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

Prepared for:

cPacket™

Network Management Megatrends 2026:

Automation, Hybrid and Multi-Cloud Networks, and AI Transformation

April 2026 EMA Research Report
By **Shamus McGillicuddy**, VP of Research
Network Infrastructure and Operations

Table of Contents

2 Introduction: Benchmarking NetOps
3 Demographics
3 Infrastructure Snapshot
5 Key Findings
6 NetOps Teams are Struggling
6 Tool Trouble
6 Enterprise AI Adoption Requires NetOps Transformation
6 Network Engineers are Hard to Find
6 Hybrid and Multi-Cloud Architecture is Confounding
6 AI Should Enable NetOps Transformation
7 Network Operations Strategies
8 Organizing Day-to-Day Network Operations
9 Strategic Drivers: AI and the Cloud
10 Essential Collaboration Partners
11 Network Operations Outcomes
12 Overall NetOps Success
13 Defining Success
14 Challenges to Success
15 Maturity Levels
16 NetOps by the Numbers
18 Root Causes of War Room Incidents
19 Network Operations Toolsets
20 General Tool Requirements
21 Tool Sprawl Persists
23 Agentic AI Adoption
24 Replacing Network Observability Tools
26 Tool Satisfaction
27 Network Operations Data
28 Do You Trust Your Data?
31 Network Observability is All About Data Diversity
33 Megatrend #1: Enterprises Struggle to Hire Network Engineers
35 Premium Networking Skills
36 Closing Skills Gaps
37 Megatrend #2: Automating Day 2 Network Operations
39 Automation Solutions
40 Tasks Targeted for Automation
41 Barriers to Automation
42 Megatrend #3: Hybrid and Multi-Cloud Networks Challenge NetOps
43 Observability of Cloud Networks
44 Hybrid Cloud Networking
45 Multi-Cloud Networking
46 Importance of Unifying Cloud Networking
46 Effectiveness of Cloud Networking Strategies
47 Cloud Networking Challenges
48 Megatrend #4: Preparing Network Observability for AI Transformation
49 AI Deployment Plans
50 Network Domains NetOps Must Actively Manage for AI Workloads
51 Network Performance Concerns for AI Workloads
52 Readiness of Network Observability Tools
54 EMA Perspective: Can Agentic Network Management Address Long-Term Challenges?
55 Best Practices for NetOps Teams
56 Appendix: Demographics

Executive Summary

Published biennially since 2008, the “Network Management Megatrends” report is the definitive benchmark of enterprise network operations practices. It explores tools, processes, drivers, and challenges to monitoring, troubleshooting, and optimizing enterprise networks. The 2026 edition of this report is based on a survey of 352 IT professionals.

Introduction: Benchmarking NetOps

EMA's "Network Management Megatrends" research is the definitive benchmark of enterprise network operations practices. We have published this research biennially since 2008, surveying IT leaders and subject matter experts about the state of their network operations groups, the tools they use, and the challenges they face. This research also explores a constantly evolving set of industry megatrends that are shaping how IT organizations approach network operations.

In the IT industry, "network operations" often refers to the people, processes, and tools applied to ongoing management, monitoring, trouble-shooting, and maintenance of network infrastructure. It encompasses a frontline team of tier-1 responders who react to and triage events and tier-2 and tier-3 engineers who address complex problems. IT organizations vary in how they organize these teams, but traditionally, companies maintain a network operations center (NOC) and one or more network engineering teams, the latter of which are also responsible for network deployments, optimization, and change management when they are not responding to incidents escalated by the NOC.

Network operations teams strive for efficiency. Good tools and processes can lead to a proactive posture, in which problems are detected and resolved before they impact IT services. Tier 1 personnel have good tools in place to resolve recurring problems quickly via automation. Complex problems are escalated to the right senior engineer quickly. Not everyone achieves this level of efficiency. Many network operations teams perpetually react to disasters and put out fires. In these organizations, network problems can bring IT services down for lengthy periods, leading to costly disruptions to the business.

EMA's ongoing "Network Management Megatrends" research strives to provide a standard of network operations maturity. It tracks how effective network teams are at detecting and resolving problems. The research also identifies best practices for network operations strategies.

Demographics

For this report, EMA surveyed 352 IT professionals in February 2026. **Figure 1** offers a demographic overview. EMA surveyed North Americans (United States and Canada) and Europeans (France, Germany, United Kingdom) across multiple industries and company sizes. All respondents were directly engaged with the management of their enterprises' networks or managed people and teams responsible for network management.

Infrastructure Snapshot

EMA asked survey respondents to describe what sits at the core of their networks, specifically the environment that hosts their applications and data. **Figure 2** reveals that most respondents have a hybrid environment, with a mix of private data centers and public cloud infrastructure services. Only 14% were cloud-only and only 17% claimed to use private infrastructure exclusively.

Figure 3 reveals that most of the companies represented in this survey have multi-cloud footprints, with nearly 52% operating in two cloud service providers and 14% using three or more.

Figure 1. Demographic Overview

Job titles

- **28%** Technical personnel (admin, engineer, architect)
- **49%** IT middle management (manager, supervisor, director)
- **23%** IT executives (VPs/CIOs/CTOs)

Company size (employees)

- **28.4%** Midsized enterprise (1,000 to 4,999)
- **36.3%** Large enterprise (5,000 to 19,999)
- **15.3%** Very large enterprise (20,000 or more)

Region

- **64.2%** North America
- **35.8%** Europe

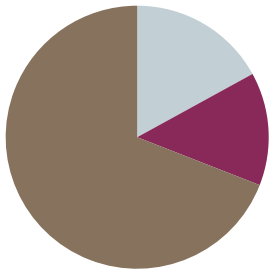
Top industries

- **25.9%** Banking/Financial services/Insurance
- **22.7%** Manufacturing
- **12.5%** Retail/Wholesale/Distribution
- **12.2%** Software/SaaS
- **6.3%** Health care/Hospitals/Life sciences
- **5.4%** Transportation/Logistics

IT groups

- **24.4%** IT executive office
- **18.2%** Network engineering
- **17.3%** Network operations (NOC)
- **15.1%** IT architecture
- **13.4%** Cybersecurity/information security
- **8.0%** Cloud infrastructure and operations
- **3.7%** IT tool engineering (observability, automation)

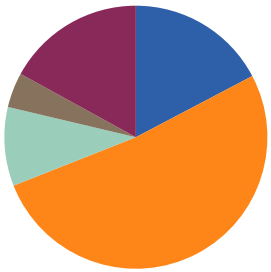
Figure 2. Which of the following best describes the infrastructure that hosts your organization's applications and data?



- **17.0%** 100% private infrastructure (on-premises data centers and/or colocation data centers)
- **13.9%** 100% public cloud services (IaaS, PaaS)
- **69.0%** A mix of private infrastructure and public cloud (i.e., hybrid cloud)

Sample Size = 352

Figure 3. How many public cloud providers does your organization use?



- **17.3%** One provider
- **51.7%** Two providers
- **9.7%** Three providers
- **4.3%** Four or more providers
- **17.0%** No cloud providers

Sample Size = 352

Key Findings

NetOps Teams are Struggling

Only 31% of network operations strategies are fully successful today. EMA identified several best practices. For example, effective teams prioritized automation of Day 2 operations, integration to address tool sprawl, and aggressive adoption of AI solutions for network management.

Tool Trouble

Only 32% are completely satisfied with the tools they use to monitor and troubleshoot their networks, and 73% believe they may replace some of these tools within the next two years. The typical network team uses four to 10 tools for network monitoring and troubleshooting.

Enterprise AI Adoption Requires NetOps Transformation

AI is the top strategic driver of NetOps strategies today. Only two years ago, it was the number-seven driver. Within two years, 97% of the companies represented by this survey will have AI application workloads deployed on their on-premises or cloud infrastructure. Only 35% of research participants believe their network observability tools are ready to support operations for these AI workloads.

Network Engineers are Hard to Find

The labor market is challenging network operations, with 52% of enterprises indicating that they find it difficult to hire and retain people with network technology expertise. They are especially struggling to find people with network security, networking for AI, and network automation expertise.

Hybrid and Multi-Cloud Architecture is Confounding

Only 36% believe they are completely successful at managing networking and security in the public cloud. Their top challenges are complexity of cloud native networking constructs, skills gaps on the networking team, and limited end-to-end visibility across on-premises and cloud networks.

AI Should Enable NetOps Transformation

More than half of organizations now consider AI-driven features a top requirement of network management tools, and a similar number have already started using such capabilities. They perceive AI as an essential enabler of automation. This research found that users of AI tended to have more mature, proactive, and predictive network operations teams.

Network Operations Strategies

Organizing Day-to-Day Network Operations

Figure 4 reveals how IT organizations primarily organize the people who are responsible for monitoring and troubleshooting networks. The chart reveals that strategies have changed over the last three iterations of the "Megatrends" report. From 2022 to today, distributed, informal teams have become less common, while cross-domain operations centers have grown increasingly popular.

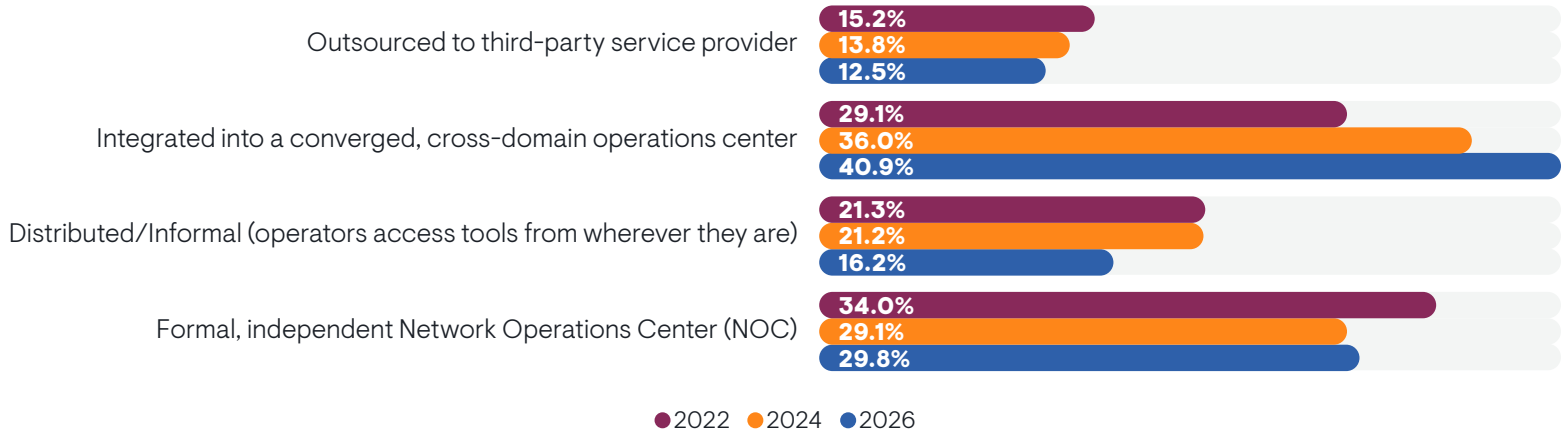
"It's tough to have the perfect path, because to me, there isn't one," said a network tools lead with a multinational bank. "Ideally, having everyone together in a cross-domain operations center would be best, but how do you manage that? For us, we'd have a VP managing 5,000 employees. We separate operations and engineering, and we're split into engineering functions. We communicate with the engineering teams that are designing and building networks, so they know they need to account for tooling, like where they should put probes when designing a new data center."

Traditional network operations centers (NOCs) dropped in popularity from 2022 to 2024, but they have held steady since. Outsourcing of network operations is slowly becoming less popular, but larger enterprises are more likely to do it today.

"Our team structures are very old-school," said a network tools lead with a Fortune 500 retailer. "We have a network team, cloud team, and incident management team all working in silos. We did some research that found that we need to create an observability center of excellence where everyone works together and consolidates tools as much as they can. That's where we want to be, but we're not there yet."

"I think [outsourcing to] a managed service provider is extremely challenging and super frustrating," said a network operations manager with a Fortune 500 retailer. "I don't want to do cross-domain, either. That's a bad model. You want expertise in the field. If you put too many skillsets on the operations team, you get jack-of-all-trades personnel, master of none. You run into an issue in which you don't know who can solve problems."

Figure 4. Which of the following best describes the way in which your organization primarily conducts network monitoring and management?



Strategic Drivers: AI and the Cloud

Figure 5 shows which technologies and trends are most influential on network infrastructure and operations priorities. AI emerged as the primary strategic driver of network operations strategy. In the 2024 "Megatrends" report, AI was the number-seven driver.

Most respondents also cited hybrid and multi-cloud architecture as a driver. The top secondary drivers are network and security convergence (e.g., SASE), network automation, and compliance. Organizations that have hybrid cloud infrastructure cited all three of these latter drivers more often.

"Cloud adoption has been going on for a while, but we're getting more and more involved in it," said a network tools lead with a multinational bank.

"It's a more complex environment than a traditional network because things are always changing and we can't draw static diagrams of a network that makes it easier to troubleshoot."

Organizations with more successful network operations strategies tended to report the following as drivers:

- Hybrid and multi-cloud architecture
- Convergence of operational technology and IT
- Unified communications/video
- Wi-Fi upgrades

Figure 5. Which of the following technologies and trends are driving your organization's current priorities for network infrastructure and operations?

Sample Size = 352

Essential Collaboration Partners

Figure 6 reveals which groups have become more important for the network infrastructure and operations team to collaborate with. Cybersecurity tops the list, which is no surprise. EMA research observed a steady increase in collaboration and convergence between these groups for many years.

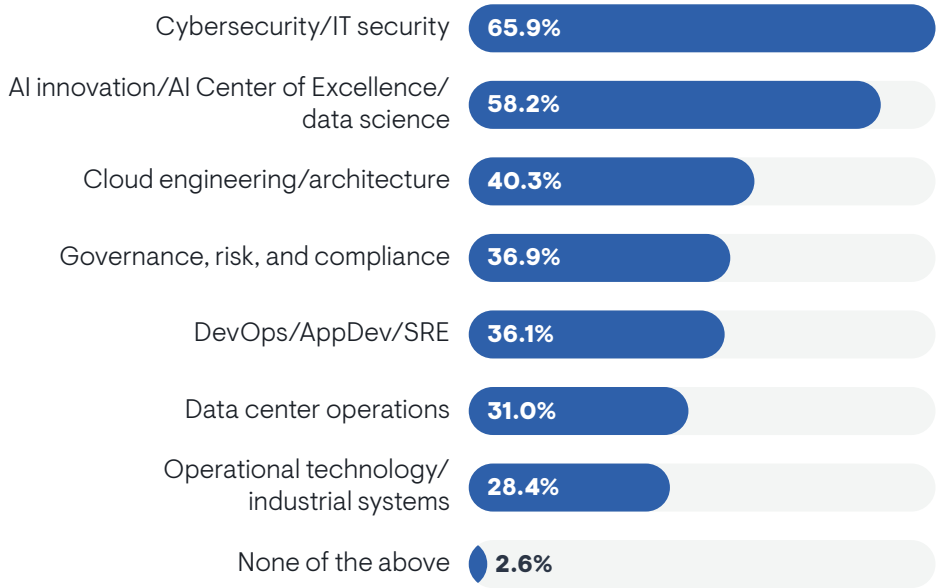
Given the gold rush around AI investment, the AI group's position near the top of this list is also unsurprising. AI training and inference workloads have strict networking requirements, and they are highly sensitive to adverse network conditions. The network team will have to partner with AI stakeholders to ensure infrastructure can support AI investments. Notably, technical personnel were much less likely to cite collaboration with AI groups than IT executives and middle management.

More successful NetOps teams were more likely to report increased collaboration with data center operations and operational technology groups.

NetOps teams that support a hybrid cloud environment were more likely to see increased collaboration with:

- Cybersecurity
- AI group
- Cloud engineering
- DevOps

Figure 6. Over the last two years, has it become more important for the group responsible for network infrastructure and operations to collaborate with any of the following groups/teams?



Sample Size = 352

Network Operations Outcomes

Overall NetOps Success

Figure 7 reveals that only 31% of survey participants believe their company's overall network operations strategy is completely successful. This number is down from 42% in 2024.

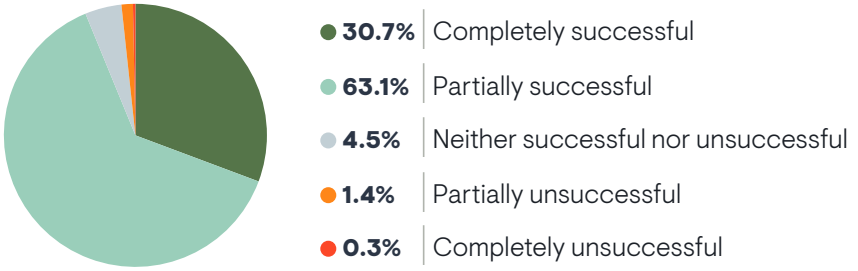
EMA identified the following as factors that correlate with NetOps success:

- Trust in network observability data accuracy
- A focus on automating Day 2 operations
- Use of AI-driven or agentic network management tools
- Prioritizing integration of tool sprawl, especially via workflow integrations across tools and MCP support for agentic access
- Confidence that existing tools are ready to monitor and manage AI workloads and traffic on the network
- Effective management of networking and security in the public cloud
- Extending incumbent network monitoring tools to public cloud networks
- Establishing end-to-end network observability and integrated IPAM across hybrid clouds
- Unified network security controls across multi-cloud infrastructure

EMA also found that the following issues correlated with less NetOps success:

- Difficulty with hiring network technology personnel, especially people with network security expertise and cloud networking knowledge
- Budget constraints that specifically prevent teams from automating Day 2 operations
- Cost concerns that undermine network observability data collection
- Unclear ownership of major network incidents
- Skills gaps as a top cloud network management challenge

Figure 7. Over the past year, how would you rate the success of your organization's network operations strategy?



Sample Size = 352

Defining Success

Measuring Outcomes

Figure 8 reveals that IT organizations typically measure the success of network operations via two factors:

- Uptime/Resilience
- Security compliance/audit readiness

Uptime is the traditional measure of NetOps success. Indeed, organizations that conduct operations within a traditional NOC were more likely to cite uptime. Security compliance is a relatively new target for operations, and it was cited more often by companies with a cross-domain operations center.

"We do it by number of P1, P2, and P3 outages and how long they last," said a network tools lead with a Fortune 500 retailer. "What was the impact? What was the revenue loss?"

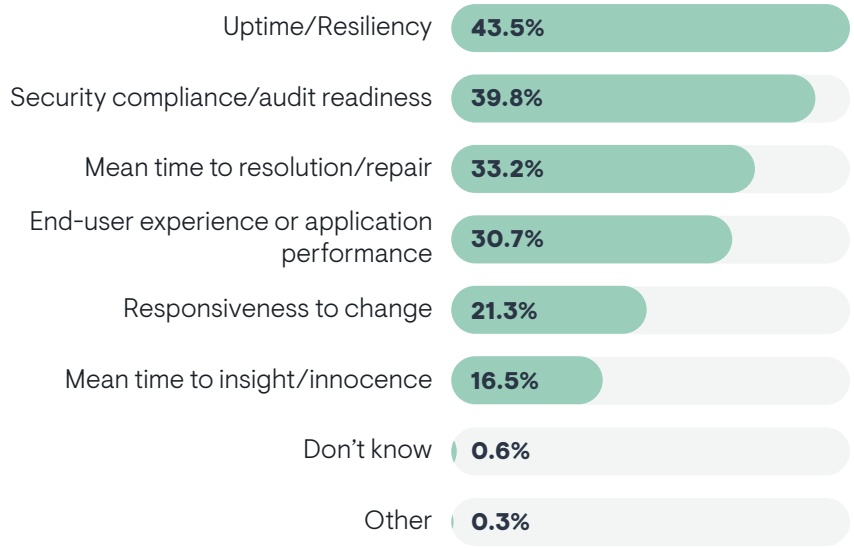
"I would say you want to have data-driven SLAs," said a network operations manager with a Fortune 500 retailer. "You want to know the ticket closure count. You want to make sure there is network availability. But you also want to measure by enhancements. What have they done to lower ticket counts and dispatch calls?"

"It's about having efficient operations and how quickly they are acknowledging alerts and working on them," said a monitoring architect with a Fortune 500 entertainment company. "Also, rather than be reactive, you have to look for ways to be more proactive. So, you need to see if there are underlying issues that are causing alerts and look for ways to address it at a bigger level, rather than just individual alert handling.

Larger companies cited the top secondary measure of success, mean time to resolution, more often. Responsiveness to change was a less common measure, but organizations that hosted all their data and applications in the public cloud were more likely to select it.

"We do KPIs like MTTR and reduced major incident hours," said a network tools lead with a multinational bank. "Another thing we look for on the change management side is low percentages of impact-causing changes."

Figure 8. How does your organization's IT leadership primarily measure the success of the team responsible for network operations?



Challenges to Success

Figure 9 reveals the major challenges to network operations success. The number-one issue is related to labor. Enterprises are struggling with a shortage of skilled networking personnel. This report will devote an entire section to this issue. Notably, people who selected this response to the question were more likely to report less overall success with network operations. IT middle managers were also more aware of this issue.

"When an incident comes up, it's a struggle to find people with the expertise to figure out that issue in a timely manner," said a network operations manager with a Fortune 500 retailer.

"We are being asked to do more with less. What used to be done by a 25-person team, management now wants us to do with a ten-person team," said a monitoring architect with a Fortune 500 entertainment company.

The other top challenges were lack of end-to-end visibility across network domains and data quality and access issues. IT executives more often called out the number-four issues, tool sprawl and a lack of integration.

"Sprawl is a major issue for us," said a network tools lead with a multinational bank. "We want to have fewer tools that cover different things."

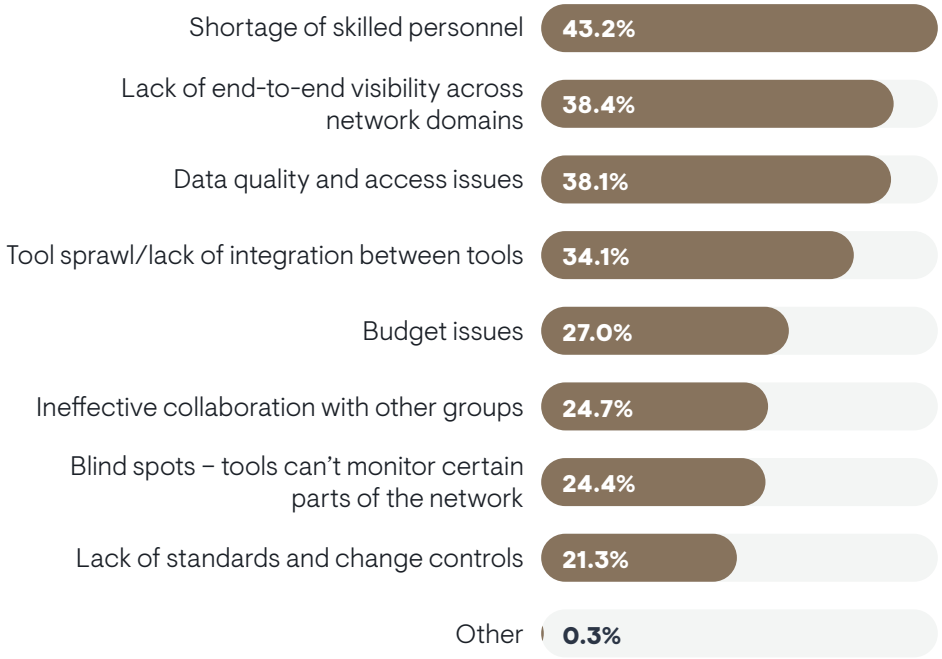
Companies that had a hybrid cloud environment were more likely to struggle with:

- Tool sprawl
- End-to-end visibility across domains

EMA identified some variation in challenges based on how an IT organization organized the network operations function:

- NOCs struggle with tool sprawl and personnel shortages
- Distributed/informal operations struggle with data quality and blind spots
- Both NOCs and cross-domain operations centers struggle with lack of end-to-end visibility across domains

Figure 9. Which of the following are the biggest challenges to success for network operations in your organization?

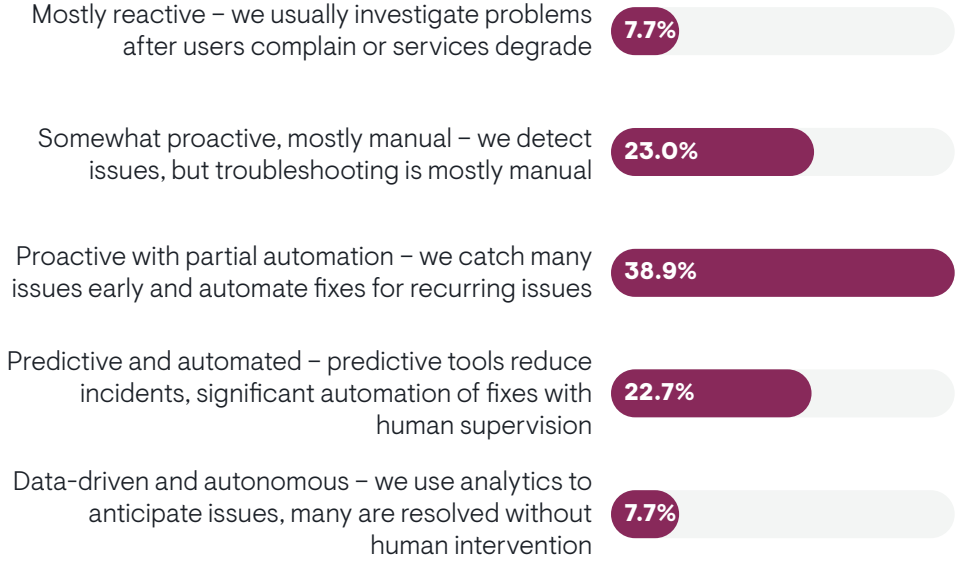


Sample Size = 352

Maturity Levels

Figure 10 reveals network operations maturity levels. Respondents were presented with five options of increasingly mature operational postures, from mostly reactive and highly manual operations to predictive and highly automated operations. The typical enterprise fell in the middle, "proactive with partial automation." These organizations can detect many issues before services degrade, and they have automated fixes in place for recurring problems. Overall NetOps success correlated very strongly with rising levels of maturity. Unsuccessful teams tended to be mostly reactive, while more successful teams were more often predictive or data-driven and autonomous.

Figure 10. Which of the following describes your organization's overall maturity in network operations?



Sample Size = 352

Regardless of capability, some companies will be reluctant to step fully into autonomous operations. "Being a heavily regulated company, we can't let AI do full automation and push changes yet, but recommending things on troubleshooting and doing a lot of ticket and alert management is helpful," said a network tools lead with a multinational bank.

Technical personnel tended to perceive less maturity than middle managers and executives. For example, 32% of technical personnel described their NetOps group as "somewhat proactive, mostly manual," versus only 22% of middle managers and 16% of IT executives. And, 35% of IT executives claimed their NetOps groups were "predictive and automated."

More mature NetOps teams tended to focus on automating:

- Incident remediation
- Capacity and performance optimization

Less mature NetOps teams tended to cite the following as major barriers to automation of day 2 network operations:

- Lack of trust in automation tools
- Poor tool quality and lack of tool integration
- Budget constraints

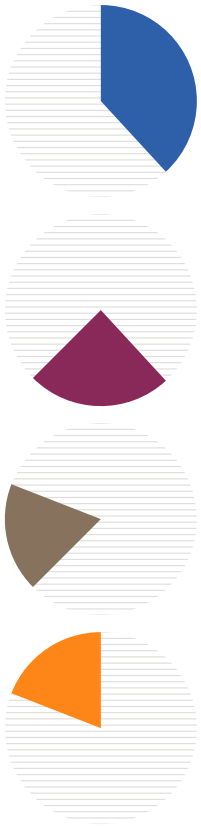
Organizational structure correlated with maturity

- Distributed and informal operations teams were least mature
- NOCs were moderately mature
- Cross-domain operations teams were more mature

NetOps by the Numbers

EMA uses the Megatrends research to gather some real-world numbers about network operations outcomes. **Figure 11** provides an overview.

Figure 11. A snapshot of NetOps posture by the numbers



58% The network problems detected proactively before users experience their impacts

37% Alerts produced by network observability tools that are indicative of a real problem that must be fixed

28% Network-related problems caused by manual administrative errors (bad config changes, bad firewall rules, etc.)

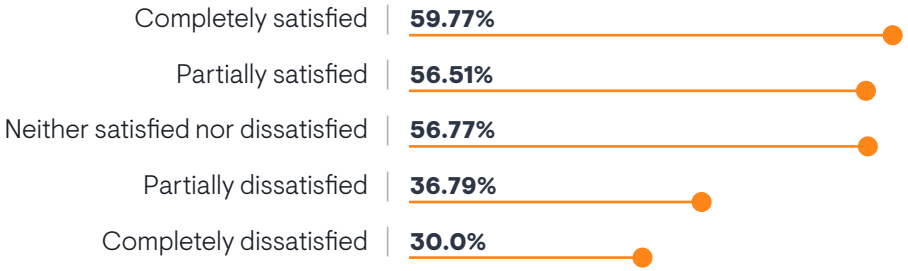
29% Percentage of a survey participant's day spent on troubleshooting the network

Now, let's dig deeper.

Proactive Network Problem Detection

The previous chart revealed that the average network operations team detects 58% of network problems proactively before users experience impacts. **Figure 12** shows that tool quality influences this number. Network teams that are less satisfied with their network observability tools are detecting fewer problems proactively. Successful NetOps teams also had higher detection rates.

Figure 12. In a typical month, what percentage of network problems (performance issues, outages, etc.) is detected proactively by IT operations before users experience their impacts? By How satisfied are you with the tools your organization uses to monitor and troubleshoot its networks?



We found that data confidence correlates with detection. Organizations that were most confident in the accuracy of data collected by their tools reported a higher rate of proactive detection.

Members of network operations teams were the least optimistic about their detection rates. The CIO's suite, cybersecurity, and IT architecture groups all reported better numbers.

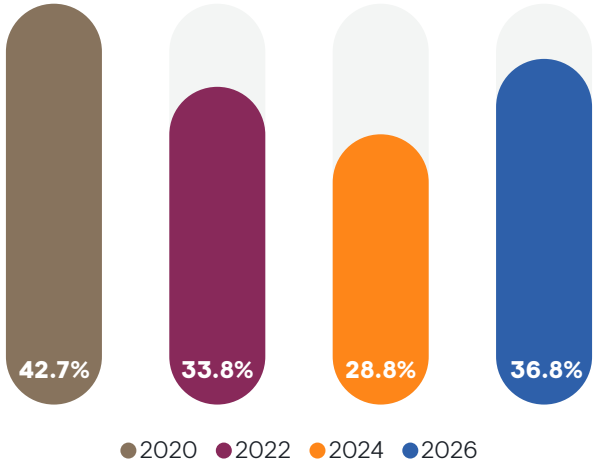
Sample Size = 352

Actionable Alerts

Alert noise is a perennial source of pain for network operations teams. EMA once spoke to a network architect at a Fortune 500 company who said that on any given day, his team has 1,000 uncleared alerts because his team knows those alerts are not actionable. They aren't tied to a problem that requires a fix. Instead, they are left unattended until someone can find the time to clear the tickets associated with them.

Figure 13 reveals that alert noise had been getting steadily worse from 2020 to 2024, but there was a rebound in 2026. This year, 37% of alerts are tied to actual problems.

Figure 13. What percentage of the alerts your network monitoring tools produce is indicative of a real problem that must be fixed?

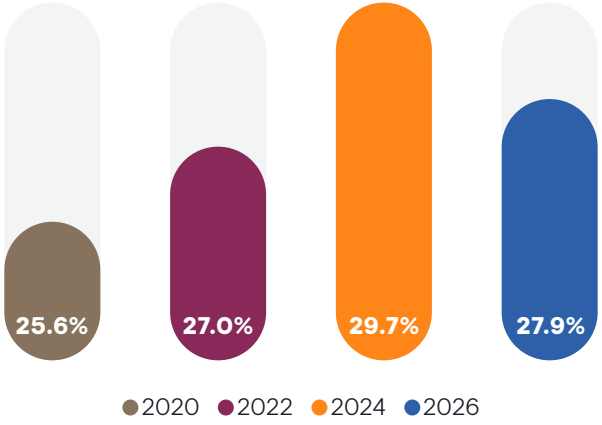


This reversal of fortunes is a pleasant surprise. EMA suspects that this improvement in alerting is tied to the rise of AI-driven technology, which is improving event correlation and problem isolation.

Network Incidents Caused by Manual Errors

Over the last six years, EMA asked survey respondents four times to estimate how many of their network problems are caused by manual administrative errors, such as bad config changes. **Figure 14** reveals that the answers to this question are remarkably consistent, hovering between 26% and 30%. EMA has observed three straight cycles of incidents increasing slightly before it dropped from 30% in 2024 to 28% this year. This slight decline might be attributable to a rise in network automation maturity, something that EMA observed in the enterprise space over the last few years. Or, this decline could be a blip.

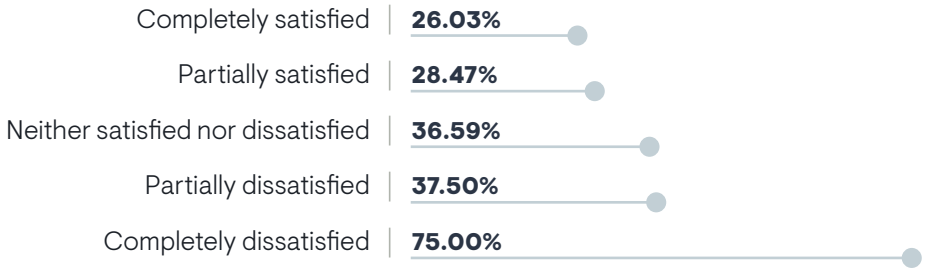
Figure 14. What percentage of your network-related problems is caused by manual administrative errors (bad configuration change, etc.)?



Time Spent on Network Troubleshooting

Survey respondents told EMA that they spent an average of 29% of their day on network troubleshooting. Respondents who reported less success with network operations strategy devoted more time to troubleshooting. **Figure 15** reveals that NetOps tool satisfaction also correlates strongly with troubleshooting time. Less satisfaction led to more time spent on these tasks.

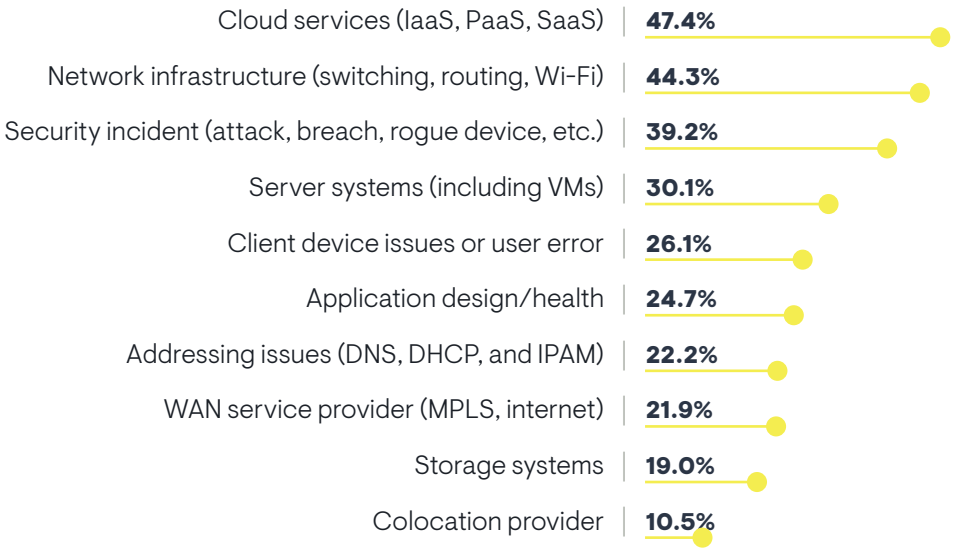
Figure 15. What percentage of your day is spent on troubleshooting problems? by How satisfied are you with the tools your organization uses to monitor and troubleshoot its networks?



Root Causes of War Room Incidents

Figure 16 reveals the root causes of the last three service performance incidents that forced IT organizations to assemble war rooms. It shows that cloud services, network infrastructure, and security incidents are the most likely root cause of such complex problems. This top three is unchanged from the last time we asked this question in 2024. In fact, the top six on this chart are unchanged from 2024, except for a flip of client systems and server systems.

Figure 16. Think about the last three difficult IT service performance issues that required your networking team to collaborate with other groups (e.g., war room responses). Which of the following turned out to be the primary root cause(s)?



Sample Size = 352

Network Operations Toolsets

General Tool Requirements

IT professionals can see the promise of AI-driven network operations. **Figure 17** identifies the top business requirements that enterprises are setting for their network management products, and AI features top the list. IT professionals want tools that offer AI-enabled insights and automation.

Integration with other IT management solutions was the other top requirement. More mature network operations groups were likely to want both AI and integrations.

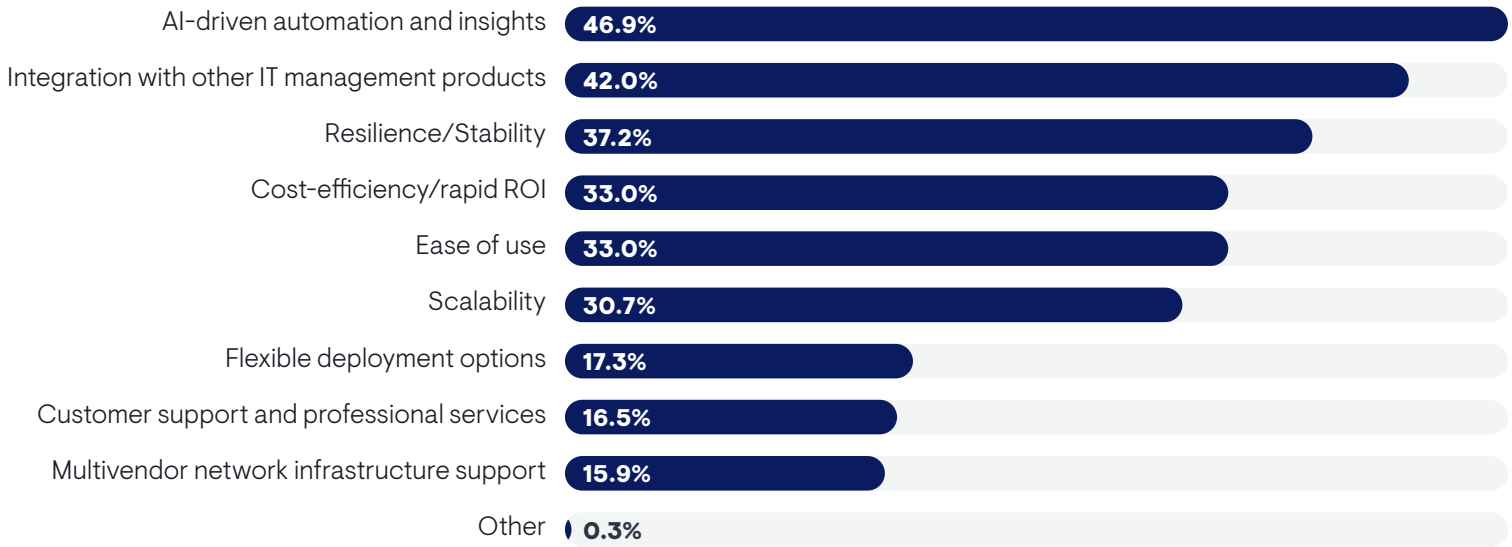
Resiliency was the top secondary requirement and technical personnel were more likely to want it. Scalability was a priority for larger companies, while deployment flexibility was important to smaller companies.

A network operations manager with a Fortune 500 retailer said he needs tools are that scalable. His core tools perform poorly because they are overextended by the scale of his network. "When you click on something, you have to wait and wait. Your boss is asking for something, and I get an ulcer by the time it pulls up the data I need."

A network tools lead with a multinational bank said reliability and stability are becoming top considerations because his current vendors have been delivering buggy releases lately. "It's happening more and more when every major release has major issues. The tools that have been stable for years are not coming out with major bugs. I think they are using a lot more junior developers who use AI to write code, and the quality is lower."

Customer support was a low priority, but less mature organizations selected it more often. On the other hand, more successful NetOps groups also prioritized customer support.

Figure 17. What are your organization's top business requirements for network management products?

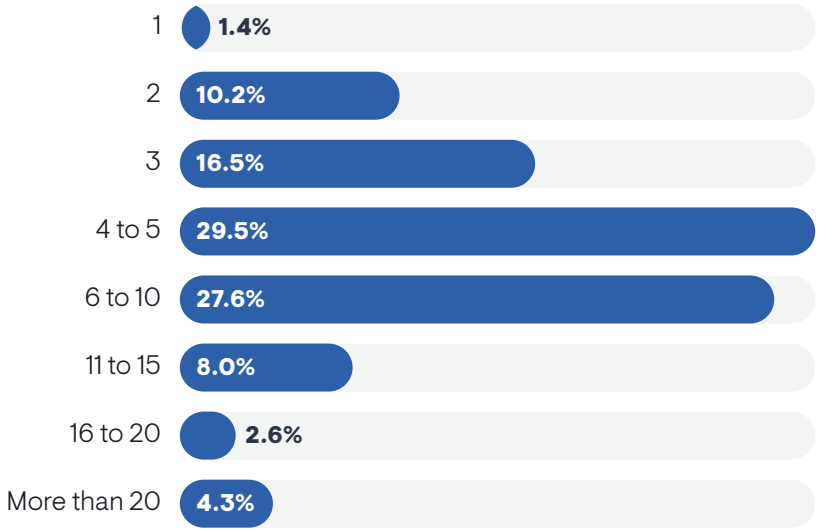


Sample Size = 352

Tool Sprawl Persists

Figure 18 reveals that the typical IT organization uses four to 10 tools to monitor and troubleshoot its networks. This extent of tool sprawl has persisted for years, with EMA's Megatrends report finding similar numbers of tools in use for well over a decade. NetOps outcomes did not significantly correlate with the size of a toolset.

Figure 18. In total, how many tools does your organization use for network monitoring and troubleshooting?



Sample Size = 352

"Tool sprawl has always been a problem," said a network tools lead with a multinational bank. "There has never been a good single pane of glass, so you do end up with a few tools at minimum to cover all the gaps. We are looking at some vendors who could use AI to eliminate some of our tools."

"Over time many tools have come into the picture and overlap increased," said a monitoring architect with a Fortune 500 entertainment company. "We might be doing one thing domestically and then overseas, the network team is using something else. Then we have to go through a process of tool consolidation. We've gone through that process a couple times."

EMA found that larger companies tended to have larger toolsets. For instance, 25% of companies with 20,000 or more employees used 11 or more tools, versus 13% of midsized enterprises (1,000 to 4,999 employees).

Tool Sprawl Integration is Essential

Figure 19 reveals that integration of these toolsets is essential. Among NetOps teams with two or more tools, 61% say it is very important for these tools to be integrated. Less than 1% said it was not important at all. Organizations that emphasize integration reported more overall success with network operations.

Figure 19. You indicated that your organization uses multiple tools to monitor and troubleshoot its network. To what extent is it important for these tools to be integrated?

61.1% Very important

34.3% Somewhat important

4.0% Neither important nor unimportant

0.6% Very unimportant

"I see a problem with tool sprawl," said a network tools lead with a Fortune 500 retailer. "It's too expensive. Everyone has their favorite tool and some get more attention than others. The less attention a tool gets, the staler it becomes. It's just sitting in a corner."

IT executives and middle managers were more committed to integration than technical personnel. Larger companies (20,000 or more employees) were less likely to prioritize integration. It was also a lower priority for companies that take an informal, distributed approach to network operations, versus those that maintain a NOC or a cross-domain operations center.

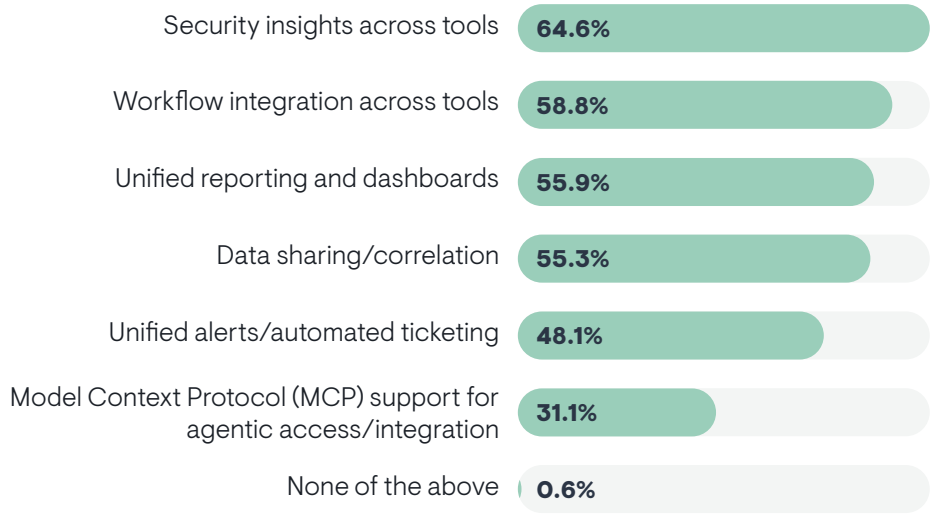
"We have five tools, and we use one of them for the majority of monitoring," said a network operations manager with a Fortune 500 retailer. "There is no integration between them. If we need to drill down, we go to secondary tools, and that's mostly not a problem."

Sample Size = 352

How NetOps Tools are Integrated

Figure 20 shows the types of integrations IT pros want between their network observability tools. The top requirement is integrated security insights across tools. Organizations that have a NOC were more likely to select this.

Figure 20. What kinds of integrations do you require between your network monitoring or network observability tools?



More mature network operations teams seek workflow integrations across tools, data sharing and correlation, and unified alerting and automated ticketing. Companies with hybrid clouds also need unified alerting and automated ticketing.

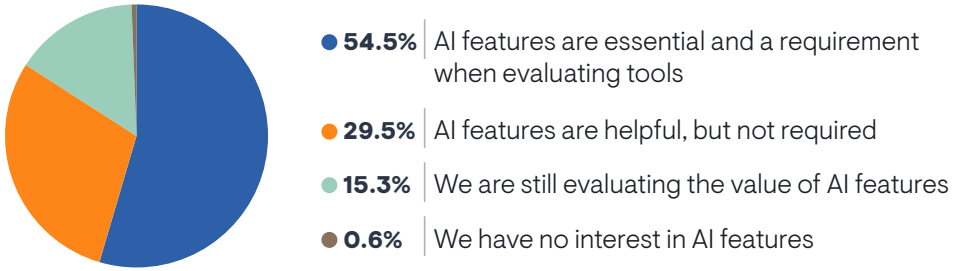
MCP support for agentic access was the lowest priority, but more successful NetOps teams were especially likely to want it.

Sample Size = 352

Agentic AI Adoption

Figure 21 shows that 55% of IT organizations have identified AI features as an essential requirement when they evaluate network management products. Less than 1% of organizations claim to have no interest in applying AI to network management. The IT executive office expressed more interest in AI than network operations or cybersecurity teams.

Figure 21. Which of the following best describes your attitude toward AI features that your network management tools offer?



"I'm absolutely interested in using AI," said a network operations manager with a Fortune 500 retailer. "We are just starting to dip our toes into it right now. It would be foolish for us not to investigate it. I don't think we're ready for AI to replace our people yet."

"Vendors are starting to push their AI products, so we are looking at where we can get the benefit from that," said a network tools lead with a multinational bank.

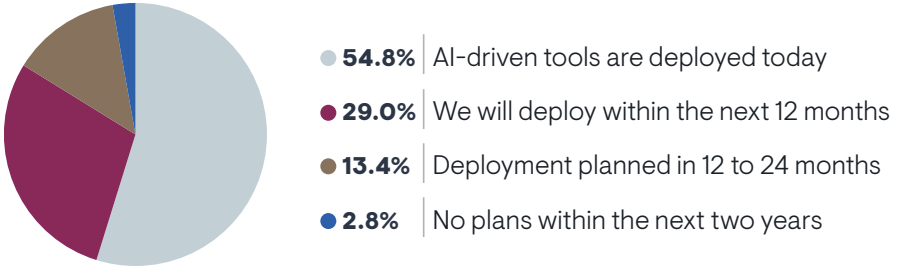
IT organizations that require AI from their tools tended to be:

- More successful with NetOps
- More proactive, predictive, and automated with NetOps
- Conduct NetOps within a NOC or cross-domain operations center rather than an informal, distributed operations group

Sample Size = 352

Figure 22 reveals current adoption of AI, with 55% using it today and 29% expected to deploy AI capabilities within 12 months.

Figure 22. When does your organization expect to adopt AI-driven network management tools in its environment?



Current AI adoption correlated with:

- Higher NetOps tool satisfaction
- More mature NetOps teams
- More NetOps success

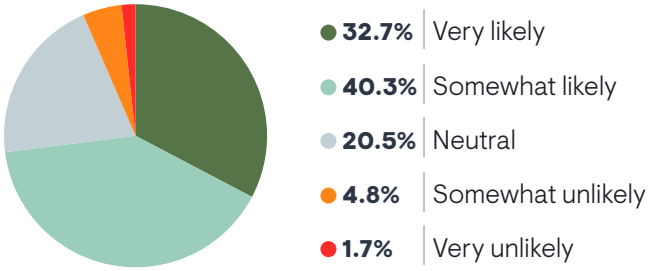
Keep in mind that more mature network teams are able to predict problems before they impact services, and they have extensive automation capabilities to streamline remediation and change management. AI appears to be a significant enabler of these capabilities.

Sample Size = 352

Replacing Network Observability Tools

Figure 23 reveals that 73% of IT organizations are at least somewhat likely to replace a network observability tool over the next two years. In 2024, this figure was at 74%, but the number of respondents who think it is very likely to happen increased from 26% to 33% over the last two years. In other words, a growing number of companies are committed to making a change. This inclination to replace tools is lower if the NetOps team can proactively detect a high number of network problems before they impact users and services.

Figure 23. How likely is your organization to replace a network monitoring or network observability tool over the next two years?



A monitoring architect with a Fortune 500 entertainment company said he isn't necessarily replacing tools with new vendors' tools. Instead, he is building custom tooling to fill in gaps. "We are insourcing a lot of our tooling and taking more control. We are building a lot of our AI tooling in house and using a lot of open source."

"I don't think we'll replace our tools," said a network operations manager with a Fortune 500 retailer. "We've already paid for them for the next couple years. But I have seen other tools that would be better for us."

Sample Size = 352

Network teams are more likely to replace a tool if:

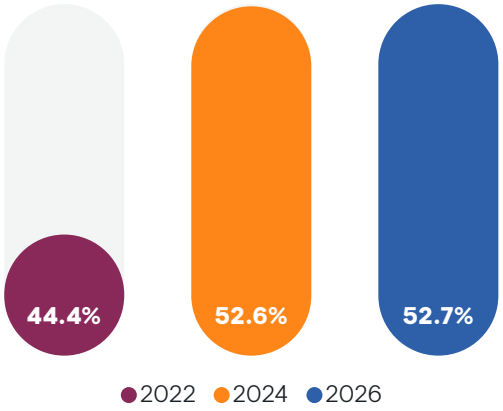
- AI features are a major tool requirement
- NetOps teams are increasing their collaboration with cloud, DevOps, data center operations, and AI teams
- NetOps wants to automate more Day 2 operations, especially if data quality and tool limitations are stalling these automation efforts
- The organization wants to unify networking across on-premises and cloud networks
- The following types of data are becoming more important to network observability:
  - Packets
  - Network flows
  - Logs/events
  - Synthetic traffic
  - DNS logs
  - Routing info
  - Cloud VPC flow logs
  - Topology info
- Incumbent tools struggle to monitor remote sites/branches, public clouds, networks for AI, and private 5G

Estimated Impact of Better Tools

EMA asked respondents to estimate the percentage of network-related problems that could be prevented if they had better network management tools. The average response was 52.7%.

Figure 24 reveals that this estimate is virtually changed from the responses received to this question in 2024. Notably, in 2022, the estimate was significantly lower.

Figure 24. What percentage of your network-related problems do you think would be preventable with better network management tools?



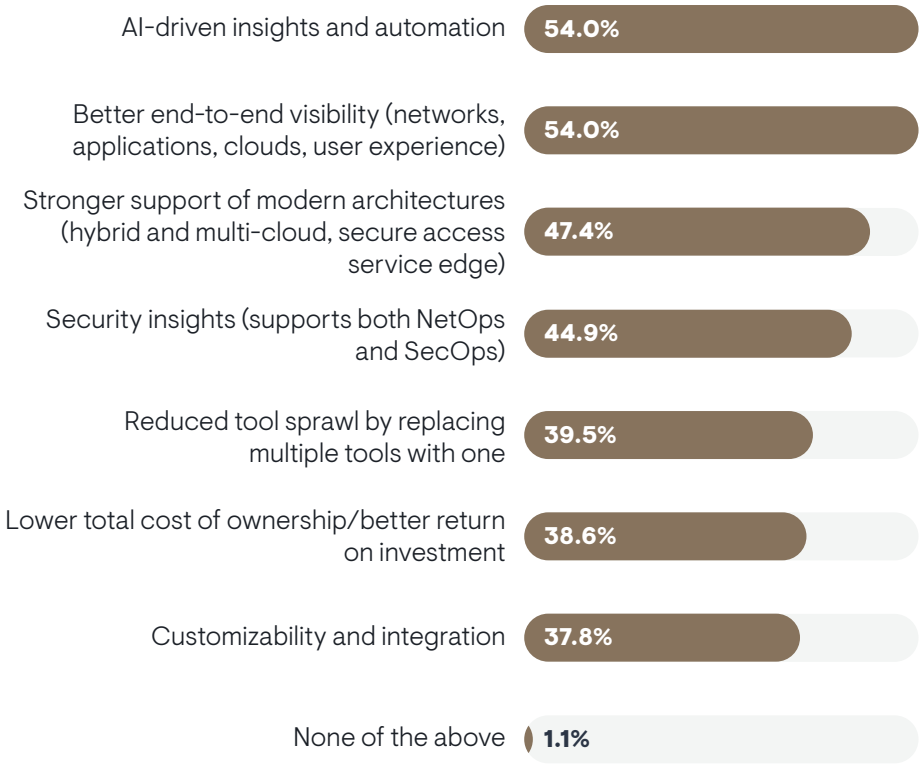
Top Drivers of Tool Replacement

Figure 25 shows the factors that would motivate network teams to replace an incumbent tool. Most organizations indicated that AI-driven insights and automation and better end-to-end visibility are the biggest drivers.

"We definitely want something agentic that is actively working on problems," said a network tools lead with a multinational bank. "I don't see us changing vendors in the next fiscal year. It's something we would do in the future."

Strong support of modern architectures, like hybrid and multi-cloud networks, was the top secondary driver to tool replacement. This was especially a factor for organizations that conduct network operations within a cross-domain operations center. Technical personnel and middle managers cited this driver more often than IT executives. Very large companies (20,000 or more employees) were not motivated by modern architecture support.

Figure 25. Which of the following would most motivate you to replace an incumbent network monitoring or network observability tool with a new tool?



Sample Size = 352

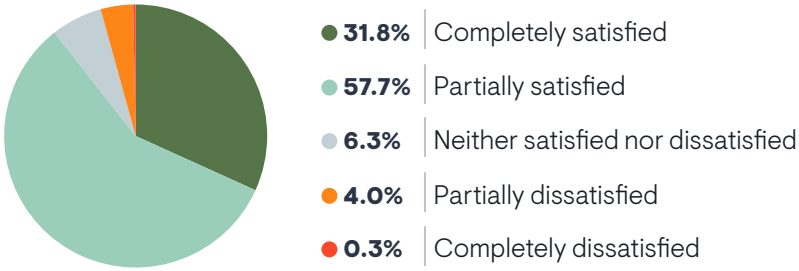
More mature NetOps teams were more likely to cite AI as a motivator, while less mature teams were moved by lower total cost of ownership. In other words, chasing savings is not a path to improving operations.

"We're looking to replace one of our tools because of scale," said a network tools lead with a Fortune 500 retailer. "We need to monitor hundreds of thousands of devices and our existing tool's database isn't built for it."

Tool Satisfaction

Figure 26 reveals that only 32% of IT pros are fully satisfied with the tools they use to monitor and troubleshoot their networks. Executives were more satisfied than middle managers and technical personnel. Larger enterprises (20,00 or more employees) were the least satisfied.

Figure 26. How satisfied are you with the tools your organization uses to monitor and troubleshoot its networks?



Sample Size = 352

Low tool satisfaction correlated with:

- Less NetOps success
- Less effective management of cloud networks
- Less trust in the data collected by these tools

Lower tool satisfaction also correlated with two specific cloud network management challenges:

- Limited end-to-end visibility across on-premises and cloud networks
- Inconsistent tools across cloud providers

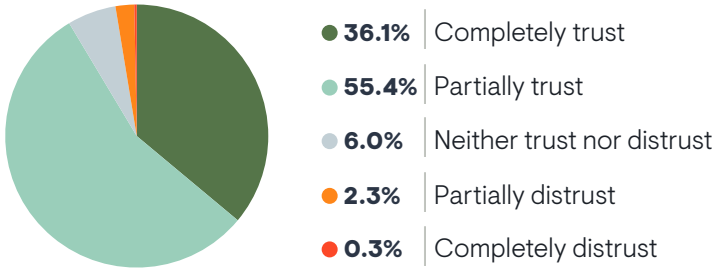
Companies that had an informal and distributed approach to NetOps were less satisfied, suggesting that there is no true champion for network observability tools in these organizations. Companies that operated with a NOC were happier with their tools.

Network Operations Data

Do You Trust Your Data?

Only 36% of survey participants told EMA that they completely trust the accuracy of the data collected by their network observability tools, as **Figure 27** shows. Data accuracy is essential to operations. Lower levels of trust correlated with less network operations success and less effective management of cloud networks.

Figure 27. How much do you trust the accuracy of the data your organization's network monitoring or network observability tools collect?



Sample Size = 352

"We're moving to managed platforms like Meraki, Juniper Mist, and Aruba Central, and a lot of the old management tools don't have the integrations to manage them," said a network tools architect with a Fortune 500 retailer. "Those tools are all SNMP-based. Most of these platforms are getting ready to release streaming telemetry using things like OpenTelemetry and GRPC, sending streaming data to web sockets. But traditional platforms are not ready."

Cybersecurity teams were the least likely to trust data accuracy. The CIO suite was more optimistic about this data. Large companies (20,000 or more employees) were especially pessimistic about their network observability data.

Challenges to Network Observability Data Collection

Figure 28 reveals why trust in data accuracy is so limited. Security risk is the biggest issue. There are a number of ways this concern could manifest itself. For example, if an organization is using a SaaS-delivered observability tool, it may have issues with securing how data collected by a local probe is forwarded to the cloud.

The second biggest issue is tool quality. Organizations are seeing issues with scalability, stability, and errors that impact their ability to consistently collect observability data.

The third issue is around skills gaps. The network team lacks the expertise to properly configure tools and instrument the network, which limits their ability to collect all data properly. Larger enterprises were especially likely to struggle with skills gaps.

Organizations that are more reactive than proactive or predictive with NetOps were more likely to cite cost as a major issue.

Finally, respondents who didn't trust the accuracy of their network observability data were more likely to struggle with proprietary data formats.

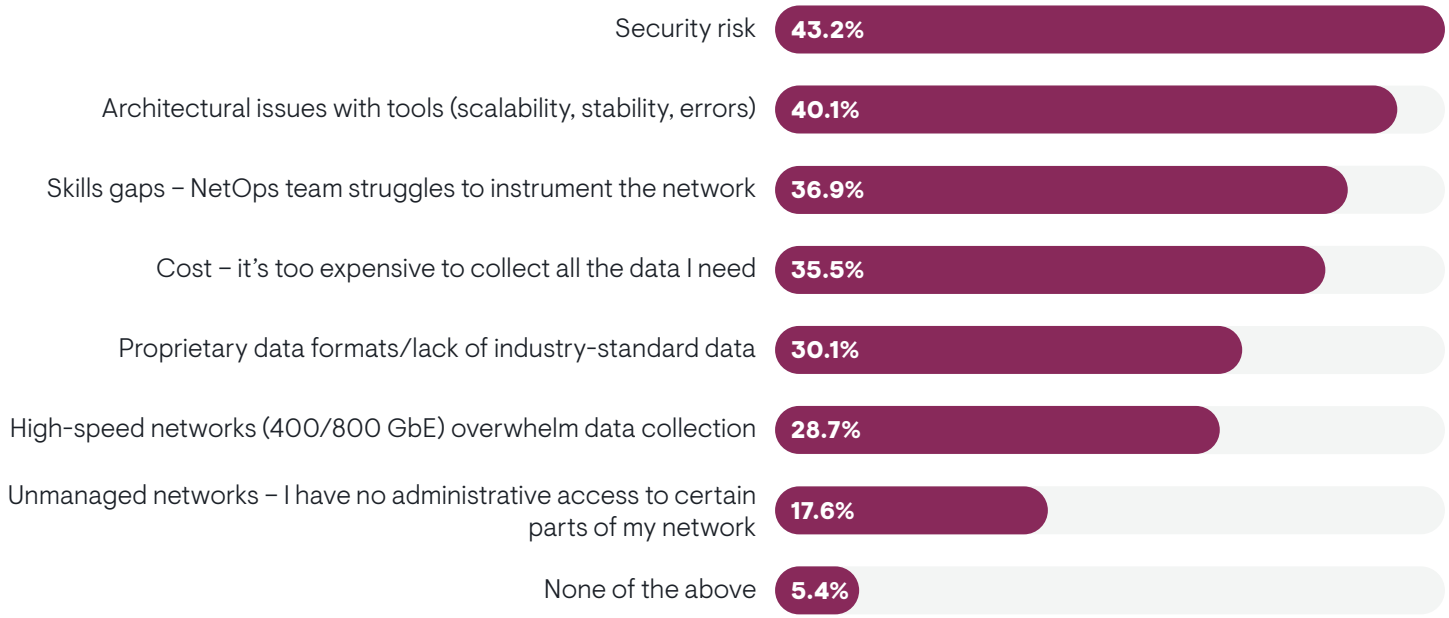


Figure 28. Which of the following are most challenging to your organization's ability to collect network data with its network monitoring or network observability tools?

Sample Size = 352

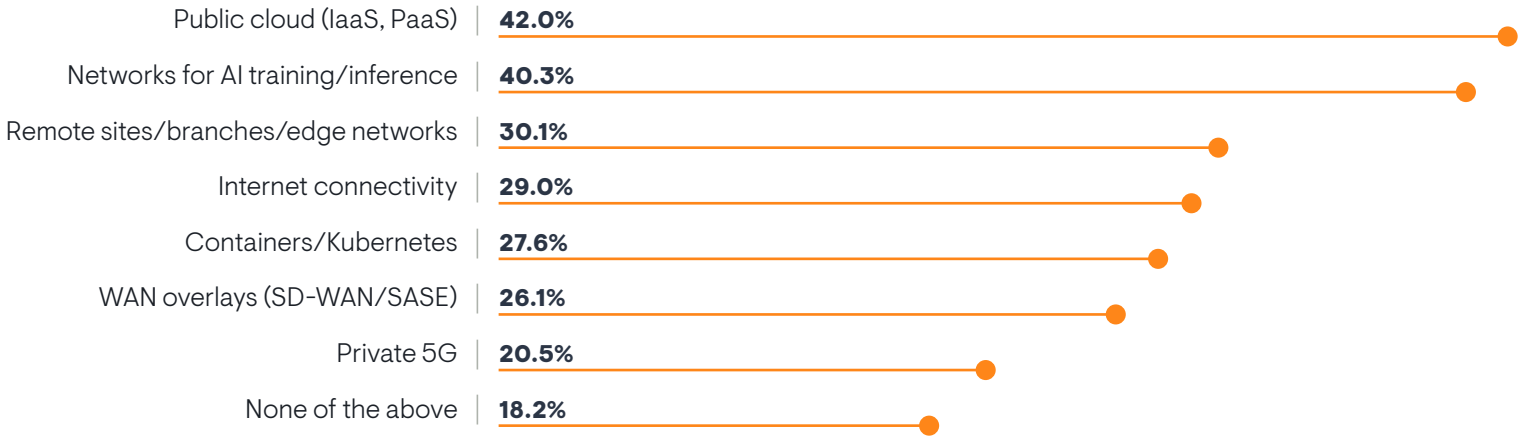
Network Domains that Challenge Tools

Figure 29 reveals which network domains are most challenging for network teams to monitor and manage with their tools. The biggest issues are the public cloud and networking for AI training/inference (which can include specialized cloud services and highly optimized data center network fabrics). Smaller companies (1,000 to 9,999 employees) were more likely to struggle with AI networks.

Less trust in the accuracy of data collected by network tools correlated with struggles with remote sites and branches and internet connectivity, suggesting that tools are particularly bad at collecting good data consistently from these environments. Larger enterprises (20,000 or more employees) were especially challenged by the internet.

Organizations that conducted network operations via a NOC were more likely to struggle with the public cloud and Kubernetes. Companies that had a cross-domain operations center struggled with networking for AI.

Figure 29. Do your network monitoring or network observability tools struggle to monitor and manage any of the following environments?



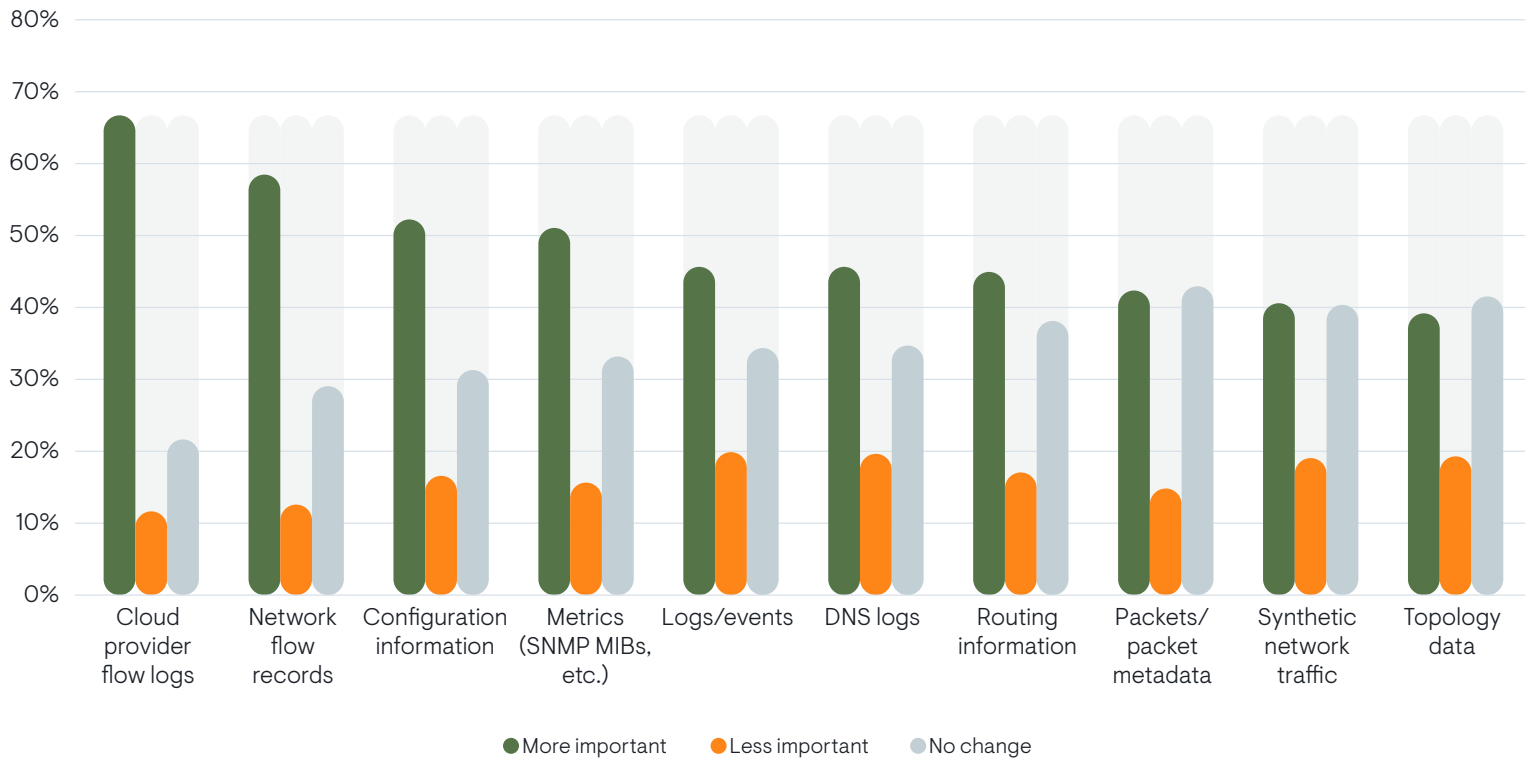
Network Observability is All About Data Diversity

In the DevOps and application performance management world, operators focus on metrics, logs, and traces (MELT) to measure the health and performance of applications. Network operations is more complex. **Figure 30** explores all the data that network teams use to monitor their networks. EMA asked respondents to identify whether the importance of each of these 10 classes of network data was changing. Overall, respondents made it clear that each type of data is more likely to be getting more important than less important.

Four types of data stood out as especially critical:

- Cloud provider flow logs
- Network flow records
- Network configuration info
- Network metrics

Figure 30. 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?



"We collect VPC flog logs from the cloud," said a network tools lead with a Fortune 500 retailer. "We're not doing much with it, but it's nice to have when you have a problem. It required a new tool – Grafana – because we were not able to use flow logs with our primary network monitoring tool."

Successful NetOps teams were more likely to perceive the growing importance of DNS logs and topology.

EMA observed some differing priorities based on the IT silo that a respondent worked within.

- Metrics – The IT executive suite, network engineering, and NetOps teams saw more value than cloud teams
- Logs/Events – Cybersecurity teams saw more value than the IT executive suite, NetOps, and IT architecture
- Packets – The IT executive suite, IT architecture, and cybersecurity teams saw more value than NetOps and cloud teams
- Routing info – The IT executive suite, network engineering, NetOps, IT architecture, and cybersecurity saw more value than cloud teams
- Topology – The IT executive suite, IT architecture, and cybersecurity saw more value than NetOps

Megatrend #1: Enterprises Struggle to Hire Network Engineers

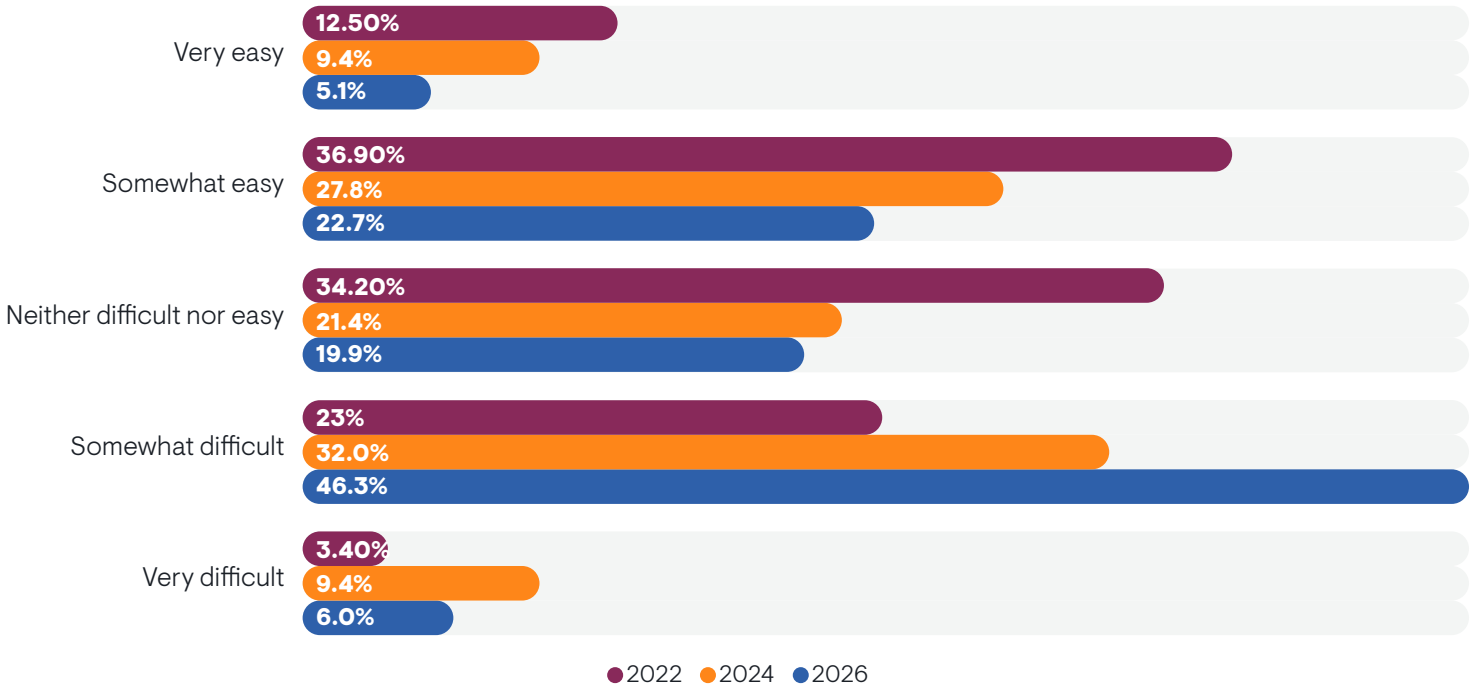
In 2022, EMA began asking Megatrends survey participants to characterize how easy or difficult it is for them to hire and retain network technology experts. **Figure 31** reveals that hiring conditions have become more and more challenging over the years. The number of people who say it is somewhat to very difficult to hire networking experts increased from 26% in 2022 and 41% in 2024 to 52% today.

"We're trying to hire a senior engineer and an intermediate person, but all we're seeing are resumés from people with 20 years of experience and multiple CCIEs. And the junior people are too junior," said a network tools lead with a multinational bank.

"We're having a hard time finding good people, especially at the architect and senior engineer level," said a network tools lead with a Fortune 500 retailer.

EMA found a direct correlation between hiring challenges and NetOps success. The more pain they had with hiring, the less success they experienced. Very large companies (20,000 or more employees) reported the highest level of pain.

Figure 31. Does your organization find it difficult or easy to find, hire, and retain personnel with network technology expertise?



Premium Networking Skills

Figure 32 reveals the networking expertise that IT organizations most struggle to find when hiring personnel. There are three skillsets that engineers should focus on developing if they want to make themselves ideal candidates:

- Network security
- Networking for AI
- Network automation

Network monitoring and troubleshooting skills were the biggest secondary gap in the labor market. "A lot of the junior people we consider do not have hands-on experience on the tooling side," said a network tools lead with a multinational bank. "They don't know how to work with NetFlow and packet captures because they're all relying on GUI-based tools."

In other words, network engineers should build skills around designing, enforcing, and auditing security polices, learn how to build and manage networks that support AI workloads, and learn the tools and programming languages that organizations use to automate their networks.

Challenges with hiring network security experts correlated with less overall success with network operations, highlighting how important it is for organizations to address this gap.

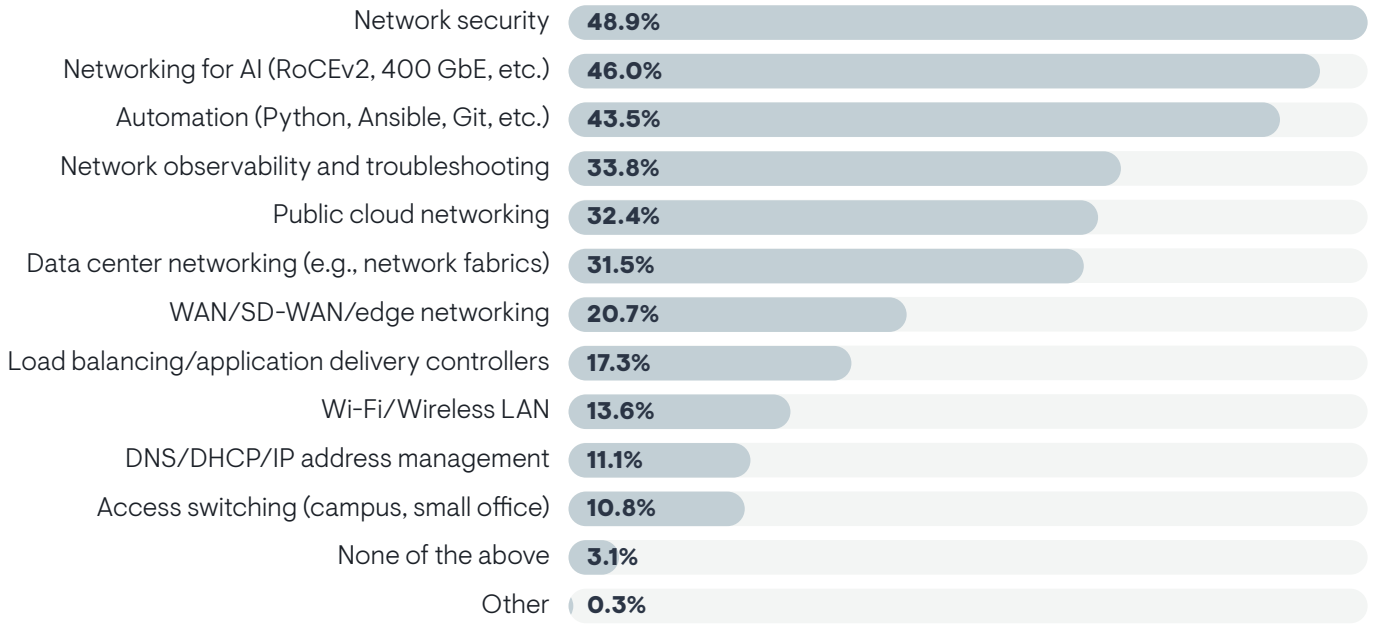


Figure 32. Which of the following areas of networking expertise are the most difficult for your organization to find in new hires?

Sample Size = 352

Closing Skills Gaps

In the face of this hiring crisis, what can IT leaders do? **Figure 33** reveals that most enterprises are taking a three-pronged approach to this labor issue:

- Adopting AI-driven network management solutions to streamline and automate operations
- Upskilling and training existing personnel, such as tier 1 analysts and technicians
- Implementing network automation and orchestration tools

Organizations that reported the most success with network operations were more likely to rely on network automation and orchestration to address skills gaps. Larger enterprises were more likely to choose upskilling and training of existing employees.

The top secondary approach to solving the hiring crisis is the standardization and simplification of network architecture and tooling. If things are simpler and consistent, they should be easier to manage, thus requiring fewer skilled personnel. IT executives and middle managers were more likely to select this. Technical personnel were unlikely to believe in this remedy.

"We had an architect role open for half a year in the network automation team, and we were not able to find someone," said a network tools lead with a Fortune 500 retailer. "We ended up hiring someone internally and training him ourselves."

Notably, outside help was least popular, with professional services and outsourcing appearing to be last resorts.

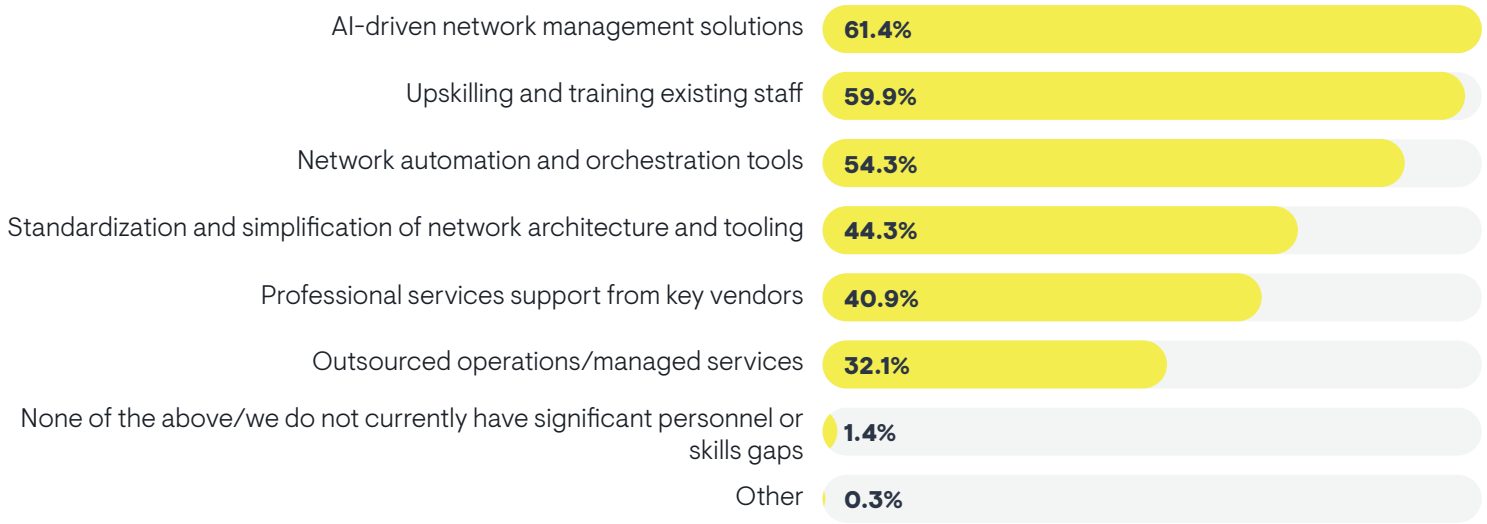


Figure 33. Which of the following can best help your organization address personnel and skills gaps in your network infrastructure and operations group?

Sample Size = 352

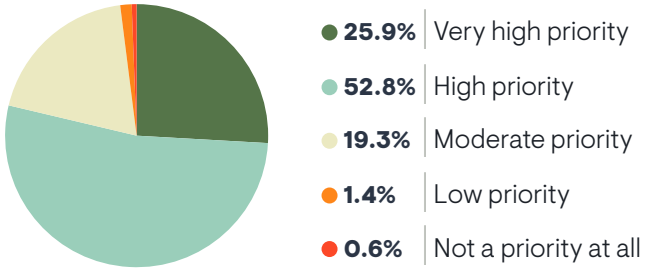
Megatrend #2: Automating Day 2 Network Operations

In conversations with IT organizations, EMA analysts have observed a maturing, comprehensive focus on network automation. This includes a strong commitment to automation of day 2 operations, such as problem detection, triage, troubleshooting, remediation, and optimization. **Figure 34** reveals this focus. Nearly 79% of organizations say this automation is a high or very high priority. Organizations with a successful network operations strategy were more likely to prioritize automation.

"We're looking at making processes more and more efficient and more and more automated to do more with less people," said a monitoring architect with a Fortune 500 entertainment company. "We're using automation and AI, and a lot of that falls on the monitoring platform engineers who are responsible for tooling."

Respondents who typically get complex problems escalated to them were more likely to prioritize this automation. For instance, members of network operations teams were least likely to focus on Day 2 automation, but members of network engineering, cybersecurity, IT architecture, and network tool architecture groups made it a higher priority.

Figure 34. In your organization today, how high a priority is it to automate Day 2 network operations (for example, event management, troubleshooting, optimization)?

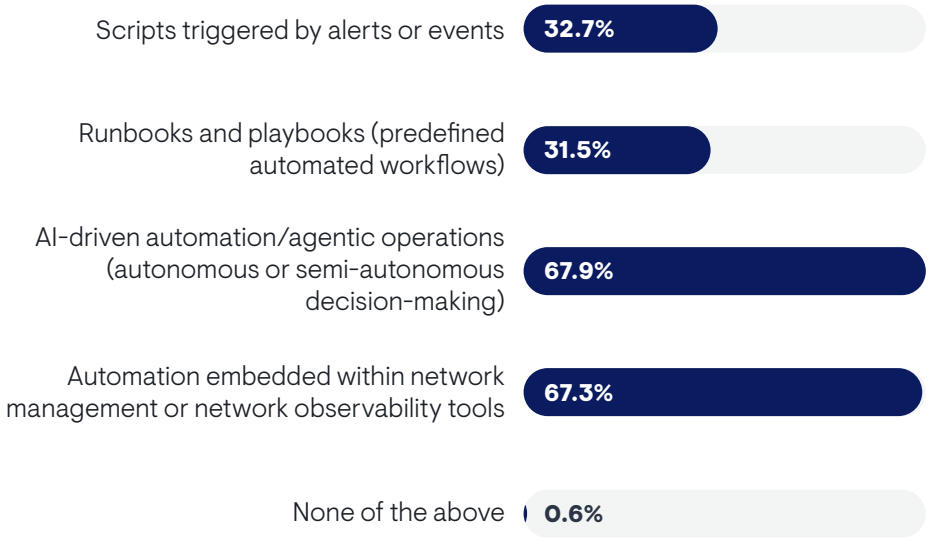


Sample Size = 352

Automation Solutions

Figure 35 reveals that most organizations intend to achieve this automation via agentic AI solutions and automation embedded in their network management tools. More successful organizations favored the latter. Fewer organizations leverage scripts or runbooks and playbooks.

Figure 35. Which of the following approaches best describes how your organization wants to automate Day 2 network operations (event management, troubleshooting, optimization)?



Sample Size = 352

Organizations that are less mature with network operations – particularly those who are highly reactive rather than proactive – rely on scripts trigged by events. More mature organizations expressed a stronger interest in AI-driven automation.

"We're trying to automate alert reduction, and a lot of that can be done with deduplication. But you can go deeper with that, and that is where AI and ML come in handy," said a monitoring architect with a Fortune 500 entertainment company. "We're also trying to automate how we handle carrier maintenance windows. We apply AI to the emails we get from carriers to automate that."

"We don't have a timeline on AI yet," said a network tools lead with a multinational bank. "We're talking to vendors. Right now, we're using scripts and an in-house tool that we built. And some of it is through an inventory management tool."

"We're working on a platform to create some custom agents and test them and guide them to do some responses based on what the issue is, basically replacing what the NOC engineer does," said a network tools lead with a Fortune 500 retailer.

IT executives and middle managers were more interested in AI automation than technical personnel.

Tasks Targeted for Automation

Figure 36 reveals that enterprises are primarily focused on automating security responses and optimization of performance and capacity. These priorities suggest a prevailing focus on using automation to improve overall resilience by minimizing the impact of security incidents and by optimizing the network's ability to absorb increases in utilization or other events.

Many organizations also want to automate incident remediation, root-cause analysis, configuration optimization, and event management.

"We're focused on incident automation and ticket routing," said a network tools lead with a Fortune 500 retailer.

Organizations that conduct NetOps via a NOC were more likely to automate event correlation and change validations/rollbacks. Organizations with a cross-domain operations center sought to automate configuration optimization and security responses.

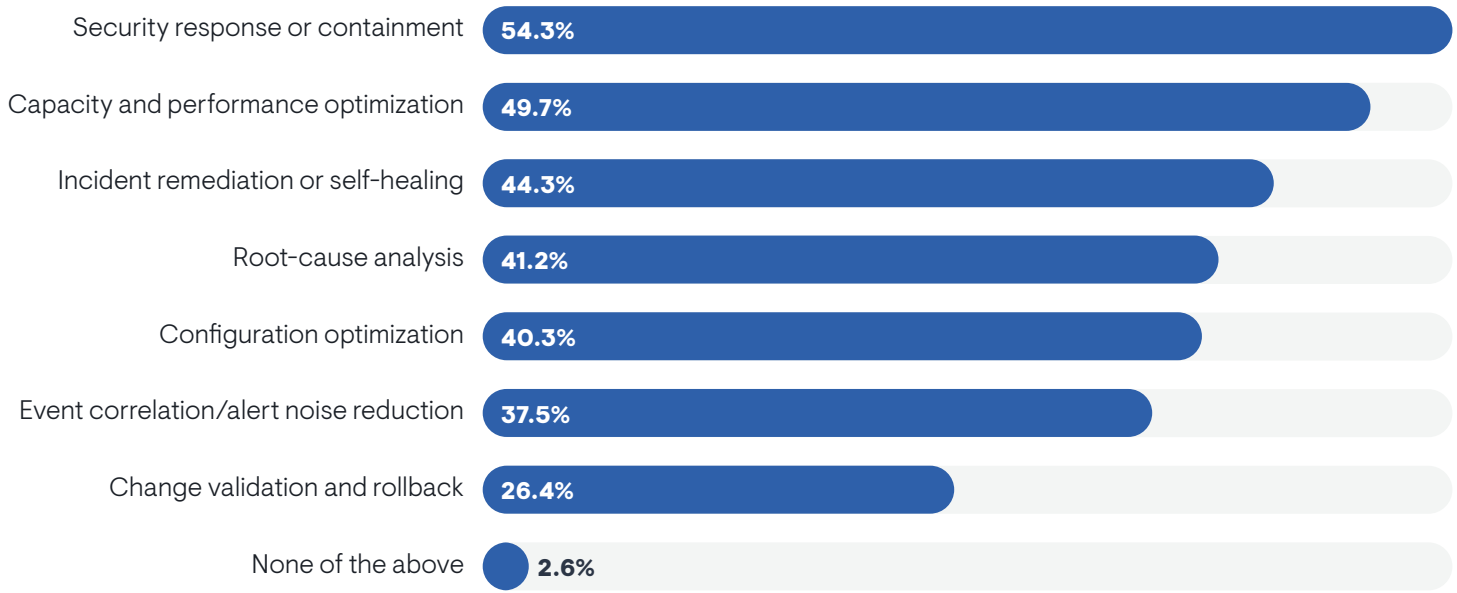


Figure 36. Which Day 2 network operations processes are currently automated or planned for automation?

Sample Size = 352

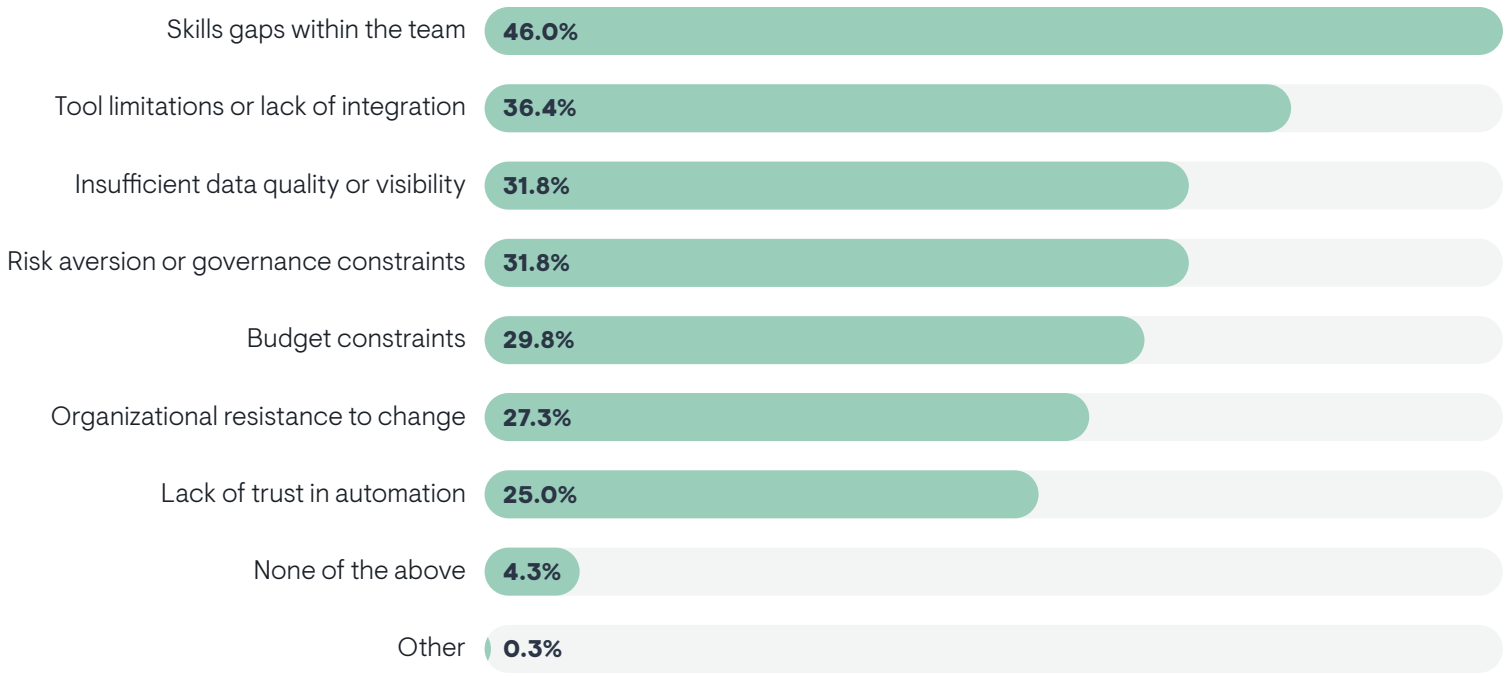
Barriers to Automation

Figure 37 highlights the roadblocks to Day 2 automation. Skills gaps are the biggest challenge, followed by issues with tools and integration.

Among other secondary challenges, budget constraints were cited more often by larger companies (20,000 or more employees). Budget also impacted less successful NetOps teams more than successful ones. Network engineering personnel were more aware of data quality issues than network operations personnel.

Finally, technical personnel were more aware of organizational resistance to change than middle managers.

Figure 37. What are the biggest barriers preventing your organization from automating Day 2 network operations today?



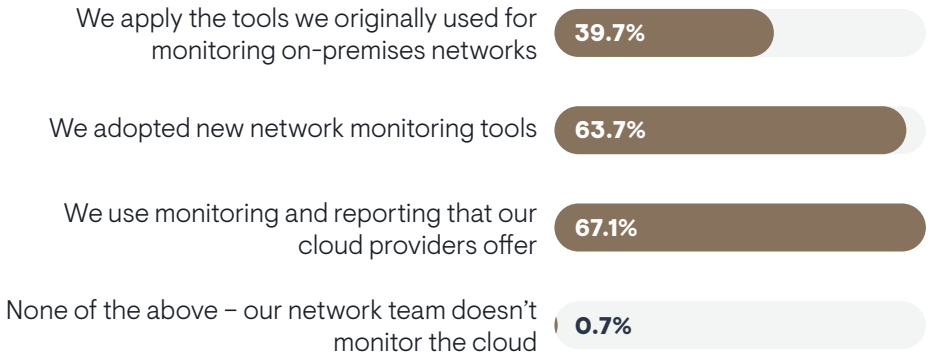
Sample Size = 352

Megatrend #3: Hybrid and Multi-Cloud Networks Challenge NetOps

Observability of Cloud Networks

EMA asked the 291 respondents from companies that use at least one public cloud provider to describe their approach to monitoring and troubleshooting network issues in the public cloud. Less than 1% claimed not to monitor networking in the cloud at all, as revealed by **Figure 38**. Most organizations use the monitoring and reporting tools their individual cloud providers offer, and they have adopted new tools to specifically address their cloud network observability needs. Only 40% claim that they extended their legacy on-premises network monitoring tools into the cloud.

Figure 38. What does your network team use to monitor and troubleshoot network issues in the public cloud?



Sample Size = 292

"We don't get involved with the cloud," said a network operations manager with a Fortune 500 retailer. "Most NetOps people don't know how to automate and don't know Terraform. In my last company, if we had network-related cloud issues, we'd have to call in a senior network engineer."

Successful network operations teams were more likely to extend their on-premises tools into the cloud. Members of the network engineering team were also more likely than cloud teams and cybersecurity teams to see this approach.

"It's gone from just infrastructure monitoring to monitoring at the application level," said a network tools lead with a multinational bank. "We're using tools that look more at NetFlow than we did in the past. We also use Google's in-house tools."

IT executives were more likely than technical personnel and middle managers to perceive adoption of new network monitoring tools.

Hybrid Cloud Networking

EMA asked the 243 respondents who have both data center and public cloud environments whether they are integrating any aspects of these hybrid environments. **Figure 39** reveals that hybrid cloud connectivity is extremely common. Most companies are also extending network observability and network automation tools across these architectures. End-to-end observability and automation are clearly a priority for hybrid cloud networks.

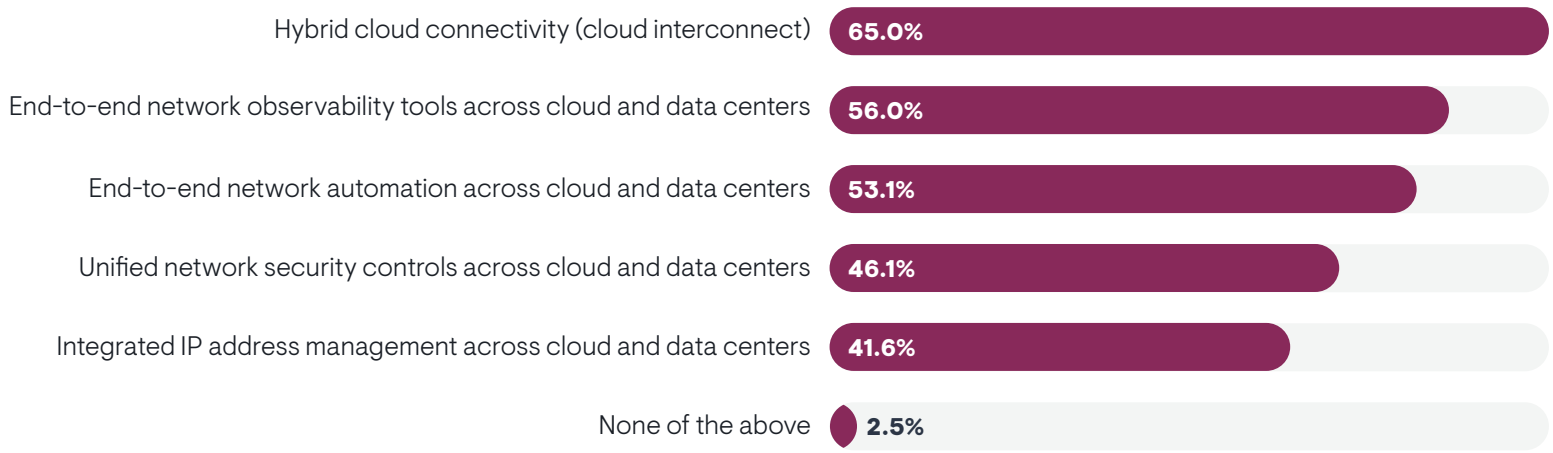
Unified network security and integrated IP address management are also quite common secondary measures.

Successful network teams were more likely to adopt end-to-end observability and integrated IP address management. End-to-end automation and observability were both cited more often by mature network teams (proactive or predictive operations, rather than reactive).

The CIO's office perceived more adoption of hybrid cloud connectivity and end-to-end observability, while the network engineering team perceived more adoption of integrated IP address management.

Finally, adoption of end-to-end network observability correlated with a stronger inclination to replace tools. This suggests that many enterprises run into limitations when they try to extend their network observability tools across a hybrid cloud.

Figure 39. You indicated that your organization uses both public cloud and data center infrastructure. Is your organization adopting any of the following across those two domains?



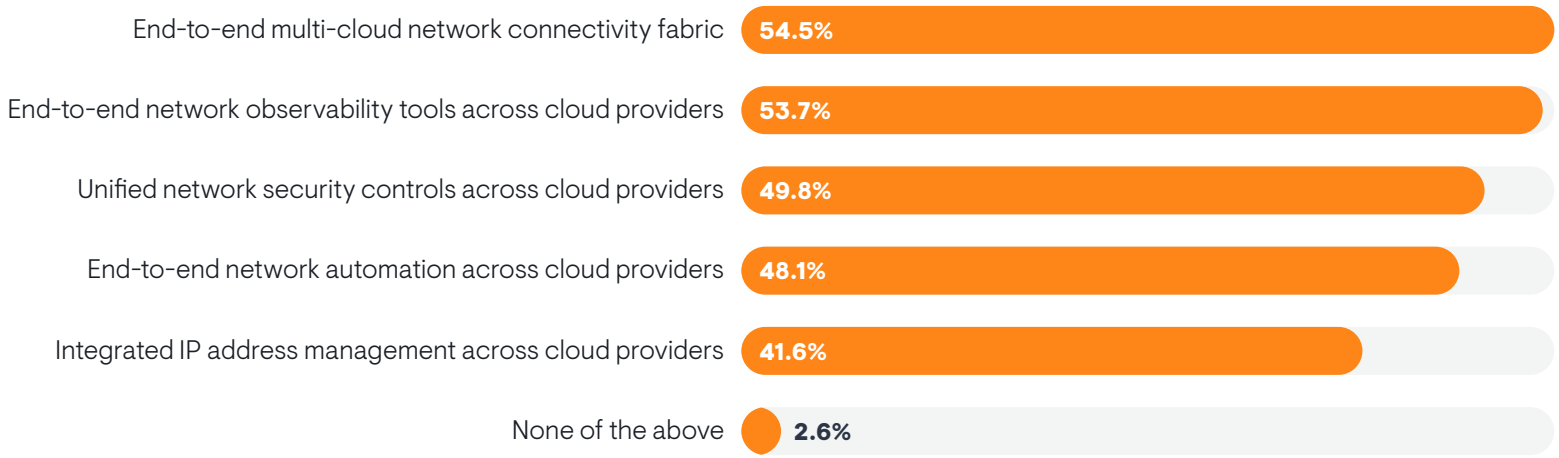
Sample Size = 243

Multi-Cloud Networking

Figure 40 shows how enterprises build and manage networks across multi-cloud environments. Most of the 231 multi-cloud companies in this survey have adopted end-to-end connectivity fabrics and end-to-end network observability tools across their cloud providers. Half are also adopting unified network security across their cloud providers. Successful network operations teams were more likely to report unified security.

Many are applying end-to-end network automation across clouds. IT middle managers were the most likely to perceive such automation efforts.

Figure 40. You indicated that your organization uses multiple cloud providers. Is your organization adopting any of the following across those clouds?



Sample Size = 231

Importance of Unifying Cloud Networking

Figure 41 reveals that 59% of organizations believe it is very important to unify their approach to networking across on-premises, hybrid, and multi-cloud networks. Companies that emphasize this unification tend to report more network operations success and more effective management of networking and security in the public cloud.

Figure 41. How important is it for your organization to have a unified approach to networking across on-premises, hybrid, and multi-cloud environments?

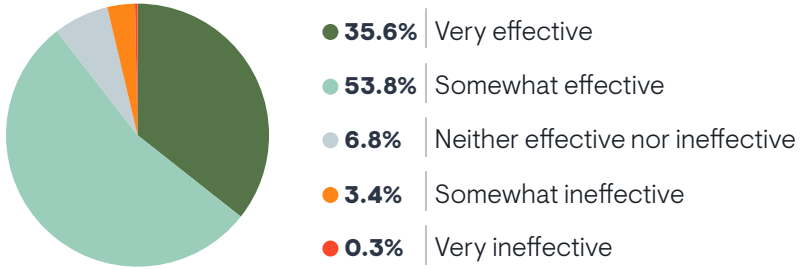
Large enterprises (20,000 or more employees) were less likely to commit to unified cloud networking.

Sample Size = 292

Effectiveness of Cloud Networking Strategies

Figure 42 reveals that only 36% of enterprises are very effective at managing networking and security in the public cloud. The rest see room for improvement. Unsurprisingly, effectiveness correlated with overall NetOps success.

Figure 42. How effective is your organization at managing networking and security in the public cloud?



Effective organizations were more likely to:

- Apply end-to-end network automation across hybrid clouds
- Apply integrated IP address management across multi-cloud environments
- Maintain a cross-domain operations center rather than a NOC or an informal/distributed network operations practice

Technical personnel were more pessimistic about cloud networking and security than middle managers and executives. Larger enterprises (20,000 or more employees) were struggling the most.

Sample Size = 292

Cloud Networking Challenges

Figure 43 examines the challenges organizations encounter when managing networking in the public cloud. First, the networking constructs that cloud providers offer are too complex. Companies with a hybrid cloud environment struggle with this issue more than those that are 100% in the cloud, suggesting that this issue intensifies as organizations try to implement end-to-end hybrid cloud architecture.

Second, many companies are facing cloud networking skills gaps. Enterprises with 5,000 or more employees are especially likely to struggle with skills gaps.

Limited end-to-end visibility across cloud and on-premises environments is the top secondary challenge. Organizations that conduct network operations via a NOC were more likely to struggle with this issue than those that maintain a cross-domain operations center. Respondents who were less trusting of the data their network observability tools collected were more likely to cite this issue.

The other top secondary challenge, inconsistent tools across cloud providers, was cited more often by technical personnel than executives.

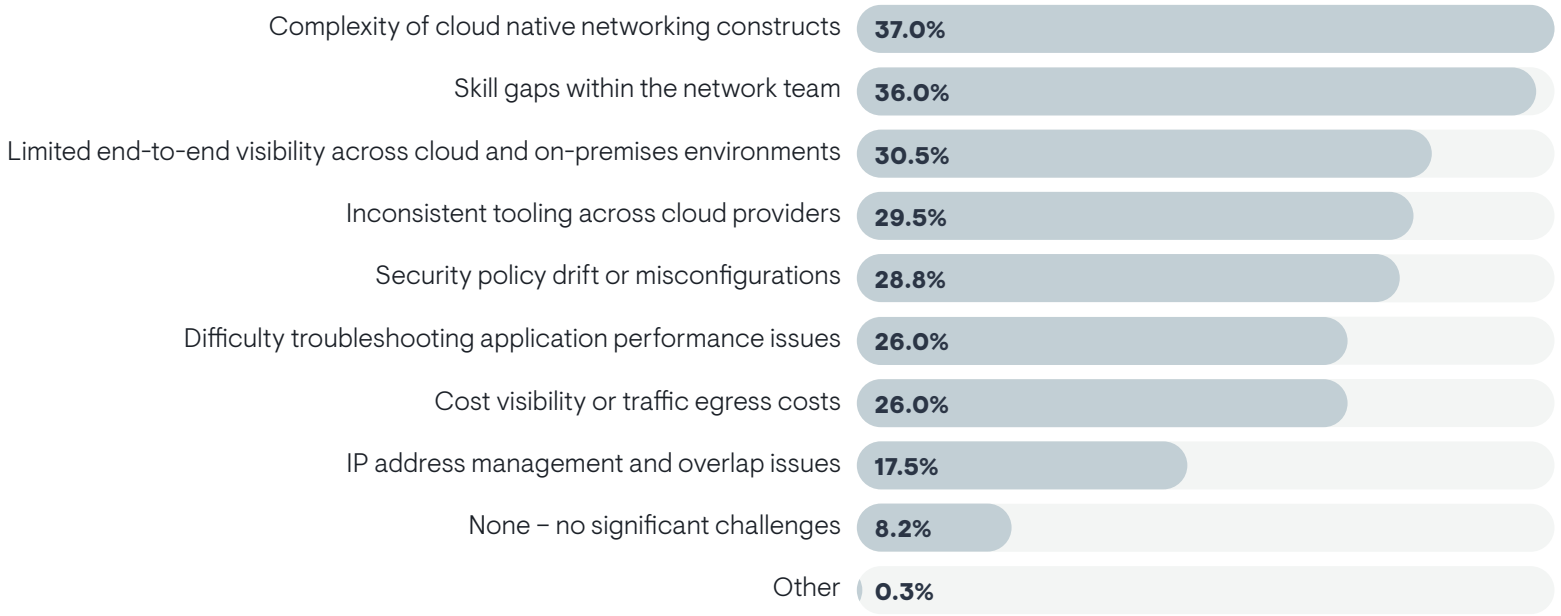


Figure 43. What are the biggest challenges your organization faces when managing networking in the public cloud?

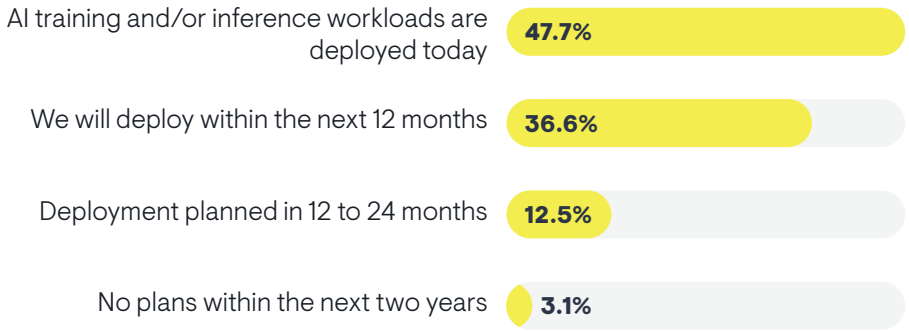
Sample Size = 292

Megatrend #4: Preparing Network Observability for AI Transformation

AI Deployment Plans

The AI hype cycle continues to spin, with many companies implementing AI applications to transform their products, services, and business operations. Nearly 48% of the enterprises represented in this research have deployed AI training or inference workloads on their networks, as **Figure 44** reveals. Only 3% have no plans to deploy such workloads over the next two years.

Figure 44. When does your organization expect to deploy AI training workloads or AI inference workloads in its environment (including data centers, public cloud, and/or edge infrastructure?

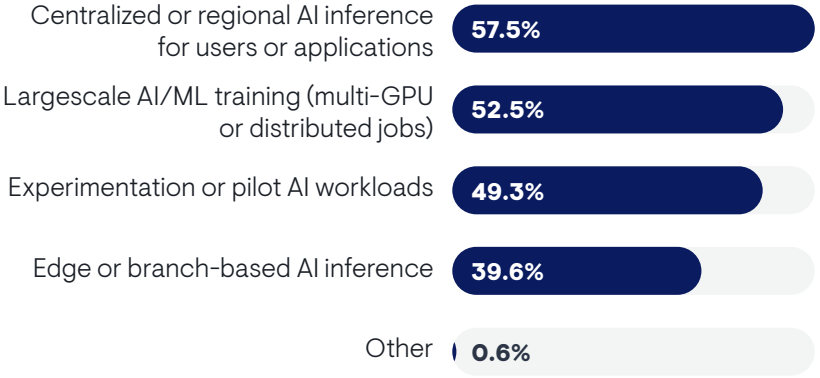


EMA believes that network infrastructure and operations teams will be essential to successful AI implementation. Not only must these teams build and optimize networks to support AI workloads and AI traffic across data centers, clouds, and the enterprise edge, they must also make sure their network observability tools can properly manage this infrastructure to meet the exact networking requirements of AI applications.

Figure 45 reveals what kinds of AI workloads have been deployed or will be deployed over the next two years by the 97% of enterprises that indicated plans to do so. Most companies have or will have centralized or regionalized AI inference workloads for users or applications. Most will also have largescale training deployments.

Sample Size = 352

Figure 45. Which types of AI workloads do you expect to have in your environment within the next two years?



Nearly half of companies have or expect to have some experimental workloads in place. A smaller but significant number of companies will have edge inference workloads.

Successful NetOps teams are more likely to perceive:

- Centralized/regional inference
- Edge inference

IT executives perceived more largescale training workloads, while middle managers perceived more experimentation. Large enterprises (5,000 to 19,999 employees) were more likely to have largescale training workloads than midsized enterprises (1,000 to 4,999). Large enterprises were also more aggressive with edge inference workloads than midsized and very large enterprises.

"We are hiring AI experts right now," said a network operations manager with a Fortune 500 retailer. "We're putting AI bots in stores to help people."

Sample Size = 341

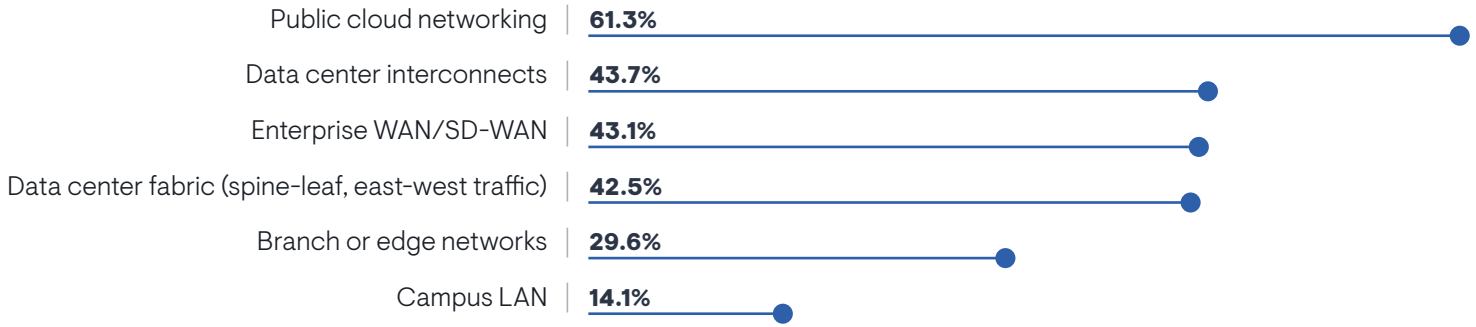
Network Domains NetOps Must Actively Manage for AI Workloads

Network teams expect that public cloud networking will be a critical area of focus as they try to manage the performance of networks for AI. **Figure 46** shows that most NetOps teams expect to focus on that domain.

Data center interconnects, the WAN, and data center network fabrics are all critical secondary targets for managing AI networking. Branch networks and campus networks are a minor, which makes sense given that most enterprises have no current plans to deploy edge inference workloads. The current focus of most companies is the public cloud and data centers and connectivity between those hubs.

However, technical personnel were more likely to see a need to manage branch/edge networks, especially members of network engineering and security teams.

Figure 46. Which network domains are most critical to monitor and troubleshoot for AI performance?



Sample Size = 341

Network Performance Concerns for AI Workloads

Figure 47 reveals the AI network performance management issues that NetOps teams find most challenging. There are two major concerns. First, they are struggling with the impact of security controls on AI performance. Larger companies (20,000 or more employees) were more likely to cite this issue. Second, network teams are struggling to isolate performance issues across networks, applications, and GPUs.

That performance isolation issue was more likely to challenge:

- Less successful NetOps teams
- IT pros who are less satisfied with their network observability tools

There are certain issues that might motivate NetOps teams to replace their tools. The following three challenges were selected more often by respondents who indicated a strong intention to replace network observability tools:

- Network impact on inference latency/tail latency
- Network-induced GPU idling/underutilization
- Difficulty isolating performance issues

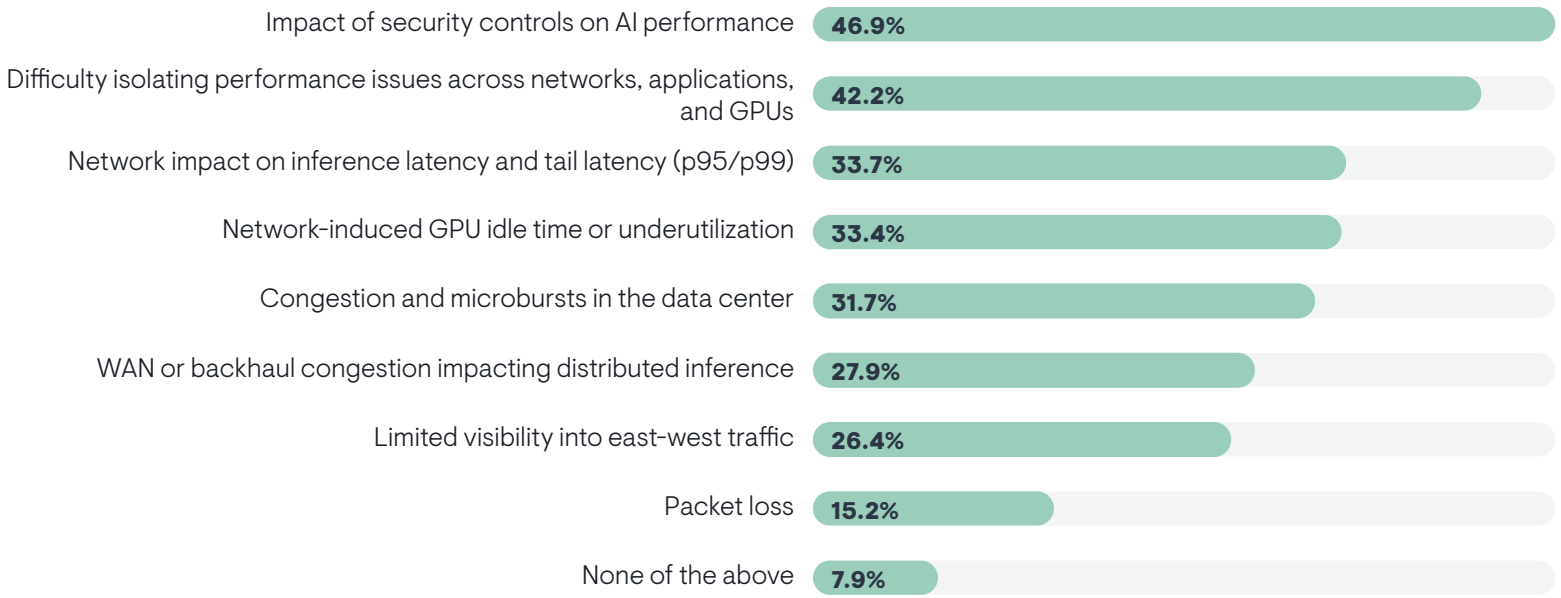


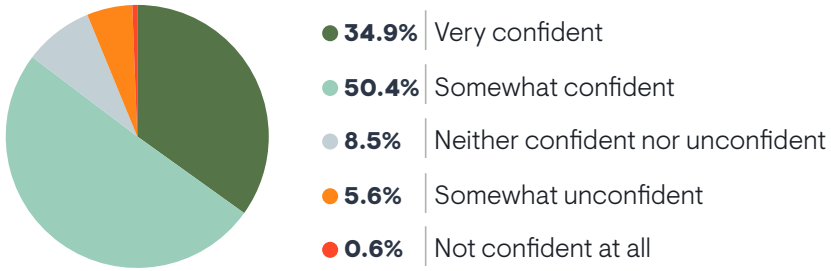
Figure 47. Which AI-related network performance issues concern you the most?

Sample Size = 341

Readiness of Network Observability Tools

Figure 48 reveals that only 35% of survey participants are completely confident that their network observability tools are ready to manage network performance for AI workloads and traffic. Confidence was lower when network teams struggled with inconsistent network observability tooling across cloud providers.

Figure 48. How confident are you that your current network monitoring or network observability tools can support operations for AI workload training and inference workloads?



"We're starting to think about this," said a network operations manager with a Fortune 500 retailer. "The monitoring vendors are coming to us and saying 'we're going to help you with AI.' It feels like we have to drive that and see what's out there."

Sample Size = 341

Very large companies (20,000 or more employees) had less confidence in their tools, as did members of NetOps teams. IT executives were more confident.

EMA observed that confidence in tools correlates with:

- NetOps success
- Effective cloud network management
- Confidence in tool data accuracy
- NetOps maturity (proactive/predictive)
- Fewer struggles with hiring engineers
- A focus on Day 2 operations automation
- A focus on integrating tool sprawl
- Adoption of AI-driven network management tools
- Deploying end-to-end network observability across hybrid clouds
- Use of hybrid cloud interconnects and multi-cloud connectivity fabrics
- Integration of IPAM across hybrid and multi-cloud networks

Tool Enhancement Wish List

Figure 49 reveals the kinds of enhancements that network teams need to properly manage AI traffic and workloads on their networks. The three big asks are AI-powered troubleshooting and remediation, proactive alerting for AI-related performance risks, and packet analytics features that offer AI application awareness. Real-time telemetry was the top secondary requirement.

NetOps teams that are most likely to replace a network observability tool over the next couple years were more likely to want the following:

- Correlation of performance problems across GPUs, applications, and networks
- Per-flow and per-job visibility into training traffic
- SLA/SLO tracking for inference latency/availability
- Topology-aware visibility into AI workloads across sites
- Proactive alerting for AI-related performance risks

"We're standardizing to OpenTelemetry at the edge where our customer-facing AI agents are deployed," said a network tools lead with a Fortune 500 retailer. "We're also implementing data pipelines, and we're doing a lot of filtering and deduplication and standardization to take control of that data."

Very large companies (20,000 or more employees) were more likely to seek packet analytics features that provide awareness of AI applications and workloads.

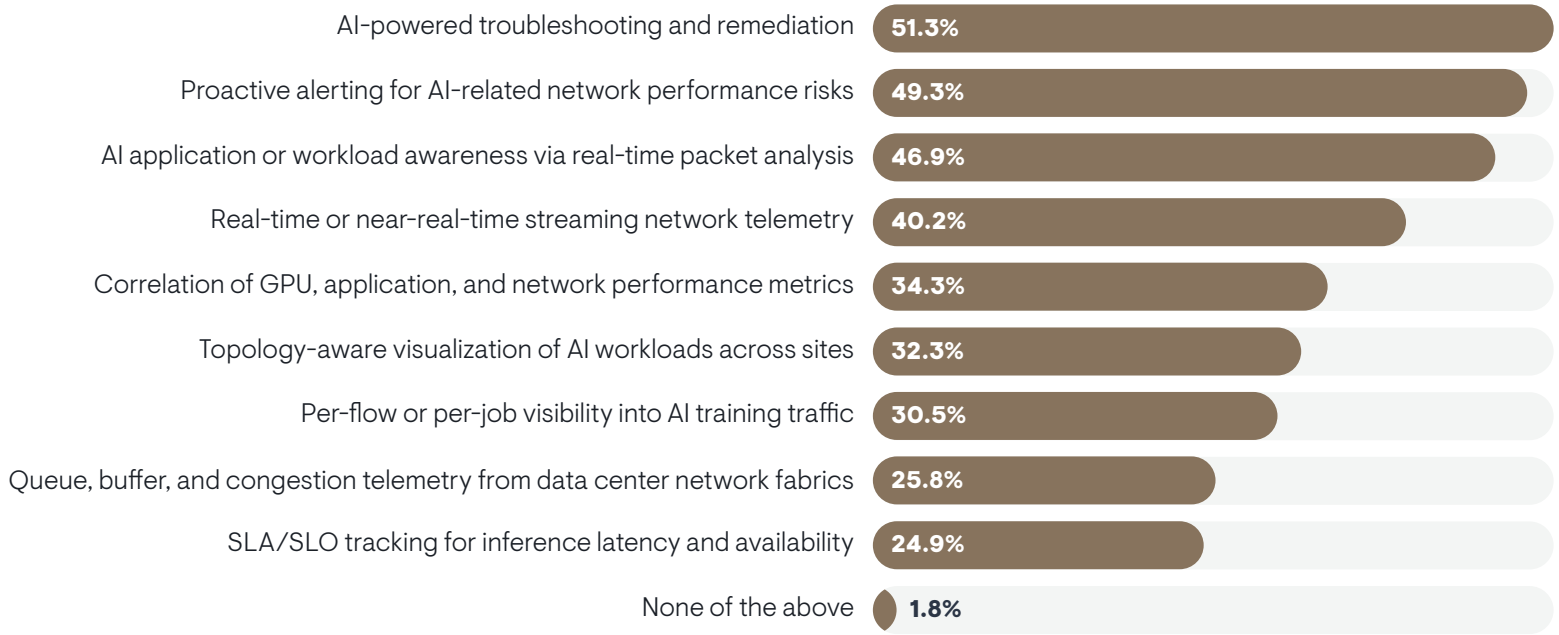


Figure 49. Which of the following enhancements to your network observability tools would best help you with managing AI traffic and AI workloads on your network?

Sample Size = 341

EMA Perspective: Can Agentic Network Management Address Long-Term Challenges?

Network operations teams continue to struggle with a familiar set of hurdles. Hybrid and multi-cloud complexity remains unsolved for technical and cultural reasons. Tool sprawl persists, manual errors continue, and alert noise drones on. Looming over all these issues, IT organizations are struggling to hire network engineers, making it hard to solve these operational problems by throwing more people at them.

AI presents both a challenge and a solution. On one hand, enterprises are adopting AI applications for business transformation, and those applications will push networks to their limit. Network teams need to be prepared. Very few organizations believe their network observability tools are fully capable of managing networks for AI workloads and traffic.

On the other hand, AI is also an opportunity. Network operations leaders clearly believe that AI tools can help improve how they monitor and manage their networks. Network teams now make AI features their top requirement when evaluating network management tools, and more than half of organizations in this survey are using such capabilities. They perceive AI as an essential enabler of automation and optimization, and this research found that users of AI tended to have more mature, proactive, and predictive network operations teams.

It remains to be seen whether AI will solve the problems that persist in network operations, but our data suggests that it is already having a positive effect. AI skeptics should explore this opportunity, but tread carefully. Previous EMA research found that data quality is a potential roadblock to agentic operations success. Organizations must evaluate AI solutions carefully while also considering their own readiness to adopt such technology.

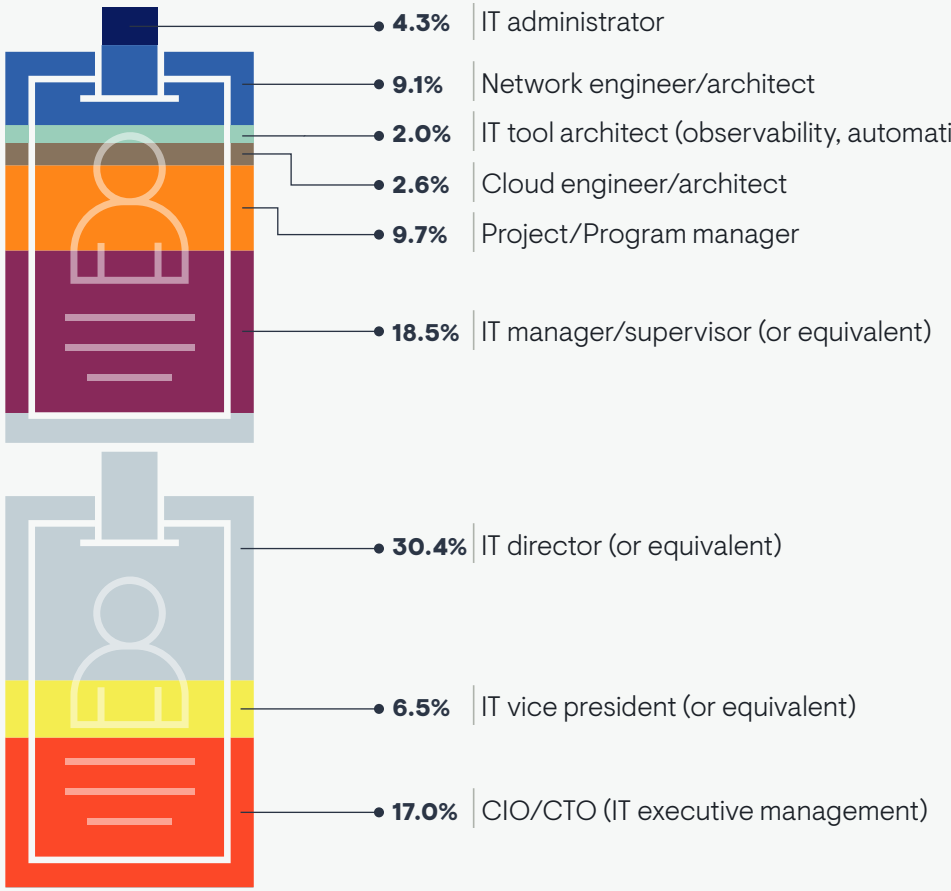
Best Practices for NetOps Teams

Finally, EMA uncovered the following network operations best practices in its analysis of the survey data for this report:

- Designate a functional group as the owner of responding to major service incidents; it doesn't matter which group if ownership is clear
- Focus on network observability data accuracy; don't tolerate glitches, tool collection limits, etc.
- Prioritize automating operations, particularly using AI tools and automations embedded in commercial network management products
- Embrace AI-driven or agentic network management solutions
- Address tool sprawl by integrating network management solutions, especially via workflow integrations and MCP support for agentic access
- Modernize network observability tools to ensure they can monitor and manage AI workloads and traffic on the network
- Emphasize the unification of network and security management across hybrid and multi-cloud architecture
- Establish end-to-end network observability and integrated IPAM across hybrid clouds
- Unify network security controls across multi-cloud infrastructure

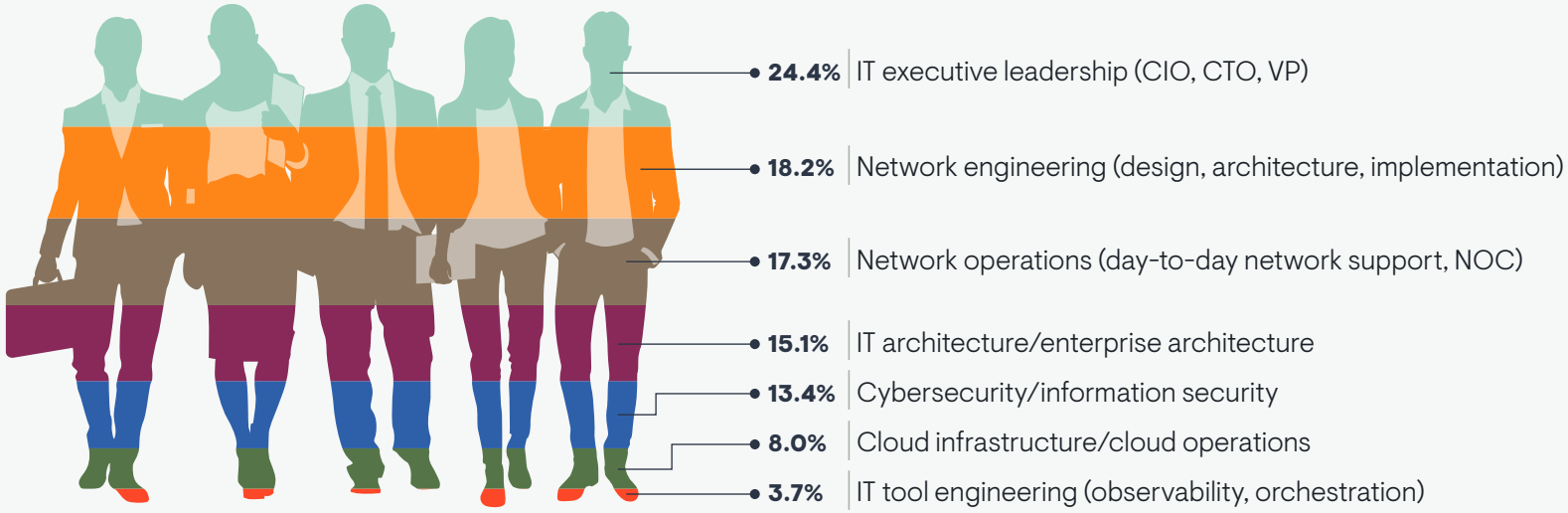
Appendix: Demographics

Figure 50. Which of the following best describes your role in your employer's IT organization?



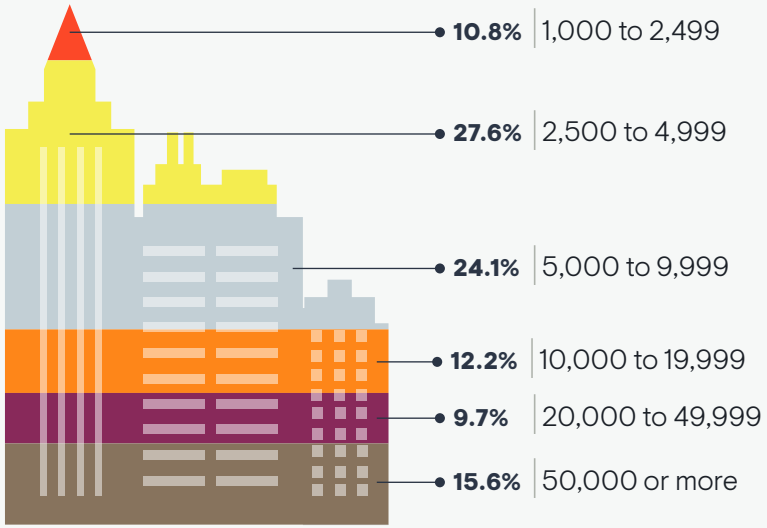
Sample Size = 352ç

Figure 51. Which of the following best describes your primary group or team within the IT organization?



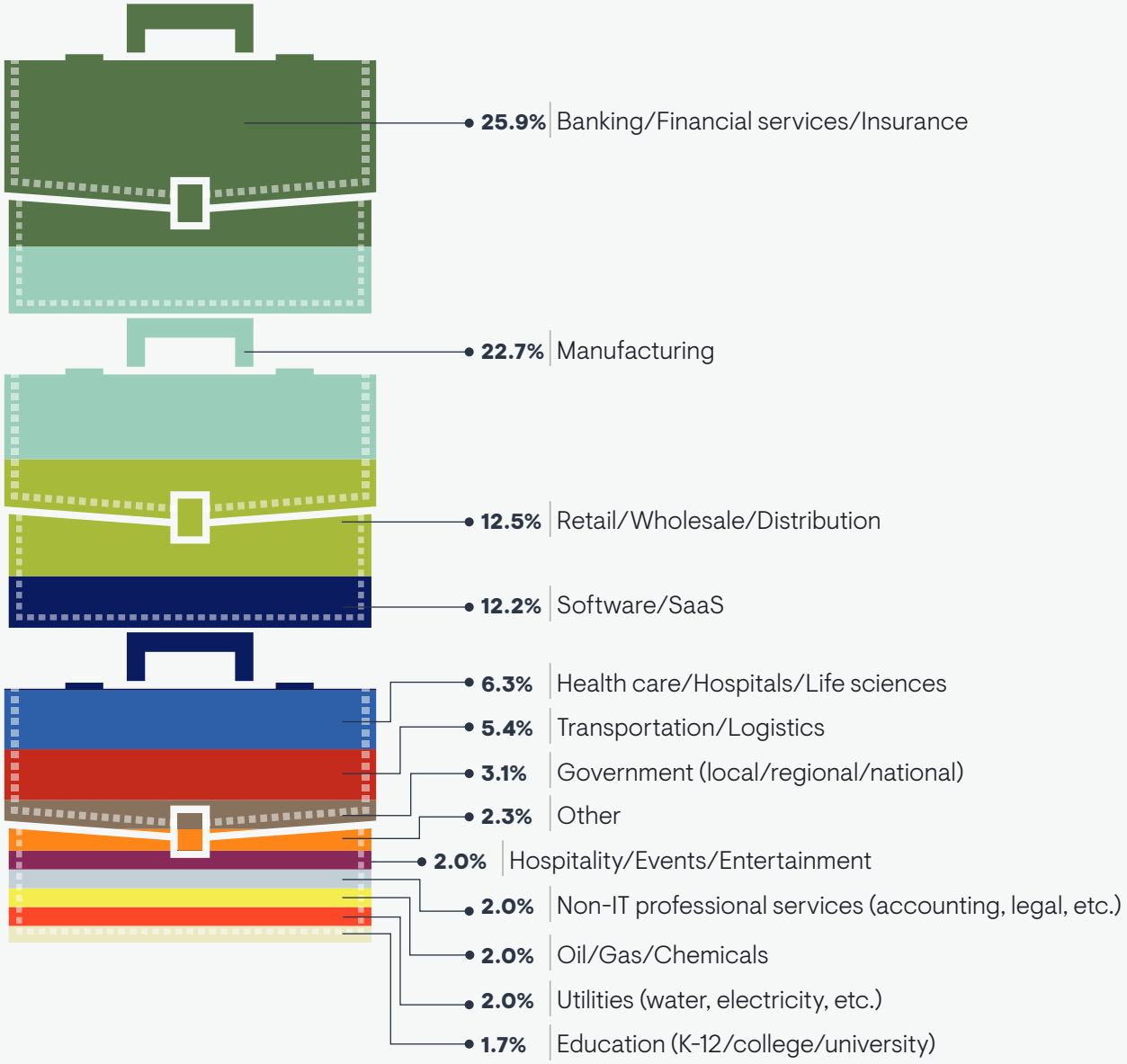
Sample Size = 352ç

Figure 52. How many employees are in your company worldwide?



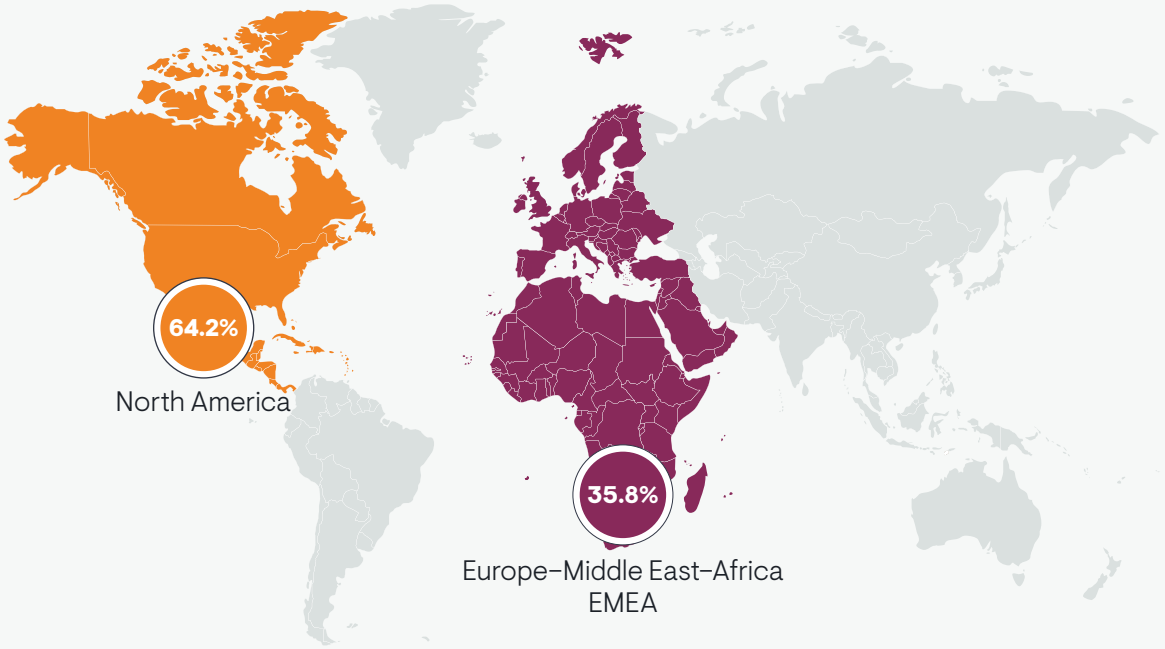
Sample Size = 352ç

Figure 53. Which of the following best describes your company's primary industry?

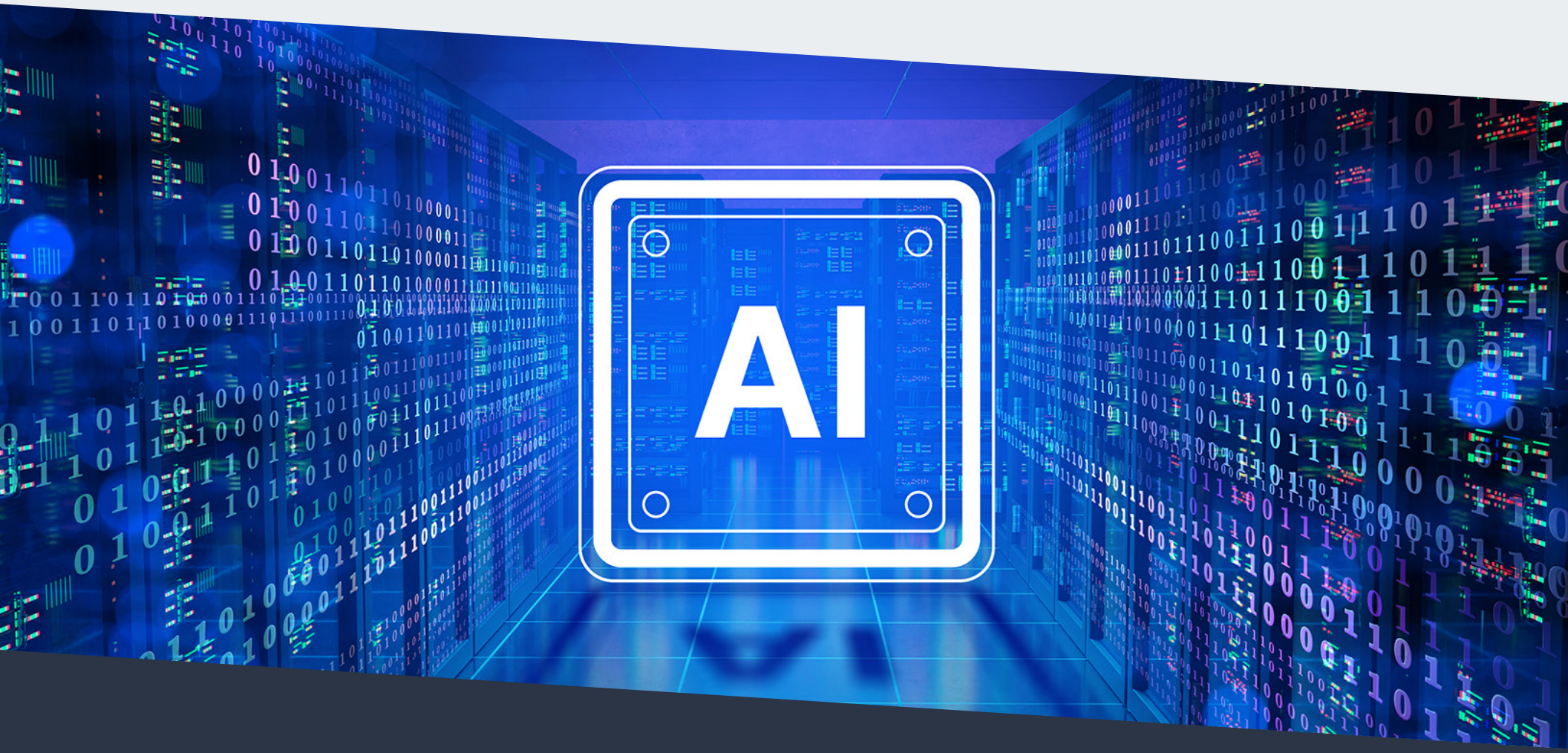


Sample Size = 352

Figure 54. In which region are you located?



Sample Size = 352


AI

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**.

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

4704.042926