EMA™
IT & DATA MANAGEMENT RESEARCH,
INDUSTRY ANALYSIS & CONSULTING

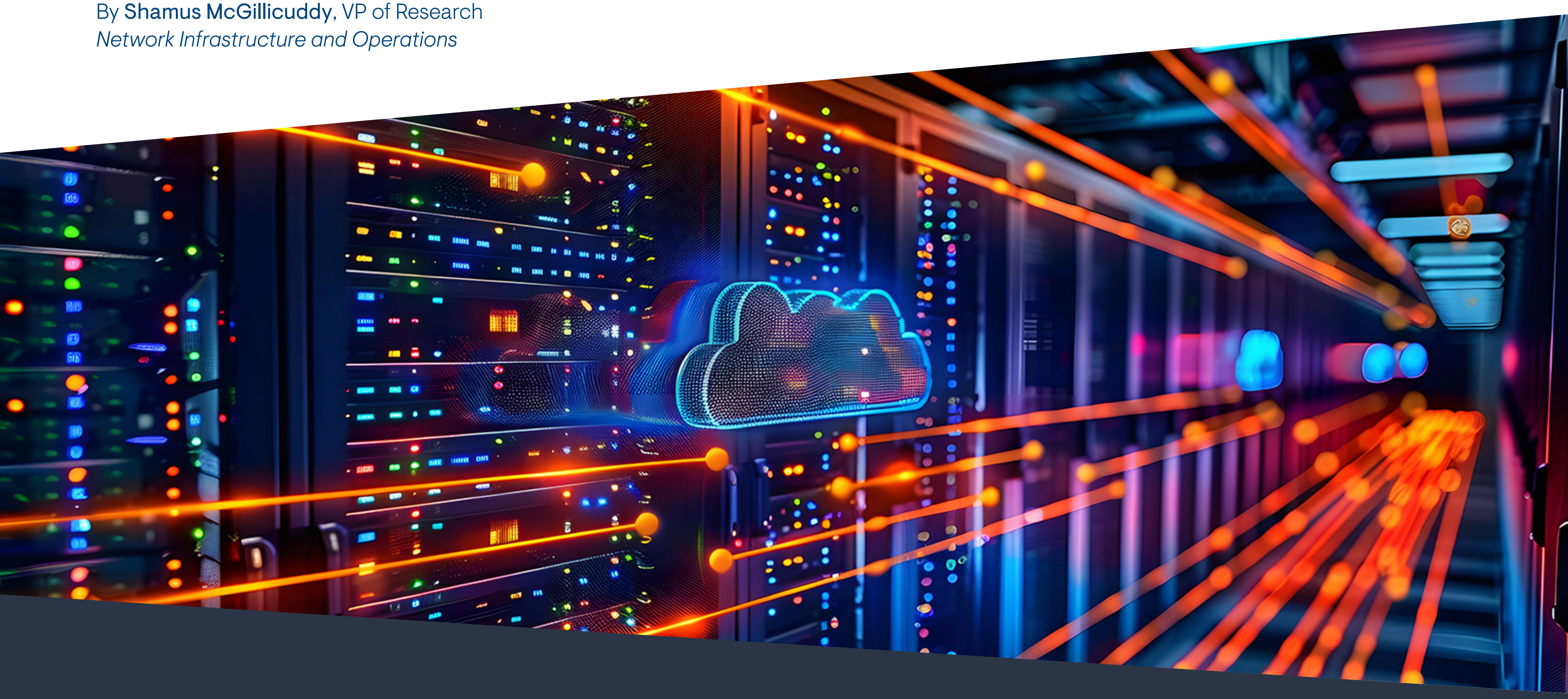
Prepared for:

BLUECAT BROADCOM JUNIPER NETWORKS NETSCOUT PARK PLACE TECHNOLOGIES

Network Observability:
Managing Performance Across Hybrid Networks

January 2025 EMA Research Report

By **Shamus McGillicuddy**, VP of Research
Network Infrastructure and Operations



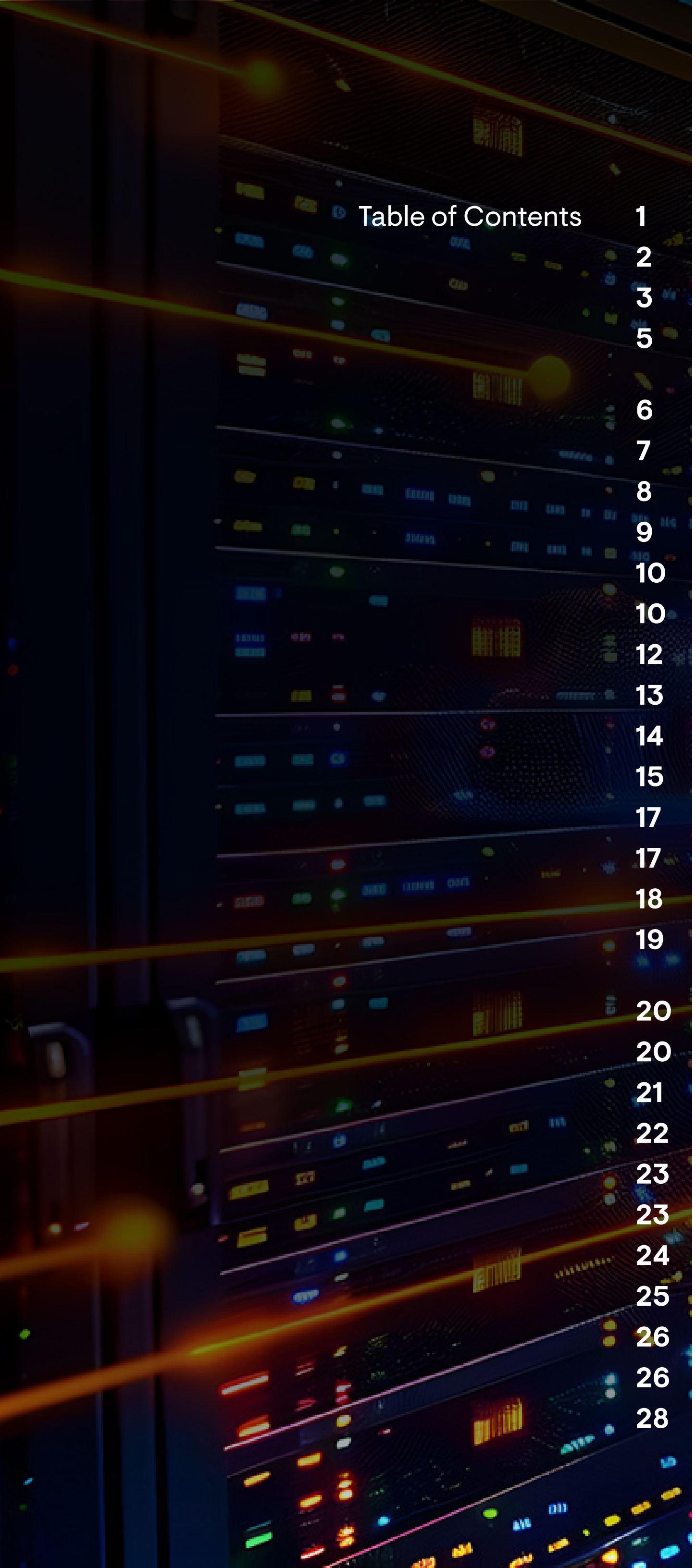


Table of Contents

Introduction

Performance and availability are essential missions of any enterprise network infrastructure and operations teams. To succeed in these missions, network teams need tools that can monitor, troubleshoot, and optimize networks by collecting and analyzing a variety of network data. Historically, Enterprise Management Associates (EMA) described such tools as network monitoring or network performance management solutions. Over the last four years, tool vendors have embraced a newer marketing term: network observability.

EMA has been tracking this market for decades. More recently, our research sought to define the novel term network observability more concretely for buyers. In 2022, we published the market **research report** "Network Observability: Delivering Actionable Insights to Network Operations." This report identified how buyers perceived the concept of network observability and explored product requirements and tool challenges. In 2024, EMA published a **buyer's guide**, the "EMA Radar Report for Network Operations Observability," which evaluated the capabilities of fourteen leading vendors.

Now, with this new 2025 report, EMA updates and expands on its ongoing exploration of emerging trends and requirements for network observability.

This report aims to identify how an IT organization can best select a toolset for managing the performance, availability, capacity, cost, and compliance of an enterprise network. For this research, EMA surveyed 351 IT decision-makers and conducted in-depth interviews with several network engineers and architects who are experts on their company's network observability tools. EMA conducted the survey and research interviews in November and December of 2024.

Demographics

Figure 1 reveals the demographic details of the 351 people EMA surveyed for this research. To qualify, survey participants had to have experience with evaluating, implementing, and/or using the tools that his or her organization uses to monitor and troubleshoot networks. Alternatively, they had to be managers of individuals or teams who had such experience.

The chart shows a broad mix of perspectives in terms of job seniority, IT groups, company size, and industry, as well as a transatlantic perspective, with respondents from the United States, the United Kingdom, France, and Germany.

Figure 1. Demographics

Job titles

13.4%	Network engineers/architects/analysts
10%	IT project/program managers
52.2%	IT managers/supervisors/directors
24.5%	IT executives (VPs/CIOs/CTOs)

Company size (employees)

23.1%	Midsized (1,000 to 2,499)
59.2%	Enterprise (2,500 to 9,999)
17.7%	Large enterprise (10,000+)

Region

66.7%	United States
33.3%	Europe (UK/France/Germany)

Top industries

22.5%	Manufacturing
20.5%	Banking/Finance/Insurance
11.4%	Retail
8.5%	Health care
5.4%	Higher education
5.1%	Professional services (not related to IT)

Functional groups/departments

30.2%	Network/IT operations
20.5%	IT executive suite
16.2%	IT project/program management
15.7%	Network engineering
8.8%	IT asset and financial management/ IT business analysis
4.6%	Cloud/DevOps
4.0%	IT architecture

Key Findings

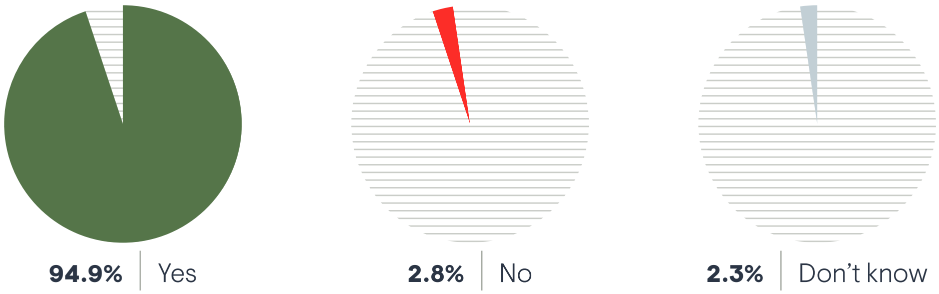
- Network observability is emerging as the preferred term for describing network monitoring and troubleshooting solutions
- Only 43% of enterprises are completely successful with these tools
- The top four complaints that IT organizations have about their network observability tools are:
  1. Limited scope ("I can't monitor everything I need to monitor")
  2. Too expensive
  3. Lack of customizability
  4. Difficult to implement/maintain
- 87% of enterprises use multiple network observability tools, and they strive to integrate and consolidate these tools as much as possible
- Nearly 59% of organizations are likely to replace their incumbent network observability tools over the next two years
- The volume and diversity of data that network teams collect with these tools are increasing
- Tools must be able to observe complex environments. Most organizations believe their tools must provide:
  - Observability of multi-vendor networks
  - End-to-end visibility and insights across multiple network domains (e.g., wide-area, local-area, cloud, etc.)
  - Observability of unmanaged networks (i.e., networks to which the IT organization does not have administrative access and control)
  - Observability of network experience of individual users, not just networks
- Tools must leverage AI to optimize and automate network management. IT organizations expect AI will enable:
  - Operational efficiency
  - Proactive problem prevention
  - Network optimization

The Concept of Network Observability: More than Monitoring

Network observability emerged a few years ago as a term to describe the tools IT organizations use to monitor, troubleshoot, and optimize their networks. As a marketing buzzword, it is slowly displacing network monitoring and network performance management.

EMA's 2022 report on this topic investigated the disposition of IT professionals toward the concept of network observability. At that time, 90% of 400 respondents told us that they considered "network observability" to be a useful term to describe the tools they use to monitor and troubleshoot their networks. **Figure 2** reveals that today, that number has risen to 95%. IT executives were the most convinced of the term's utility.

Figure 2. 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?

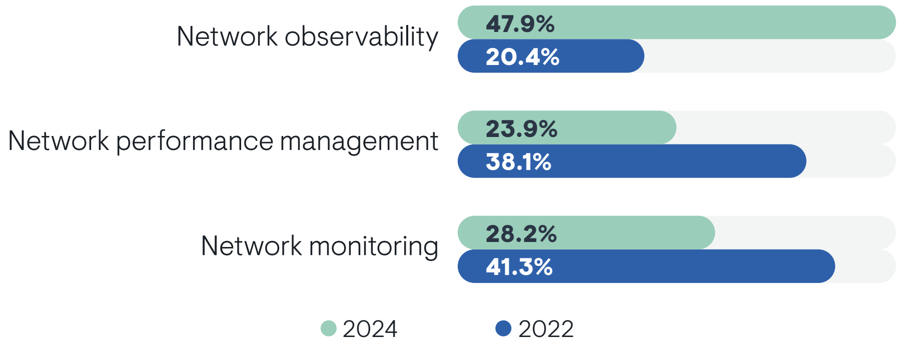


Sample Size = 351

Network Observability is Mainstream

Not only is the concept of network observability seen as a useful term, it is also taking over as the preferred way to describe the tools network operations teams use. **Figure 3** reveals that in 2022, only 20% of IT professionals chose "network observability" as the preferred term for describing their tools. Today, nearly 48% of respondents prefer it.

Figure 3. Which of the following terms do you prefer when describing the tools you use for monitoring and troubleshooting your network?



Mindshare for network monitoring and network performance management has eroded significantly. Clearly, network observability is catching on with IT personnel. From a group perspective, cloud, network engineering, network operations, and IT architecture groups have all embraced network observability as the preferred terminology. Network performance management still resonates with the IT executive suite, the IT asset and financial management group, and project management.

> In 2022, only 20% of IT professionals chose "network observability" as the preferred term for describing their tools. Today, nearly 48% of respondents prefer it.

2024 Sample Size = 351 2022 samples size = 400

Defining Observability for NetOps

We know that network observability is growing in popularity as a concept, but what does it mean? Observability entered the vernacular of the IT industry via DevOps, whose practitioners use observability to describe their monitoring tools. DevOps professionals describe observability as the comprehensive collection of metrics, logs, and traces for establishing a full understanding of the state of an application environment.

The data that can be extracted from networks is more diverse than what DevOps teams typically collect and analyze, ranging from metrics and logs to flows, packets, DNS queries, routing information, configuration data, and more. Also, the actual network environment is more complex, stretching across multiple domains such as data center networks, cloud networks, wide-area networks, campus/office networks, branch offices, and even remote workers' home offices. Forming an end-to-end understanding of network state is much more challenging.

Thus, the definition of network observability requires investigation. EMA asked research respondents to select words and phrases that they associate with the concept. **Figure 4** shows that five terms most resonate with them, suggesting the foundation of a standard definition. Network observability is a subset of network monitoring solutions that can comprehensively collect and visualize network data and present actionable insights. It is also about more than performance. More than half of respondents think network observability should also offer security insights.

Monitoring was selected less often by respondents who were more successful with their tools, emphasizing that network observability is about moving past monitoring and focusing on insights and advanced use cases. Monitoring resonated more with the IT executive suite, IT asset and financial management, and project management. It resonated less with the teams most responsible for network management, such as network engineering and operations personnel.

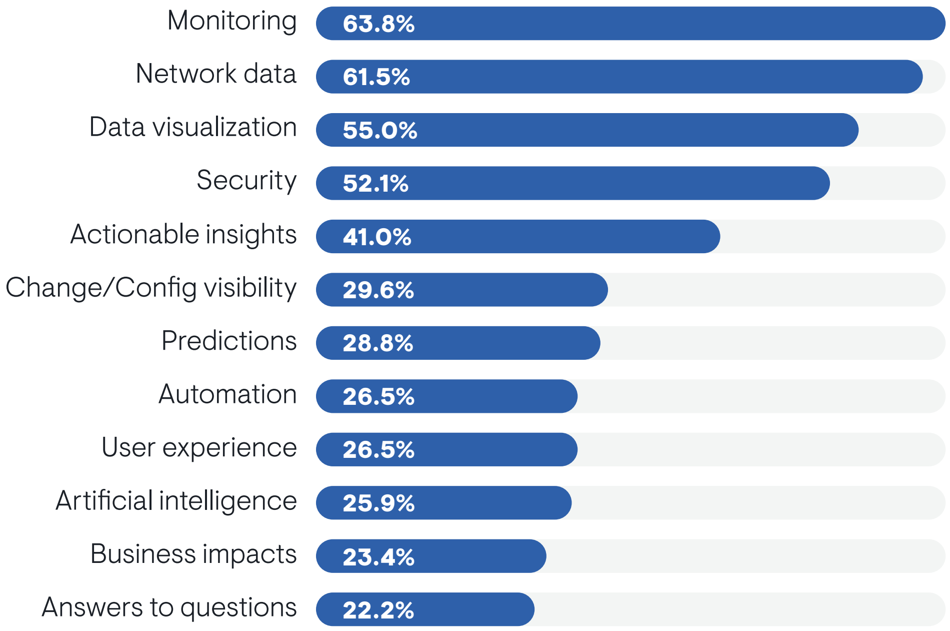
"I think monitoring is a very specific collection of certain data and metrics and identifying issues within that. It's a reactive approach to operations. As you expand, observability is a more holistic approach where you are collecting a lot more data and finding patterns of anomalous behavior," said a monitoring tool architect with a Fortune 500 media company. "It's more proactive, where you try to detect issues ahead of time."

"Network observability refers to your awareness and ability to have eyes on the network and how it's actually performing and functioning and being utilized," said an infrastructure manager with a Fortune 500 energy utility company.

"I would say it's the practice of gaining deep insight into performance and behaviors and health," said a network engineer with a health care company that operates more than 40 hospitals.

"Network observability means having that holistic view of the network, being able to see all your endpoints and nodes and what's going on with them," said a network management tool architect with a $30 billion bank.

Figure 4. Which of the following words and phrases do you most associate with the concept of network observability?



Sample Size = 351

Tool Strategy

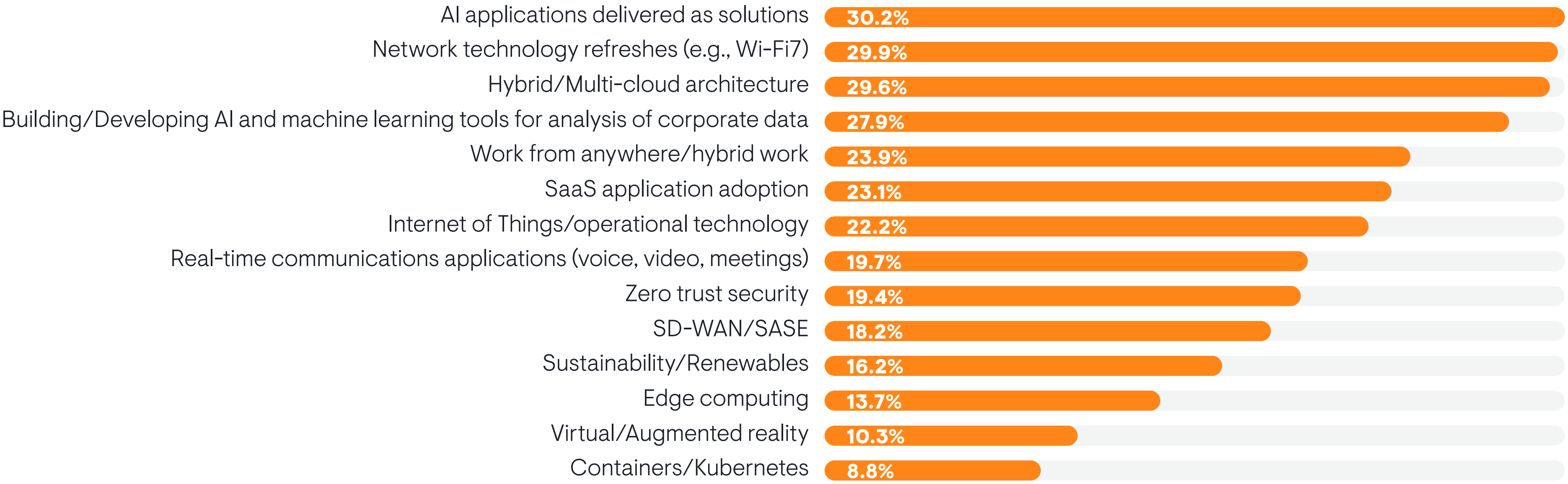
Strategic Drivers

It is important to understand where an organization's network observability requirements come from. By identifying the strategic drivers of tool strategy, we can understand the data we must collect, the metrics and measurements we need, and the systems with which a tool must integrate, and so on. **Figure 5** reveals that IT organizations have three primary drivers that are defining their network observability requirements. To begin with, there are two flavors artificial intelligence (AI) shaping their decisions. The first is the adoption of packaged AI services and solutions. In this case, organizations need to observe a network that is impacted primarily by production AI traffic. The second is the development of in-house AI solutions, which will involve observability of network traffic that AI training generates.

Network technology refreshes and hybrid/multi-cloud architecture are the other two primary drivers. Work-from-anywhere, SaaS application adoption, and operational technology are secondary influences on strategy.

EMA found that tool strategies driven by edge computing, IoT, and operational technology were more successful, but strategies driven by work-from-anywhere were less successful. Network engineering and operations personnel tended to be more aware of SD-WAN/SASE and network refreshes as drivers of network observability strategy. The IT executive suite was more aware of AI solutions, SaaS adoption, and virtual reality as drivers of tool strategy.

Figure 5. Which of the following technologies and trends are driving new requirements of your network observability tools?

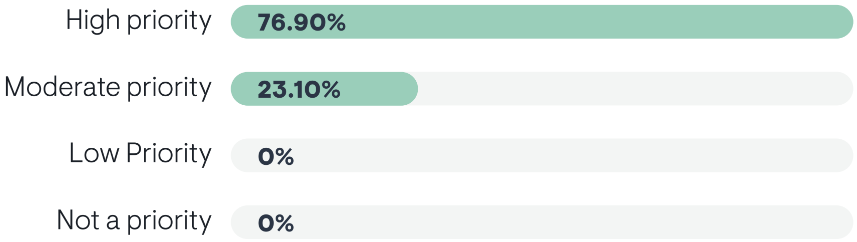


Sample Size = 351

Resource Priority

IT leaders clearly recognize that they need to invest in tools for network observability. This research found that IT organizations prioritize budget and resources for network observability. **Figure 6** reveals that nearly 77% of respondents say network observability receives a high priority for resources in their organizations. The rest characterized it as a moderate priority. No one in the survey selected "low priority" or "not a priority."

Figure 6. What level of importance does your organization place on devoting resources and budget to the tools it uses to monitor and troubleshoot its networks?



Sample Size = 351

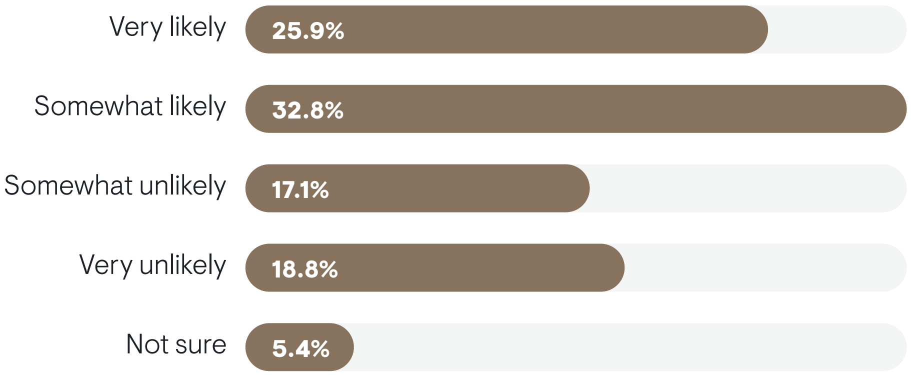
Members of network engineering and network operations teams were the most likely to believe that these tools were a high priority for organizational resources. The IT executive suite, IT architecture group, and IT asset and financial management group were less likely to perceive a high priority.

Organizations that make network observability a high priority for resources reported larger toolsets. IT decision-makers must proceed thoughtfully. Availability of budget should not be permission for tool sprawl. Those resources should be spent to ensure that any new capabilities are fully integrated into the existing toolset.

Replacing Incumbent Tools

Tool strategy is very much about being open to new tools and new vendors. Nearly 59% of respondents told EMA that they are at least somewhat likely to replace their current network observability tools within the next two years, as **Figure 7** indicates. Only 19% are completely certain that they will not. Respondents who currently use open source network observability solutions were more likely to replace a tool.

Figure 7. How likely are you to retire/replace one or more of your current network observability tools within the next year or two?



Nearly 59% of respondents told EMA that they are at least somewhat likely to replace their current network observability tools within the next two years.

Sample Size = 351

Subject matter experts (engineers, architects) were twice as likely as project managers and middle managers to report that they are very likely to replace their tools. Members of network engineering and network operations teams were the least likely to replace tools, while the IT executive suite, the IT assets/ financial management team, the project management group, and the IT architecture group were all more likely to do it.

EMA identifies many factors that can drive an IT organization to consider replacing a tool. Respondents who said that adoption of commercial AI applications and real-time communications applications were driving their network observability requirements were more likely to replace tools. Those driven by SD-WAN and SASE, containers and Kubernetes, and network technology refreshes were less likely to replace them.

IT teams are more open to replacing tools if:

- They currently conduct a lot of customization to make a tool useful, especially the following:
    - Custom coding and developing on a tool
    - Custom configuration for device support
    - Custom report building
    - Integrations with third-party tools
    - Create and document processes and workflows for using tools
- These customization requirements are causing:
    - Increased costs
    - Reduced tool effectiveness
    - Disruptions of other projects
- They are dealing with the following data challenges:
    - Data conflicts across tools
    - Data quality issues
    - Data storage limits
    - Lack of support of new data types
    - Data silos within a single tool
- They struggle to collect data from:
    - Secure access service edge
    - Public cloud
    - Private 5G
    - Containers and Kubernetes
    - Internet connectivity
- They want to use streaming network telemetry to replace SNMP
- They want AI-enabled root-cause analysis features
- They want alert management capabilities with service-level expectations
- A low percentage of alerts generated by current tools is actionable
- They need to monitor and troubleshoot the network experience of individual users
- They currently lean on remote desktop access tools to troubleshoot user experience
- They feel that their current user experience management tools are ineffective
- They think it is important to have AI/ML-driven network observability tools
- They think AI/ML technology can help with cost optimization and skills gap mitigation
- They need AI domain expertise for public cloud networks, and SD-WAN and SASE solutions

Tool Requirements

This section of the research explores the evolving requirements that IT organizations have for network observability solutions. It reviews architectural and functional needs, and it identifies next-generation capabilities that vendors should be emphasizing as they develop their products.

Critical Evaluation Criteria

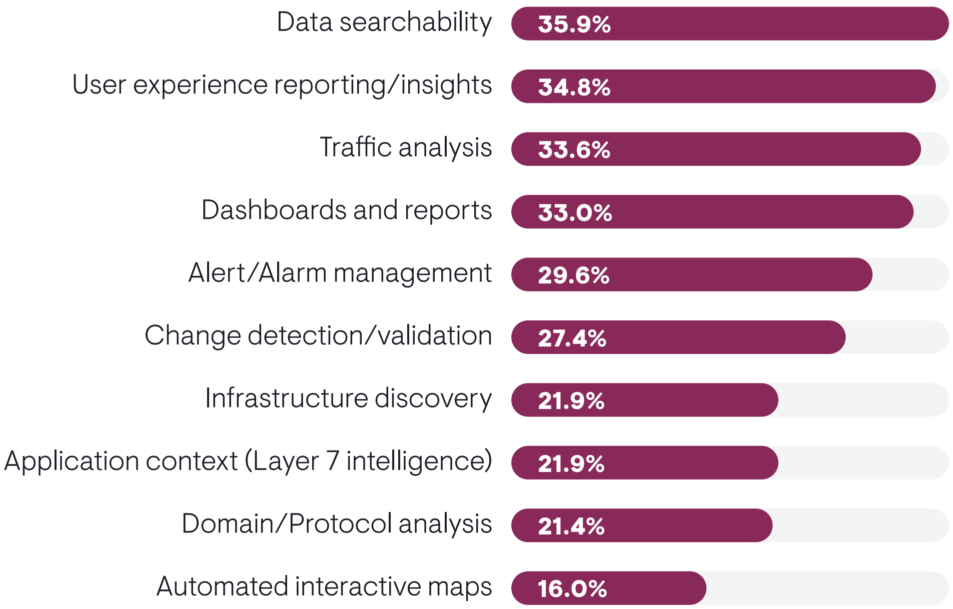
Figure 8 identifies the overall capabilities IT teams scrutinize when they are evaluating network observability tools. These are the features that they need from vendors. The chart shows a clear hierarchy. First, IT teams look for tools that have good data searchability, user experience insights, traffic analysis, and dashboards and reports. Dashboards and reports were a top requirement for the largest companies in this research.

> IT teams look for tools that have good data searchability, user experience insights, traffic analysis, and dashboards and reports.

“Powerful dashboards are important,” said a network management tool architect with a Fortune 500 retailer. “If you have only one location, even the worst dashboard is okay. It’s hard to miss problems. At our scale, it’s about how the tool can correlate the data and tell better stories. Just telling me something is up and down can get very noisy if I have 100,000 devices. Instead, I need to be able to customize the dashboard so that it only tells me that something went up and down 20 times, for instance. Ninety percent of [network observability] vendors cannot do this. Instead, I have to buy an AIOps solution, and that’s expensive.”

Secondarily, IT teams look for strong alert and alarm management features and change detection and validation. IT executives were less likely to see the importance of change detection. Members of the IT asset/financial management group especially valued change detection. Midsized and large enterprises (fewer than 10,000 employees) were most likely to prioritize alert and alarm management.

Figure 8. When evaluating network observability solutions, which of the following capabilities is most important to you?



“The most critical piece of our tools is getting an alert when something is malfunctioning or about to malfunction,” said an infrastructure manager with a Fortune 500 energy utility company. “If something goes down, we need to know if anything is going to affect our ability to do our jobs or service our customers. We need eyes on the problem and what it is as quickly as possible.”

“Always, if something breaks we must get alerted,” said a network engineer with a billion-dollar fintech company. “The worst thing that can happen is a customer comes to us and we didn’t know that someone was broken. It must let me know that something is broken, without flooding me with alerts. It has to get the severity correct.”

Sample Size = 351

The lowest priority capabilities are infrastructure discovery, application context, domain and protocol analysis, and automated interactive maps. The IT asset/financial management group prioritized discovery. Executives were more likely to prioritize application context. Application context was also more important to large enterprises (5,000 to 10,000 employees).

“I think application insights are still missing in the network context,” said a network management tool architect with a Fortune 500 retailer. “Now, you have an application that relies on two load balancers and some servers behind them, then a certificate expires and the whole application fails. Our tools will say the network is up. We’re missing the big picture. It’s hard to troubleshoot it. We’re lacking accurate topology with service mapping.”

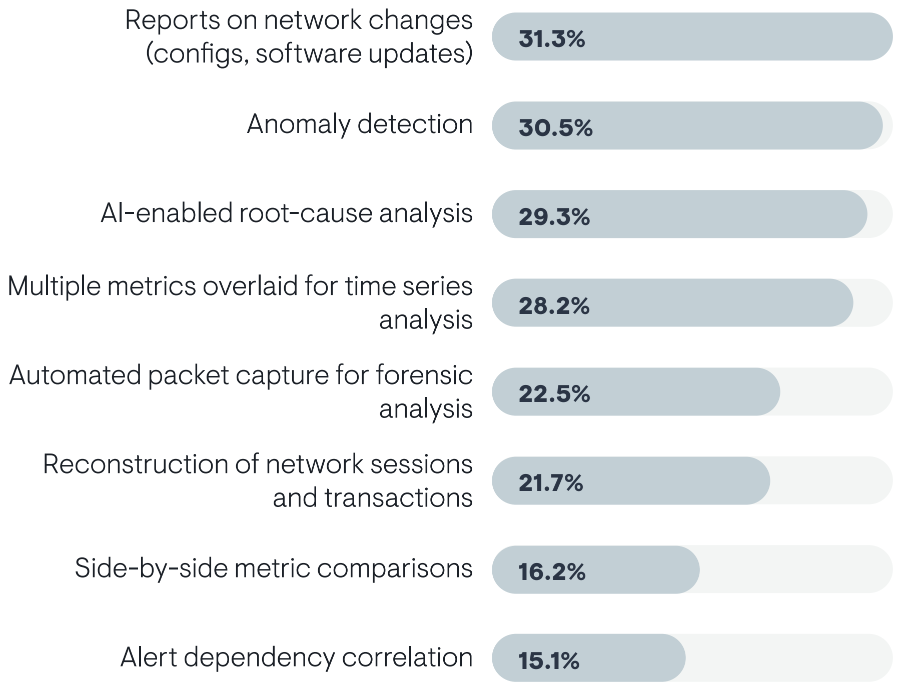
Automated interactive maps were the lowest priority, but members of the network operations team were more likely to select them.

Network Troubleshooting Features

Figure 9 explores what makes a network observability solution effective for troubleshooting. First, IT organizations need reporting on network changes, such as config changes or software updates. The next two capabilities are commonly enabled via artificial intelligence and machine learning (AI/ML) technology. EMA found that anomaly detection is one of the first features that network observability vendors deliver via AI/ML investment. Organizations that are less successful with network observability placed more emphasis on anomaly detection, suggesting its value is overblown. Also, members of the IT executive suite were more interested in it than network engineering personnel. Very large enterprises (10,000 or more employees) were especially focused on anomaly detection. Respondents who use open source network observability reported less interest than customers of commercial solutions in anomaly detection.

Automated root-cause analysis is not as widely available, but many vendors are developing capabilities in this area. Members of network engineering and network operations teams were less interested in it than the IT executive suite.

Figure 9. What kinds of troubleshooting capabilities are most valuable in a network observability solution?



Multiple metrics overlaid for time series analysis is the fourth most valuable troubleshooting capability. It requires very little analytical capability and is more about presentation of data in dashboards and reports. It allows networking personnel to contextualize patterns in disparate types of network data in context with each other. A good example is plotting a config change on top of a change in latency and interface utilization to understand whether that config change is related to network performance.

Sample Size = 351

"A good troubleshooting tool should be able to visualize data easily, and you should be able to add multiple metrics into an ad hoc dashboard so you can put things on a single graph," said a monitoring tool architect with a Fortune 500 media company. "It should also tell me if there are any active alerts on a device."

Alert dependency correlation was the least valuable troubleshooting capability, but midsized enterprises (1,000 to 5,000 employees) were more likely to seek it.

> "A good troubleshooting tool should be able to visualize data easily, and you should be able to add multiple metrics into an ad hoc dashboard so you can put things on a single graph," said a monitoring tool architect with a Fortune 500 media company.

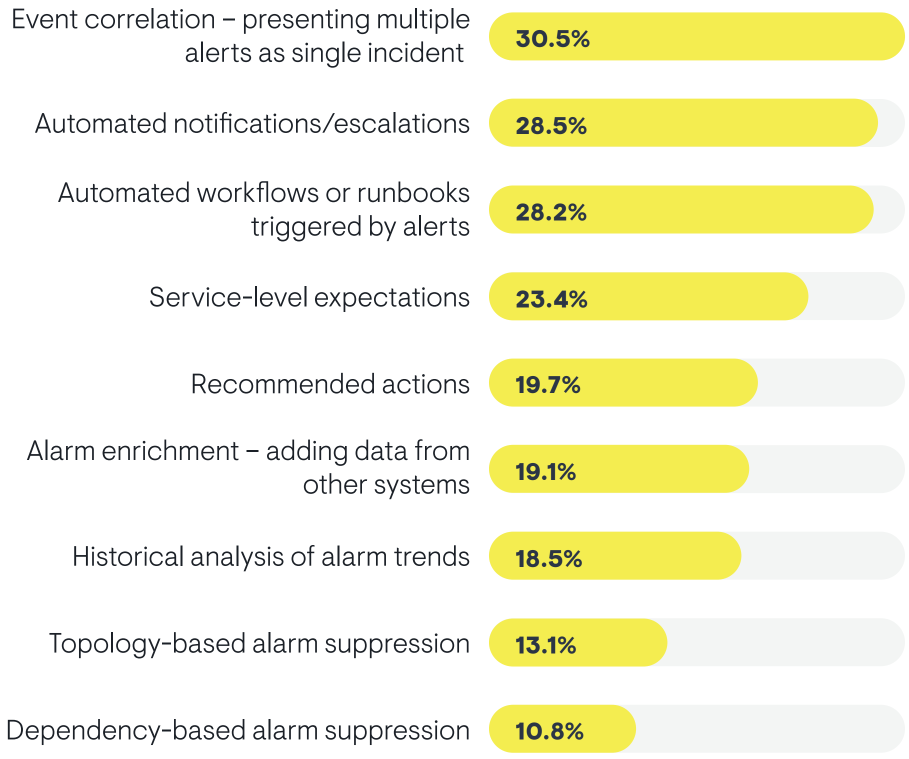
Alert Management Features

When EMA analysts speak to network engineering and operations personnel about their tools, they often cite alert management as a critical capability. Alerting is fundamental because alerts tell networking pros when something is going wrong, and they usually contain enough information to help them triage the issue. At the same time, network teams want to optimize alerting so that they don't get flooded with redundant or noncritical alerts that overwhelm their ability to prioritize and respond to events.

Figure 10 identifies the alert management features that IT personnel consider most important in a network observability tool. The top requirement is an event correlation feature that presents multiple alerts as a single incident, which is critical to limiting the noise generated by a tool. IT middle managers were more likely than IT executives to see the value of this capability.

A network management tool architect with a Fortune 500 retailer said alert management features should leverage AI to make alerts more intelligent. AI can power things like event correlation and recommended actions (or whether an action is required at all). "Vendors should build an intelligence layer where you can easily configure different layers of filtration between action and ongoing monitoring," he said. "There should be intelligence where you can configure things so it will say, 'what does this alert mean?'"

Figure 10. Which of the following alert management features are most important to have in a network observability tool?



Sample Size = 351

IT teams are also seeking automated notifications and escalations, and they want workflows or runbooks that can trigger in response to alerts. Both features streamline how IT teams triage and respond to events. Respondents who reported less success with network observability tended to believe automated notifications and escalations were very important. It was also a higher priority for very large enterprises (10,000 or more employees). IT executives were more likely than middle managers to perceive the value of triggered runbooks and automated workflows.

“I want a tool that can identify specific critical alarms, open a priority-one ticket, and notify specific groups who should respond to it,” said an infrastructure manager with a Fortune 500 energy utility company. “Right now, we have administrators who are responsible for programming our tools to reduce white noise. Vendors should have the ability to do that for customers through smarter alerting.”

> “I want a tool that can identify specific critical alarms, open a priority-one ticket, and notify specific groups who should respond to it,” said an infrastructure manager with a Fortune 500 energy utility company.

Service-level expectations are also quite valuable. This feature allows IT personnel to apply expectations for overall service performance to alerting, which provides a granular and more nuanced approach to setting alert conditions on the network. Very large enterprises were more likely than others to seek it.

Among less popular features, recommended actions were favored by respondents with less network observability success. On the other hand, successful respondents emphasized the value of dependency-based alarm suppression, suggesting that this venerable approach to noise reduction remains a viable and valuable feature. Large enterprises (5,000 to 10,000 employees) valued it more than midsized enterprises (1,000 to 5,000).

Historical analysis of alarm trends was selected more often by engineers and architects than by IT middle managers. Members of the network engineering team saw more value than others in topology-based alarm suppression.

Data Diversity and Scalability

Data collection requirements for network observability solutions are becoming more robust. EMA research found that IT organizations are diversifying the classes of data they collect from their networks and the overall volume of data is increasing.

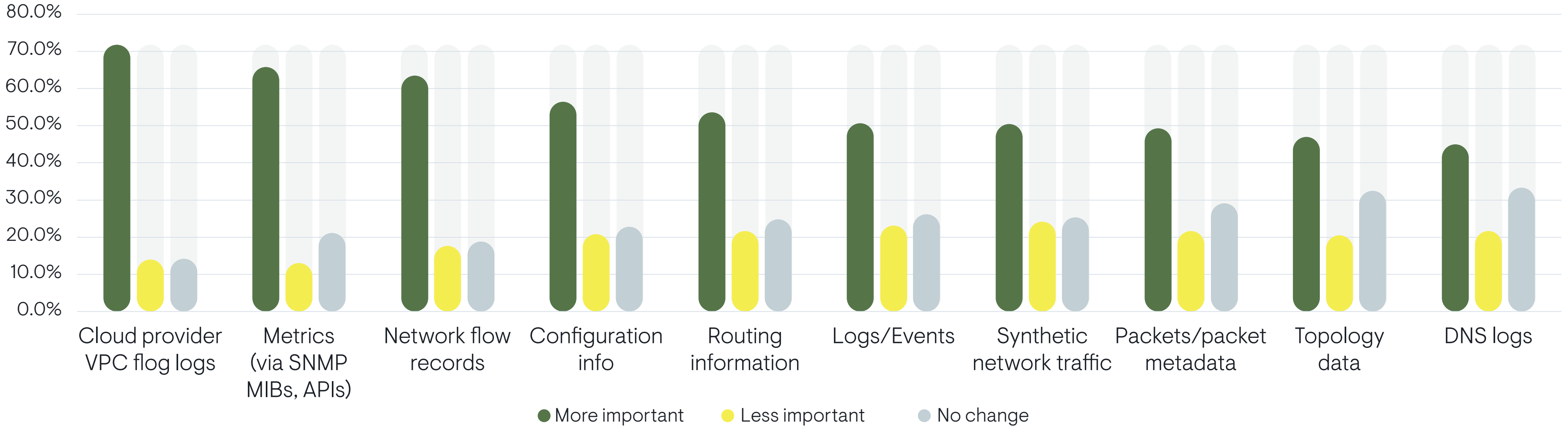
Essential Observability Data

Figure 11 reveals that IT organizations need to collect and analyze more kinds of data with their network observability tools. EMA listed 10 classes of network data and asked respondents whether any of this data was becoming more or less important to monitoring and managing their networks. In every example, respondents were more likely to say the data was becoming more important rather than less important.

Cloud provider flow logs experienced the biggest surge in importance, suggesting that network teams need better visibility into public cloud traffic. Most respondents also said that device metrics, network flow records, configuration data, routing information, logs and events, and synthetic network traffic were becoming more important.

“I consider the internet a part of our backbone now, and it’s very important to monitor our traffic from on-premises to the cloud and back again,” said a monitoring tool architect with a Fortune 500 media company. “So, it’s really important to do tests with synthetic network monitoring.”

Figure 11. 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 = 351

> "I consider the internet a part of our backbone now, and it's very important to monitor our traffic from on-premises to the cloud and back again," said a monitoring tool architect with a Fortune 500 media company.

"We need to get all the metrics so that we can monitor things like CPU load and memory usage. We also need to observe latency," said a network engineer with a health care company that operates more than 40 hospitals. "And right now, we would like to do deep packet inspection for application layer insights. That is where we need to go in the future."

"We're moving to a tool that can give us really good packet capture analysis in the cloud," said a network management tool architect with a $30 billion bank. "Having more advanced statistics through packets and good reporting is going to be huge for us."

Respondents who reported the most success with network observability were more likely to say device metrics, synthetic traffic, routing data, configuration information, and topology data are increasing in importance, while logs and network flows are less important.

The network engineering team was more likely than other groups to see the growing importance of device metrics, packets, DNS logs, configuration information, and topology data.

Data Collection Volumes are Increasing

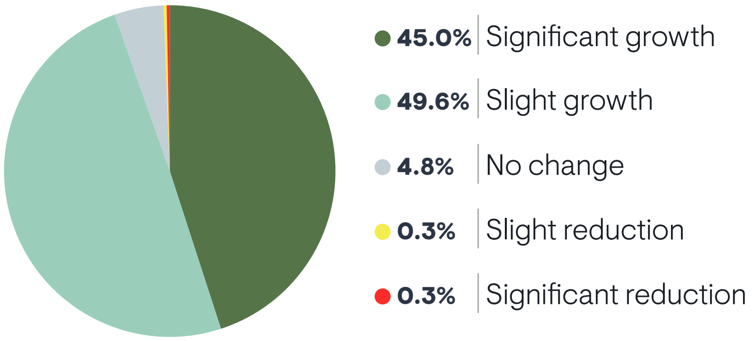
Figure 12 reveals that nearly 95% of organizations have increased the volume of data they collect with network observability tools over the last two years, and 45% describe this volume increase as significant. IT organizations may need to increase the scalability of their observability platforms by upgrading the resources and licenses for on-premises tools. Many providers of SaaS-based network observability tools charge customers by the amount of data they collect, so IT organizations may see increased costs as data volumes go up.

Subject matter experts and project managers reported significant growth in data, while IT executives were more likely to see only slight growth. DevOps and network engineering personnel perceived the most growth in data.

"Data collection scalability is really important for us," said a monitoring tool architect with a Fortune 500 media company. "We have almost 700,000 interfaces, so it's a lot of data collection. Each interface probably has 20 different metrics or more, so scalability is a huge requirement for us."

Successful users of network observability tools were more likely to report significant growth in the amount of data they collect. More data suggests more comprehensive visibility into the network. However, it can also pose a challenge. In a later section, we will explore data-related challenges with network observability tools. That section will show that the biggest source of data trouble with tools today is scalability, with many organizations struggling with increased volumes of data.

Figure 12. Over the last two years, to what extent has the overall volume of data that you collect with your network observability tools changed?



Sample Size = 351

Streaming Network Telemetry: Adoption Interest is Strong

Network monitoring and observability tools have relied on SNMP to collect device metrics and events for decades. This protocol polls devices at regular intervals for stats on resource utilization and device state. Tools typically alert on this information based on thresholds. More recently, vendors, industry consortiums, and standards bodies have developed various streaming telemetry mechanisms as an SNMP alternative. Streaming telemetry allows a tool to subscribe to device data, which is streamed in real time rather than in response to poll requests.

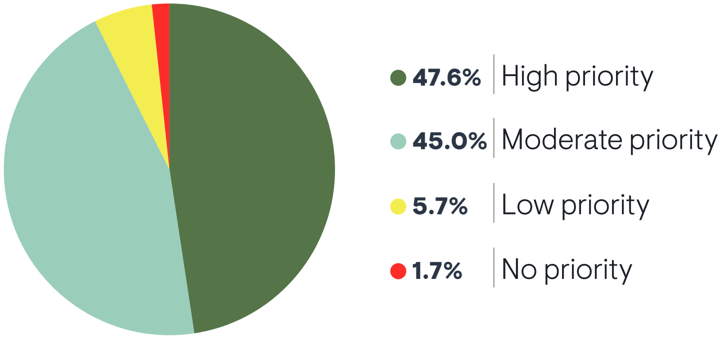
Advocates say streaming network telemetry is a superior option to SNMP polling, but adoption is low, due to a variety of reasons that we will explore here.

Figure 13 shows that interest in streaming network telemetry is strong. Nearly 48% say implementation is a high priority. Respondents who are more successful with network observability tended to make streaming telemetry a higher priority.

“I want to use it because traditional device APIs always have rate limits,” said a network management tool architect with a Fortune 500 retailer. “You can’t get all the data you need. Streaming telemetry is less performance-intensive on the hardware platforms. You can get more data.”

Respondents who use open source network observability tools were the most likely to say streaming telemetry was a high priority. Members of network engineering teams were the most likely to name this a high priority, while the IT architecture group tended to say it was a low priority and the project management group labeled it a moderate one.

Figure 13. To what extent is it a priority for your organization to apply streaming network telemetry to your network observability toolset today?



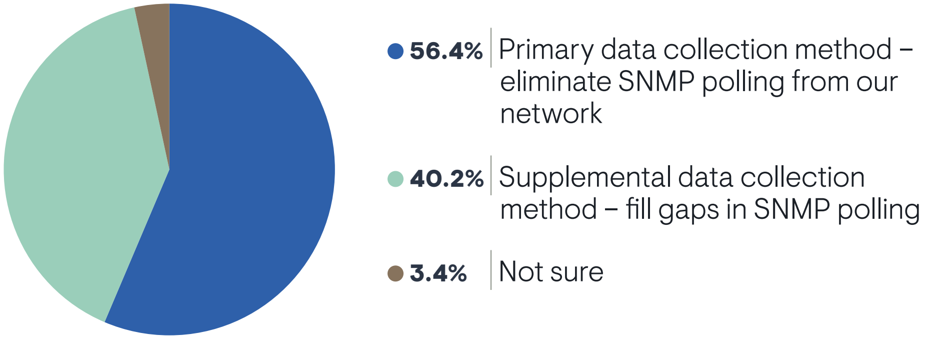
Interest in streaming network telemetry is strong. Nearly 48% say implementation is a high priority.

Sample Size = 351

A Potential SNMP Replacement

EMA asked research participants several times over the years whether they see streaming network telemetry as a potential replacement for SNMP. Usually, most respondents described it as a supplement to rather than a replacement for SNMP. This year, things changed. **Figure 14** reveals that 56% would like to use the technology to replace SNMP and only 40% see it as a supplement.

Figure 14. Which of the following best describes how you would use streaming network telemetry in your network observability tools if you adopted it?



Sample Size = 351

IT executives (71%) were the most likely to want to replace SNMP with streaming telemetry. All other job titles were closer to 50/50 on this question. From a group perspective, DevOps personnel were the most likely to see streaming as an SNMP replacement, followed by members of the IT executive suite, network operations, and network engineering. The cloud team, IT architecture team, and project management were less likely to see streaming telemetry as a supplement of SNMP.

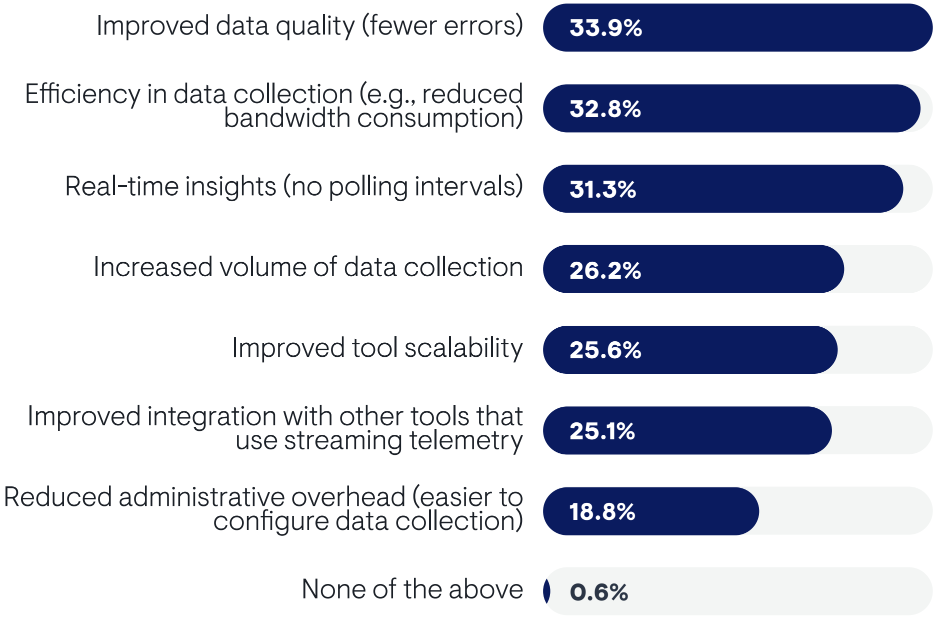
Organizations that have more success with network observability are more likely to leverage streaming telemetry as an SNMP replacement.

Potential Value

Three potential benefits primarily drive interest in streaming network telemetry, as **Figure 15** details. IT organizations believe it can improve data quality, make data collection more efficient, and enable real-time insights by eliminating polling intervals. The latter benefit reflects how many network observability vendors recommend five-minute polling intervals with SNMP. These intervals are too long for some network teams.

“You can get more data [from streaming telemetry], and it’s more efficient,” said a monitoring tool architect with a Fortune 500 media company. “You can do change detection and things like that.”

Figure 15. What do you perceive as the greatest benefits of adopting streaming network telemetry?



Sample Size = 351

Adoption Roadblocks

While interest in streaming network telemetry is strong, adoption is low. EMA rarely encounters anyone who is using it. **Figure 16** shows why this is the case. There are three primary roadblocks: network observability tools lack support for collecting such telemetry, industry standards haven't matured enough to support widespread adoption, and network equipment vendors don't fully support the technology.

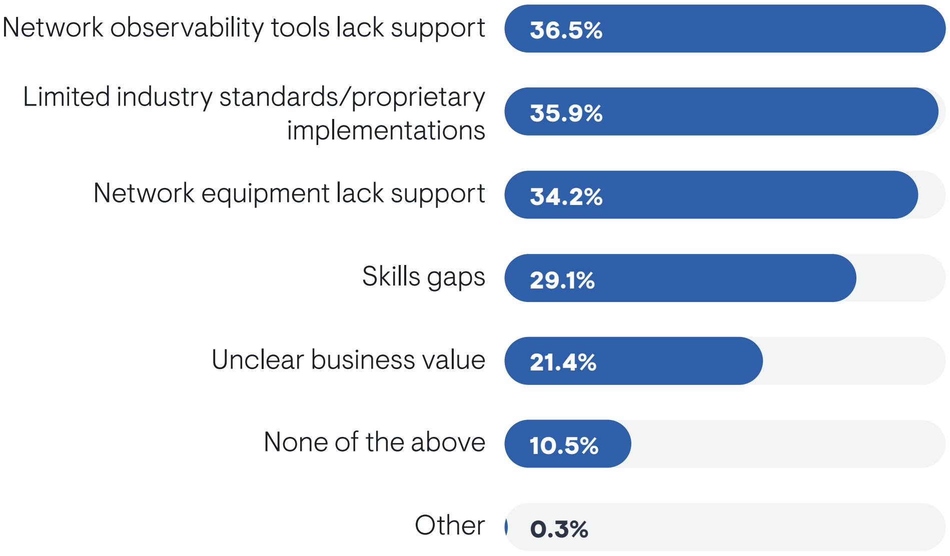
"Streaming has been around for a number of years, but it's still not mature enough where it's available in a consistent manner [across hardware vendors and tool vendors]," said a monitoring tool architect with a Fortune 500 media company. "The problem is that the device manufacturers haven't really standardized it, and the monitoring software vendors are waiting for them to do that."

Notably, only 20% cited unclear business value as a barrier to adoption, which suggests that most IT organizations perceive the value of streaming network telemetry.

Members of network engineering teams were more likely to cite limited industry standardization, network equipment support, and business value as problems, and they were less likely to worry about skills gaps. Thus, the experts know how to work with this technology, but they don't think the technology is mature enough. Very large enterprises (10,000 or more employees) were more likely to struggle with skills gaps.

> "Streaming has been around for a number of years, but it's still not mature enough where it's available in a consistent manner [across hardware vendors and tool vendors]," said a monitoring tool architect with a Fortune 500 media company.

Figure 16. What are the primary challenges to adopting streaming network telemetry with your network observability tools?

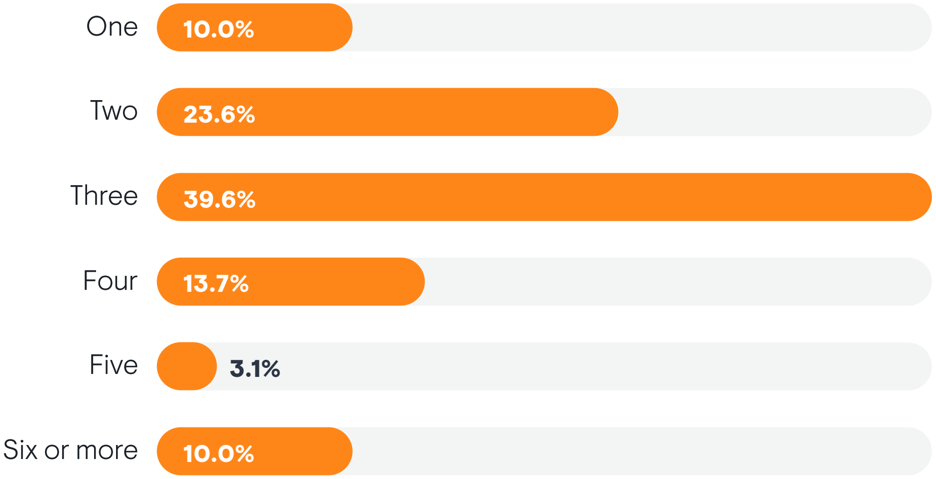


Sample Size = 351

Multi-Vendor Support

Figure 17 reveals that 90% of the organizations represented in this research have multi-vendor networks. Nearly 27% have four or more network vendors.

Figure 17. How many network infrastructure vendors (including providers of switches, routers, Wi-Fi, SD-WAN, load balancers, and firewalls) are installed in your company's network today?

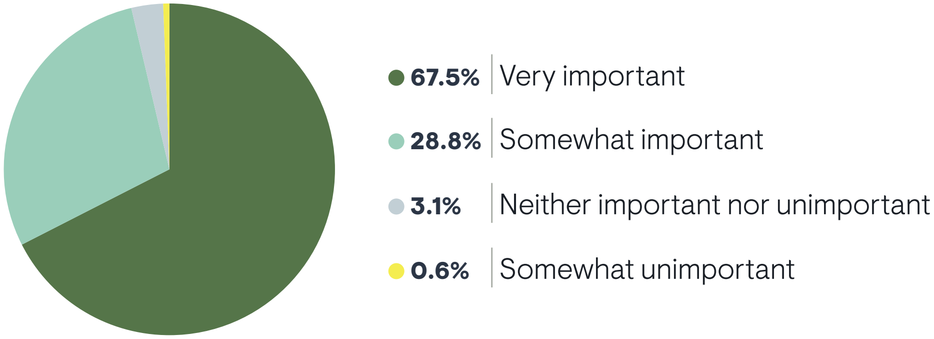


Respondents who work within an IT executive suite reported the smallest number of networking vendors. Members of network engineering, network operations, project management, and IT assets and financial management all perceived a larger number of vendors.

Sample Size = 351

Network observability solutions must support multi-vendor networks. This is a long-standing requirement, and it's a major reason why third-party network management tool vendors have remained prevalent for decades, because the network monitoring tools a network infrastructure vendor provides tend to focus primarily on managing and monitoring that infrastructure vendor's own products. **Figure 18** reveals that multi-vendor support is at least somewhat important in almost all IT organizations, with nearly 68% describing it as very important. Organizations who place more importance on multi-vendor networks reported more success overall with their network observability tools.

Figure 18. How important is it for your network observability tools to support multi-vendor networks?



Members of DevOps and network engineering teams were more likely to demand multi-vendor support than the IT executive suite, cloud engineering, and IT asset/financial management.

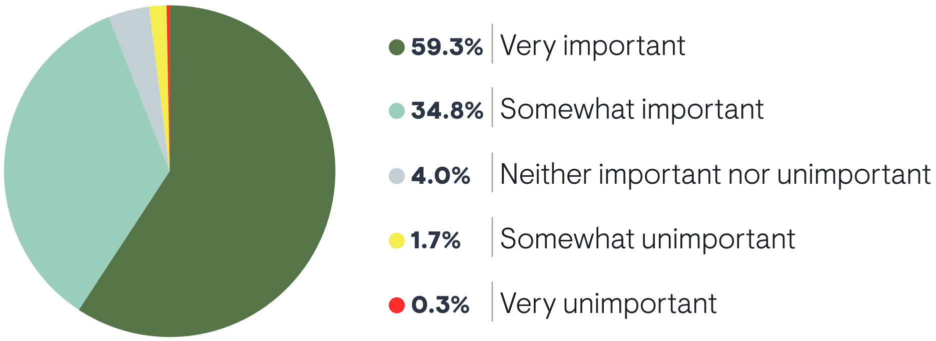
Sample Size = 351

Visibility into Unmanaged Networks

Traditionally, network observability tools have monitored the network infrastructure that IT organizations administratively own. This administrative ownership allows network teams to configure or instrument the network to allow tools to collect data. For instance, network teams have no control over an internet service provider's (ISP's) network, and they cannot configure that ISP's routers to export flow records or device metrics to a tool. The same goes for an employee's home office Wi-Fi and internet. As these unmanaged networks become more integral to an enterprise's overall end-to-end network, IT organizations need tools that can observe unmanaged infrastructure. **Figure 19** indicates that 96% of respondents believe it is at least somewhat important for this kind of observability, and most describe it as very important.

> Frontline operations personnel are recognizing the need to close observability gaps with unmanaged networks.

Figure 19. How important is it for your network observability tools to be able to monitor and troubleshoot unmanaged networks for which you have little or no administrative control (e.g., internet, home office, public cloud)?

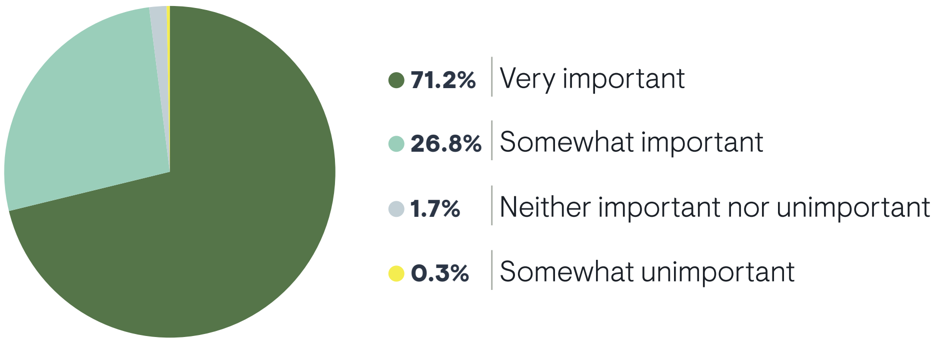


Subject matter experts, such as engineers and architects, were more likely than IT executives and middle managers to consider this a very important requirement. This highlights the fact that frontline operations personnel are recognizing the need to close observability gaps with unmanaged networks. In fact, members of the network engineering group were more likely to demand this capability than the IT architecture or project management groups. Respondents who reported more success with network observability placed more importance on having this kind of insight in their tools.

End-to-End Insights

Given the complexity of today's networks, IT organizations sometimes struggle to understand the end-to-end state of infrastructure. Network teams manage data center networks, cloud networks, campus switching, Wi-Fi, internet connectivity, and managed WAN services, like MPLS. Their tools often specialize in subsets of these domains. **Figure 20** reveals that most network teams need solutions that can give them end-to-end visibility and insights across all these domains. In fact, 71% say it is very important to have end-to-end network observability.

Figure 20. How important is it for your network observability tools to provide visibility and insights end-to-end across different domains, such as switching, Wi-Fi, data center, WAN, network security, and cloud networks?



Sample Size = 351

“Troubleshooting of issues is very difficult because there are so many different domains,” said a network management tool architect with a Fortune 500 retailer. “If you go into our tool, you’re going to see different dashboards and reports for DNS, for Windows servers, for network devices. It’s like all of them are in their own little world of data and everything is happening separately. Events are all being tracked separately and there is no correlation layer.”

“It takes some tooling to figure out if there is an ISP or Wi-Fi issue in the environments of our remote users,” said a network engineer with a billion-dollar fintech company. “We also serve a lot of external clients over the public internet, so we have challenges with managing paying customers too. There aren’t a lot of off-the-shelf tools that do outside-in monitoring.”

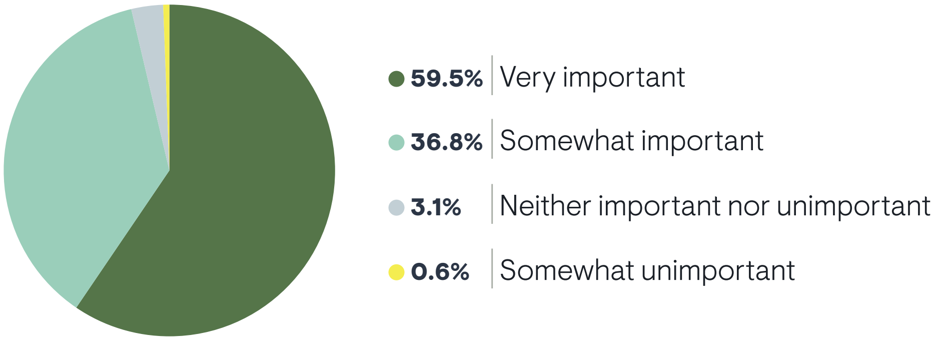
Respondents who reported more success with network observability said this end-to-end capability was more important to them. Organizations that most want this capability tended to have a larger network observability toolset, suggesting that they struggle to get this capability from a single tool. EMA also found that this capability is more important to organizations that have a larger number of network vendors installed.

End-User Experience

Figure 21 reveals that network operations teams need tools that show more than network performance. They also need insights into the experience of individual users on the network. More than 96% believe it is at least somewhat important to have this capability. This kind of visibility requirement will drive interest in network observability tools that incorporate digital experience management capabilities, such as synthetic network traffic monitoring, endpoint monitoring, and real-user monitoring (RUM).

Subject matter experts (engineers, architects) were the most likely to say this capability is very important, suggesting that frontline personnel are seeing the need to manage individual users’ network experience via network observability. In fact, members of network engineering and network operations teams were the most likely to say this was very important. Respondents who reported more success with network observability placed more importance on this network experience management capability.

Figure 21. How important is it for your network observability tools to help you monitor and troubleshoot the network experience of individual users?



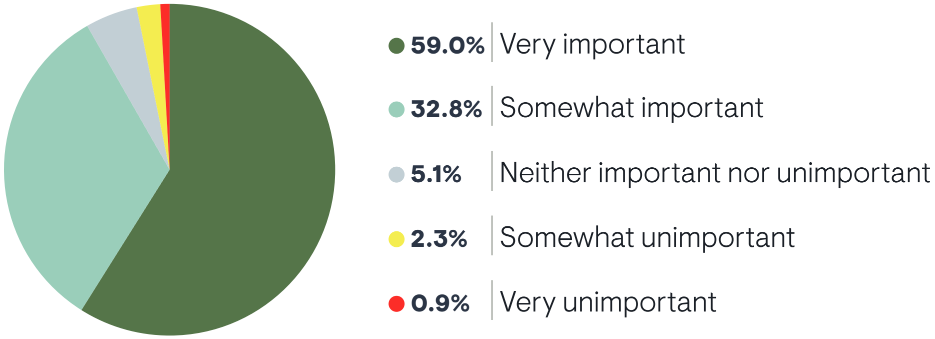
Sample Size = 351

AI-Driven Network Observability

IT organizations increasingly recognize that their network observability solutions must leverage AI/ML capabilities. **Figure 22** shows that nearly 92% believe it is at least somewhat important for network observability vendors to optimize and automate network management with AI/ML technology.

> 92% believe it is at least somewhat important for network observability vendors to optimize and automate network management with AI/ML technology.

Figure 22. How important is it for your network observability tools to offer features based on artificial intelligence and machine learning (AI/ML) to optimize and automate network management?

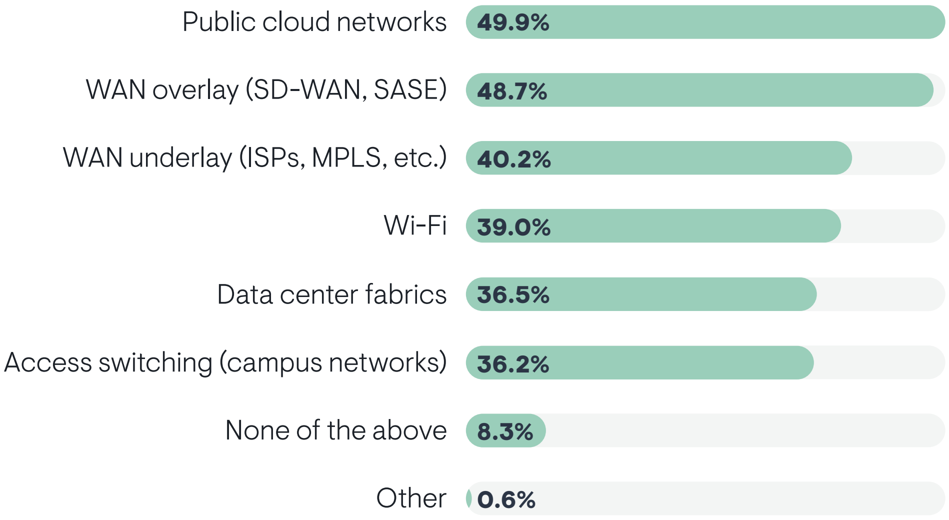


Organizations that are more successful with network observability are more likely to believe AI/ML capabilities are important. Members of network engineering teams were the most likely to say AI is very important, followed by the IT executive suite and the network operations team. IT architecture and project management were least enthusiastic. Organizations that operate multi-vendor networks placed more importance on AI.

Sample Size = 351

Vendors often train their AI/ML models to have specific domain expertise, especially network infrastructure vendors that offer hardware and software for specific network domains (e.g., SD-WAN, Wi-Fi). **Figure 23** reveals the types of domain expertise IT organizations are most interested in leveraging with AI/ML. Public cloud networks and SD-WAN overlays and underlays are the main priorities.

Figure 23. Do you need network observability tools that have AI-driven domain expertise for any of the following parts of your network?



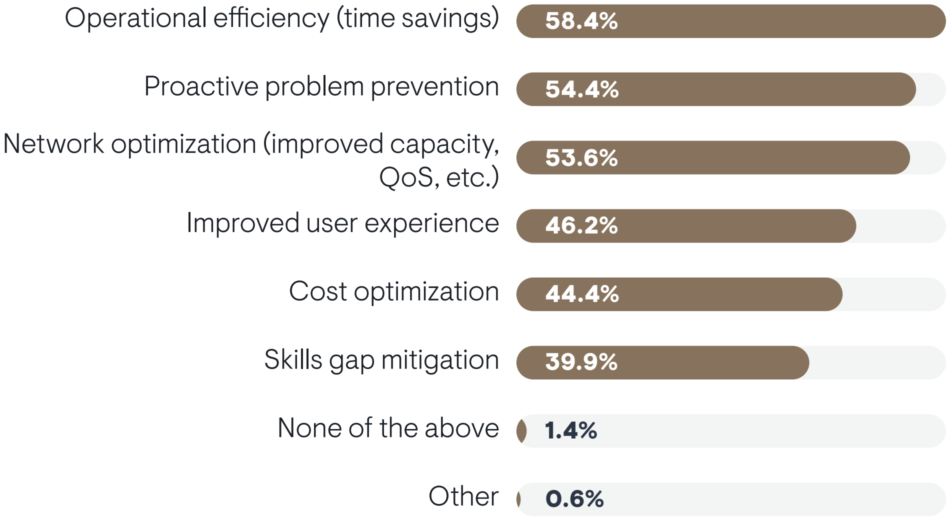
Wi-Fi expertise is a lower priority overall, but organizations that enjoy the most success with network observability were more likely to seek it in an AI solution.

Sample Size = 351

AI/ML Benefits

Figure 24 reveals why interest in AI/ML-driven network observability is so high. Most respondents believe it can deliver three key benefits: operational efficiency, proactive problem prevention, and network optimization. Organizations that are less successful with network observability are more likely to strive for proactive problem prevention.

Figure 24. Which of the following potential benefits of applying AI/ML to network observability is most appealing to you?



Sample Size = 351

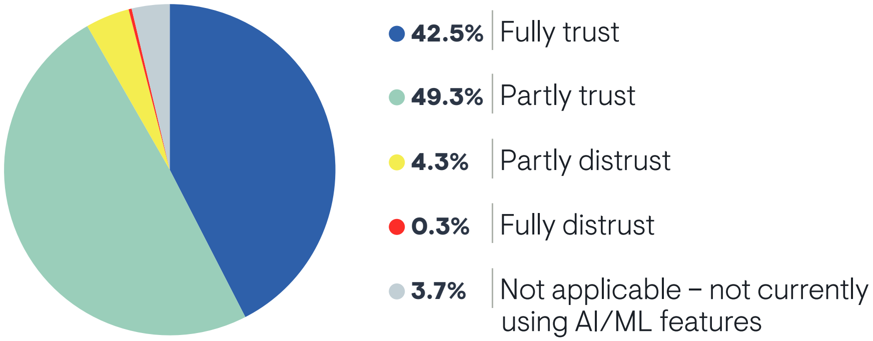
Many also perceive that AI/ML will improve user experience and optimize costs. Subject matter experts (engineers, architects) are more likely to see an opportunity for cost optimization. Respondents overall were most skeptical about AI's ability to mitigate skills gaps.

Organizations that operate multi-vendor networks were more interested in AI that could enable proactive problem prevention, cost optimization, and skills gap mitigation.

Trust in AI

While interest in AI/ML-driven network observability is strong, trust in AI is less robust. **Figure 25** reveals that 43% of respondents fully trust AI-driven network management capabilities today. More than 49% only partly trust them. Only 4% actually distrust AI. Organizations that place a higher priority on applying budget and resources to network observability solutions were more likely to trust AI/ML capabilities, suggesting that organizations get what they pay for. Respondents who reported using a larger number of individual network observability tools also trusted AI more. These respondents likely have experience with a wide variety of AI offerings from multiple vendors, allowing them to identify solutions that are most trustworthy within their toolsets. This trust was even more robust when these multiple tools are tightly integrated.

Figure 25. To what extent do you trust the AI/ML-generated recommendations and insights your network observability tools offer?



> 43% of respondents fully trust AI-driven network management capabilities.

Sample Size = 351

"In most cases, vendors are using models that are not well-trained, and there are a lot of false positives," said a network management tool architect with a Fortune 500 retailer. "So, I'm not 100% trusting it. And those insights don't work at scale. They work at an individual level with limited value for large organizations. If one store's network is down, the only person who cares about it is the owner of that store. At any given point, there are close to 30 going down, and if you are below that number, management is fine with it. There's not a lot of revenue loss. This is where AI fails. We need to train models on broader data sets."

Respondents who reported that their AI solutions have domain expertise in Wi-Fi and WAN overlay solutions, like SD-WAN and SASE, tended to have more trust in that AI. Members of network engineering and network operations groups indicated the most trust in AI insights. The cloud team was the most skeptical.

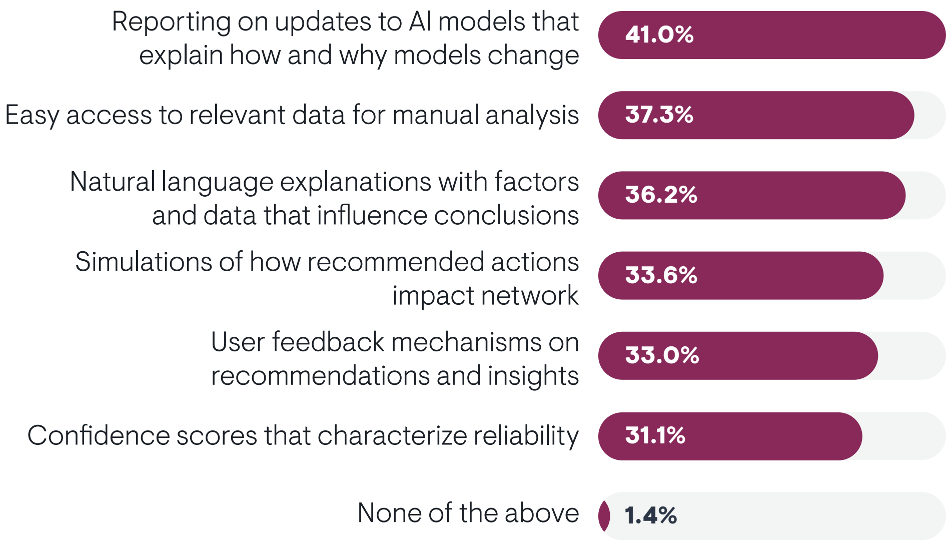
When IT teams have network observability tools that fail to correlate insights across multiple classes of data (metrics versus flows, for instance), they are less likely to trust AI. EMA also found that organizations that embrace open source network observability solutions have less trust in AI.

Figure 26 reveals what IT professionals want to see from vendors to build trust in AI/ML capabilities. First, they want transparency on how vendors update and change their AI models. IT middle managers were more likely to see the value in this reporting, and project managers were least likely. This option was most popular among midsized enterprises (1,000 to 5,000 employees).

Second, they want to verify AI insights by having easy access to underlying data for manual analysis. Many also want natural language explanations about how an AI technology reached its conclusions and they want simulations of how recommended actions will impact the network. The least compelling options are user feedback mechanisms and confidence scores, although plenty of respondents saw value in both. Respondents who reported less success with network observability were more likely to select confidence scores. Confidence scores appealed to large and very large enterprises (5,000 or more employees) than midsized (1,000 to 5,000).

"It's great right now for recommendations, but I'm not comfortable enough in its maturity level to let it make changes without authorization," said a network management tool architect with a $30 billion bank. "Show me what we should do and why we should do it and let us make the decision."

Figure 26. Which of the following is most helpful for building trust in AI/ML capabilities in network observability tools?



Sample Size = 351

How to Get Actionable Insights

Given that actionable insights are a top consideration for network observability tools, EMA asked research interviewees to tell us how their tool providers could better supply these insights to customers. Here are some of their responses.

"It's easy to collect data and present data. The challenge is surfacing insights. Rather than show a static dashboard, how about a system that knows what metrics are behaving in an abnormal fashion? Highlight those issues at the top of the dashboard. Explore how systems can apply AI/ML techniques to show anomalous behavior. Then, fine-tune those parameters so that you can reduce noise from those anomalies."

Monitoring tool architect with a Fortune 500 media company

"There are too many sites and domains in a network, and all of them are their own little worlds of data sources, like DNS, network devices, and network controllers. Every tool is generating single alerts that are being tracked separately and there is no correlation layer that tells you why something is happening. I need a tool that can triage data and tell me what occurred and when, and what the possible root cause is and what I can do to fix it."

Network management tool architect with a Fortune 500 retailer

"If you are a tool vendor with a lot of bells and whistles, don't show them to me all at once. Tailor the tool to the customer's business. When you implement something for us, talk to the major stakeholders and get their input for what they would like to see and what they would use it for."

Infrastructure manager with a Fortune 500 energy utility company

"Our previous tool was very powerful, but it relied on someone understanding packet capture data. The tool would pull out stuff for our review on a specific thing, like bandwidth utilization, but you still need a network expert to set it up and review it. We need more powerful dashboarding and analytics out of the box that junior engineers can decipher."

Network management tool architect with a $30 billion bank

"We used to have a tool with graphical data, where you could hover over a particular time or area, and you could go into different subsets of data. You could double-click into different streams of UDP and TCP, hover over the TCP stream, and it would tell you how many packets were lost, how many resets and retransmits occurred. It saves so much time."

Network engineer with a Fortune 500 aerospace and defense company

Current Toolsets

Tool Sprawl is the Norm

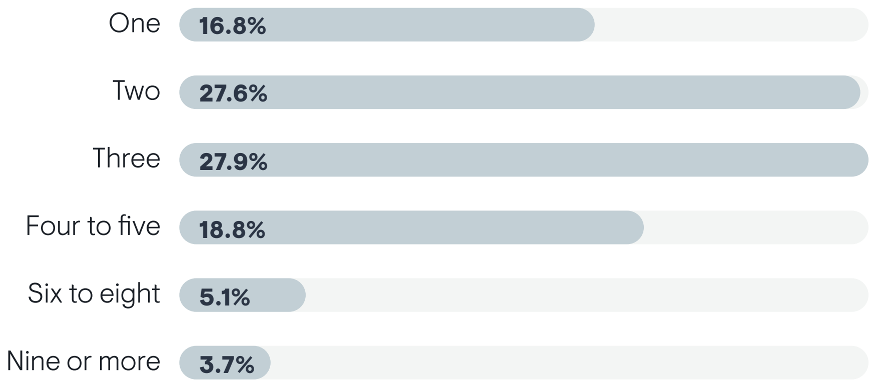
At the beginning of a typical conversation about network observability, network infrastructure and operations professionals will tell EMA analysts how many tools they use. As the conversations progresses, they will often say, “Oh, there’s another tool that I forgot to tell you about.”

In other words, tool sprawl is so common in network operations that networking pros struggle to provide a comprehensive list of them. **Figure 27** makes this situation clear. Fewer than 17% of IT organizations claim to have a single network observability tool. Typically, organizations have two or three, but more than 26% have four or more tools. Larger companies tended to have more tools. For instance, 44% of companies that have 10,000 or more employees had four or more network observability tools.

> Tool sprawl is so common in network operations that networking pros struggle to provide a comprehensive list of them.

“There isn’t one thing in the market that can do all the things we need it to do,” said a network management tool architect with a $30 billion bank. “We are still looking for something that can do everything, but right now, it’s pieces. We have one synthetic monitoring tool for circuit monitoring, another for [metrics], and a third for topology. We also have another synthetic monitoring tool that does additional testing.”

Figure 27. How many network observability tools does your organization use today?



Sample Size = 351

Organizations that use open source network observability reported larger toolsets than customers of commercial tools. IT executives appear uninformed about the true state of tool sprawl in their organizations. More than 31% of them believe their organization has only one network observability tool. Meanwhile, engineers and architects perceive sprawling toolsets. More than 17% of these SMEs claimed their organizations use six or more tools. Additionally, members of the network engineering and network operations groups perceived more tool sprawl than other groups.

Organizations with larger toolsets tended to identify operational technology/IoT and network technology refreshes as drivers of network observability requirements. Larger toolsets also correlated with multi-vendor networks. The more network infrastructure vendors an organization had, the more tools they used.

Integrating Toolsets

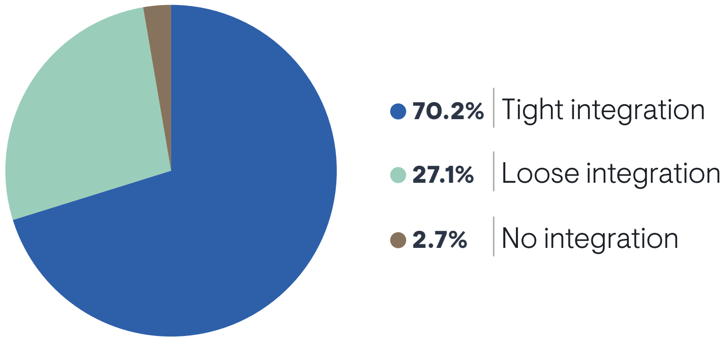
More than 97% of organizations with multiple network observability tools have integrated those tools, according to **Figure 28**. More than 70% of respondents described this integration as tight. Organizations with tight integration between tools reported more network observability success. Failing organizations usually had loose integration. IT executives were more likely to report tight integration of network observability toolsets than others, suggesting a perception gap between people who implement and use these tools and those who are managing from above.

“We’re trying to consolidate multiple views from several tools into a single dashboard so the NOC can really see the health of the environment,” said a monitoring tool architect with a Fortune 500 media company.

Notably, members of network engineering and network operations teams reported tighter integration than members of cloud engineering and DevOps. This suggests that DevOps and cloud pros are struggling to integrate their preferred tools with the network observability toolset. Larger companies (10,000 or more employees), which tend to have larger toolsets, also reported less integration. Nearly 40% indicated that they had only loose integration between their tools.

“I think the APIs and the integrations between a lot of tools have really improved over the last five years or so,” said a network management tool architect with a $30 billion bank. “It’s to a point where we are able to get really good data out of tools and our alerting is much better than it used to be.”

Figure 28. You indicated that you have multiple network observability tools. To what extent are these tools integrated?



Sample Size = 292

> 97% of organizations with multiple network observability tools have integrated those tools.

Figure 29 reveals that the most common integration between tools is data sharing. By streaming or importing data from elsewhere, a network observability solution can present more context in dashboards and reports. Some tools can apply algorithms to third-party data.

Many organizations also create integrated workflows, unified alerting, and event correlation across tools. AI-driven insights across tools is a secondary integration priority, and one that middle managers in IT organizations valued more than project managers.

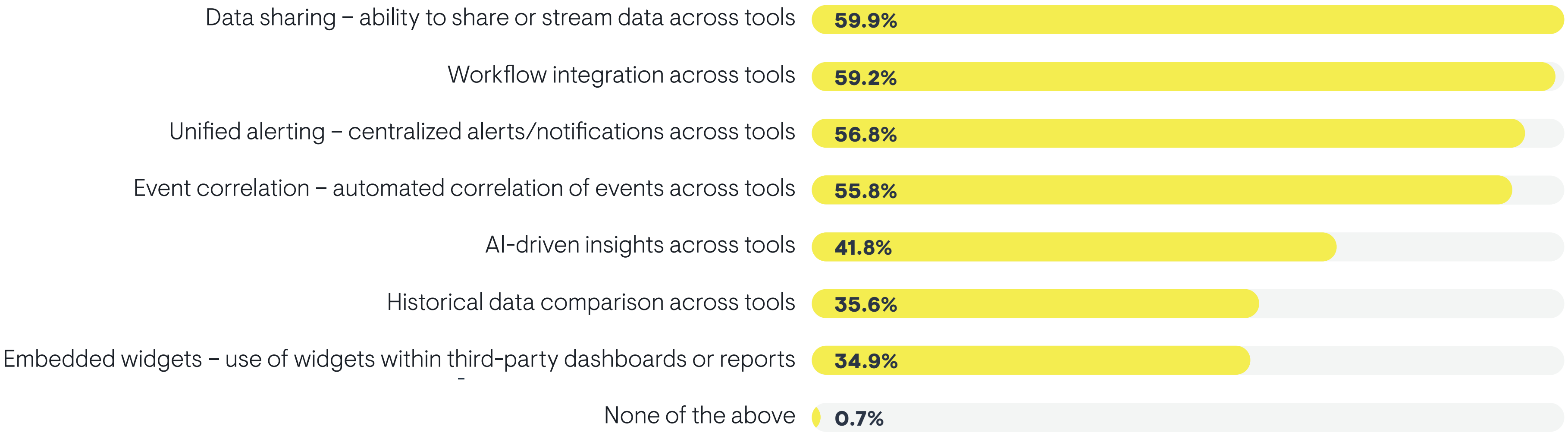
Workflow integration is an ongoing challenge for a network management tool architect with a $30 billion bank. "We have one tool that is our primary alerting tool. We're doing active polling on interfaces and hardware stats, but it's only at the device level. We see these alerts come in and troubleshoot some basics through that. But a lot of the time, our alerts are not a hardware issue. So, we have to jump to another tool to look at the circuits. It is not always easy, and sometimes the circuit is fine. So now we dig into the packets, which is another tool. I'd like to see all that information at once through one tool."

Embedded widgets in third-party dashboards and reports were not very popular overall, but organizations that reported the most success with network observability tended to make them an integration priority. IT executives were more likely than middle managers to perceive the value of embedded widgets.

Organizations with larger network observability toolsets had three distinct integration priorities between those tools: event correlation, unified alerting, and embedded dashboard widgets.

From a group perspective, the IT executive suite and project management both perceived data sharing across tools and unified alerting as integration priorities, while network engineering teams were less likely to select these.

Figure 29. Which types of integration are most important between your network observability tools?

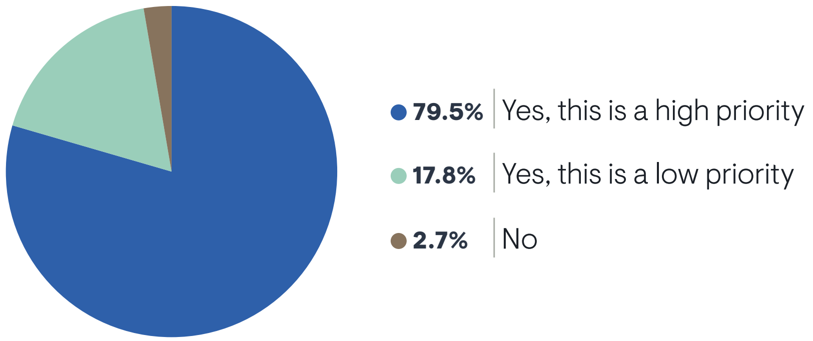


Sample Size = 292

Sprawl Consolidation

Figure 30 reveals that 97% of organizations with multiple network observability solutions are looking for ways to consolidate tool sprawl. Nearly 80% identify this as a high priority.

Figure 30. Given that you use multiple network observability tools, is your organization looking for ways to consolidate these tools?



Sample Size = 292

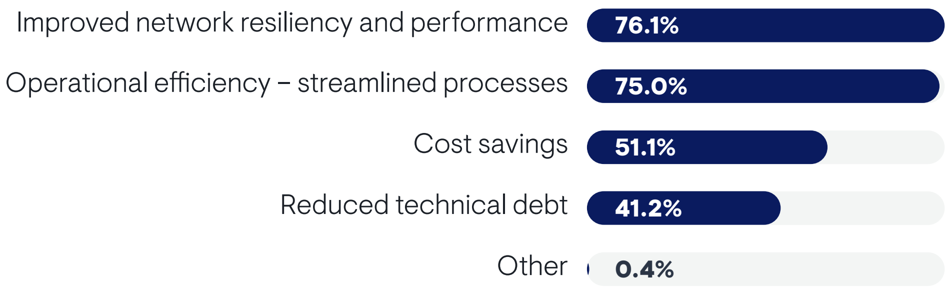
This consolidation won't be easy, as many IT professionals have told EMA. "No one tool does everything that I want," said a network engineer with a billion-dollar fintech company. "I need multiple tools. You have to look here to do X and look there to do Y."

The network team is on an island with this issue. Members of network engineering and network operations teams were more likely to describe this as a high priority, while DevOps, IT architecture, IT asset and financial management, and project management were less likely. Users of open source tools made tool consolidation a higher priority.

Figure 31 shows why consolidation is so important. Most organizations think that a streamlined tool set will drive improved network resiliency and performance and overall operational efficiency. Most also think they can save money through consolidation. A smaller number are aiming at reduced technical debt. Technical debt is especially a motivation for organizations that use open source tools and organizations that have a large number of network infrastructure vendors installed.

> Most organizations think that a streamlined tool set will drive improved network resiliency and performance and overall operational efficiency.

Figure 31. What are the top drivers of your organization's interest in network observability consolidation?



Sample Size = 284

Organizations with larger toolsets were more likely to cite cost savings and improved network resiliency and performance as drivers. Cost savings motivates members of IT asset and financial management groups more than the IT executive suite. This is also a higher priority for organizations that use network observability tools provided by their network hardware vendors. The need for operational efficiency drives the IT executive suite and the network operations team, but network engineering is less motivated by this. Finally, the network operations team is more motivated by improved network resiliency than the IT architecture group.

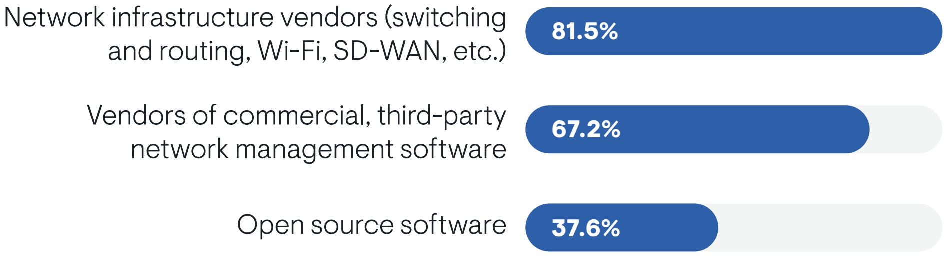
"We are trying to consolidate to fewer tools," said a monitoring tool architect with a Fortune 500 media company. "We are trying to get rid of three tools in favor of one so we can simplify our architecture and do more with less. It reduces our technical debt."

Tool Providers

In EMA's view, there are two general types of vendors that provide commercial network observability tools. First, there are network infrastructure vendors that offer observability capabilities via the element management tools they bundle with their infrastructure products. The second group consists of third-party tool vendors that specialize in vendor-neutral observability of networks. There is a third source of observability tools, too: EMA finds that many IT organizations use open source software for network observability.

Figure 32 shows how enterprises are sourcing network observability today. Nearly 82% have solutions that network infrastructure vendors provide, and more than 67% are using solutions from a specialist tool vendor. Aside from commercial solutions, nearly 38% are using open source observability software. Open source tools were more common in larger companies.

Figure 32. Which of the following are sources of the network observability tools that your organization uses to manage its network?



Sample Size = 351

"There is a lot of interest in my company to use open source," said a monitoring tool architect with a Fortune 500 media company. "Organizations get better control of their data and the workflows, but there's a cost associated with it in terms of having more development resources. So, we're in this hybrid approach, where we have some vendor solutions but we're also building internal tools with open source, not just for observability, but also configuration management."

"I like being able to customize solutions," said a network management tool architect with a Fortune 500 retailer. "That's why I like open source tools like Grafana."

"I'm not content with tools we can get off the shelf," said a network engineer with a billion-dollar fintech company. "That's why we go custom with Prometheus and other open source tools. You can customize them and make them as smart as you want to. I've never been limited by them, but It's a lot of work. I would like to go all customized and open source. You just need the time and the skills. I would do it, but other people don't have the same skillsets and right comfort level."

> "I'm not content with tools we can get off the shelf," said a network engineer with a billion-dollar fintech company. "That's why we go custom with Prometheus and other open source tools.

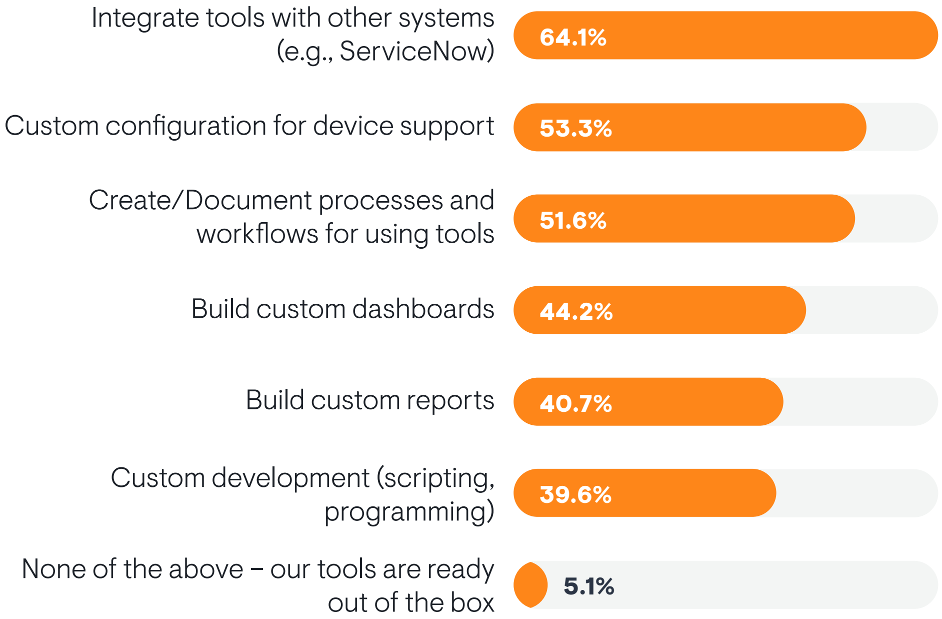
The IT executive suite was more likely than other groups to perceive specialist tool vendors as a source of network observability solutions. Multi-vendor networks tended to rely more on tool vendors and open source for network observability, and open source was particularly common in companies that used six or more networking vendors. Organizations that had fewer networking vendors installed were more likely to use network observability solutions offered by those hardware vendors.

Network Observability Outcomes

Integrating Tools into Network Operations

Figure 33 reveals some of the complexity involved in implementing a network observability solution. Installation is only the beginning. More than 64% must integrate the solution with other IT management tools. More than 53% must conduct custom configuration of the tool for device support, especially for support of devices that the tool doesn't work with out of the box. Nearly 52% must create and document processes and workflows for using the tools.

Figure 33. To get full value from your network observability tools, does your organization have to do any of the following?



Many organizations also build custom dashboards and reports and nearly 40% perform custom development on a tool via scripting and programming.

Sample Size = 351

"There were a couple of data analysts who reported to me, and they would send out monthly reports of limited value," said an infrastructure manager with a Fortune 500 energy utility company. "I told them I wanted to see reports that analyze what we're providing to the business and insights into how we saw an uptick of tickets from this carrier, or we saw a high percentage of self-inflicted outages from this group. Those insights are key, because what's the point of looking at numbers in a report unless you're trained to know what they mean? Now, we use Grafana to produce some of these custom dashboards and reports that show us what the data means with the correct labels and customized for the groups that need to know the information."

"I create customized dashboards that have to tell a story," said a network engineer with a billion-dollar fintech company. "But I have to know what I want. We have different business units that use dashboards that mean something specific to them. If a tool vendor has a UI that is easy to customize, but more customizability requires more skillsets."

Organizations that use open source network observability tools were more likely to report that their tools required custom development, custom configuration for device support, and integration with other systems in order for the tools to be ineffective. Customization requirements of open source network observability tools led to increased costs and delayed time to value.

> Customization requirements of open source network observability tools led to increased costs and delayed time to value.

Organizations that have a larger number of network infrastructure vendors installed were more likely to need custom tool development, custom configuration for device support, custom reports, and integration with other systems.

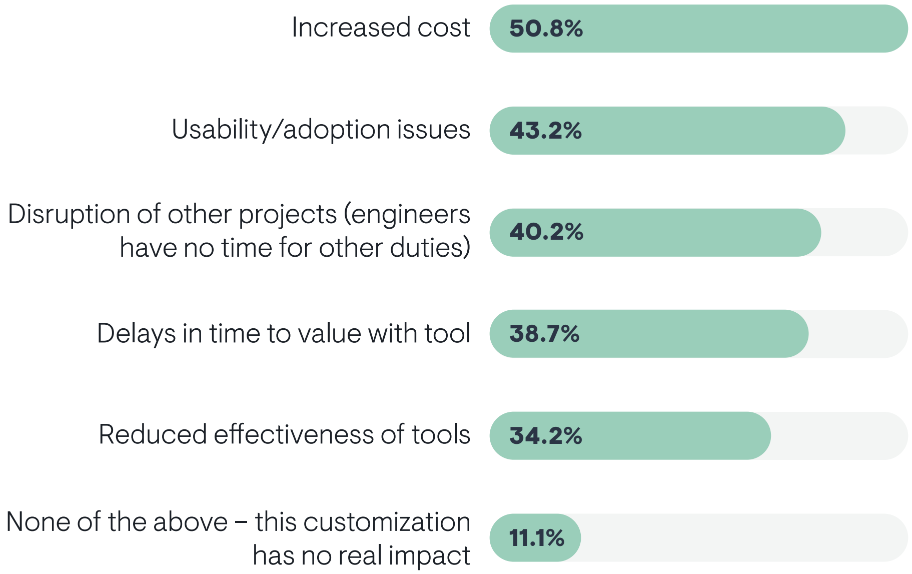
Subject matter experts were more likely than project managers and IT executives to know that tools require the creation of custom dashboards and custom reports.

Overall, members of the IT executive suite were less aware than other groups of the need for custom tool development and custom tool configurations for device support, but they were more aware than others of the need to create and document processes and workflows around tools. Larger companies were more likely to perform custom development on a tool and build custom dashboards.

Figure 34 reveals that 89% of organizations experience negative impacts from these customization and integration efforts. Nearly 51% cited increased costs. Members of project management and IT asset/financial management groups were more aware of cost issues, while the IT executive suite and network engineering teams were less aware. Many also see usability and adoption issues, disruptions to other projects as engineers devote cycles to observability implementation, and delayed time to value with the tool.

The least likely outcome of this work is reduced effectiveness of the tool. However, members of the IT executive suite were much more concerned than the project management group about this issue. This issue was more common in enterprises (5,000 to 10,000 employees) than midsized enterprises (1,000 to 5,000). The largest companies in this survey (10,000 or more employees) were more likely than others to report no issues, suggesting that they have enough resources to mitigate any negative impacts of tool customization.

Figure 34. You indicated that your organization must customize and/or integrate your network tools to get full value. Does this custom work impact your organization in any of the following ways?



Sample Size = 333

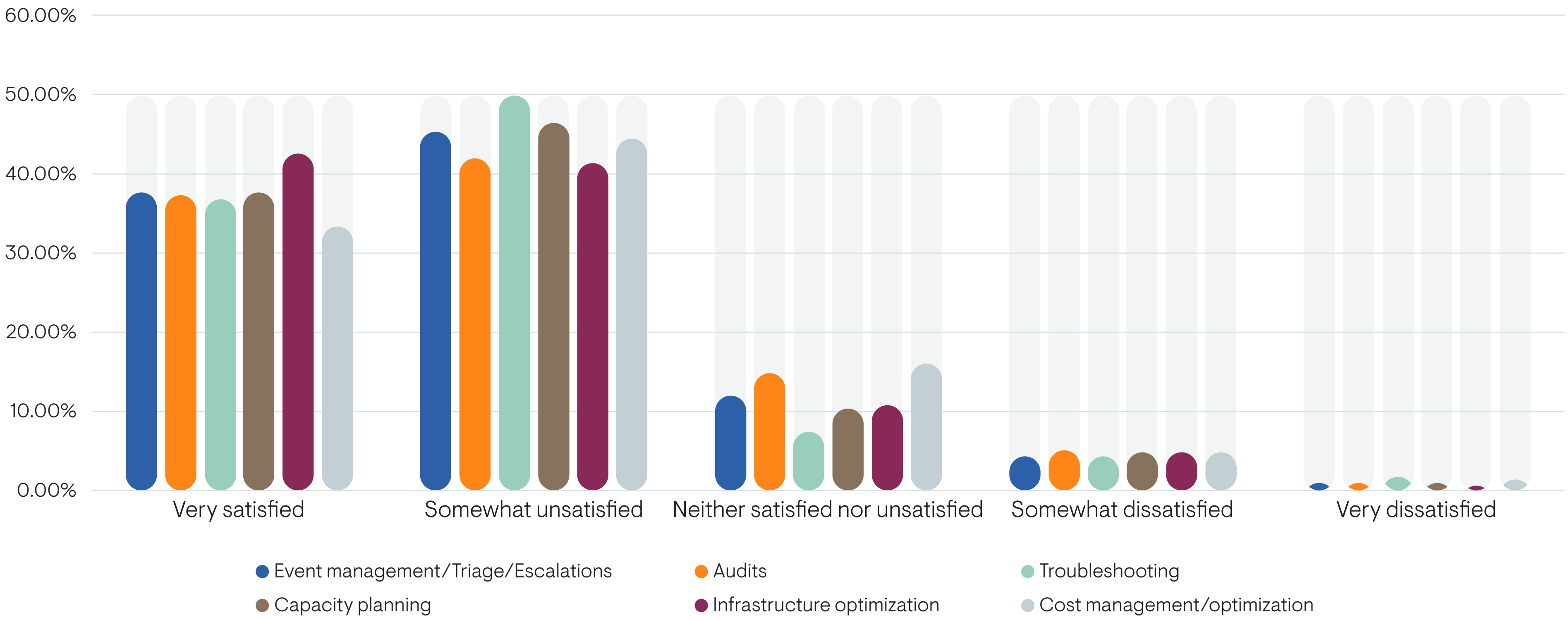
Tool Satisfaction

Use Case Support

Figure 35 reveals how satisfied respondents are with how their network observability tools support six core use cases. Overall, respondents are mostly partially satisfied with each use case. Infrastructure optimization (tuning networks via observed insights) garners the most satisfaction. Cost management and optimization generated the least amount of satisfaction. IT executives tended to be more satisfied than others with cost management.

Event management, audits, troubleshooting, and capacity planning all received similar markets, with less than half completely satisfied. Respondents who reported the most success with network observability were more satisfied with support of all use cases, although even they tended to be only modestly satisfied with cost management support. Organizations that use open source network observability tools were more satisfied with event management support than customers of specialist tool vendors.

Figure 35. How satisfied are you with how your network observability tools support the following use cases?



Sample Size = 351

"The innovation in tools has been stagnant," said a network engineer with a Fortune 500 aerospace and defense company. "There hasn't been a lot of evolution that really wows us."

"Right now, our tools are lacking," said a network engineer with a billion-dollar fintech company. "Every couple years I look around and say there has got to be something better out there."

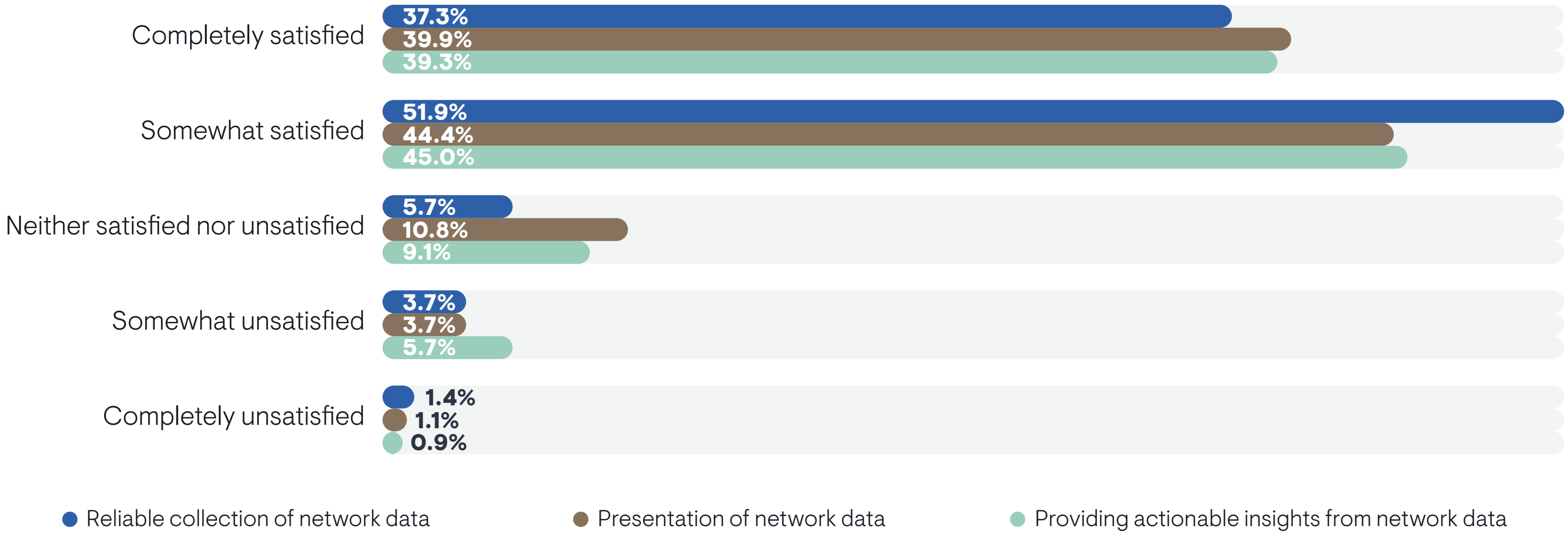
"Right now, our tools are lacking," said a network engineer with a billion-dollar fintech company. "Every couple years I look around and say there has got to be something better out there."

Platform Requirements

Figure 36 reveals how satisfied respondents are with how their network observability solutions reliably collect network data, present that data, and provide insights into that data. Overall, less than 40% are completely satisfied with how their tools fulfill any of these requirements. Data collection is the weakest.

"Our tools are solid. The data is accurate," said a network engineer with a Fortune 500 aerospace and defense company. "It gives us an excellent current and historical perspective."

Figure 36. How satisfied are you with the ability of your network observability tools to fulfill the following requirements?



Sample Size = 351

Tool sprawl (larger toolsets) correlated with less satisfaction with actionable insights. Respondents who reported more success with network observability were more satisfied with all three of these platform capabilities. Subject matter experts (engineers, architects) tended to be less satisfied than IT managers and executives with how their tools present data and provide actionable insights. However, from an organizational perspective, the IT executive's suite was less satisfied with data collection than the network engineering and network operations teams. Respondents who use open source network observability reported more satisfaction with their tools' abilities to provide actionable insights.

Alert Noise

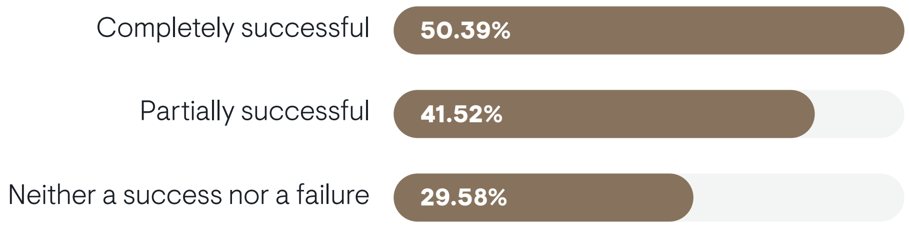
EMA asked respondents to tell us the percentage of the alerts generated by their network observability tools that are actionable and indicative of a problem that must be addressed. The mean response was less than 45%. In other words, more than 55% of the alerts network observability tools generate are false alarms or issues that don't require a fix.

> More than 55% of the alerts network observability tools generate are false alarms or issues that don't require a fix.

"Alerting is usually not a tool problem. It's a human problem," said a network engineer with a billion-dollar fintech company. "Every tool allows you to create an alert and configure how you want it to notify you. I think maybe tools could make it easier to tune alerts, but every tool has something."

Figure 37 reveals that success with network observability tools correlates directly to a higher percentage of alerts being actionable. Efficient and effective alert management is essential to successful network observability.

Figure 37. Percentage of alerts generated by network observability tools that are actionable and indicative of a problem that must be addressed, cross-tabbed by success with network observability tools.



Members of the network engineering team perceived a higher percentage of actionable alerts (57%) than network operations (44%), project management (43%), and the IT executive suite (43%).

Sample Size = 351

Observability Challenges and Pain Points

Data Problems

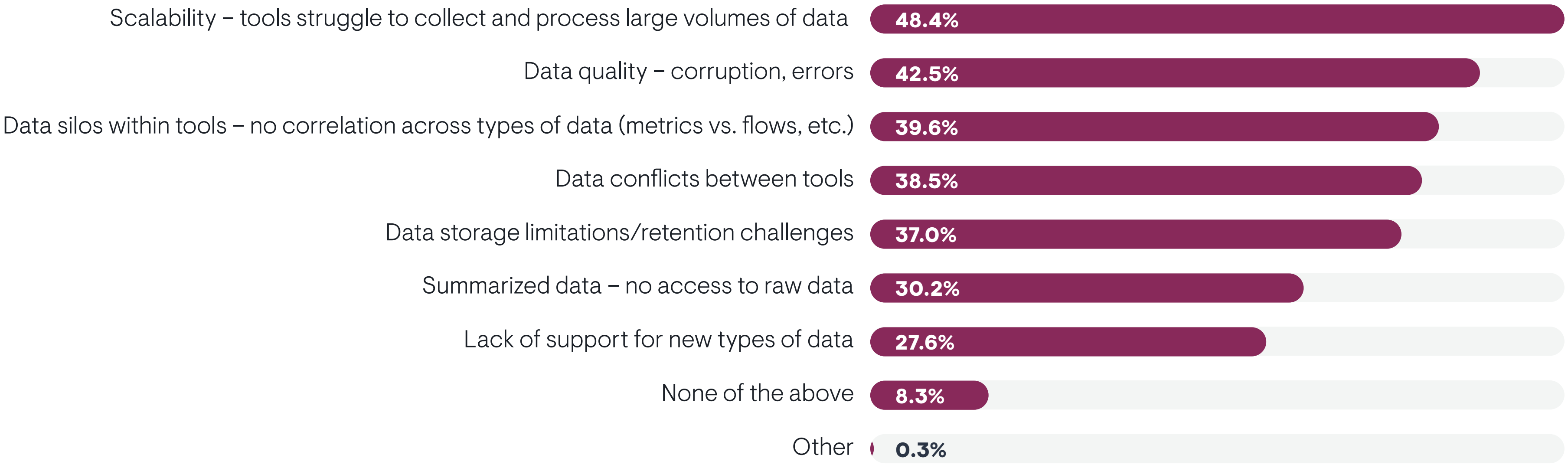
Figure 38 explores the most challenging data-related issues that organizations have with their network observability tools. Scalability is the biggest source of pain. Their tools are struggling to collect and process large volumes of data. This issue affects large and very large enterprises (5,000 or more employees) more than midmarket enterprises (1,000 to 4,999 employees).

"Scalability seems to be a problem even with SaaS tools," said a network management tool architect with a Fortune 500 retailer. "We were deploying a few thousand devices with our [SaaS-based network observability vendor]. I kept having to add more and more collectors into the platform to onboard more devices, but all the data collection was delayed because there is a huge queue."

Respondents identified data quality, data siloes within tools, data conflicts across multiple tools, and data storage or retention as their secondary problems. Respondents who are less successful with network observability were more likely to report problems with data silos within tools. Respondents who were uncertain about their success with tools cited a lack of support for new types of data. Overall, lack of support for new data was a minor issue, but it still affects more than one-quarter of companies.

"Many network vendors are lacking APIs or have totally crap APIs, so I have to go through a lot of effort to build custom tooling to get structured data from every device in the format that I want," said a network engineer with a billion-dollar fintech company.

Figure 38. Which of the following data-related issues present the most significant challenges when using your organization's network observability tools?



Sample Size = 351

"Back in the day, everything was simpler," said a network management tool architect with a Fortune 500 retailer. "There were network devices and servers. Now, data can be in any shape and form and from anywhere. Trying to onboard data that isn't supported out of the box is too much work."

Organizations that use open source network observability were more likely to struggle with data retention limits, data quality problems, and a lack of support for new types of network data.

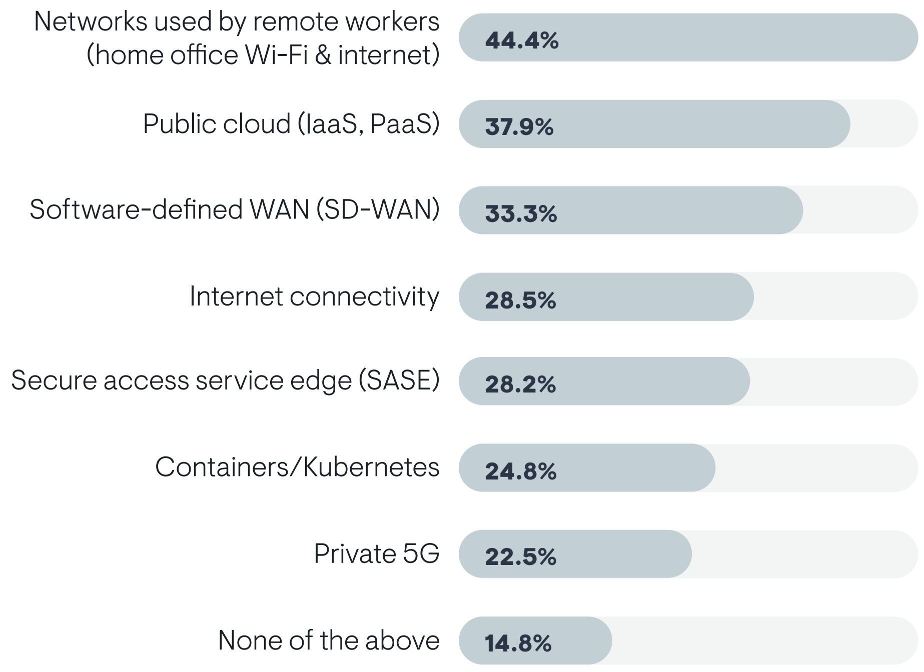
Tool sprawl correlates with data pain. The smaller a toolset, the more likely a respondent was to select "none of the above." On the other hand, respondents with larger toolsets tended to report problems with data conflicts between tools, issues with summarized data, and scalability problems.

> Respondents with larger toolsets tended to report problems with data conflicts between tools, issues with summarized data, and scalability problems.

Subject matter experts were more likely than middle managers and executives to perceive challenges with data quality, scalability, data storage, and support for new types of data. Summarized information with no access to raw data was a minor issue overall, but members of the network engineering team were nearly twice as likely as members of the IT executive suite to select it as a top problem.

Figure 39 looks at the data challenges from a different angle. EMA asked respondents to identify any parts of their networks from which they find it difficult to collect data. The chart shows that networks used by remote users are the biggest blind spots, whether it's an employee's home office Wi-Fi and internet or a coffee shop. These remote network setups tended to challenge organizations that are less successful with network observability, suggesting that they are a make-or-break issue for tools.

Figure 39. Do you find it challenging to collect data with your network observability tools from any of the following technologies?



"SDN is a challenge," said a monitoring tool architect with a Fortune 500 media company. "We can monitor the devices themselves using traditional SNMP methods, but a lot of [data center] SDN and SD-WAN solutions are controller-based, and these controllers manage the underlying devices. One of our SDN vendors is not supported by our tool vendor, so it's on the roadmap."

"We just completed an SD-WAN upgrade, and it's maddening," said a network engineer with a Fortune 500 aerospace and defense company. "We keep getting alarms from the orchestrator saying that it's getting out-of-order packets, but our other tools aren't showing any indicators of it. Our third-party tools are monitoring it and see nothing wrong."

Sample Size = 351

Many respondents also pointed to the public cloud and software-defined WAN technology as data collection problems. The IT executive suite was more aware of the cloud networking issue than project management personnel. Internet connectivity was a tertiary challenge. Everything else were relatively minor sources trouble.

“Cloud is 100% the biggest challenge right now,” said a network management tool architect with a $30 billion bank. “None of our tools are monitoring the cloud fully yet. When we’re looking at the cloud from a networking perspective, we have to get our cloud operations team to dig into their tools. We’ll hear that an application isn’t reaching the cloud, and we’ll look at our tools and see that everything is fine on the network. But the cloud team will say they’re not seeing anything on their end, either. So where is the disconnect? That’s been a big issue.”

“A lot of cloud-managed networking vendors offer switching and Wi-Fi, but mostly push you to use their platform as your main source of monitoring,” said a network management tool architect with a Fortune 500 retailer. “They’re making it difficult to make data available to other tools. If I SNMP to their devices, I can’t get much data. And their cloud-based tools don’t have the amount of data retention I need, and they don’t have all the alerting and dashboard capabilities I want.”

> “Cloud is 100% the biggest challenge right now,” said a network management tool architect with a $30 billion bank. “None of our tools are monitoring the cloud fully yet.

IT executives tended to be oblivious to several challenges. For instance, they were less likely than subject matter experts to see observability issues with SD-WAN and public cloud, and they were less likely than middle managers to perceive issues with containers and Kubernetes. Containers were a top issue for IT architecture personnel, but not for network engineering.

Large enterprises (5,000 to fewer than 10,000 employees) were more likely than midsized enterprises (1,000 to fewer than 5,000) to struggle to collect data from SD-WAN and container/Kubernetes environments. Very large enterprises (10,000 or more) were least likely to struggle with collecting data from internet connectivity.

User Experience Blind Spots

Earlier in this report, EMA found that 96% of respondents need network observability tools that monitor and troubleshoot the network experience of individual end users. **Figure 40** identifies the challenges to obtaining this kind of observability. The primary issue is network complexity. Secondarily, many struggle with their lack of administrative control and access over the networks that remote employees use, such as home offices.

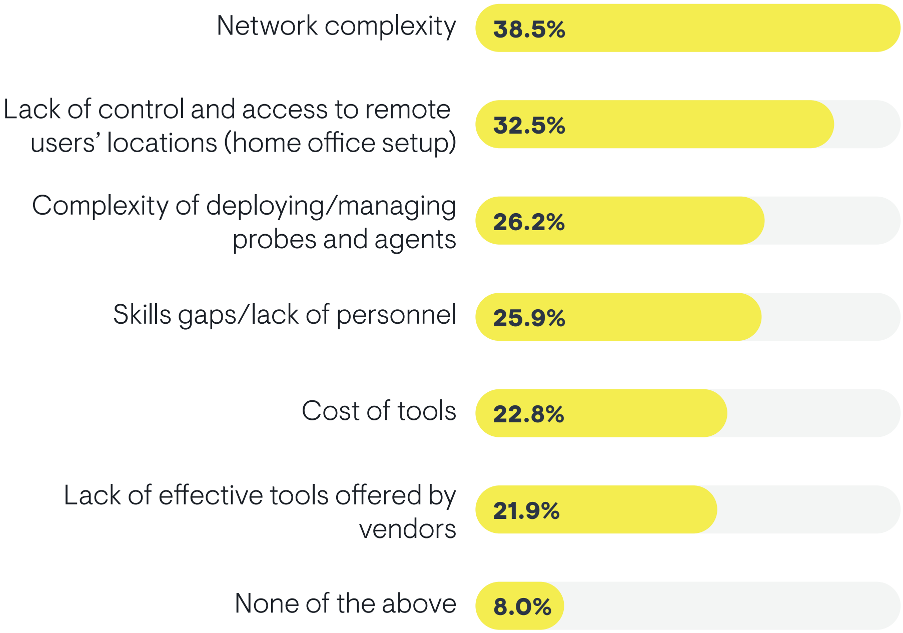
"It's definitely not just the tools," said a network management tool architect with a $30 billion bank. "It's the network's fault for how complex it is with many geographical locations and different types of environments, from branch offices to corporate offices to data centers to trading floors."

Some also discover that deploying agents and probes (such as for synthetic network monitoring) adds to toolset complexity.

Many organizations are also struggling with skills gaps and costs. Skills gaps are more common in larger enterprises. Tool costs were cited as a bigger issue for the IT executive suite and project management, but less of an issue for network operations groups.

"We were trying to get a synthetic network monitoring tool, but there was sticker shock, and not everyone was on board," said a network engineer with a Fortune 500 aerospace and defense company.

Figure 40. What do you find most challenging about monitoring and troubleshooting the network experience of individual users?

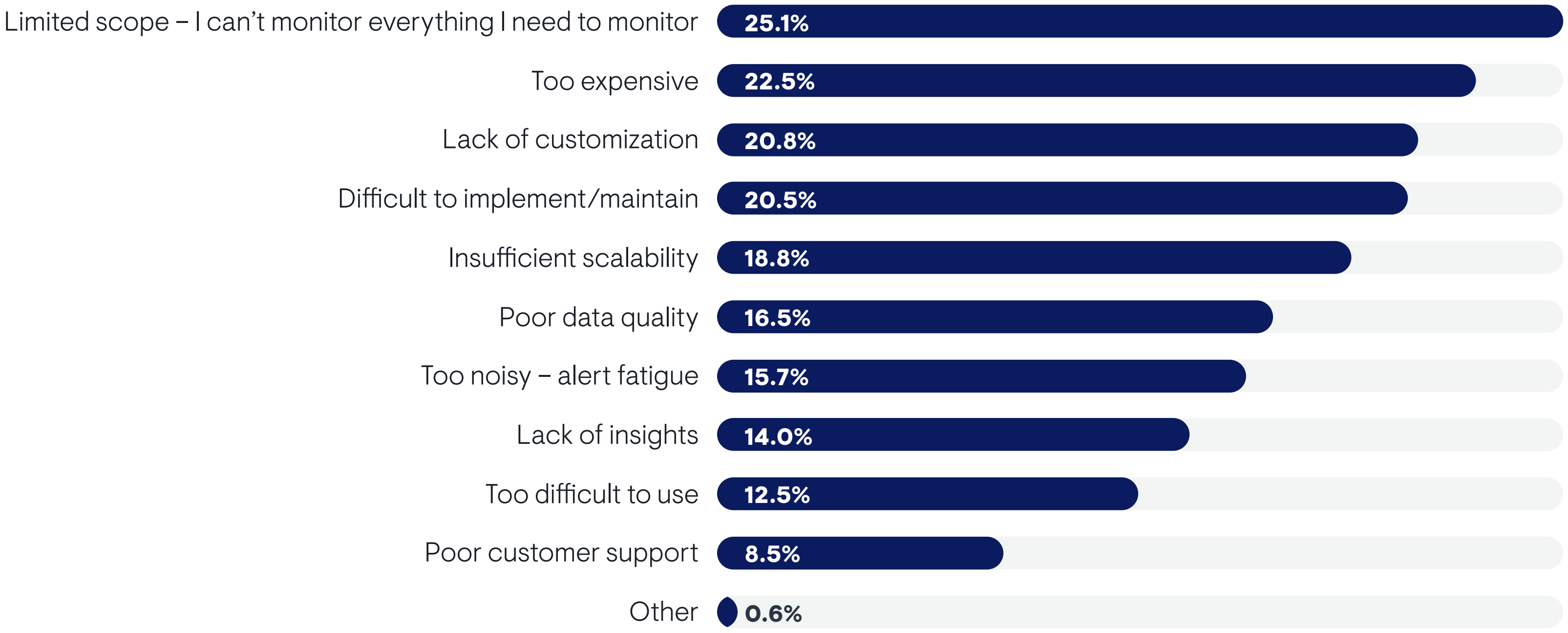


Sample Size = 351

Overall Tool Complaints

Figure 41 explores what most dissatisfies respondents about their network observability tools. The top issue is scoping of tools. Users find that they can't monitor everything they need to monitor. For instance, perhaps their core network observability solution doesn't support public cloud monitoring. Project managers were twice as likely as subject matter experts (engineers, architects) to consider this a problem. Respondents who tackle more complex issues or have a broader scope of responsibilities were more likely to struggle with this issue. For instance, members of the IT executive suite, the network engineering team, and project management team were more likely to cite this issue than the network operations team.

Figure 41. Which of the following are your biggest complaints about your network observability tools?



Sample Size = 351

Next, organizations are unhappy with the cost of their tools. “Everyone is trying to get rich quick,” said a network management tool architect with a Fortune 500 retailer. “Vendors are more focused on price than value. These vendors are heavily focused on marketing and sales, trying to grow their company without improving their products.”

After that cost, a lack of customization options offered by tools and the difficulty of implementing and maintaining them round out the top complaints. Implementation and maintenance were bigger issues for subject matter experts than IT middle managers and executives. Members of the network engineering team were the most likely to cite implementation and maintenance. This issue was cited by larger companies in general, suggesting that the complexity of larger networks comes into play.

Customization is as a big issue in many of the one-on-one conversations that EMA analysts had with IT professionals.

“Nothing does what I want it to do. Anything you want to customize around correlations and grouping, it’s very proprietary,” said a network engineer with a billion-dollar fintech company. “You have to go on user forums and figure out how to do it, or you have to make feature requests and wait a year.”

“The biggest thing for me is the ability for users to customize how they want to see the data,” said a monitoring tool architect with a Fortune 500 media company. “I want to use different visualizations. I want more flexibility in visualization engines. As a system architect, I can come up with multiple use cases and build them into the tool, but I can’t predict everything that users will need. So, tools need customization features to personalize user experience.”

“The biggest thing for me is the ability for users to customize how they want to see the data,” said a monitoring tool architect with a Fortune 500 media company. “I want to use different visualizations. I want more flexibility in visualization engines.

“One of the main problems with our vendor-provided tools is the customization of dashboards,” said a network management tool architect with a Fortune 500 retailer. “A lot of things are hard-coded. Let’s say you want an inventory report, there is an out-of-the-box report. But if you want to add labels for filtration and other customizations, it doesn’t work. It doesn’t allow you to customize its dashboards and reports enough.”

Insufficient scalability is also a major problem for that network management tool architect. “I’ve seen so many different tools where you open a dashboard, change the data retention from one day to one month, and the dashboard takes two or three minutes to load. It’s really slow. These are things that a lot of vendors are struggling with, basic fundamental issues.”

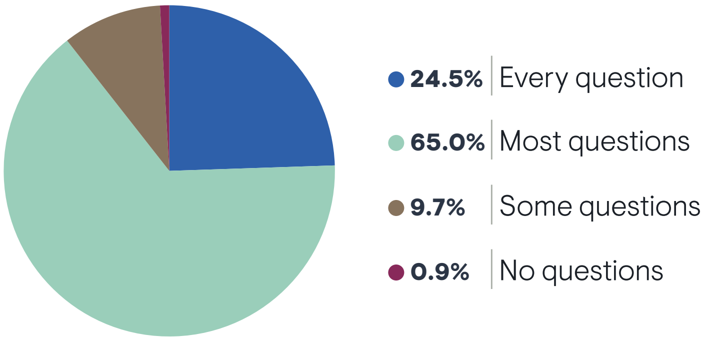
Organizations that use open source network observability were more likely to struggle with a lack of insights and ease of use issues. Poor data quality was also a bigger issue for subject matter experts than middle managers and executives. Insufficient scalability was a relatively minor issue, but members of network operations and IT architecture groups named it a top issue.

Poor customer support and poor ease of use are the least problematic aspects of today’s tools. The network engineering team was more likely than the network operations team to complain about customer support.

Observability Insights and Answers

When EMA discusses the differences between network monitoring and network observability with IT professionals, they often suggest that network observability tools should be able to provide insights and answers to questions about the network. **Figure 42** looks at how well today's tools can answer questions. Fewer than 25% of respondents have tools that can answer all their questions about their networks. Most told us that their tools can answer most questions.

Figure 42. Tell us how well your network observability solutions support this by selecting an option to fill in the blank in the following sentence: "Our tools can quickly and easily answer ____ that we have about our network."

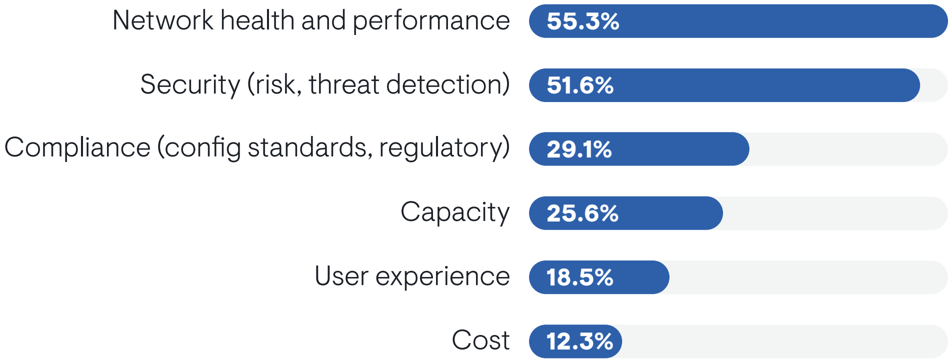


Sample Size = 351

Tool sprawl worked against this outcome. Respondents with larger toolsets got fewer answers to their questions from their tools. Network expertise of research participants influenced this question. The network engineering team was most likely to say that their tools can answer every question. This team typically has the most knowledge about networks and its personnel is capable of extracting answers to questions that other groups would struggle with. For example, the DevOps team and the cloud team were able to answer the fewest questions with network observability tools.

Figure 43 reveals the answers and insights that today's toolsets are best capable of providing. Most organizations' tools can provide answers about network health and performance and security state. Answers about compliance and capacity are less readily available. The network operations team and the IT executive suite were the most confident in tools' answers to questions about network health and performance. The network engineering team was twice as likely as other groups to be able to find answers to compliance questions.

Figure 43. Which types of questions about your network are your tools best capable of answering quickly and efficiently?



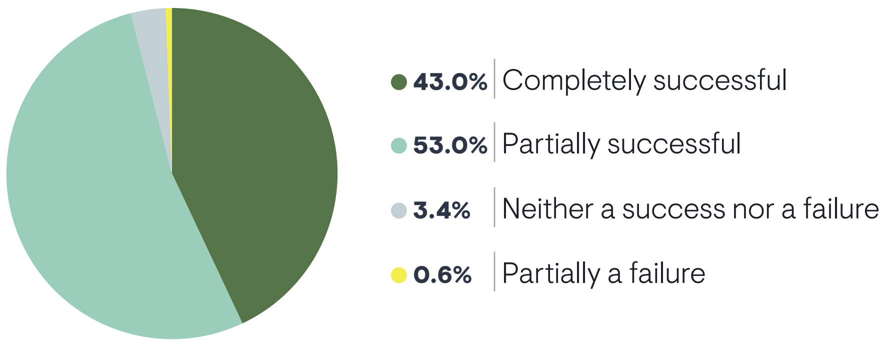
Sample Size = 351

User experience and cost information are hard to find. Organizations that have the most success with network observability are more likely to have tools that can answer questions about both. Organizations with larger network observability toolsets were less likely to get answers to questions about costs and compliance.

Success with Network Observability

Figure 44 reveals that 43% of respondents believe their organizations are completely successful with their use of network observability tools. Most only feel partially successful. Heavier users of these tools reported more success. For instance, members of network engineering and network operations teams were more successful than the project management team.

Figure 44. How successful do you think your organization is with its use of network observability tools?



> 43% of respondents believe their organizations are completely successful with their use of network observability tools.

Sample Size = 351

"I'm about 80% satisfied with my tools," said a network management tool architect with a Fortune 500 retailer. "I think we have the best possible setup we can have, but there are still things I'm not happy with."

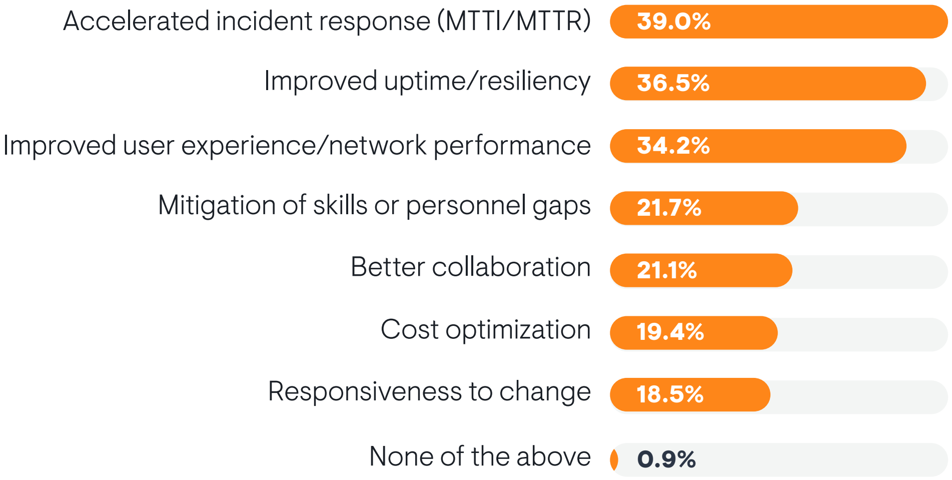
EMA found that organizations experience more success with network observability when they:

- Prioritize resources and budget for tools
- Require support for multi-vendor networks
- Require end-to-end visibility and insights across network domains
- Require insight into unmanaged networks (e.g., internet, cloud, remote users' connections)
- Collect higher volumes of data with their tools
- Tightly integrate multiple network observability tools
- Are aggressive with streaming network telemetry adoption and perceive it as an SNMP replacement
- Have efficient and effective alert management (noise is minimized)
- Prioritize tools that can monitor and troubleshoot the network experience of individual users
- Prioritize and trust AI/ML-driven network observability capabilities

Benefits of Effective Solutions

Figure 45 reveals the benefits that IT organizations usually experience when they are successful and effective with network observability. The top benefit is accelerated response to network incidents. Network teams can understand and resolve problems faster. This benefit was perceived more by IT middle managers and project managers and less by subject matter experts.

Figure 45. Which of the following are the top benefits that your organization currently experiences from the effective use of its network observability tools?



The other top benefits are improved resiliency or uptime and improved user experience and network performance. The project management team was more likely to perceive improved resilience than the network engineering team.

Skills and personnel gap mitigation was an infrequent benefit, but members of the network engineering and IT asset/financial management teams were more likely to experience it than network operations and project management teams.

Cost optimization is an infrequent benefit, but larger companies tended to select it more often.

Sample Size = 351

Unplanned Network Downtime

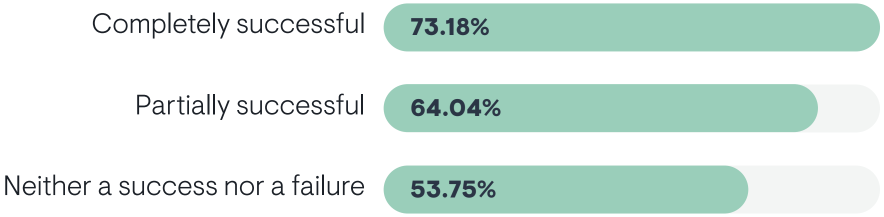
Improved uptime is a top benefit of effective network observability. EMA explored this further by asking survey respondents to estimate how many hours of unplanned network downtime their organizations experienced over the last six months. The average response was nearly 28 hours. Organizations that rely on open source network observability reported more hours of downtime (40) than organizations that use solutions provided by third-party tool vendors (24).

Proactive Problem Prevention

EMA also asked respondents to estimate how many network problems their IT organizations can detect proactively before they impact the business. The average response was nearly 68%.

Figure 46 reveals that proactive problem prevention is more complete when IT organizations have a successful network observability strategy.

Figure 46. Percentage of network problems that IT organizations can detect proactively before the business is impacted, cross-tabbed by overall success with network observability tools.



Sample Size = 351

50%
80%
55%
75%
80%
20%
A
B
C
D
Level_1
Level_2
Level_2
Level_3
5371
15%
10%
14%
17%
13%
10%
Day
Week
Month
Year
All

Conclusion

Over the last two years, IT organizations embraced the concept of network observability to describe the tools they use to monitor and manage their networks. This reflects a desire for next-generation capabilities from incumbent vendors and emerging solution providers.

Network operations teams need tools that can collect increasingly diverse network data at greater volumes than ever before. For instance, device metrics remain as important as ever, and network teams need tools that can scale to collect more of them. However, they also need to collect VPC flow logs from their cloud providers and synthetic network traffic. At the same time, they want to explore alternatives to legacy data collection methods, like SNMP, by embracing streaming network telemetry, which remains too immature for mainstream adoption.

Still, it’s not just about data collection. Network operators need actionable insights, which demand innovation. IT professionals recognize that AI is a potential path toward actionable insights, but they also expect innovation in how tool vendors deliver dashboards and reports, both out of the box and via highly customizable features.

This innovation will occur in an industry in which network complexity and tool sprawl remain the norm. Network teams recognize that no single tool will deliver end-to-end network observability that addresses all their requirements. Tool vendors must strive to provide as much capability as possible while also enabling customers to tightly integrate their solutions into a multi-vendor suite that includes tools from network management solution specialists, network infrastructure vendors, and open source communities. Flexibility, openness, and customizability are the keys to network observability success.

Appendix: Demographics

Figure 47. Which of the following best describes your role in your employer's IT organization?v

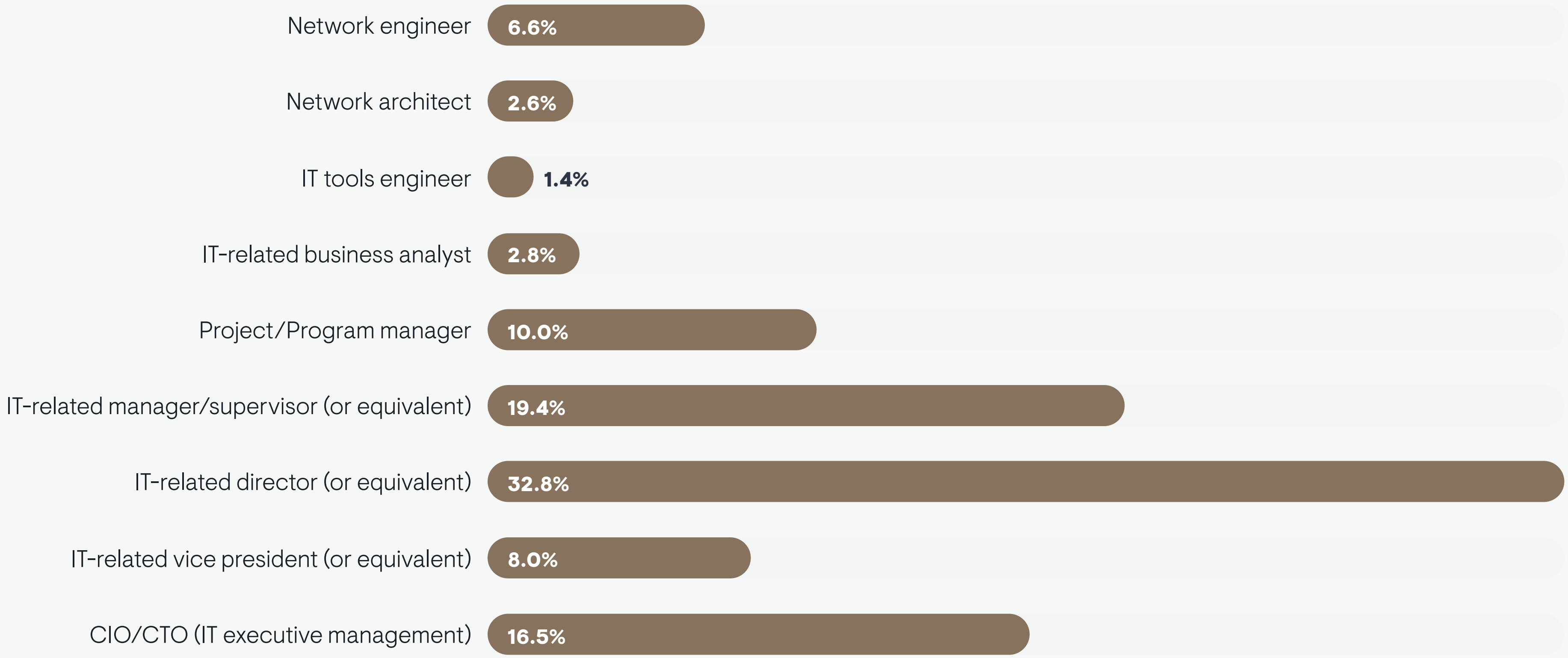


Figure 48. Which of the following best describes your group or team within the IT organization?

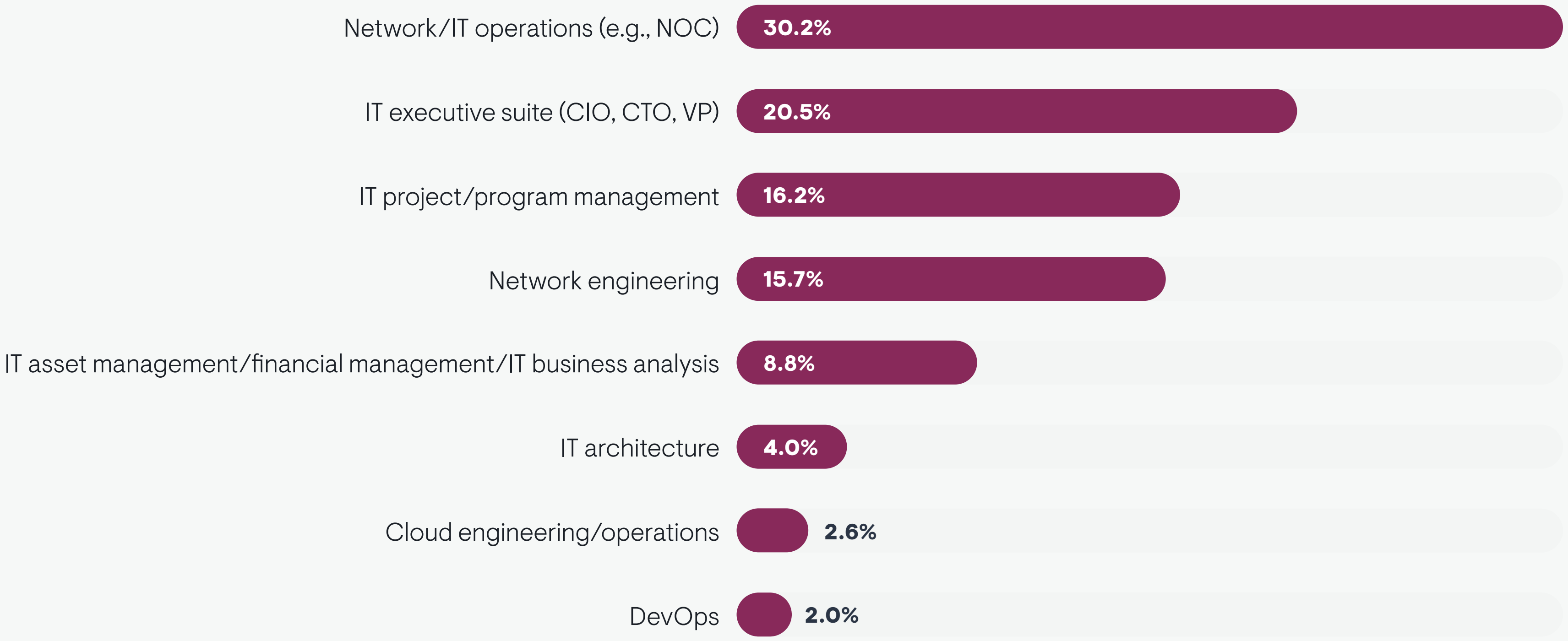


Figure 49. How many employees are in your company worldwide?

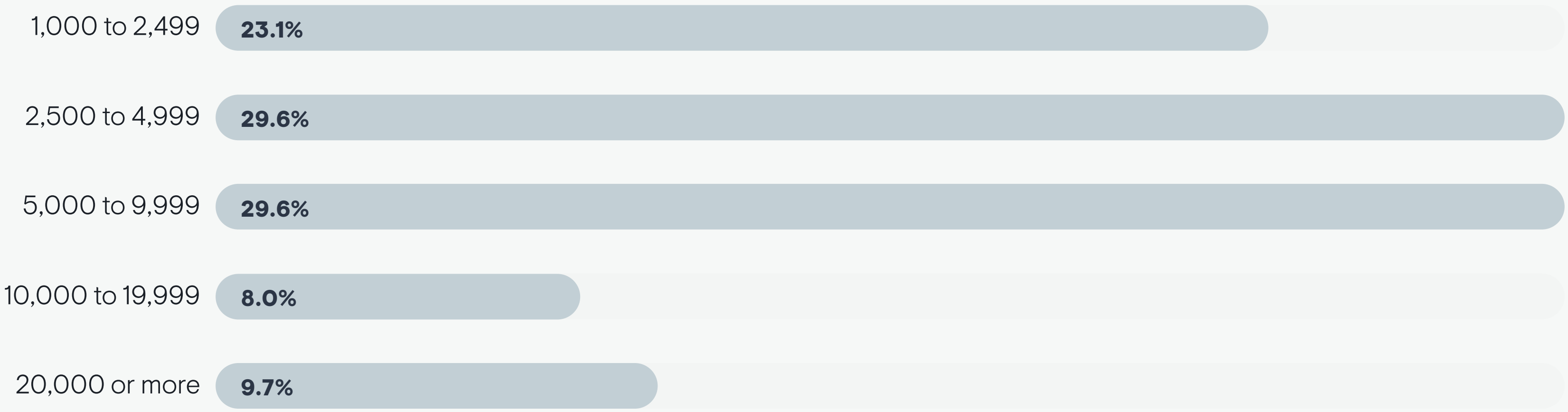


Figure 50. Which of the following best describes your company's primary industry?

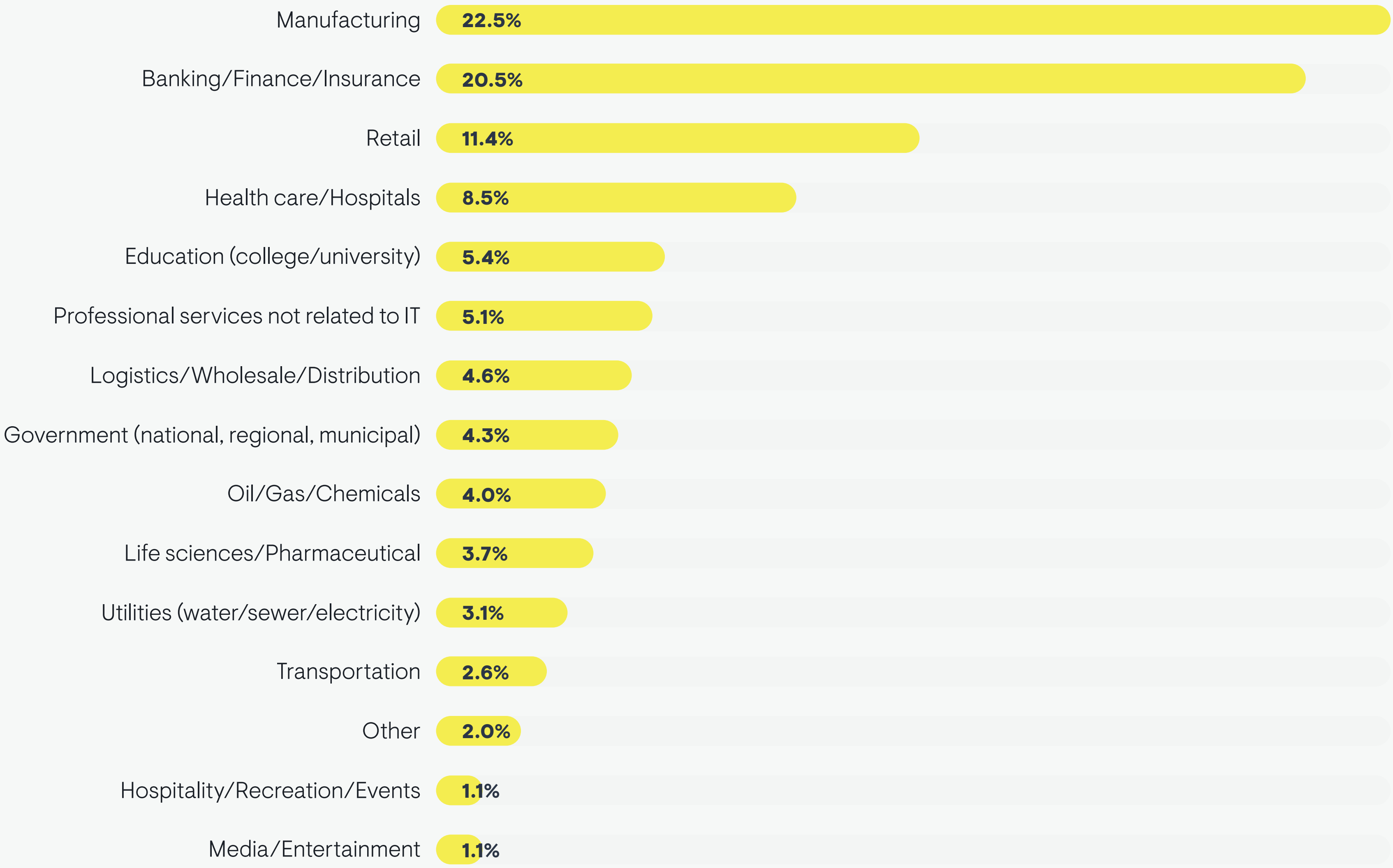
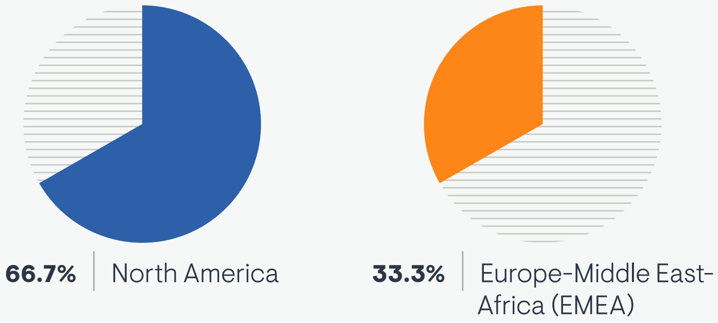


Figure 51. In which region are you located?



Case Study: Manufacturer Accelerates Troubleshooting with NETSCOUT Observability in Remote Factories

Plant Operational Technology Challenges

As a global manufacturer expanded the amount of automation in its plants and had production lines expand over the last decade, it recognized the need to ensure consistent performance levels in order to meet daily production quotas and avoid slowdowns or shutdowns. Fortunately, the manufacturer's IT organization had the right tool for the job. The network operations team implemented NETSCOUT observability solutions across its data centers, cloud environments, and factories worldwide to safeguard performance, user experience, and manufacturing line objectives.

Recently, the manufacturer discovered slowdowns with the custom application that powered automated assembly lines in a few of its factories. The IT team was responsible for helping the manufacturer meet company objectives in the areas of performance monitoring and observability, troubleshooting, capacity planning, and maintaining predictable quality of service levels. It quickly recognized the need to identify the root cause of the slowdowns and fix them before they negatively impacted production levels, which could delay downstream operations that relied on the components built at these factories. Knowing that this could become a very costly problem, the IT organization quickly jumped into their troubleshooting processes.

Importance of Ecosystem-Wide Observability

As the network operations team responded to this issue, they applied the NETSCOUT nGenius Enterprise Performance Management solution to the problem. The team began its investigation of the slowdown by leveraging the NETSCOUT Remote InfiniStreamNG (ISNG), which was deployed onsite for continuous deep packet inspection (DPI) at scale from the WAN edge of the factories. The network operations team combined their analysis of this packet data with metadata from the InfiniStreamNG instances that were monitoring the manufacturer's data centers and public cloud. NETSCOUT'S nGeniusONE monitoring and analytics component revealed several service dependencies for the custom manufacturing automation application—one of which was the database. The troubleshooting effort swiftly revealed an issue in how transactions were flowing between the custom application server and database servers, resulting in slowdowns in certain routes.

Using evidence from the nGenius Enterprise Performance Management solution, which detailed the factory and servers involved, the network operations team corrected the transaction paths and restored service levels and user experience for the application.

Avoiding Costly Outages with Observability

By leveraging NETSCOUT's observability solution, the network operations team immediately improved overall performance for the factory's production line. This had a clear financial benefit because it reduced production cycles. It also avoided a protracted troubleshooting process that would have likely involved a time-consuming war room session, with contentious exchanges between stakeholders over which vendors or service providers were at fault. For example, without proper observability, some may have pointed fingers at the WAN provider.

The value of observability from NETSCOUT's nGenius solution was demonstrated through its unique ability to continuously analyze the custom manufacturing application, identify service dependencies, and provide visibility into the communication paths across the manufacturer's ecosystem using DPI. Collaboration was quick, accurate, and efficient, and reduced the time to resolution. Ultimately, the bottom-line benefit was that the factory's service level and user experience requirements were met and the company avoided a costly production outage due to this critical observability throughout their environment.

About Enterprise Management Associates, Inc.

Founded in 1996, Enterprise Management Associates (EMA) is a leading IT research and consulting firm dedicated to delivering actionable insights across the evolving technology landscape. Through independent research, market analysis, and vendor evaluations, we empower organizations to make well-informed technology decisions. Our team of analysts combines practical experience with a deep understanding of industry best practices and emerging vendor solutions to help clients achieve their strategic objectives. 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.

©2025 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 4475.012825