but people with a shallow knowledge of network technology often get lost when they dig deeper. EMA believes that network observability solutions of the future should offer more value to a broader constancy of users.

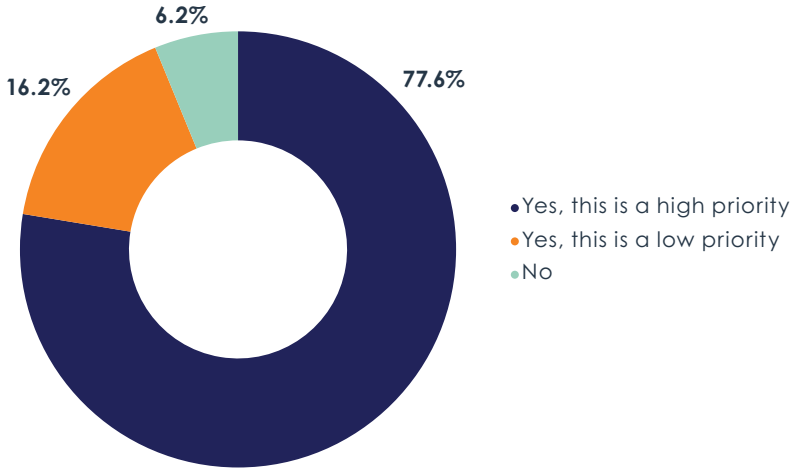
Reduce Escalations by Empowering Admins

Figure 21 reveals that IT organizations need to democratize tools now. More than 77% of organizations have made it a high priority to optimize their network tools so that lower-skilled admins can take on a larger share of problem-solving. Today, most NOCs are staffed by Tier 1 admins and analysts who often escalate complex problems to experts in network engineering, IT architecture, DevOps, and other groups whose primary missions are to design, build, and optimize infrastructure and services. Figure 21 makes it clear that organizations want tools that enable the NOC to solve more problems without escalating to other experts.

Technical experts who are on the receiving end of escalations from lower-skilled personnel were more likely to make this a high priority than IT executives. IT executives appear to be less aware of how critical this issue of empowering lower-skilled personnel has become.

"Transferring knowledge is my biggest challenge," said a network operations manager at a $500 million SaaS provider. "It's tribal knowledge. I am someone who tends to develop a deep knowledge and understanding of my platforms. I feel like I can take them to the next level. If I'm not available or my monitoring engineer is not available, it will be difficult for someone else to come behind us and understand how and why we did certain things. We try keep user experience as friendly as possible, but there are things that are necessarily complicated in order to achieve certain ends."

Figure 21. Does your organization's network operations strategy include a focus on enabling lower-skilled personnel to solve a larger share of problems with network monitoring or network observability tools?

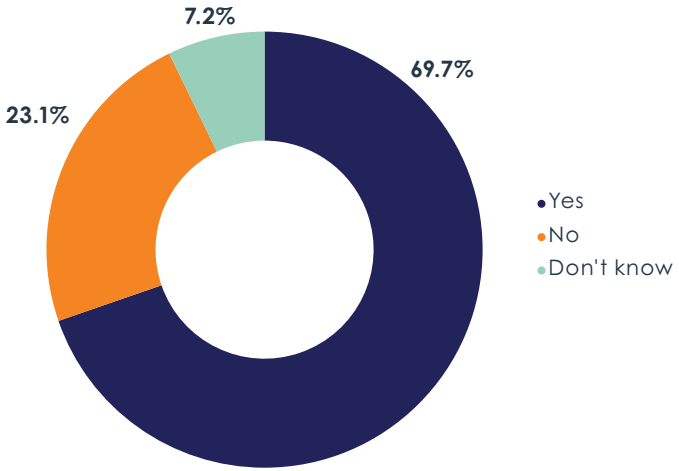


Sample Size = 402

Tool Democratization Across Silos

Figure 22 reveals that organizations also want to boost the relevance of their network monitoring and network observability tools to people outside network operations. Nearly 70% of network operations teams share their tools with other groups. This tool sharing is especially popular among organizations that are the most successful with their tools. Technical personnel were also more likely to report this cross-silo sharing of network tools, suggesting that it's very much an informal, bottom-up movement that IT executives and middle management are missing. They should provide more leadership here to ensure this tool sharing is as effective as possible. EMA found that organizations that are focused on empowering lower-skilled personnel with network tools were more likely to share those tools across siloes.

Figure 22. Other than the network operations team, are your network monitoring or network observability tools useful to any other teams in your IT organization?

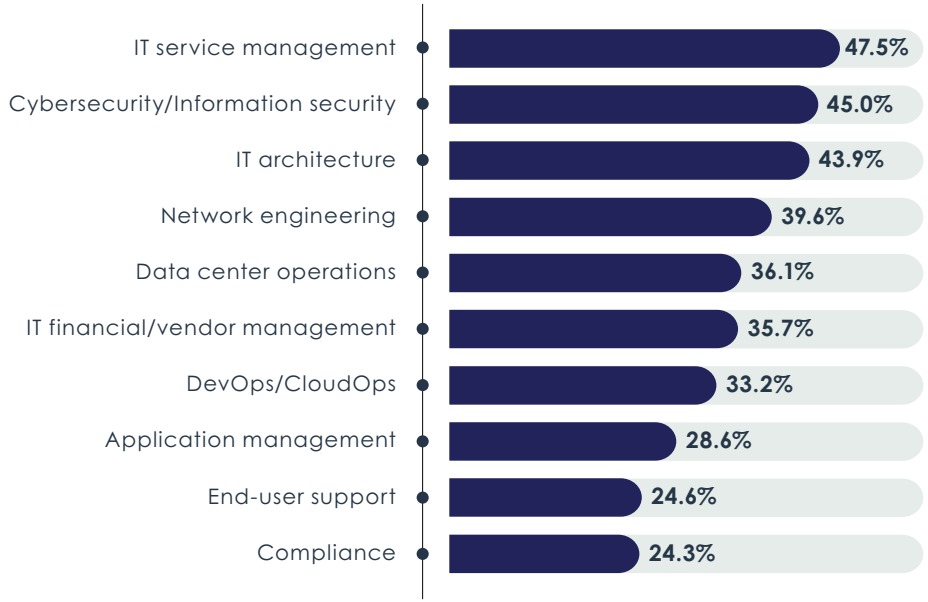


Sample Size = 402

Members of the network engineering and network operations teams were the most likely to report this tool sharing. DevOps and cloud teams were less aware, suggesting that network observability tools are either not offering them value or network teams are simply refusing to share with these groups. In either case, IT organizations need to focus on enhancing opportunities for these groups to leverage network tools.

Figure 23 reveals which groups are using network monitoring and network observability tools among the 280 organizations that share tools across silos. It points to three groups that are making extensive use of network tools: IT service management, cybersecurity, and IT architecture. Organizations that reported the most success with network monitoring and network observability tools were more likely to share these tools with all three of these groups.

Figure 23. Groups outside the NOC that use network monitoring and network observability tools



Sample Size = 280, Valid Cases = 280, Total Mentions = 1,004

"Our security team, cloud team, and help desk are all using our network tools," said a network tools engineer with an $8 billion technology company. "Some of them are able to use it because we developed a process for them and we developed dashboards. But it can be challenging for companies if they don't spend enough time to develop those processes."

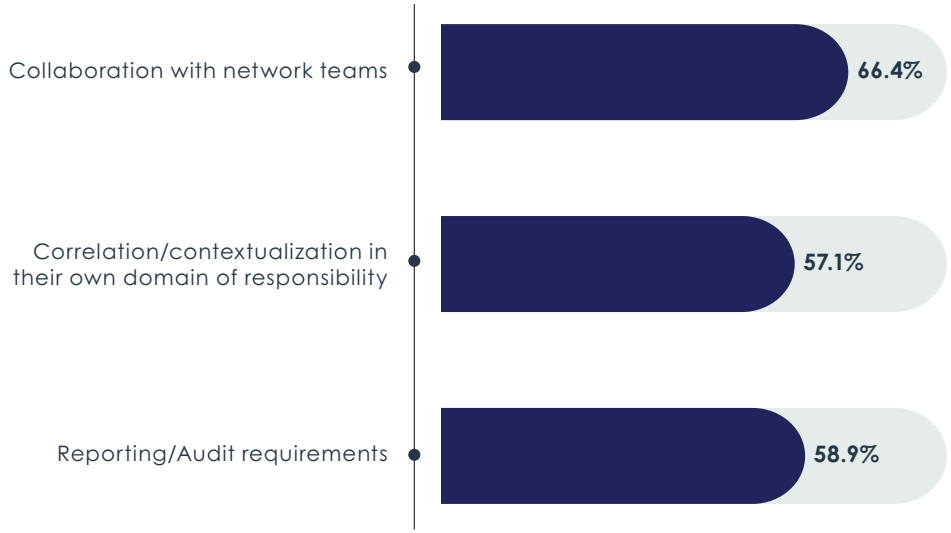
DevOps/CloudOps, application management, end-user support, and compliance teams are least likely to use these tools. In organizations that report the most success with tools, DevOps/CloudOps was a heavier user of network tools, suggesting that sharing tools across network operations and DevOps is an emerging best practice.

Figure 24 reveals how outside groups use the network operations team's tool. Collaboration with network teams is the top priority, but most organizations also reported that outside groups use network tools for correlation and contextualization in their own domains and for reporting and auditing requirements. Organizations that are the most successful with network tools are more likely to target collaboration and domain contextualization.

Tool engineering teams have some influence here. Reporting and auditing are more likely to be targets of this tool sharing when an organziation has a cross-silo tool procurement strategy, and less likely in organizations in which tool procurement is very siloed.

Technical personnel were less likely than middle management and IT executives to select collaboration. However, collaboration was more popular in organizations with the largest networks.

Figure 24. How other groups use insights from network monitoring or network observability tools



Sample Size = 280, Valid Cases = 280, Total Mentions = 511

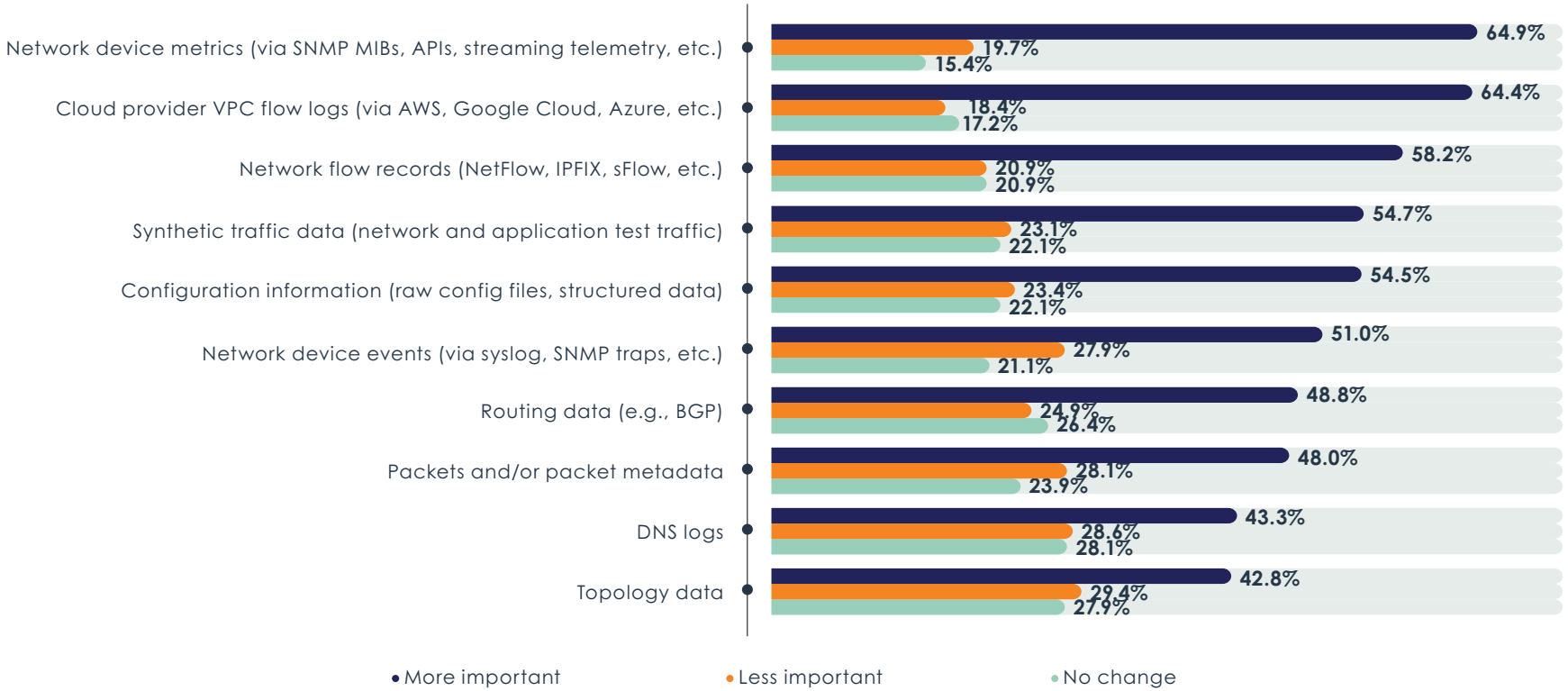
Network Data Requirements

Early in this report, EMA noted that data volume and diversity are a critical foundation of the concept of network observability. Metrics, logs, and traces are the currency of observability in the DevOps and CloudOps realm, but any veteran network engineer knows network operations requires a much broader set of data.

Data Diversity is Critical to Network Observability

Figure 25 reveals how the relative importance of various network classes of data has changed over the last three years for network teams. It reveals that the appetite for data diversity has increased across the board. Every class of data that EMA asked about is more likely to increase in importance than decrease. The most successful users of network tools were more likely to say every class of network data is growing more important.

Figure 25. Have any of the following types of network data become more important or less important to the management and monitoring of your network over the last three years?



Sample Size = 402

Network device metrics and VPC flow logs are seeing the most growth in importance. Device metrics have been a foundational source of data for decades, but somehow network teams perceive it as becoming even more important. Clearly, network teams believe VPC flow logs are a means for improved visibility into public cloud environments, which this report has already established as a significant challenge to network teams.

A majority of respondents also reported the network flow records, synthetic traffic data, configuration information, and network events are growing more important. Network teams are more likely than not to report that routing data, packets, DNS logs, and topology data are also becoming more essential.

Operators of larger networks were more likely to believe that device metrics, network flows, synthetic traffic data, and configuration information are becoming more important.

Volumes of Collected Network Data Exploding

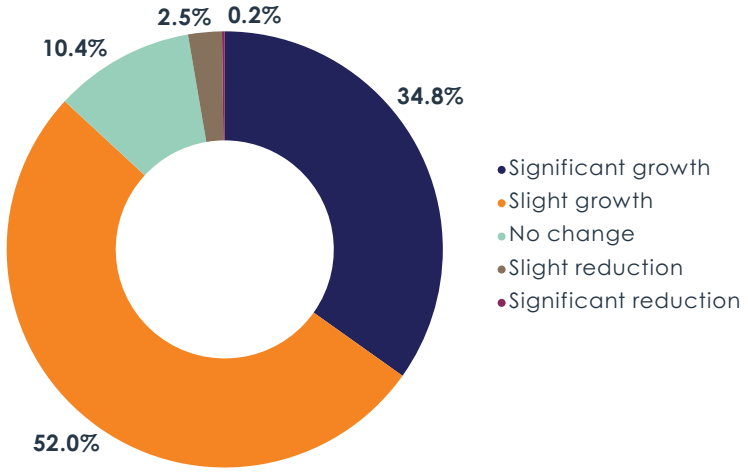
Nearly 87% of enterprises are experiencing growth in the volume of data they are collecting with their network monitoring and network observability tools, which points to the desire to build a complete picture of the state of the network. However, it also presages issues with tool scalability and costs.

Large enterprises and operators of larger and more distributed networks are reporting the most growth in data volumes. IT executives perceive more growth than middle management and technical personnel.

"We are collecting so much data," said an IT operations manager at a very large government agency. "Some of the things we collect, we have to store for years. We're also monitoring more things. It's not just about whether a box is up or its CPU is running. Now, we're monitoring transactions."

"Capacity constraints are a concern for our platform team," said a network operations manager at a $500 million SaaS provider. "The volume of data we send through analytics platforms is causing real performance concerns."

Figure 26. Changes in the overall volume of data collected by network monitoring or network observability tools



Sample Size = 402

Streaming Telemetry is Needed

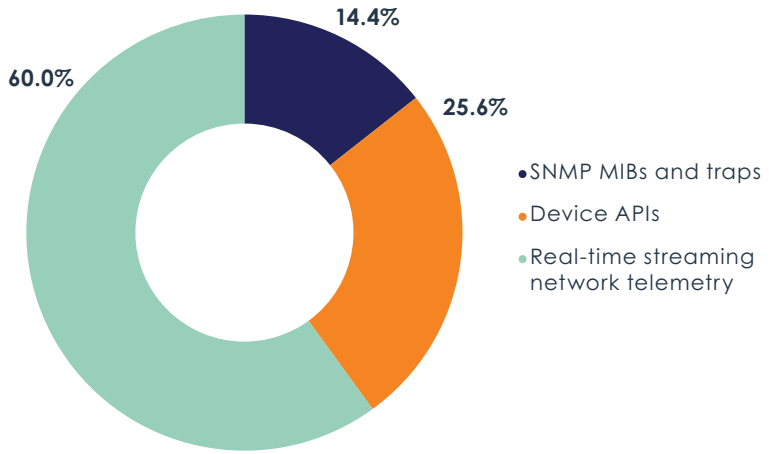
Given the increased focus on network device metrics and events, EMA is paying close attention to how network teams collect this data. For decades, tools have used SNMP to poll devices, but network engineers constantly complain about long polling intervals and other issues with SNMP. Network devices can also be configured to push device events to tools via SNMP, but these SNMP traps, as they are known, are unreliable. More recently, network device APIs have offered an alternative to SNMP. However, real-time streaming telemetry is emerging as the preferred means of collecting this data, as **Figure 27** reveals. Streaming telemetry allows tools to subscribe to device metrics and events. As conditions change on devices, the data is pushed to the tool in real time. SNMP has become the least popular means of data collection.

"Our legacy systems are collecting data at a five-minute frequency using the SNMP polling method," said a monitoring architect with an $35 billion media company. "We're looking at streaming telemetry so that we can get to 10-second intervals. We want to see microbursts. A lot can happen in five minutes. Streaming telemetry is also more efficient with data transfer. You no longer have request-response."

"We wanted to get SNMP off our network," said a network operations manager at a $500 million SaaS provider. "It's difficult to handle. You have to update MIBs, deploy collectors, point devices at collectors. We needed these SNMP traps in place to trip important fault alerts, but other traps that we don't care about are also generated, so we can get millions of events that we don't care about."

However, streaming telemetry is still an emerging technology. The industry hasn't settled on a standard, although a few candidates are out there. Some tool vendors haven't yet started supporting the technology and network device vendors vary in the extent of their support, with some of them offering it only on newer devices. Overall, support is spotty, but the appetite for streaming telemetry is massive, especially among operators of larger networks.

Figure 27. Preferred method for collecting metrics and events from network devices

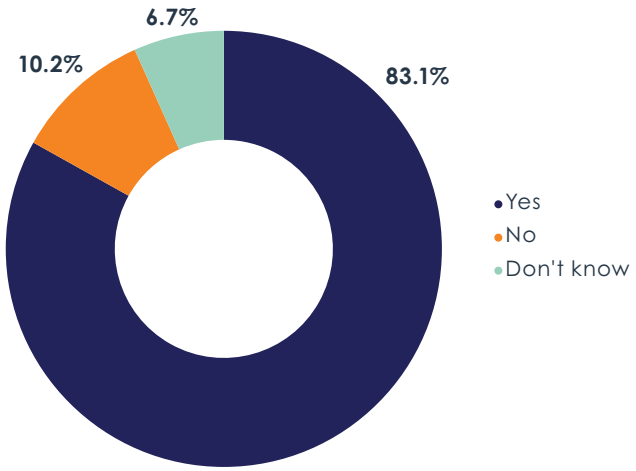


Sample Size = 402

Network Data Lakes are the Future

With network observability data diversity and volume expanding, EMA believes that many enterprises will seek a common platform for storing this data for ongoing analysis, especially since our research shows that both structured and unstructured data are becoming more important. In recent years, some network engineers and architects have revealed to EMA their intent to establish a data lake for networking data upon which they can perform queries and analysis with a variety of tools. **Figure 28** reveals that 83% of organizations are interested in streaming data from their tools to a central repository, like a data lake.

Figure 28. Are you interested in streaming data from your network monitoring or network observability tools to a central data platform, like a data lake?

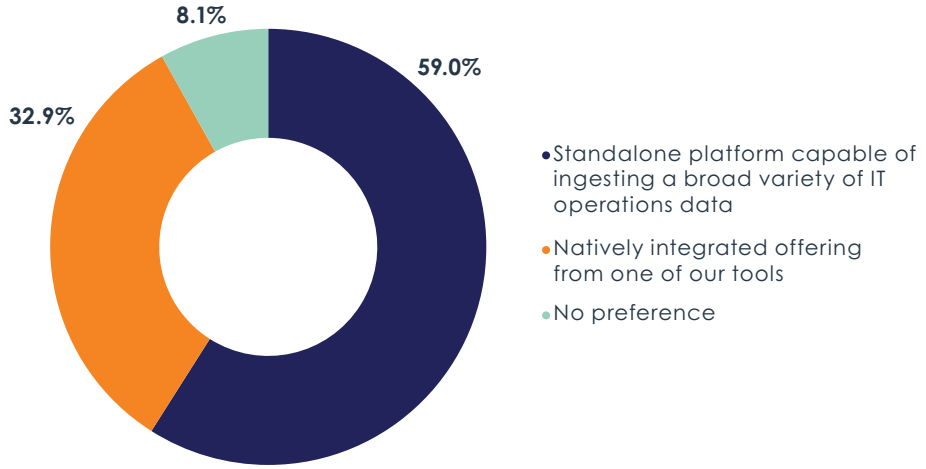


The most successful users of network tools were the most likely to have interest in these data lakes. Moreover, when teams outside the network operations group have interest in gleaning insights from network observability tools, an organziation is more likely to want to stream network observability data to a data lake. Respondents from the CIO suite and the network engineering team were more likely than other groups to express such interest.

Sample Size = 402

Figure 29 reveals that most organizations prefer to use a standalone data lake platform for this network data. Nearly one-third prefer a solution that is integrated with or native to one of their network observability tools. The standalone data lake is more popular in organizations in which multiple groups need insights from network observability tools.

Figure 29. Platform preferences for a centralized network data repository or data lake

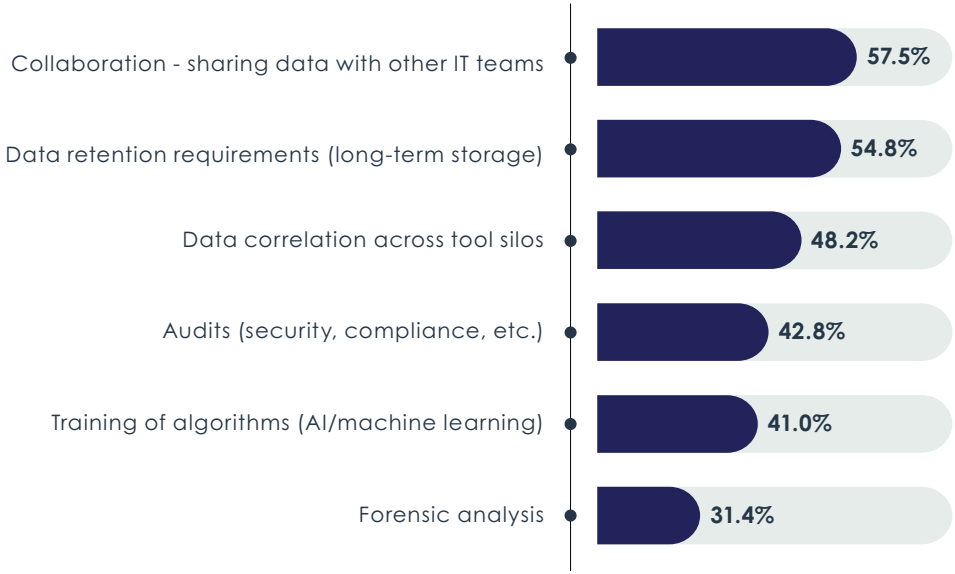


More successful users of network tools expressed a preference for a standalone data lake. Members of network operations and cybersecurity teams also had a stronger preference for the standalone data lake, but members of IT architecture groups preferred a data lake native to a tool.

Sample Size = 334

Figure 30 reveals how organizations plan to use these data lakes. Collaboration across groups in the IT organziation is the top priority. Operators of more distributed networks (250 or more WAN-connected sites) had the strongest affinity for this use case.

Figure 30. Top use cases for streaming data from network tools to a central data platform



Data retention was the other major driver of data lake interest. A majority of companies stream data from their network observability tools to a central data lake to address long-term storage requirements. The most successful users of network tools were the most likely to target this use case.

Correlation of data across individual network tools, audits, and algorithmic training (AI and machine learning) were the secondary use cases. Operators of very large networks were more likely to target audits.

"We need the ability to integrate data from other systems, show the data side by side so it's more correlated," said a monitoring architect with a $35 billion media company. "That will provide us with more insights."

"We have all this data. I'd love to stream all my monitoring data through something to identify anomalies," said a network operations manager at a $500 million SaaS provider.

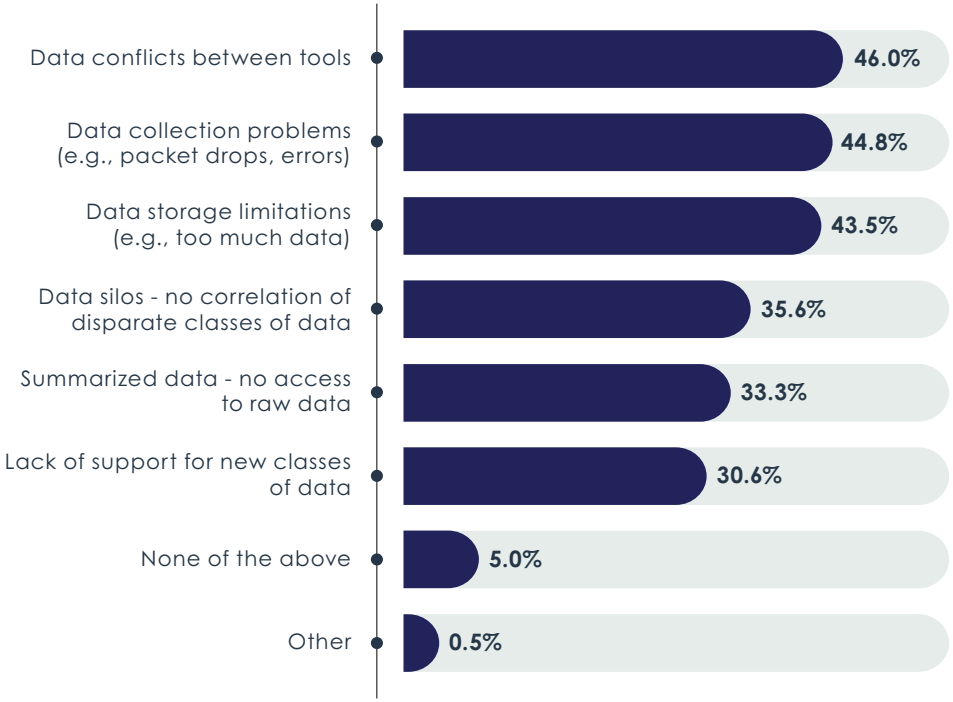
Forensic analysis was a niche use case, although it was immensely popular among network teams that acquire their own tools rather than relying on a dedicated tool engineering team. It was also a higher priority for organizations that prefer to adopt a data lake that is natively integrated with one of their tools, rather than a standalone platform.

Sample Size = 334, Valid Cases = 334, Total Mentions = 921

Data Challenges That Must be Addressed

Figure 31 identifies the challenges that organizations are having with data that their network tools collected. The top issue is related to tool sprawl. They have data conflicts between individual tools, which is probably limiting their ability to correlate insights across data types. This data silo conflict was a bigger problem for larger enterprises.

Figure 31. Data-related issues that present the most significant challenges when using network monitoring or network observability



Data collection problems and data storage limitations are the other two major issues. More distributed enterprises (with 250 or more WAN-connected sites) were more likely to complain of data collection problems, suggesting that they struggle to pull data from multiple sites into a central tool. Organizations that are the most successful with their use of network tools were more likely to struggle with data storage. Larger enterprises and operators of the largest networks were also more likely to struggle with this issue. In Figure 30, we revealed that data retention is one of the top use cases of a network data lake.

"We cannot keep up with the amount of data we are sending to tools," said a network engineer at a $15 billion aerospace and defense company. "People are demanding that our enterprise management team tune their logging when they add new devices to the network so that only minimal data is sent."

"I've had issues with systems not reporting the right data," said a network engineer at a privately held gaming company. "The basic input data is junk. The tooling can only help so much with that. There are problems with data classification being wrong sometimes. I also have issues around data retention. It costs money to store stuff long-term, and I don't have as much history at a level of granularity as I would like."

Data silos, summarized data, and lack of support of new types of data were secondary problems. Technical personnel and middle management were more likely than IT executives to complain about support for new data, suggesting that executives are less aware of the potential of cutting-edge data sources (e.g., streaming network telemetry) to improve network observability.

Sample Size = 402, Valid Cases = 402, Total Mentions = 962

Network observability vendors are constantly updating their solutions so that they can collect and analyze data from new and emerging technologies. On the one hand, as network infrastructure vendors introduce new versions of their existing hardware and software, tool vendors can usually adapt their tools with minor tweaks. On the other hand, completely novel technologies can require significant tool upgrades, as newer technologies challenge the data collection methods and data modeling techniques of vendors. **Figure 32** reveals the technologies that most challenge organizations' network monitoring and network observability tools today.

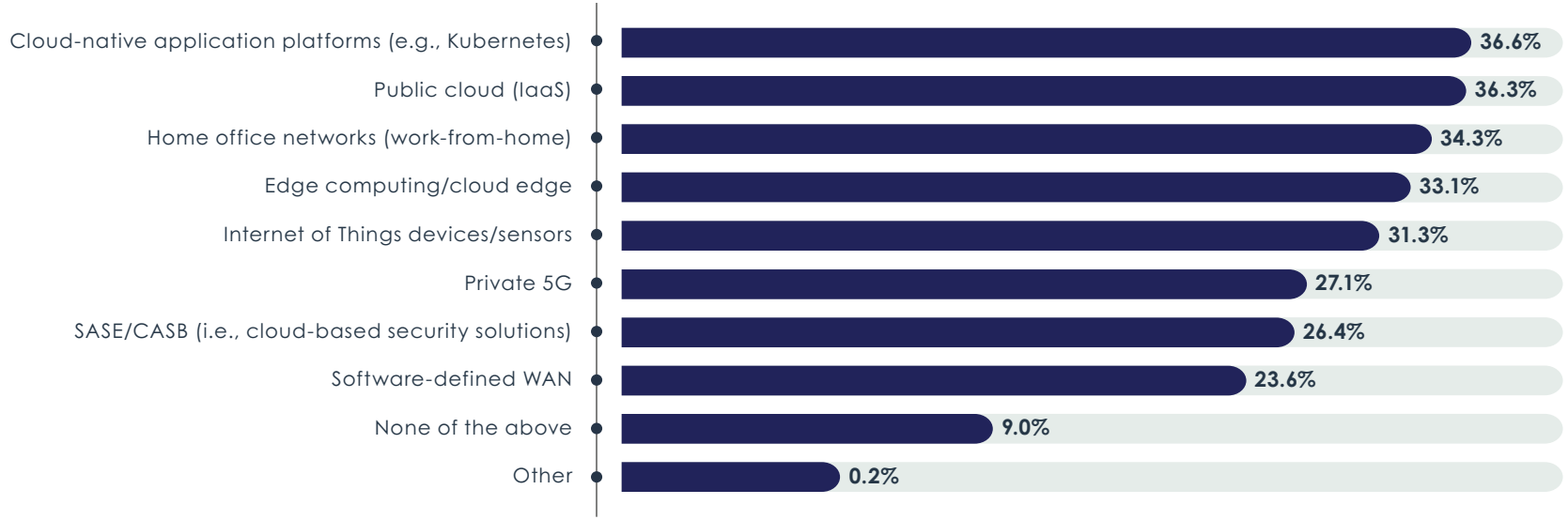
Cloud-native application platforms are the top challenge. In EMA's experience, most network management vendors are still developing solutions for capturing data about the network traffic that occurs between elements of a cloud-native microservices platform.

The other top challenge is public cloud. This research has already established that most network teams are dissatisfied with the visibility they're getting out of the cloud with their tools. IT executives were more likely than middle management and technical personnel to perceive a problem with cloud data collection. Members of the cloud architecture and operations teams were also troubled by the ability of network tools to collect cloud data, but the cybersecurity team was less concerned.

The technologies that are secondarily disruptive to data collection are home office networks, edge computing/cloud edge environments, and the Internet of Things (IoT). Technical personnel were more likely than IT executives to perceive a problem with home office networks and IoT. Organizations that are the least successful with their network tools in general were also more likely to identify IoT as a major problem.

Independence appears to bear fruit in this area. Network teams that procure and implement their own tools were more likely than those who rely on dedicated tool engineering teams to report that no technologies are particularly problematic.

Figure 32. Technologies that present significant challenges to collecting network observability data



Sample Size = 402, Valid Cases = 402, Total Mentions = 1,037

Critical Insights

As defined by EMA, network observability solutions must provide IT personnel with actionable insights. **Figure 33** reveals the types of insights that organizations consider most important. Security-related insights are the most valuable, and the most successful users of network tools were the most likely to rank security insights highest.

Figure 33. Organizations ranked the importance of insights offered by network monitoring or network observability tools, 1 through 7: mean responses

Root-cause insights into network problems are also a very high priority. Cybersecurity professionals were particularly interested in these insights.

Application performance, capacity, business impacts, and user experience are all secondary priorities for insights. Operators of larger networks ranked application performance insights as more important. DevOps, network engineering, IT governance, and the CIO's office were all more likely to embrace capacity insights. Network operations and security were cooler toward them.

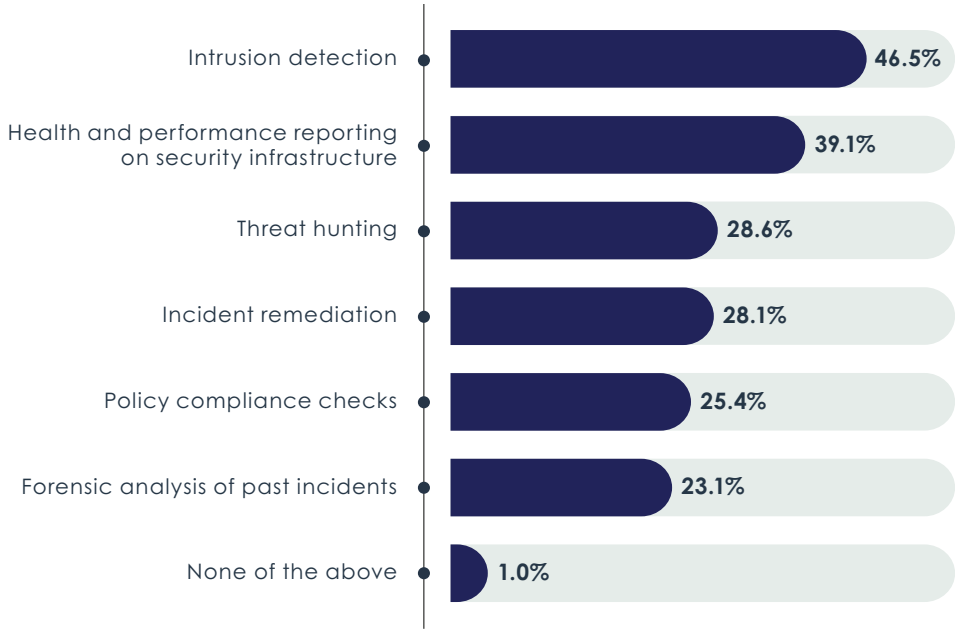
Sample Size = 402

Climate sustainability is a niche insight, ranked lowest by research participants. However, the most successful users of network tools were more likely to prioritize it, suggesting a potential emerging best practice.

Security Insights

Given the importance of security insights, EMA dove deeper into the topic as seen in **Figure 34**. Nearly half of organizations rely on these tools for intrusion detection, which points to the growing number of network tool vendors that have expanded into network detection and response solutions. Members of an IT architecture group were more interested in intrusion detection, but network architecture, network operations, and cybersecurity teams were less interested.

Figure 34. Security-related insights that are most important to get from network monitoring or network observability tools



Sample Size = 402, Valid Cases = 402, Total Mentions = 771

The other prioritized insight is the health and performance of security infrastructure. Many network operations professionals often tell EMA that cybersecurity teams rely on network tools to report on the state of firewalls and other security solutions.

Threat hunting, incident remediation, policy compliance, and forensic analysis are the niche insights that organizations seek. Threat hunting is particularly popular among network teams that procure and implement their own tools, rather than relying on tool engineering teams. Members of a cybersecurity organization were also more likely to have interest in threat hunting.

The most successful users of network tools were more likely to prioritize forensic analysis and health and performance reporting on security technology. Less successful organizations prioritized intrusion detection.

Observability Features

EMA asked research participants to rank the importance of various features when evaluating network monitoring or network observability solutions. **Figure 35** reveals that data visualization, traffic analysis, change detection and validation, alert management, and automated escalations are the most essential features.

"It would be good if [our tool] could tell us when we need to escalate something," said a NOC analyst at a private communications technology company. "Sometimes there is a lot of stuff happening in the NOC at the same time, and we are multitasking."

Survey respondents were clear that domain and protocol-specific analysis and application context (Layer 7 intelligence) were the least important, trailing the six most in-demand features by a significant margin.

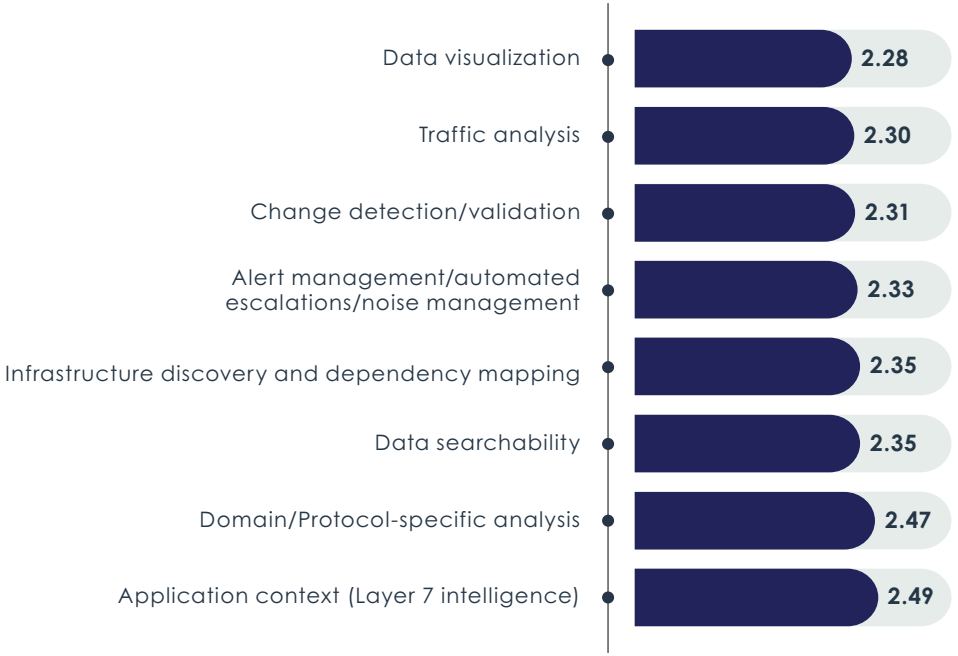
DevOps teams were most likely to list data visualization capabilities as a top priority. The cloud and IT governance teams joined them, while the NOC and IT architecture teams were least interested in data visualization. IT executives were more interested in it than technical personnel or middle managers.

Members of the CIO's office and the IT asset management team were more likely to rank the need for domain and protocol-specific analysis highly. The cloud team and IT asset management team were more likely to rank application context high.

Successful companies were the most likely to value change detection, data searchability, data visualization, and traffic analysis as the most important features when selecting a network monitoring or observability solution. Change detection is also highly valuable to highly distributed companies.

Technical personnel aren't focused on alert management and automated escalations to the same extent as IT leaders and middle management.

Figure 35. Importance of general network observability features on a scale of 1 to 5, with 1 being most important and 5 being least important

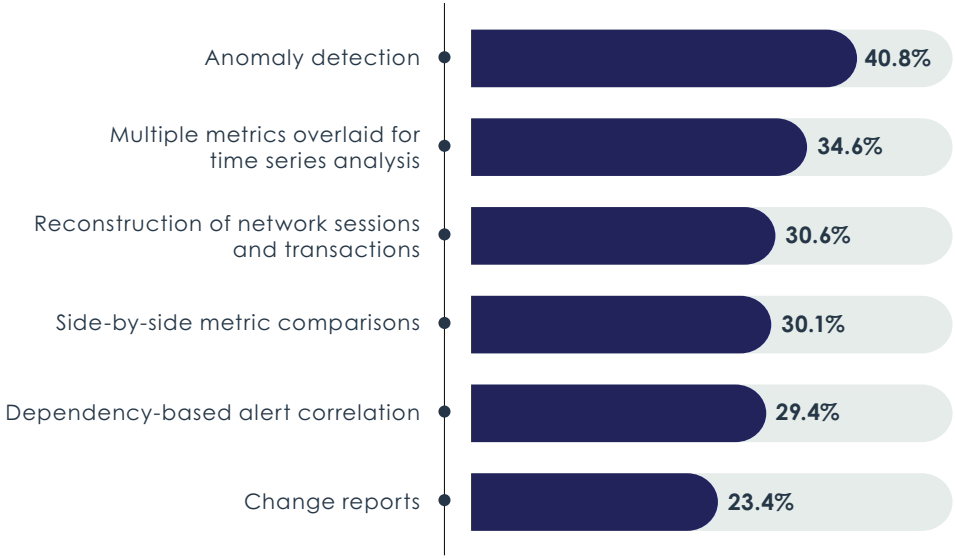


Sample Size = 402

Rethinking Troubleshooting Workflows

Figure 36 reveals the most critical troubleshooting features. Anomaly detection is the top priority. Also important is having multiple metrics overlaid for time series analysis. Operators of more distributed networks and larger networks were more likely to require multiple metrics overlaid for time series analysis, as well as side-by-side metric comparisons.

Figure 36. Troubleshooting capabilities most valuable in a network monitoring or network observability solution



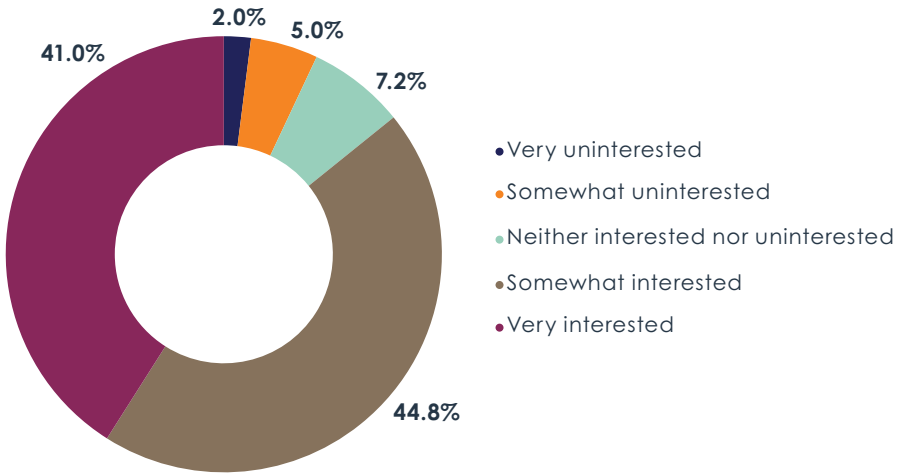
Very successful users of network tools were more likely to need solutions that can present multiple metrics overlaid for time series analysis. Successful teams are also more likely to want a feature that can reconstruct network sessions and transactions.

Change reports are a lower priority and were favored more by less successful organizations. However, technical personnel and middle management were more likely to require change reports than IT executives.

Sample Size = 402, Valid Cases = 402, Total Mentions = 759

Figure 37 shows that nearly 86% of respondents have at least some interest in automating troubleshooting with their network monitoring and network observability tools. Successful tool users were much more likely to have strong interest in this automation. IT executives had more interest than technical personnel and middle management. Members of network engineering and network operations teams were less interested than cybersecurity, cloud, and IT architecture teams. Interest was also higher among operators of larger and more distributed networks.

Figure 37. Interest in automated network troubleshooting

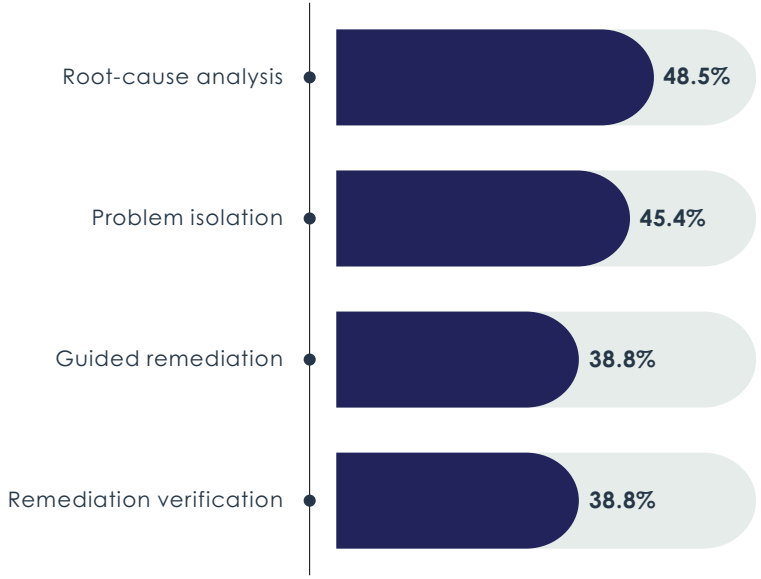


"When something happens, we want a seamless fix with automation," said a network tools engineer with an $8 billion technology company. "It should trigger an alert that triggers an automation script that checks issues, fixes the problem, and close the ticket, all without paging a person. I don't see many tools that can do it, but you can build it in-house if your vendor has web hooks or APIs. Productized automated troubleshooting with AI and machine learning would be great."

Sample Size = 402

Figure 38 reveals that enterprises are most interested in automating root-cause analysis and problem isolation.

Figure 38. Troubleshooting tasks that organizations want to automate



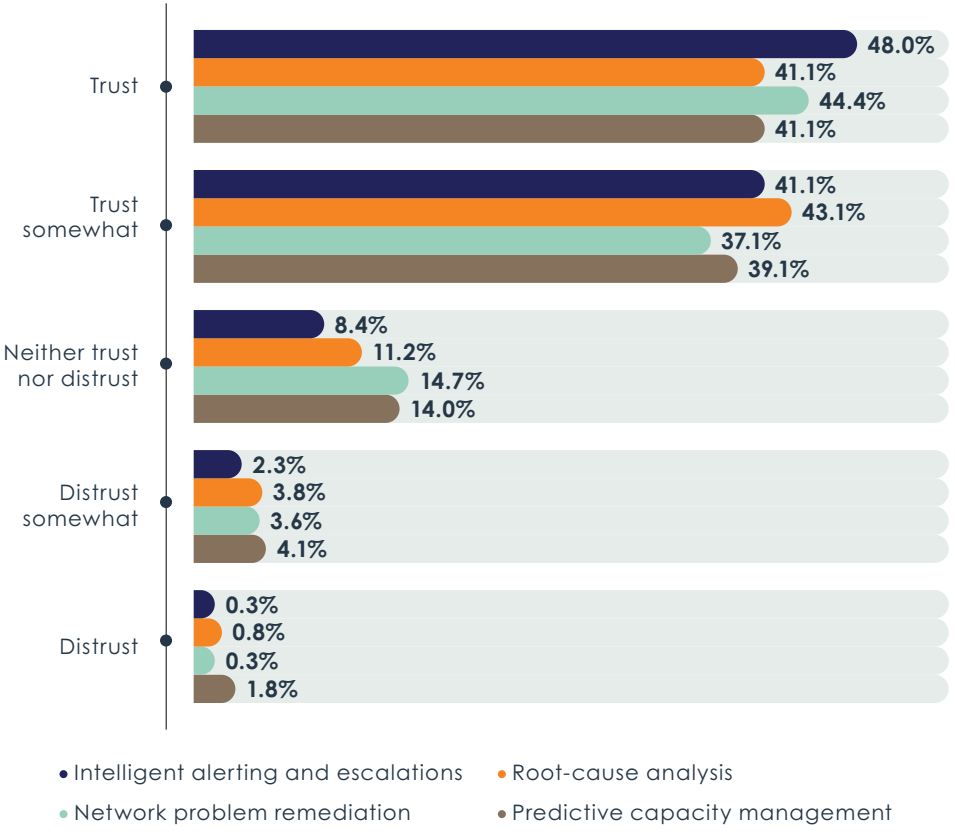
Guided remediation and remediation verification are secondary priorities for troubleshooting automation. However, technical personnel were more likely than middle management to want both capabilities. The most successful users of network tools were more likely to prioritize remediation verification. Members of the network operations team had a strong affinity for guided remediation.

Sample Size = 402

Intelligent Observability with AIOps

AIOps technology uses AI and machine learning to automate various aspects of network management. EMA believes it is a key capability for network observability now and in the future. However, network teams will need to develop trust in this technology before they allow it to automate network operations. **Figure 39** reveals the extent to which networking professionals trust AIOps today. A minority of survey respondents fully trust AIOps to do any of the four use cases explored in the chart.

Figure 39. Trust in AIOps to support the following network monitoring or network observability use cases



Sample Size = 394

"I think AIOps can be useful if it can be harnessed and utilized properly," said a monitoring engineer at a $15 billion financial services company. "Ideally, if I get 500 hits from one IP in a minute, I would rather have it all automated so there is no human interaction involved in blocking that. It should be automated."

Intelligent alerting and escalations are the most trusted. Organizations with dedicated tool buying teams (both cross-domain and network-specific) are most trustful of intelligent alerting and escalation, versus decentralized buying teams that acquire and implement their tools as needed.

Network problem remediation is trusted a little less than intelligent alerting, but more so than other AIOps use cases, suggesting some openness to closed-loop operations.

Automated root cause analysis with AIOps is less trusted, but the most successful users of network tools are more likely to trust it, suggesting that striving for this kind of AI-assisted automation is a potential best practice.

Organizations are also less likely to trust AIOps with predictive capacity management, but again, the most successful tool users had more trust in it.

"I want systems to use predictive analysis of collected data to tell us when things could potentially break. I want to be proactive, rather than reactive," said a monitoring architect with a $35 billion media company.

Overall, successful users of network tools tended to trust AIOps to automate all aspects of network operations in Figure 39. This suggests that effective implementations of network tools with AIOps solutions tend to deliver strong value to IT organizations.

Conclusion

EMA hopes that this research settles the question of exactly what network observability is. We observed an astonishing and confounding array of takes on what the term could mean. One (unnamed here to protect the innocent) blogger recently wrote that network monitoring is essentially fault management, and network observability is essentially performance management. If that's the case, what have network performance management vendors been doing over the last 20 years?

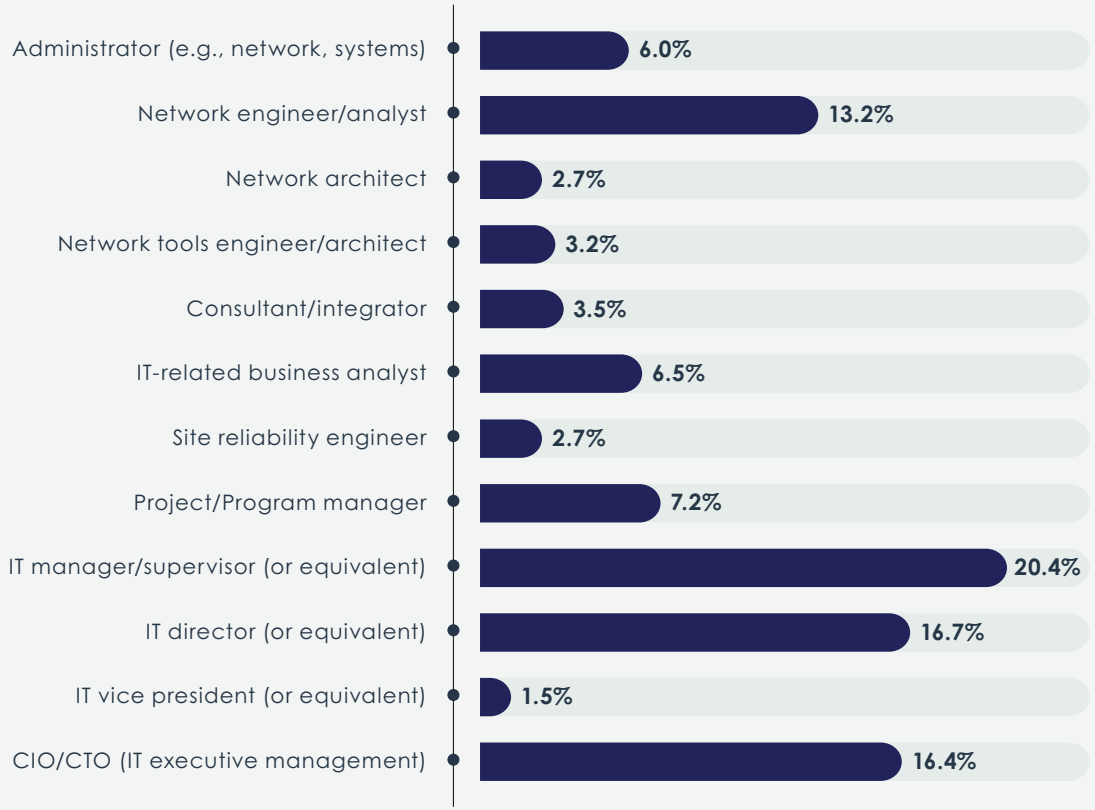
Specificity is the best remedy for the marketing whiplash that IT professionals have experienced when trying to understand the idea of network observability. By combining quantitative market research with qualitative interviews with expert stakeholders, EMA has established the following authoritative definition:

Network observability refers to a network monitoring system that collects a complete and diverse set of network data to provide deep visibility and actionable insights into the current and future state of a network. Those actionable insights include network performance, application performance, network security, and end-user experience.

Network observability might involve a single tool, or it might include several tools linked together via integration and a common data lake. Regardless of the path one takes, this research offers a roadmap to IT stakeholders for how to get to a state of total network observability.

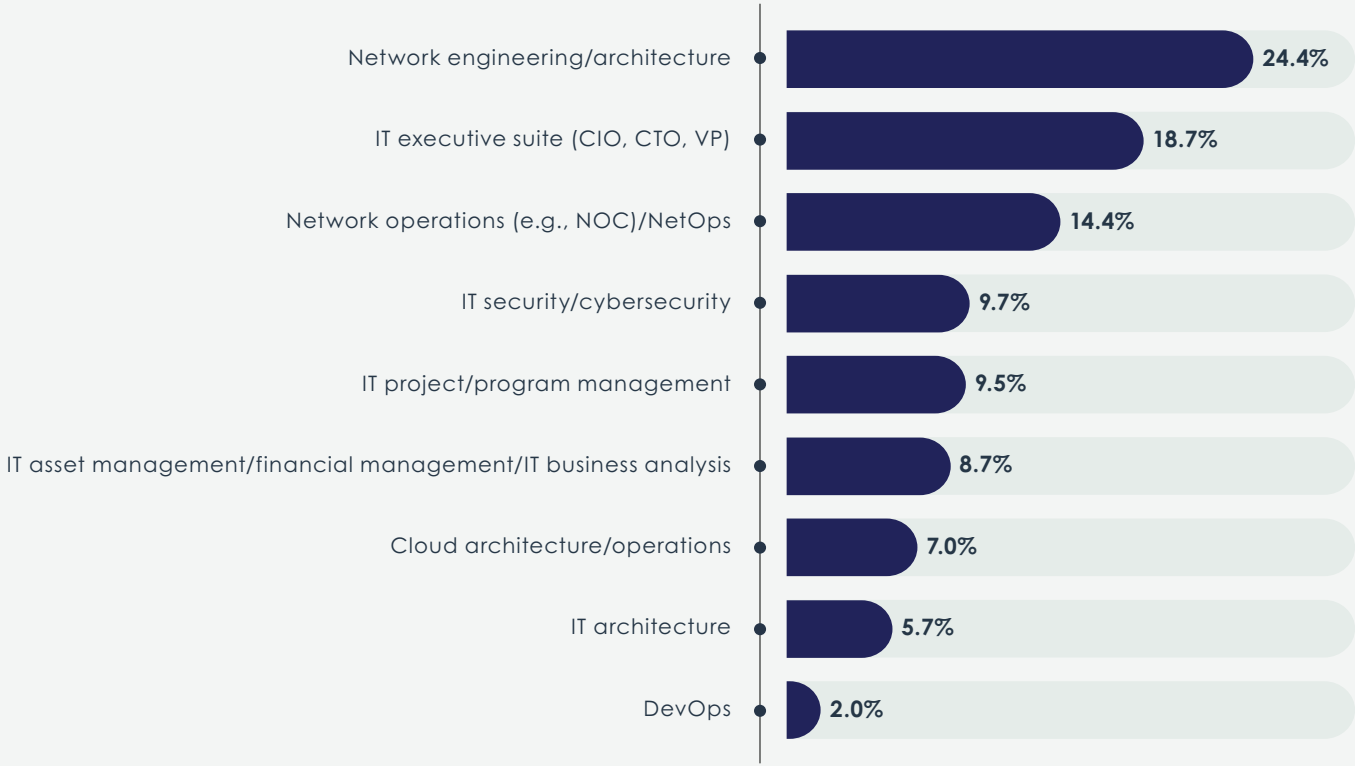
Appendix: Demographics

Figure 40. Job titles



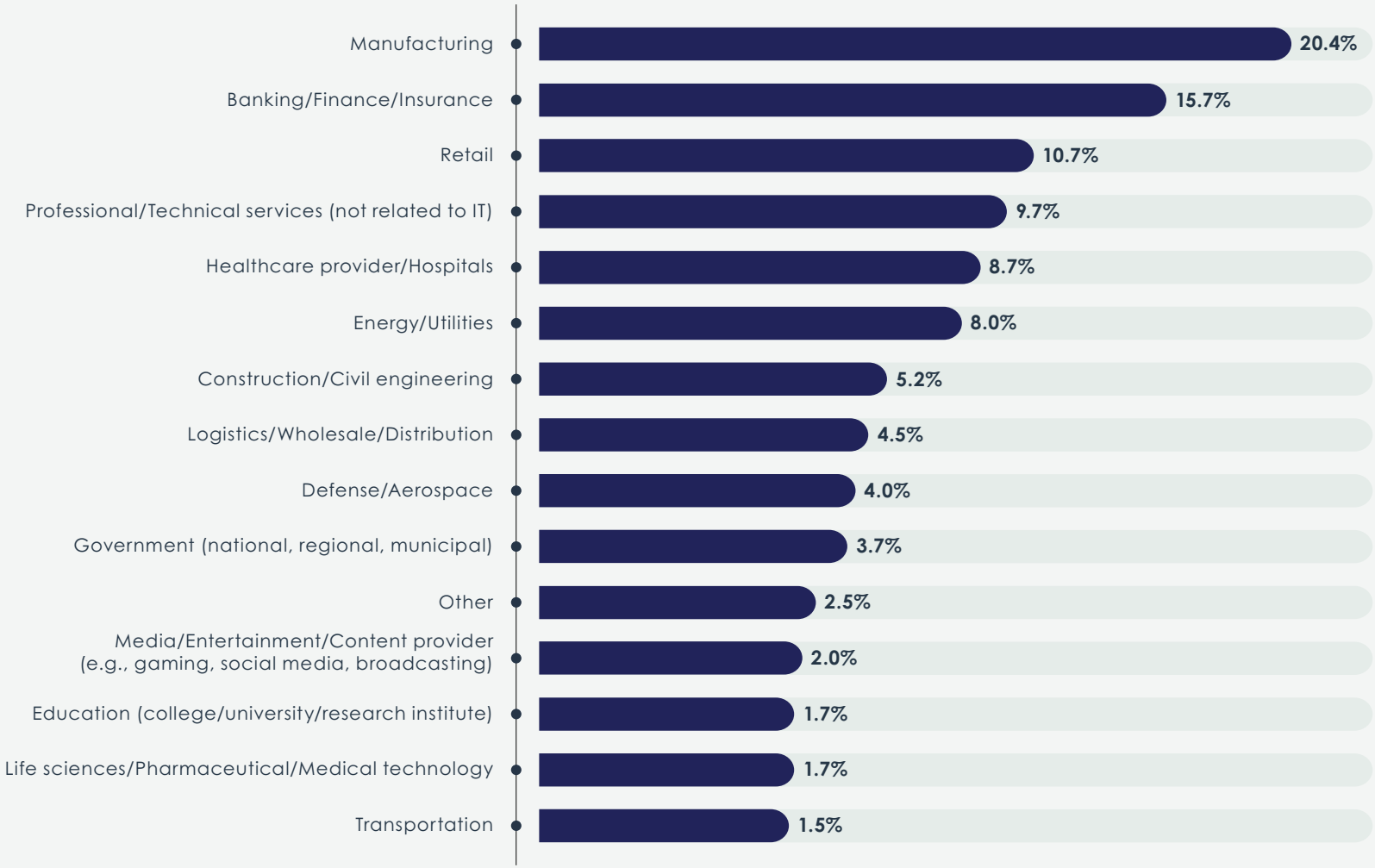
Sample Size = 402

Figure 41. Functional groups or teams within IT organization



Sample Size = 402

Figure 42. Primary industry



Sample Size = 402

Figure 43. Company size (total employees)

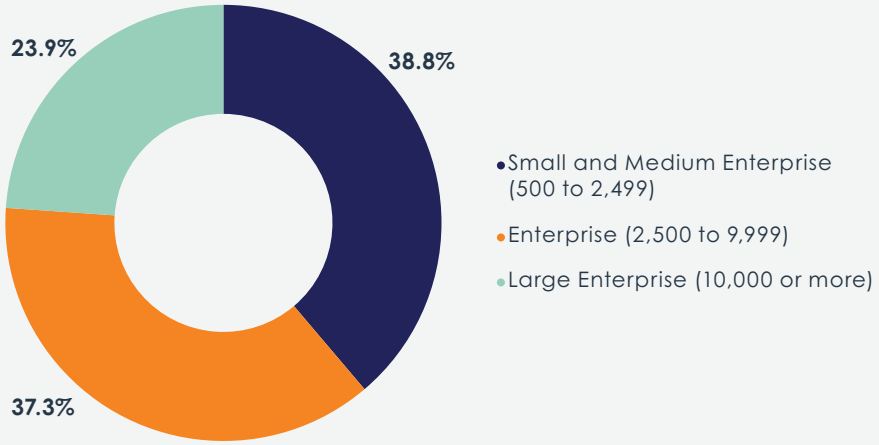
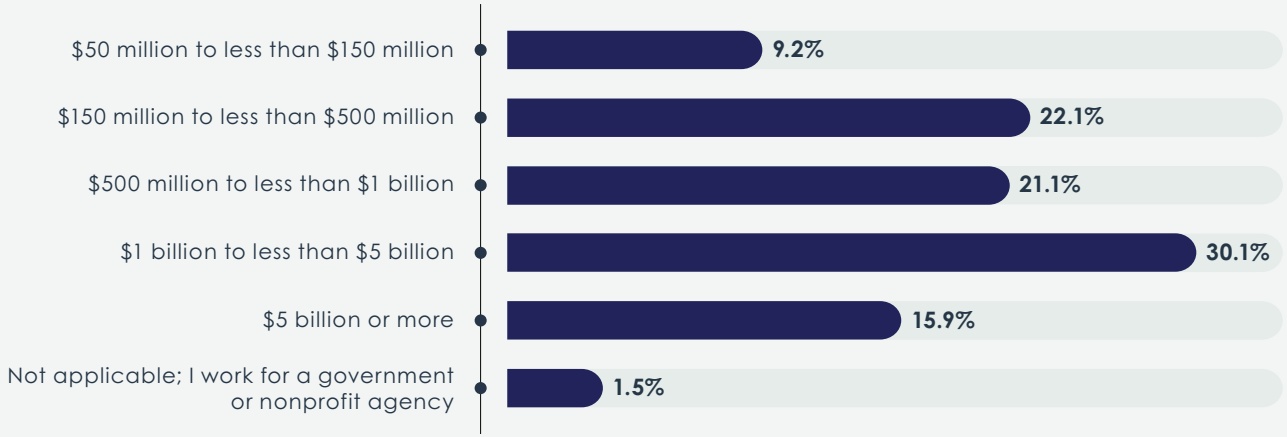
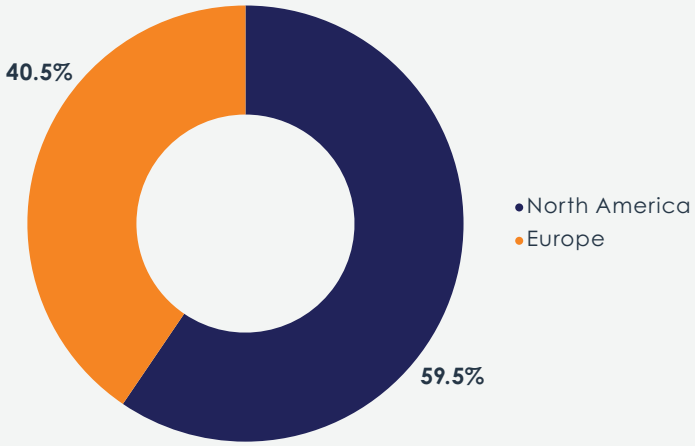


Figure 44. Annual revenue



Sample Size = 402

Figure 45. Location of survey respondents



Sample Size = 402

Case Study: Alaska Federal Credit Union Gains Visibility and Actionable Insights with Alluvio by Riverbed

Alaska USA Federal Credit Union's infrastructure management (IM) team recently replaced a fragmented monitoring toolset with Alluvio by Riverbed, a unified observability solution that delivers actionable insights from full-fidelity telemetry that spans the enterprise. Alluvio improved end-user experience across the credit union's 72 locations.

Proactive Rather Than Reactive Network, App, and End-User Monitoring

"If we have an environmental event that impacts our approximately 2,200 users and 700,000+ members, we need to provide the rapid response times our users and members expect," said Douglas Horner, Senior Vice President of IM operations at Alaska USA.

The credit union's legacy toolset was not up to the task. "We did not have complete end-to-end visibility into our environment," Horner said. "The moment we asked a question, staff would start working with various tools trying to piece together the answer. The data was also not as reliable since it was assessed and aggregated manually across applications unique to specific environments."

Portfolio That Unifies Data, Insights, and Actions

Alaska USA rolled out Alluvio by Riverbed solutions—a unified observability portfolio that unifies data, insights, and actions across IT to deliver seamless digital experiences for users. The organization leveraged Alluvio's full-fidelity network, application, and end-user experience management (EUEM) telemetry and reduced the high volume of alerts by correlating multiple high-fidelity trouble indicators into a single high-confidence incident. The solution surfaces actionable insights so IT staff can quickly resolve any business-impacting issues.

The Alluvio portfolio is helping Alaska USA eliminate data silos and improve decision-making while alerting IT of any issues anywhere across the digital ecosystem. With a simple user interface, the credit union can get an integrated view of its network, applications, and user experience.

"There are many tools out there that allow us to capture infrastructure data and network data, but there wasn't a single tool that we found previously that could aggregate all that data—from networks and apps to end users' devices—into a single pane of glass," Horner said. "However, Riverbed aggregates data across all these layers and allows all our staff to troubleshoot critical events consistently and quickly. This ensures everybody's looking at the same data and in the same way."

Proactive troubleshooting, thanks to intelligent alerts and dashboards, is helping the credit union solve issues before they become major problems. "Today, we are in a very proactive position. We have visibility into what is happening on our endpoints. For instance, we can call a branch and discuss performance issues we are seeing and work proactively with the user to correct the problem," Horner said.

"It really changes the tone of the conversation, because the end user feels someone already knows what's going on," said Sol Posenjak, Senior IM Operations Engineer at Alaska USA. "We can even have proactive engagements in which we say, 'Let's start repairs on Tuesday at midnight instead of during the day so we don't impact daily operations.' The analysis of the data and being able to report on it is equally as important as the remediation itself, because we can fix it proactively."

Alaska USA can also now measure its end-user device and application experience remotely, proactively, and non-invasively with Alluvio Aternity. The credit union used auto-remediation features in Aternity to eliminate frequent sources of trouble.

"We've used auto-remediation to reduce our incident counts by 150 to 200 in a month in one particular case," says Horner. "We analyze the user's hard drive, and if it is about to fill up, we have a script that automates the cleanup of the drive. Our goal has always been to create an environment that is as self-aware and self-healing as possible. In one case, auto-remediation eliminated over 8,500 incidents in one month, reducing significant burden on our service desk staff."

"The Alluvio unified observability solution from Riverbed has given us the ability to provide a stable, high-performing environment for our users," Horner said. "Additionally, as a Beta customer for the SaaS-delivered unified observability solution, Alluvio IQ, we've been impressed with the simplicity, analytics, and auto-remediation designed into the product. These capabilities will provide greater insight into the extensive data running across our company, helping to surface the most important issues for action and reducing alert fatigue."

About Enterprise Management Associates, Inc.

Founded in 1996, Enterprise Management Associates (EMA) is a leading industry analyst firm that provides deep insight across the full spectrum of IT and data 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 EMA's clients achieve their goals. Learn more about EMA research, analysis, and consulting services for enterprise line of business users, IT professionals, and IT vendors at **www.enterprisemanagement.com**. You can also follow EMA on **Twitter** or **LinkedIn**.

1995 North 57th Court, Suite 120, Boulder, CO 80301 +1 303.543.9500 **www.enterprisemanagement.com**

4221.102122