IT & DATA MANAGEMENT RESEARCH, INDUSTRY ANALYSIS & CONSULTING

Sponsored by:

# Network Management Megatrends 2022: Navigating Multi-Cloud, IoT, and NetDevOps During a Labor Shortage

**April 2022 EMA Research Report Summary**

By Shamus McGillicuddy, Vice President of Research

## Table of Contents

# Executive Summary

The summary of the 2022 edition of Enterprise Management Associates' biennial "Network Management Megatrends" is the definitive benchmark of the state of enterprise network operations. Based on a survey of more than 400 IT organizations and one-on-one interviews with senior networking experts in Fortune 500 companies, this report should help network managers optimize operations while planning for future initiatives.

# Network Operations: Red Alert

Enterprise Management Associates (EMA) has been publishing its biennial "Network Management Megatrends" research since 2008. The report benchmarks trends large and small from year to year, providing not only current insight into the state of network operations, but also a historical record of how things evolve over time.

This summary of the 2022 edition of EMA's "Network Management Megatrends" research will reveal how IT groups organize the function of network operations and outfit it with tools and processes to address the network management requirements of enterprises. It also explores emerging megatrends that are impacting the network management strategies of IT organizations, such as the cloud and the Internet of Things. However, in this introduction, we call the reader's attention to something ominous.

EMA sees an alarming warning sign. The effectiveness of network operations teams is declining. **Figure 1** details a half-decade's worth of data generated in response to a simple question: "How would you rate the success of your network operations organization over the past year?" There has been a precipitous decline in the number of respondents who believe their network operations groups are completely successful, from 49% in 2016 to 35% in 2020 to just 27% in 2022. EMA sees a growing number of network operations teams that believe that they could and should be doing better.

*There has been a precipitous decline in the number of respondents who believe their network operations groups are completely successful.*

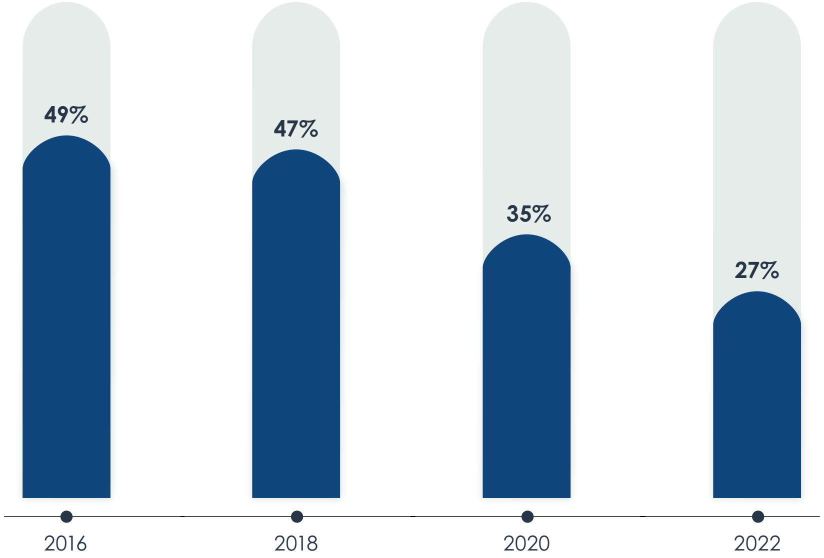

Figure 1. Percentage of IT organizations that are completely successful with network operations.

What is happening? Throughout this report, EMA will attempt to answer this question. For now, we offer some words from networking professionals interviewed for this project.

> [Network operations] is not super effective. I've seen big companies that don't put enough investment into the people in their network operations centers (NOCs). They have a lot of entry-level people and just a few senior-level people, and they have to push too many things to second- or third-tier support.
>
> *Network engineer who has worked for two Fortune 500 financial companies over the last decade*

> "If we're going to measure it against critical incidents, we're doing okay. But if we're going to measure it against low-impact incidents, I'd say no. We're doing a good job of keeping the network up and running, but the number of pending tickets for low-impact incidents is usually around 1,000. We need to develop automation focused on dealing with those."
>
> *Network engineer, Fortune 100 consumer goods manufacturer*

> Good job? Of course not. Our network is one of the biggest in the world. We have hundreds of people maintaining it, and it's still a tremendous mess. We have people who have zero networking knowledge who are reviewing and approving network changes. There is nothing that I think we do well.
>
> *Network team manager, Fortune 100 pharmaceutical company*

# Methodology and Demographics

This report combines quantitative and qualitative insights into the general state of network operations in today's enterprises. EMA began this project by interviewing a half-dozen networking professionals from Fortune 500 companies about the state of network operations inside their organizations. These interviewees are quoted anonymously throughout the report. Their response influenced the development of the questionnaire EMA used for the quantitative portion of this research.

EMA surveyaed 409 IT professionals whose roles focus significantly on network infrastructure and operations. EMA's goal was to collect data from a broad cross-section of companies in terms of size, revenue, and industry, as well as the perspectives of people from all levels of the IT organization, from subject matter experts to executives. EMA collected this survey data in March 2022.

### Location

| | |
|---|---|
| **65%** | North America |
| **35%** | Europe |

### Company Size (by employees)

| | |
|---|---|
| **14%** | 100 to 499 |
| **17%** | 500 to 2,499 |
| **62%** | 2,500 to 19,999 |
| **7%** | 20,000 or more |

### Top Industries

| | |
|---|---|
| **27%** | Manufacturing |
| **17%** | Banking/Finance/Insurance |
| **14%** | Energy/Utilities |
| **13%** | Retail |
| **6%** | Professional/Technical services – not related to IT |

### Top Job Titles

| | |
|---|---|
| **34%** | IT/network engineer |
| **17%** | IT/network architect |
| **15%** | CIO/CTO |
| **9%** | IT manager/supervisor |
| **9%** | IT director |

### Top Functional Groups

| | |
|---|---|
| **39%** | Network engineering/architecture |
| **20%** | IT executive suite |
| **10%** | IT architecture |
| **9%** | DevOps |

Figure 2. Demographics

# Key Findings

- The percentage of network operations teams that are successful is in steep decline, from 49% in 2016 to 27% in 2022
- This is the first year that network operations teams have recognized public cloud, SaaS applications, and cloud-native application architectures as the most critical drivers of their network management strategies
- Enterprises that integrate network operations into a cross-domain operations center are more successful than those that keep network operations in a standalone NOC
- When NetOps lives in a cross-domain operations center, network professionals spend more time on strategic projects
- 31% of all IT service problems are reactive. End users report them to IT before NetOps is aware
- Only 34% of alerts from network monitoring tools are actionable
- Network data quality and a shortage of skilled personnel are the biggest challenges to NetOps
- Network managers are interested in SaaS-based network management tools, but they have data security concerns and struggle with legacy tool lock-in
- Only 12.5% of IT organizations find it very easy to hire and retain networking personnel. They are especially struggling to hire people with network security, network automation, and network monitoring skills
- Most companies are multi-cloud today, and their network operations teams are using network tools to monitor the cloud. Only 18% believe there are very effective at cloud monitoring with network tools
- DevOps and NetOps teams are closely collaborating, and in some cases fully integrating. Security policies, application optimization, and network capacity planning are important areas of collaboration
- 96% of corporate networks have or will have Internet of Things devices and sensors connecting to them. IoT is driving investments in network security, network performance monitoring, and network automation

# The Network Operations Team

*The cloud has turned things upside down. Public cloud, cloud-native applications, and SaaS applications have risen to the top of network managers' minds.*

IT organizations take a variety of approaches to network operations. There is the traditional standalone network operations center (NOC), a sort of mission control center for network monitoring and management. Others take a distributed or informal approach in which people contribute to network operations from various discrete groups, such as IT architecture, network engineering, and service management. More recently, cross-domain operations teams have formed, pulling expertise from all aspects of the organization to provide a unified, full-stack approach to monitoring and management of IT services. The way a company organizes around network operations can influence the tools, processes, and procedures that it adopts.

## Drivers of NetOps Strategy

EMA is observing a fundamental shift in what drives enterprise network operations strategies. **Figure 3** reveals the IT initiatives that are influencing network management strategies. Since 2008, the number-one response to this question has always been server virtualization, which suggests an intense focus on addressing the rise of east-west traffic in data centers. This year, virtualization dropped to fourteenth on this list. What happened? The cloud has turned things upside down. Public cloud, cloud-native applications, and SaaS applications have risen to the top of network managers' minds. Members of a network engineering team were extremely likely to single out public cloud and SaaS applications. Data center modernization also eclipsed server virtualization, due in part to a shift toward hybrid cloud.

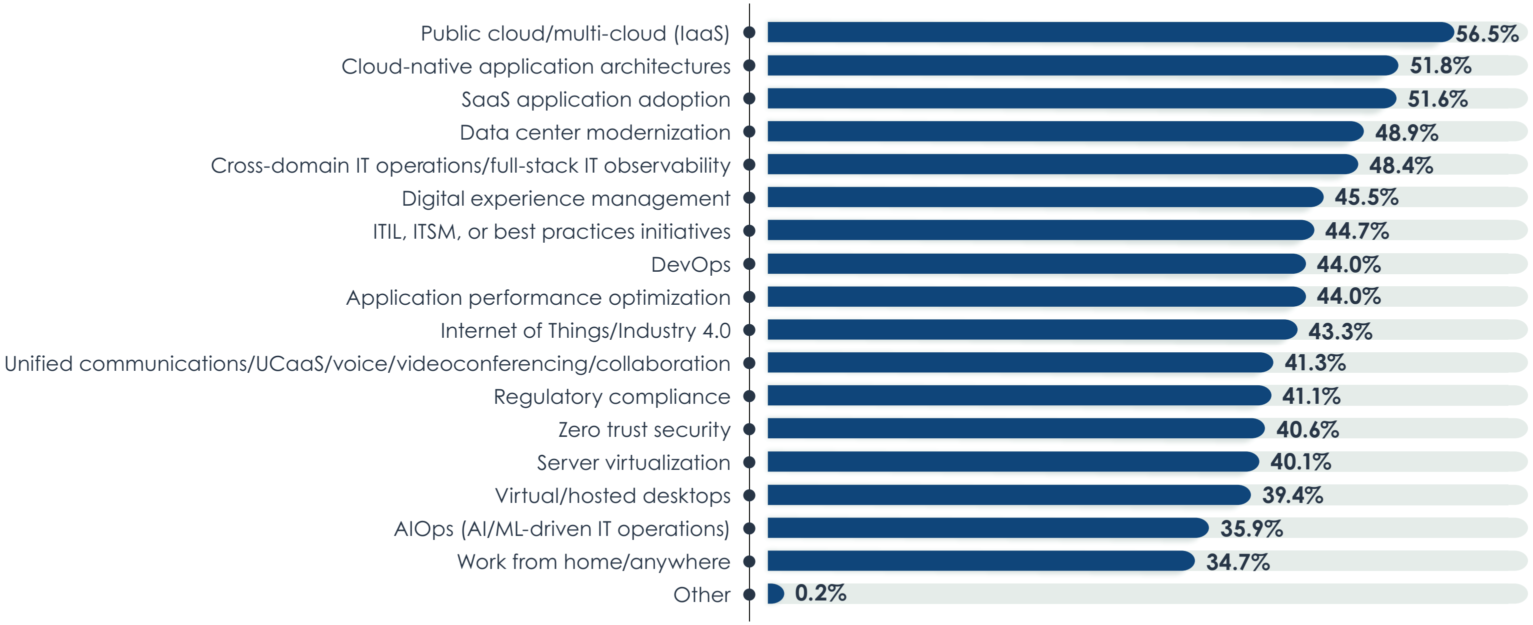

Figure 3. IT initiatives that are driving current priorities in monitoring/managing networks

Sample Size = 409,
Valid Cases = 409,
Total Mentions = 3,076

"We had to shift to cloud-first," said a network team manager with a Fortune 100 pharmaceutical company. "Instead of data centers, we are using colocation data centers, where we will shut down our data centers and move to colos with 10% of the original footprint. The rest just goes to the cloud, and we have to work on connectivity services and a DMZ for security between the cloud and colos."

Two years ago, IoT was the second-highest driver of network management strategies, but this year it's waned to a low secondary driver. However, the IT executive suite, network engineering, and the NOC all identified it as a major influence.

The influence of ITIL and other best practice initiatives, as well as unified communications and collaboration technologies, has doubled since 2020. Both were afterthoughts before this year. Members of network engineering teams listed ITIL as one of their top priorities, suggesting a desire to implement best practices around network engineering and operations.

Members of network engineering teams and DevOps teams are also very focused on zero trust security in 2022. "With everyone working from home, we're trying to determine where we hold the line of our perimeter since it's not the office anymore," said a network security architect with a large American bank. "We're waiting to see how network access control vendors adjust to working from home. Right now, a lot of heavy lifting is being done on VPN concentrators, and they weren't built do this so much of this."

SaaS applications and application performance optimization drive the most successful network teams, while less successful teams focus more on digital experience management.

**Figure 4** examines the network technology investments that are influencing network management strategy. Network security is the top driver, as it was in 2020.

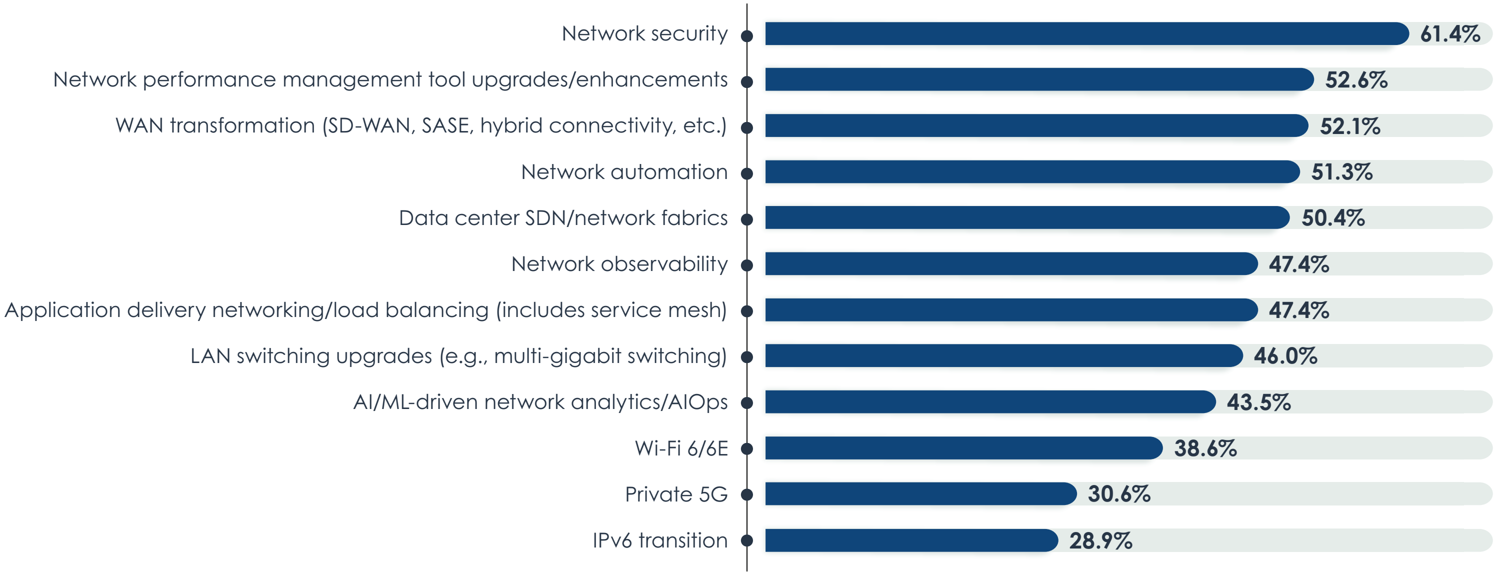

Figure 4. Networking technology initiatives/investments that are driving organization's current priorities in monitoring/managing networks

Sample Size = 409, Valid Cases = 409, Total Mentions = 2,250

*Enterprises with a cross-domain operations team were the most likely to be successful with network operations. Organizations that relied on a NOC were less successful.*

Most companies are also making investments in network performance management tools, WAN transformation, network automation, and data center SDN. WAN transformation was a minor driver two years ago, but now dominates the enterprise networking world. Larger companies are the most influenced by WAN transformation. Larger companies are also more likely to invest in Wi-Fi 6/6E and private 5G.

Network observability, application delivery networking, and LAN switching upgrades are the chief tertiary priorities. Network observability is an emerging concept that EMA expects will merge with and drive the network performance management industry in the future. Members of DevOps teams were the most likely to select network observability, which is unsurprising since DevOps groups are much more familiar with the concept than most traditional networking teams.

## Organizing NetOps

**Figure 5** reveals how enterprises generally organize network operations today. The majority have formed operations centers, with more than one-third using a traditional NOC and the rest using a cross-domain operations team. A smaller number take a distributed, informal approach to network operations. Fifteen percent are primarily outsourcing the function. The smallest companies were the most likely to outsource, and the largest companies were the most likely to have a NOC. The size of a network also had some correlation with organizational strategy. The smallest networks (15 to 149 network devices) were the most likely to outsource operations. Midsized networks (150 to 999 devices) tended to have a NOC. The largest networks (1,000 or more) often had a cross-domain operations team.

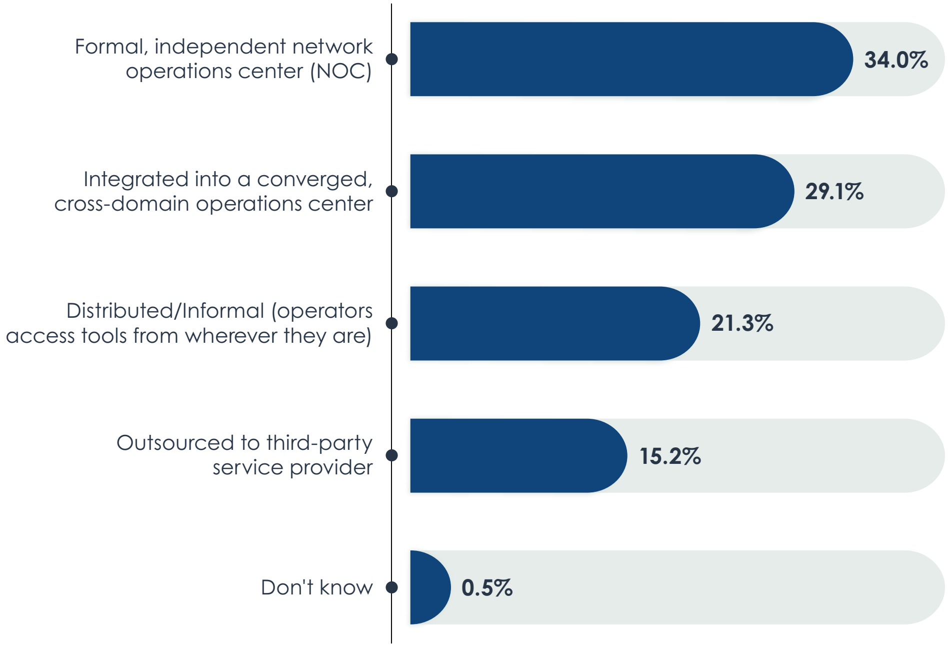

Figure 5. Overall approach to conducting network monitoring and management

The cross-domain operations team appears to be a potential best practice. Enterprises with a cross-domain operations team were the most likely to be successful with network operations. Organizations that relied on a NOC were less successful. EMA believes that cross-domain operations strategies will become more important as enterprises expand their use of the cloud. Network teams often struggle to have an equal voice in discussions about architecture and operations in the cloud. A traditional NOC will be at a disadvantage, but a cross-domain operations team may have more creditability, given its ability to bring a broad set of expertise to the table.

Sample Size = 409

# Addressing Network Trouble

## Detecting Network Trouble

In the average IT organization, end users detect and report 31% of all service problems before network operations teams are aware of them. **Figure 6** shows the results when EMA asked respondents to estimate how many IT service problems are first reported by end users, as opposed to being recognized proactively by network operations. This means that 31% of all IT service problems are already impacting end users before IT can react. While the network operations team goes into firefighting mode, productivity is already down, business processes are disrupted, and customers are inconvenienced.

This situation has improved in recent years. In 2020, end users detected 33% of IT service problems and they detected 40% in 2018. This looks like progress. However, it's occurring while overall network operations success is in decline.

## Root Causes of Complex Problems

EMA believes that network operations teams are struggling partially because of increased overall complexity in IT infrastructure and services. This is evident in **Figure 7**. EMA asked research respondents to identify the root cause of the last three complex IT service issues that forced network operations to collaborate across IT silos. Since 2016, the top response to this question has been the network. This year, security incidents, client devices, and user errors eclipsed the network.

The complexity introduced by the massive rise in remote work could be part of this shift. Home offices are extremely vulnerable to user error, for instance, where users have exclusive access to the WAN edge device and the local area network. Remote work also introduced new vectors for security incidents. Organizations with a NOC were less likely to cite security incidents as a root cause of trouble. Operators of larger networks were more likely to cite security incidents.

External service providers are also a frequent source of trouble. This points to the rise of cloud adoption and internet connectivity, two places where network operations have less visibility. When these providers have problems, tracing the problem can be impossible. Organizations with a cross-domain operations center were more likely than those with a NOC to cite external providers as a root cause.

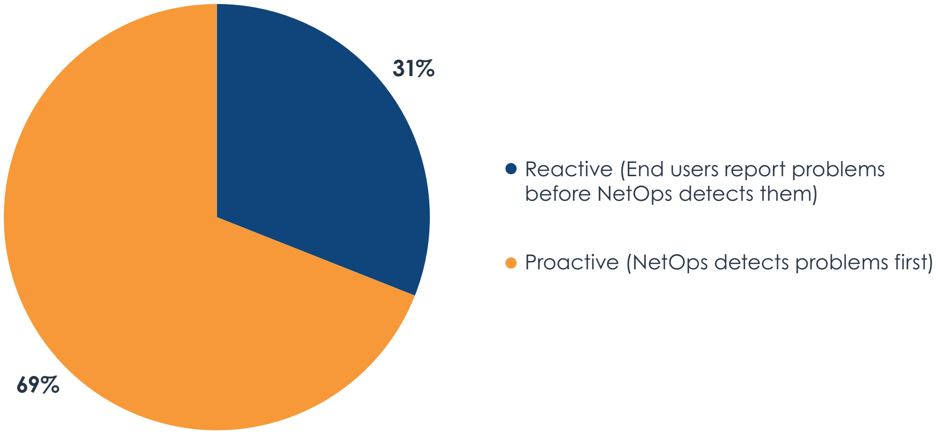

Figure 6. NetOps and detection of IT service problems: reactive vs. proactive

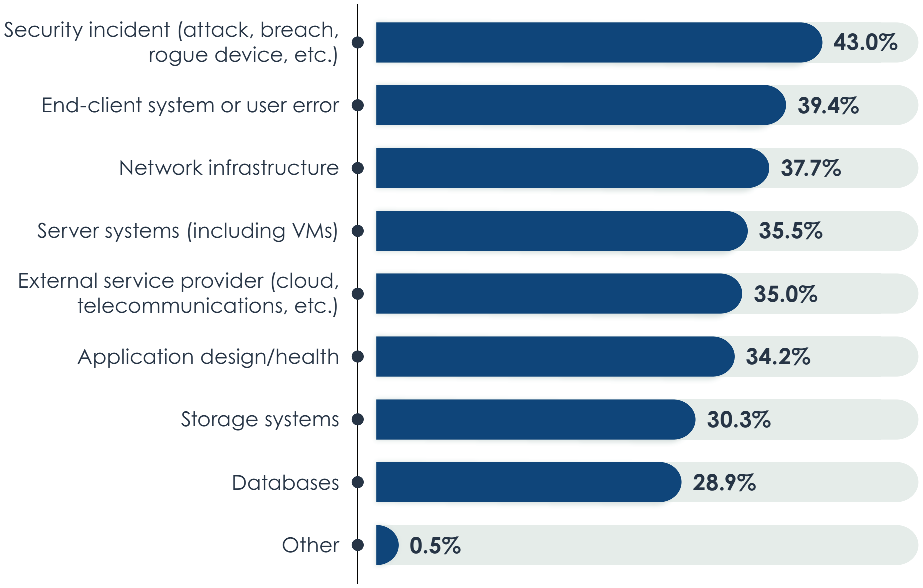

Figure 7. Root causes of the last three complex IT service issues that forced network operations to collaborate with other groups

Sample Size = 409, Valid Cases = 409, Total Mentions = 1,163

# Broken Processes and Tools

## Manual Errors

Network management is a highly manual profession. Network engineers often perform critical work within the command line interface (CLI) of network devices. For instance, network engineers often reconfigure switches and routers in CLI. These manual processes are highly susceptible to user error. On average, survey respondents in this research told EMA that manual administrative errors, such as a bad configuration change, cause 27% of all network problems. This number is up very slightly from 26% in 2020.

**Figure 8** shows that network management tool sprawl has a strong correlation with negative outcomes. Organizations with 21 or more network management tools have the highest percentage of problems caused by manual errors, while organizations with just one to three tools have the lowest percentage. EMA suspects there are several issues behind these numbers. A large toolset could encourage poor processes and policies around change controls because these tools will have overlapping capabilities around network changes that make such controls impossible to impose. Also, a fractured toolset leads to poor overall visibility into network data. For instance, a network team with 20 or 30 tools might have more than one repository for configuration data. Network admins might accidentally consult the wrong source when making a change. All of this points to the need to consolidate network management tools as much as possible.

*Manual administrative errors cause 27% of all network problems.*

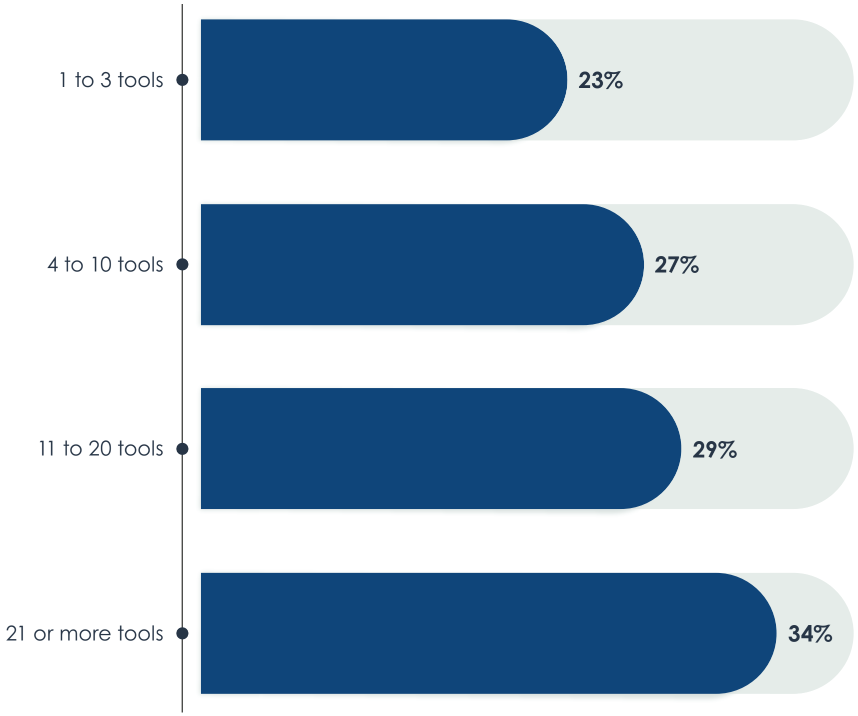

Figure 8. Percentage of network-related problems caused by manual administrative errors, by number of network management tools

Sample Size = 409

## Alert Fatigue

Network monitoring tools are infamous for producing floods of alarms and alerts. For instance, one bad interface on a network device might trigger a series of alerts associated with five, ten, or even hundreds of other devices that have a dependency on that failed interface. Network monitoring tool vendors often try to differentiate themselves by developing features that minimize this issue, such as topology-based alarm suppression.

The network management toolsets represented in this survey is not doing so well on this issue—and things are getting worse. **Figure 9** reveals that only 34% of alerts generated by network monitoring tools are actionable in 2022, down from 43% in 2020. In other words, only 66% of all alerts are indicative of a real problem.

EMA found that larger revenue companies were worse off than smaller revenue companies. Companies with more revenue in this research tended to have more network management tools and larger networks. This may help explain the problems that richer companies are having.

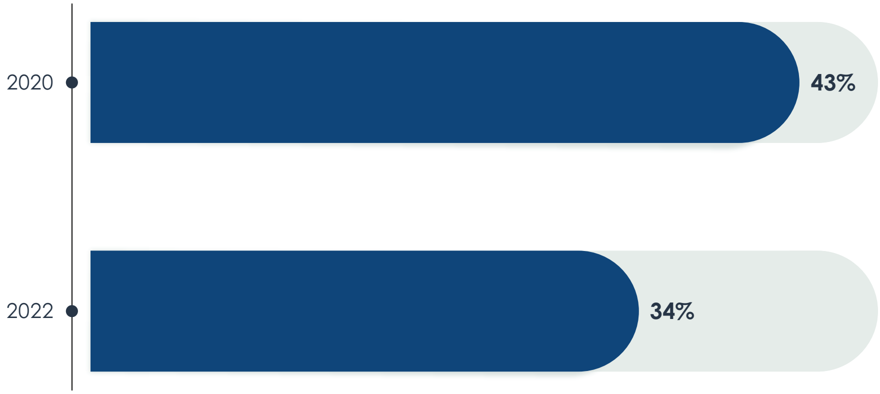

Figure 9. Percentage of the alerts produced by network monitoring tools that are actionable (indicative of a real problem)

## Can Better Tools Help?

EMA asked research respondents to estimate what percentage of network-related problems could be prevented with better network management tools. The mean response was 44%. In other words, network operations professionals believe they could reduce network problems by nearly half if they had better management tools.

Respondents in North America saw a bigger opportunity from improved management tools than Europeans. People who work within IT architecture and IT project and program management were more bullish on this idea than people who work in cloud architecture and operations and data center operations. EMA believes that network teams have a tremendous opportunity to improve operations if they can find the budgets and the time to optimize their toolsets.

*Network operations professionals believe they could reduce network problems by nearly half if they had better management tools.*

# NetOps Success and Failure

Let's revisit the statistics around self-reported network operations success and dig a little deeper into the numbers. **Figure 10** reveals that only 27% of enterprises have a fully successful network operations team.

Network teams with larger network management toolsets are feeling more confident about success than those with smaller toolsets. This is counterintuitive and conflicts with EMA's overall recommendations for consolidating and optimizing toolsets. However, this is also a trend EMA observed for several years in the data. Still, we see indicators of trouble between the lines. Network teams with larger toolsets have more problems with manual errors, for instance. They were reported a high number of IT service problems caused by manual errors in network administration.

Network engineers and CIOs are less enthusiastic about success than network architects. Europeans are less enthused than North Americans. Members of network engineering and cloud engineering teams are less sanguine than the IT executive suite.

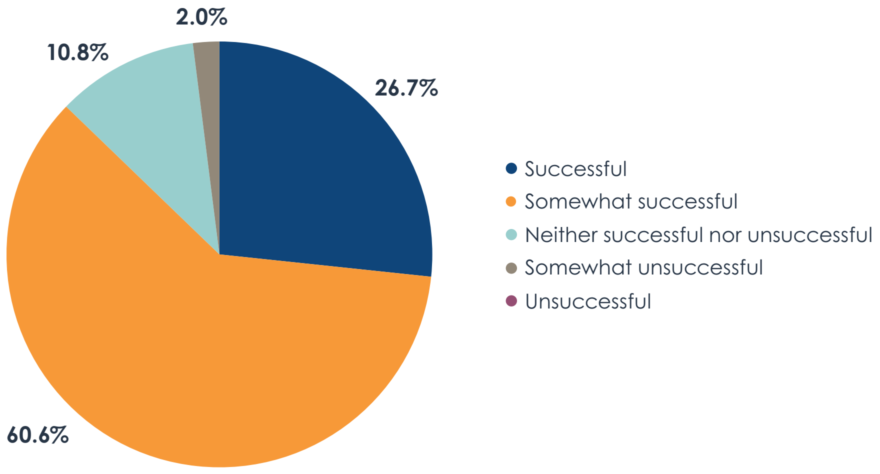

Figure 10. Respondents rate the overall success of their network operations organization over the past year

Sample Size = 409

*The two biggest issues that challenge network operations teams today are network data quality and a shortage of skilled personnel.*

**Figure 11** reveals the issues that are most challenging for network operations teams today. The two biggest issues are network data quality and a shortage of skilled personnel. The personnel issue is especially problematic for SMBs and midsized enterprises. We will explore this issue in greater depth in the Megatrends section. EMA believes this is an endemic problem that is undermining most companies today. The IT executive suite, the cloud group, and the IT architecture group are all more likely to perceive an issue with data quality. Network engineering is less concerned.

A lack of network use policies, poorly implemented infrastructure projects, and poor cross-domain collaboration are the main secondary issues. Less effective network operations teams identified bad infrastructure projects as their biggest issue. It's also an issue in general for larger companies, which are more likely to struggle with cross-domain collaboration and end-to-end network visibility. Smaller companies are struggling more with a lack of budget.

A network team manager with a Fortune 100 pharmaceutical company said he is struggling with a combination of poorly implemented infrastructure and a lack of end-to-end visibility, a consequence of complexity created by mergers and acquisitions. "We perform 15 to 30 acquisitions a year. We buy a company and absorb their network. Sometimes we rip and replace and other times we just provide connectivity and standardize later when there is time. These acquisitions have created all these snowflake topologies."

Large toolsets (fragmentation of tools) are generally a minor issue. However, network operations teams with very larger toolsets are struggling more with data quality and with cross-domain collaboration, suggesting that network teams need to optimize these large toolsets to address these issues. The IT governance group (asset management, financial management) identified tool sprawl as their top issue.

NOC staff singled out a lack of defined processes as a major problem. Network engineering team members pointed to a lack of change management controls.

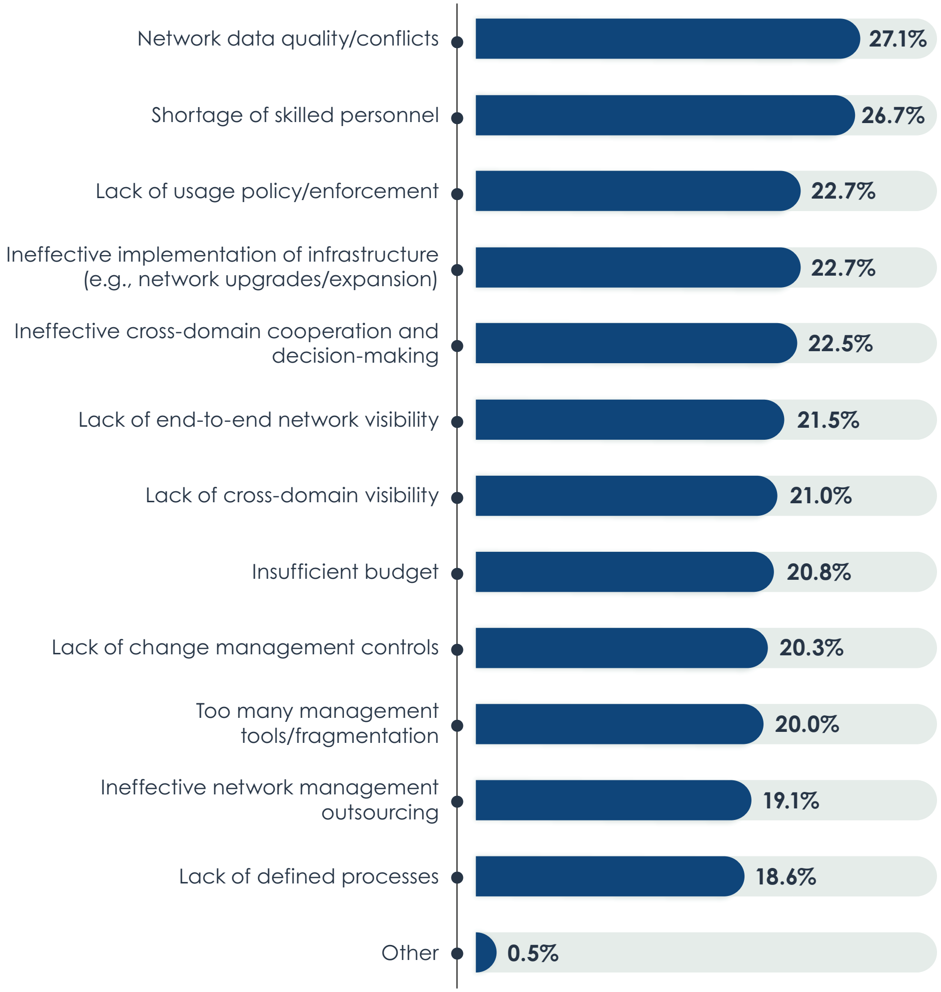

Figure 11. Biggest challenges to success for network operations

Sample Size = 409, Valid Cases = 409, Total Mentions = 1,078

# Network Management Tool Strategies

# Large Toolsets are the Norm

Although many network management tools are multifunction solutions that address a variety of use cases and workflows, EMA has long found that most network operations teams use large, fragmented toolsets. **Figure 12** reveals that the network team has anywhere from 4 to 15 tools. It is very rare for a network team to have fewer than four tools.

*The network team has anywhere from 4 to 15 tools.*

"We're close to 20 tools and six or eight vendors," said an IT operations manager with one of the world's largest government agencies. "Some of those tools don't have a lot of people using them because they are specialized, maybe for a specific vendor."

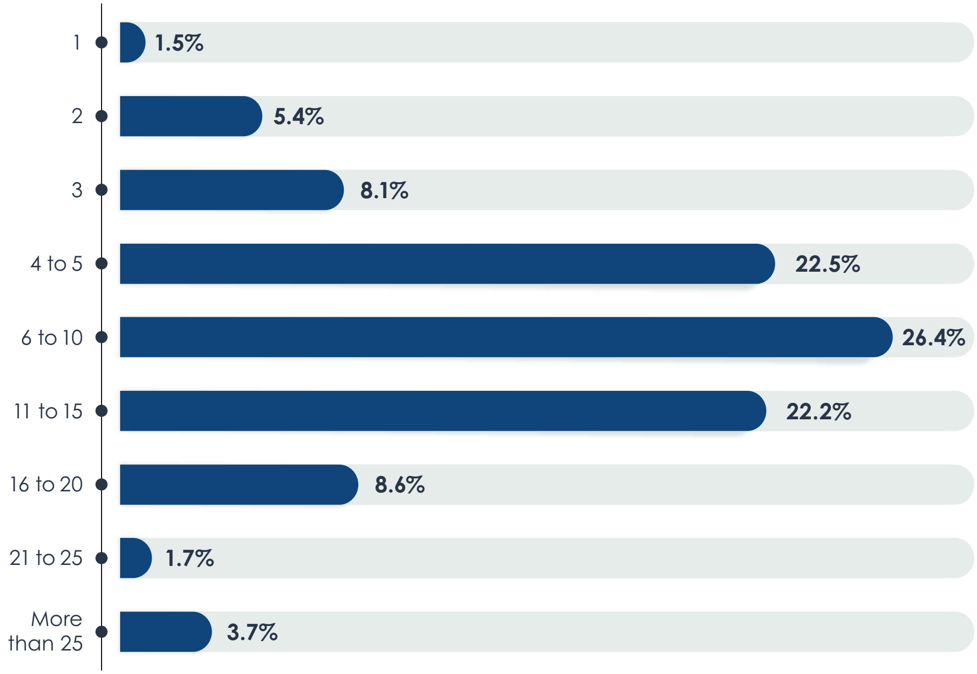

Figure 12. Total number of tools organizations use to manage, monitor, and troubleshoot networks

Sample Size = 409

# Deployment Preferences

Network operations teams are no longer married to on-premises management tools. **Figure 13** reveals that only 29% of network teams prefer an on-premises deployment of a network management tool. Instead, nearly 44% want to deploy tools in the cloud, and 29% prefer a SaaS solution from their management vendors. The least successful network operations teams in this research had a very strong preference for on-premises tools. Larger companies and operators of larger networks preferred SaaS deployments, while smaller companies and operators of smaller networks preferred cloud-based deployments.

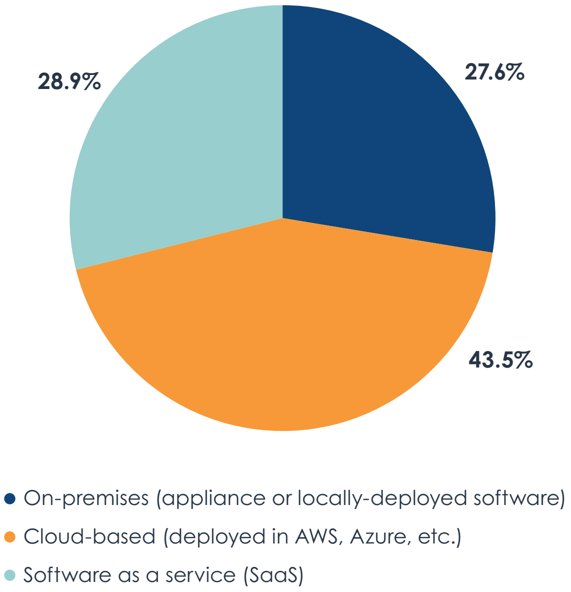

Figure 13. Preferred deployment model for network management tools

"As the guy who is implementing it, everything should be in the cloud," said a network team manager with a Fortune 100 pharmaceutical company. "As a network guy, I don't want to be involved in spinning up a VM, patching servers, dealing with tool upgrades. There is a tremendously complicated process here for requesting a VM, spinning up a tool, and paying for the bill-back. It can take three of four months. In the cloud, it's up and running fast. But then the battle is around security. Information security doesn't like it."

> *"I like SaaS-based tools because patching is a huge effort," said a network security architect with a large American bank. "Keeping up with maintenance is a huge pain."*

"I like SaaS-based tools because patching is a huge effort," said a network security architect with a large American bank. "Keeping up with maintenance is a huge pain. Anything that can offload it to the software providers is a benefit. At my previous job, we had people devoted only to patching tools."

An IT operations manager with one of the world's largest government agencies explained why he remains one of the 28% who stick with on-premises tools. "When it comes to the keys to your kingdom, you hold them close. Until we hand over our networks to a vendor, it stays in-house. I'd also like to keep anything in-house that handles certificates and domain logins."

Sample Size = 409

With SaaS emerging as the future of network management tool consumption, EMA asked respondents to identify their top requirements for SaaS-based tool delivery. **Figure 14** reveals two major considerations for buyers. They want assurances around platform security and they want the ability to integrate SaaS tools with their other management tools, whether those tools are on-premises or in the cloud. IT executives were especially focused on platform security.

The top secondary requirements are scalability and simplicity of data retention, rapid implementation, and easy-to-find pricing and licensing terms. Data retention is more important to larger revenue companies, while rapid implementation is more important to smaller revenue companies.

"The preference is now SaaS," said a network engineer with a Fortune 100 consumer goods manufacturer. "It's for savings, but also faster deployment, and you can scale it easier."

Resiliency is a low priority overall. People who work within a NOC selected it as one of their top priorities, while members of DevOps teams were least likely to focus on it. Iterative product cycles in which new features are rolled out without software upgrades especially appeal to members of network engineering and architecture groups. People who work in IT executive suites did not see the value of this.

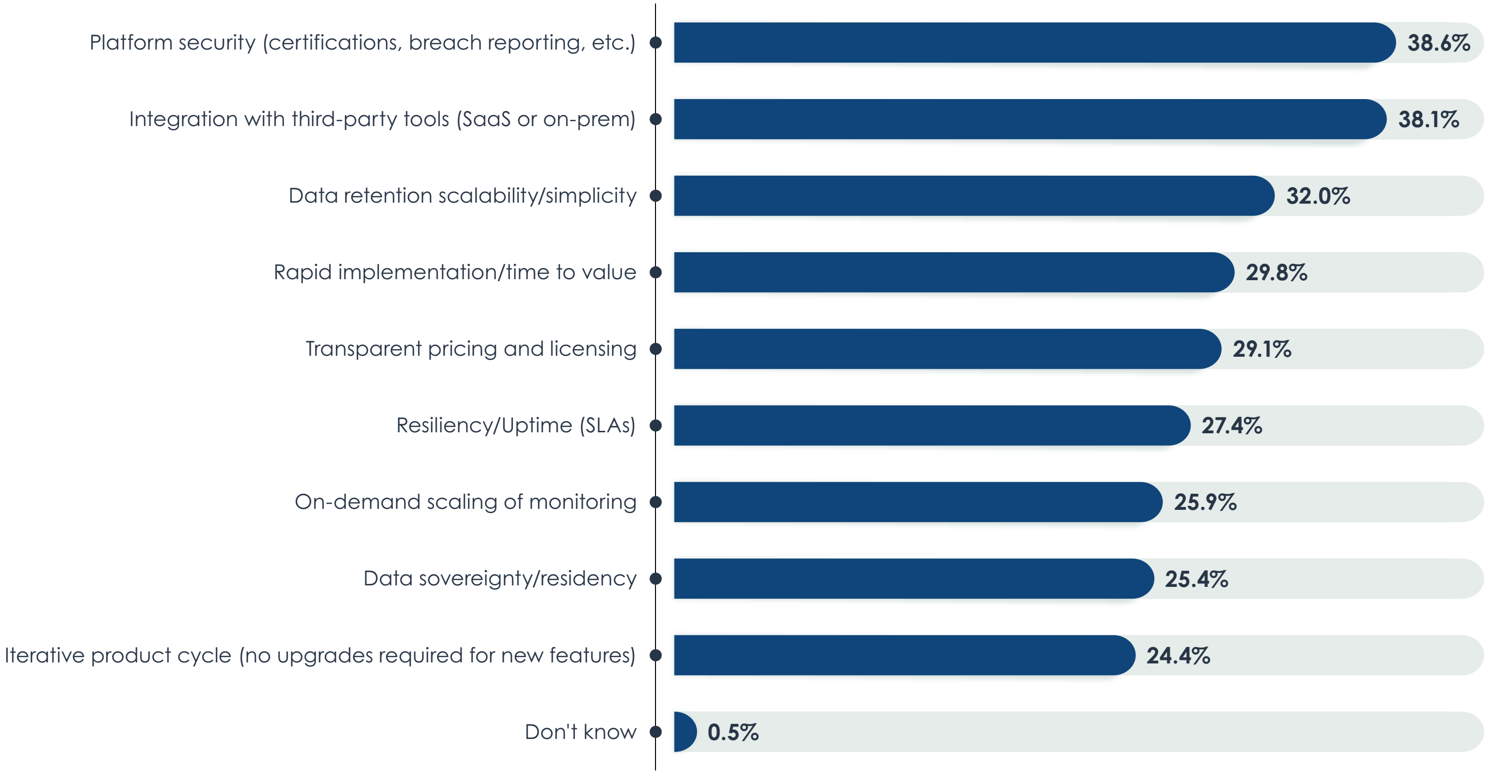

Figure 14. Most important characteristics of a SaaS-based network management tool

Sample Size = 409,
Valid Cases = 409,
Total Mentions = 1,110

# Tool Requirements

## Platform Characteristics

**Figure 15** reveals that the top three general platform and business requirements for management tools are integrations with other systems, ease of use, and low maintenance and support costs. Very large enterprises are especially concerned with integrations. SMBs are concerned most with ease of use. Organizations with large network management toolsets are the most likely to require tool integrations. Those with smaller toolsets want low maintenance and supports costs as well as ease of use. Ease of use is very important to lower-skilled admins and IT executives, but of little interest to network engineers and architects.

Rapid ROI, strong customer support, flexible deployment options, and tool resilience and stability are the chief secondary requirements.

"The deal-breaker for us is the support model," said a network team manager for a Fortune 100 pharmaceutical company. "What's the footprint? Do they have a presence in every single region, or just running on California time for eight or nine hours? Do I have a phone number to call, or do I just send an email and pray that I will get a response?"

Multi-vendor infrastructure support and role-based access control (RBAC) are the lowest priorities. However, successful network management teams make RBAC a priority, suggesting that they have a wider variety of users accessing their tools. Engineers and architects believe multi-vendor support is very important, but IT executives are unlikely to feel that way.

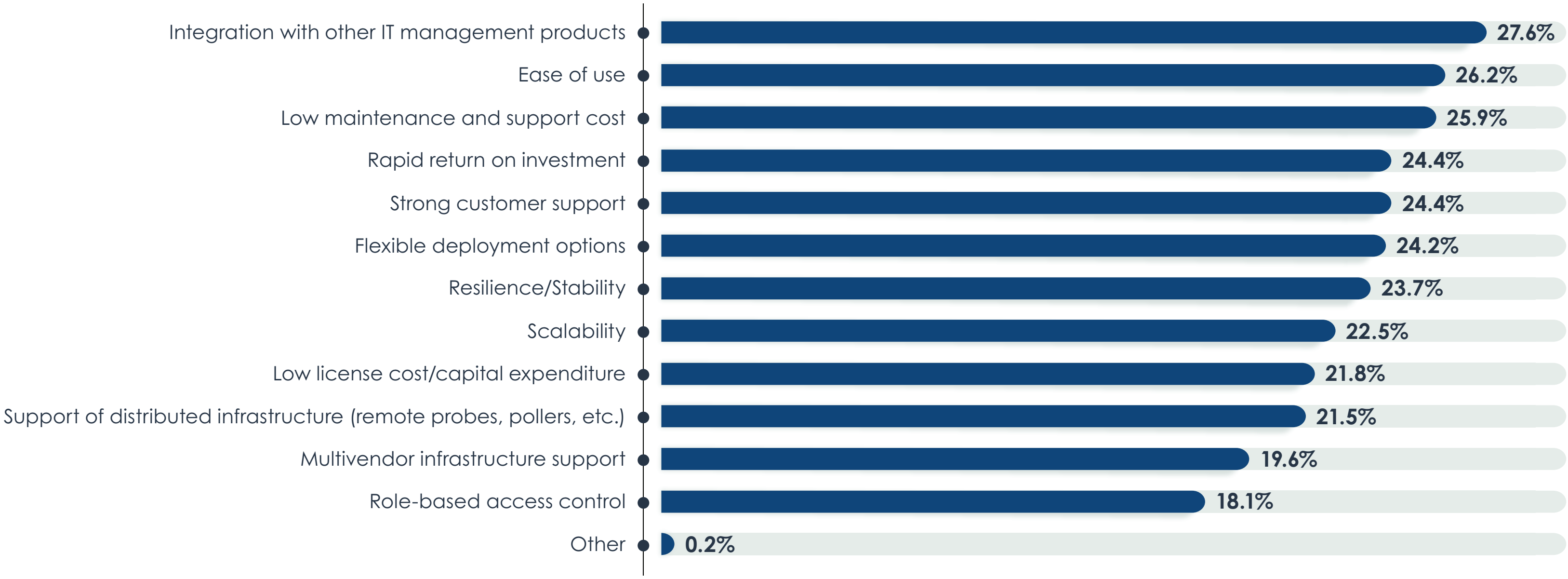

Figure 15. Top business and platform requirements for network management products

Sample Size = 409, Valid Cases = 409, Total Mentions = 1,146

## General Feature Requirements

**Figure 16** identifies the top general features requirements that IT organizations are looking for in network management tools. Four features top the list. They need integrated security insights, integrated collaboration tools and workflows, customizable reporting and dashboards, and mapping and visualization of data. Managers of smaller networks seek collaboration tools, mapping, and visualization.

Compliance scorecards and reports are a low product feature priority, but the most successful network operations teams make them a top feature priority. Service dependency mapping is a middling priority, but very large enterprises (20,000 or more employees) consider it essential. Members of DevOps teams also prioritize it.

*Compliance scorecards and reports are a low product feature priority, but the most successful network operations teams make them a top feature priority.*

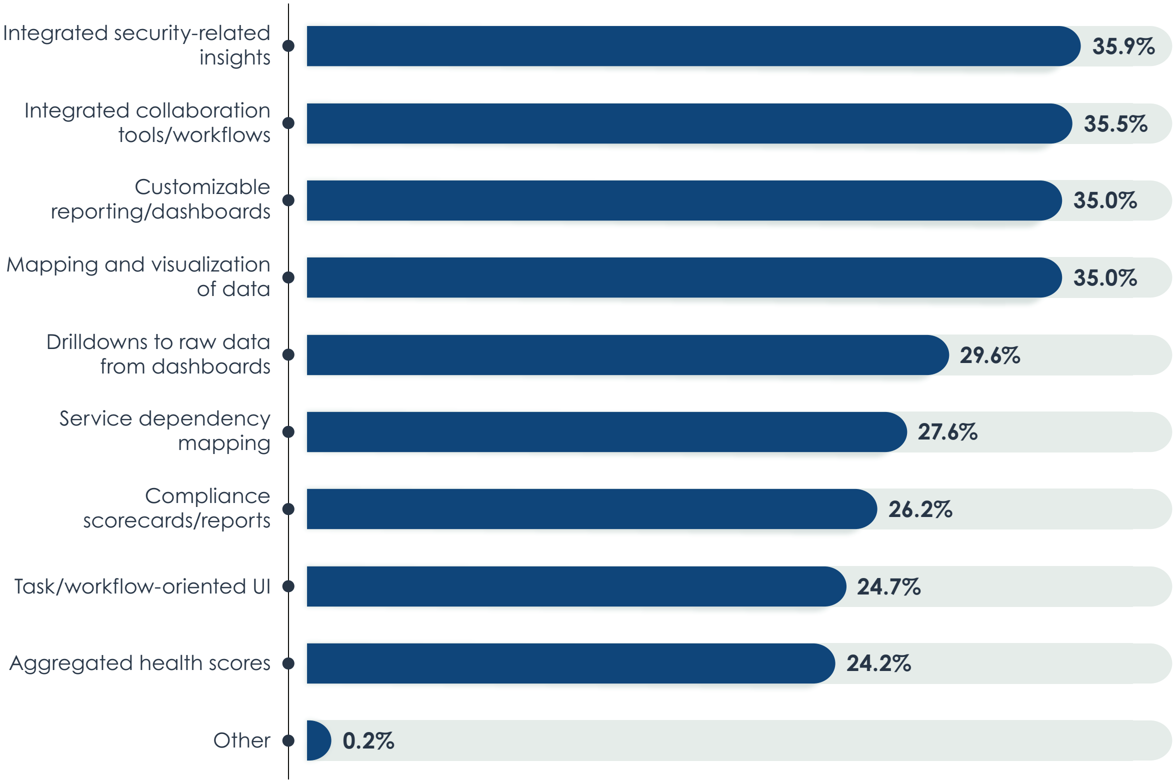

Figure 16. General network management tool features that are most important and useful

Sample Size = 409, Valid Cases = 409, Total Mentions = 1,120

## Packet Monitoring Preferences

Network packets are an excellent source of network performance data. Packet monitoring tools can deliver high-precision insights into application performance if they are intelligent enough to analyze application-layer information in packets (Layers 5, 6, and 7). Other tools focus solely on network performance, diving no deeper than Layer 4. This latter approach gives insight into the health and performance of network sessions established with transport protocols, such as TCP and UDP. EMA found that network operations teams have one of two philosophies when it comes packet-based performance monitoring. Either they focus on the network layer and leave application performance to a different team, or they manage networks from an application performance perspective. **Figure 17** reveals the current mix of perspectives on this issue. More than half prefer an application-layer packet monitoring tool. A minority prefer a network-layer view into packet-based performance.

Layer 7 intelligence can be expensive. Thus, larger companies in this survey were more likely to prefer application-centric tools. Engineers and architects were more likely to value Layer 7 tools, while lower-skilled admins were content with Layer 4 tools.

EMA analysis revealed that network operations teams that are focused on application performance optimization are more likely to seek Layer 7 intelligence from packet monitoring tools.

*Network operations teams that are focused on application performance optimization are more likely to seek Layer 7 intelligence from packet monitoring tools.*

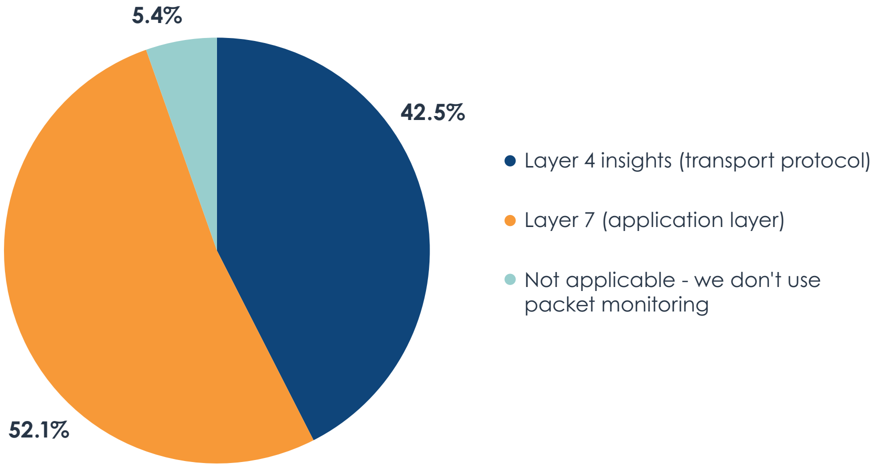

Figure 17. Preferences for the depth of insight provided by packet-based network performance monitoring tools

Sample Size = 409

# Megatrend #1: Networking Brain Drain

EMA believes that a shortage of skilled networking personnel is contributing to the lack of success many enterprises are experiencing with network operations. **Figure 18** illustrates this issue. Only 12.5% of enterprises believe it is very easy to hire and retain skilled networking professionals, meaning most companies see room for improvement with staffing. Nearly 37% claim it is somewhat easy, but things could be better. More than 26% are having true difficulty with staffing. A deeper analysis of the data found that IT organizations that struggle with hiring are less likely to report overall success with network operations. The data also revealed that companies that struggle with hiring tend to outsource network operations.

"We've had some security positions that were very difficult to hire for," said a network security architect for a large American bank. "It seems like there is not a lot of talented people applying. From my experience, when there are turbulent times, a lot of talent sits tight."

Smaller companies struggle more than larger companies with hiring. European companies struggle more than companies in North America.

*Only 12.5% of enterprises believe it is very easy to hire and retain skilled networking professionals. IT organizations that struggle with hiring are less likely to report overall success with network operations.*

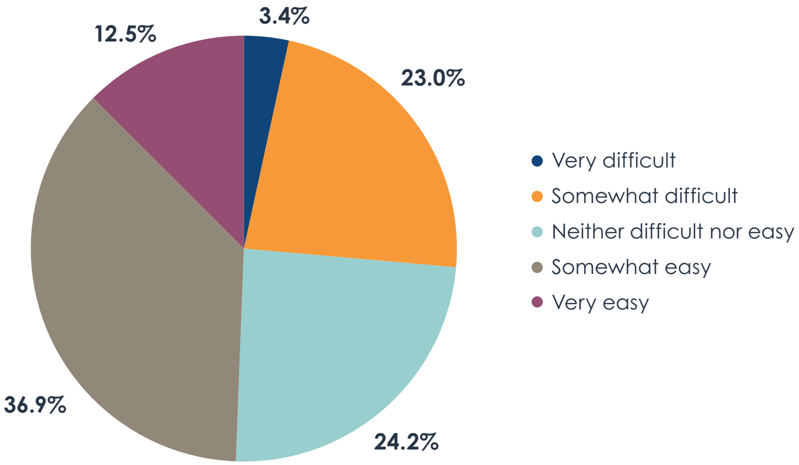

Figure 18. Does your organization find it difficult or easy to hire and retain personnel with network technology expertise?

Sample Size = 409

# Why Hiring is Difficult

**Figure 19** reveals the challenges that companies encounter when they try to hire networking professionals. All respondents were asked this question, regardless of whether they indicated in the previous question that they considered it difficult or easy to hire and retain people. Note that overall, 98% of these respondents identified at least one issue that makes hiring a challenge, which is far higher than the number of people who admitted that hiring is difficult.

Overall, the biggest issue is a technical skills among the available talent pool. Companies are struggling to find people with specialized networking skills. Organizations that maintain a standalone NOC or a cross-domain operations center are both struggling with this issue more often than organizations that take a distributed and informal approach to network operations.

The chart reveals that five secondary challenges are impacting hiring equally, starting with COVID-related issues. COVID-related difficulties are hitting higher-revenue companies harder than lower-revenue companies. “Before the pandemic, there was no issue,” said a network engineer with a Fortune 100 consumer goods manufacturer. “It is hard because we have limited travel. As a global company, if someone based in Costa Rica needs to fly to the US for a job, it’s not possible.”

Benefits expectations, leadership’s desire for a lean staff, inexperienced talent pools, and long hiring processes are all big issues, too. Benefits expectations hit lower-revenue companies harder. Leadership’s preference for a lean network operations team is an issue for very large enterprises (20,000 or more employees), but not an issue for SMBs (100 to 499 employees). The inexperienced, junior talent pool tends to hit midmarket companies the hardest. It also impacts companies that outsource network operations.

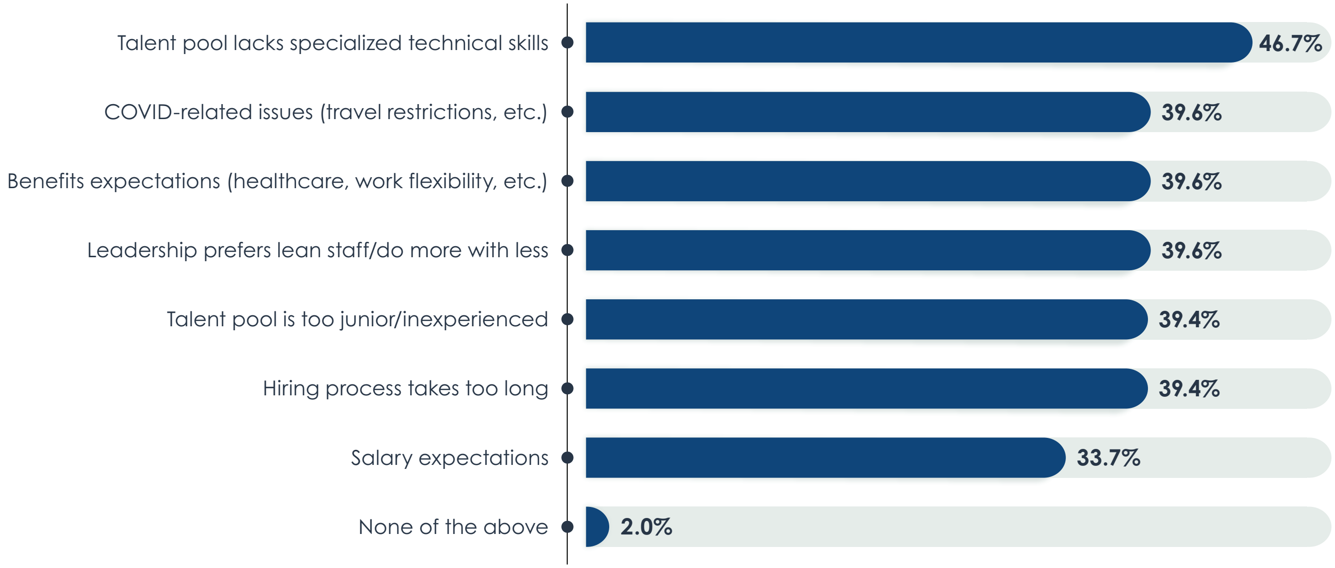

Figure 19. Top challenges to hiring personnel with network technology expertise

Sample Size = 409, Valid Cases = 409, Total Mentions = 1,145

# Can Network Management Tools Help?

EMA research has often found that an effective network management toolset will make network operations teams more efficient and effective. To some degree, improved efficiency should help mitigate shortages in skilled networking personnel.

**Figure 20** reveals that more than 78% of IT professionals at least somewhat agree that network automation tools can mitigate challenges associated with understaffed network teams. Only 22% strongly agree with this idea. Previous EMA research found that operational efficiency is the top benefit that IT organizations pursue with network automation investments. They expect the tools to reduce the amount of time personnel spend on repetitive tasks.

"The more you automate, the less human intervention is needed," said a network engineer who has worked for two Fortune 500 financial companies over the last decade. "You might have a gold standard that engineers created. It removes any typos and mistakes. On the flipside, I've seen automation freeing up those engineers so they don't have to track down an issue."

Organizations that struggle the most with hiring networking personnel are the least likely to believe automation can help. IT and network architects and network engineers are more convinced than middle managers and executives to believe in automation, which is a positive argument in favor of the notion since engineers and architects are usually the ones implementing and working closely with network automation tools. They use a tool to automatically solve problems.

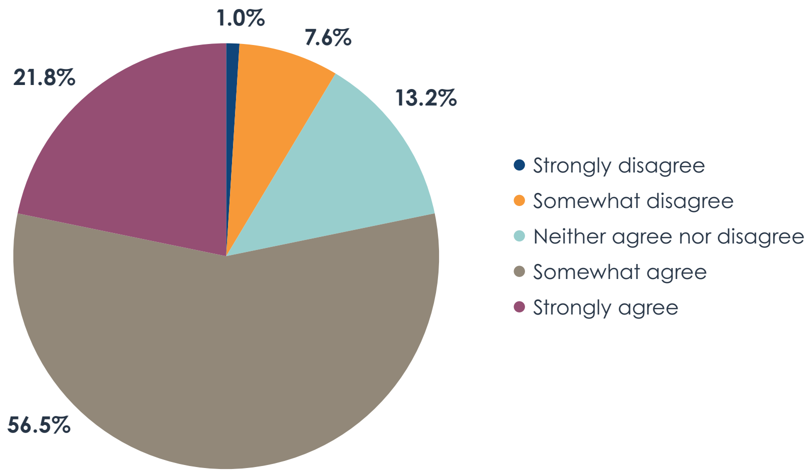

Figure 20. Do you agree or disagree with the following statement? Network automation tools can mitigate the challenges associated with a lack of skilled networking personnel.

Sample Size = 409

**Figure 21** reveals that 77% at least somewhat agree that a modern network performance management tool can mitigate a personnel shortage. Only 22% agree strongly with the idea. In its interactions with network operations professionals, EMA has seen evidence that such a tool can help.

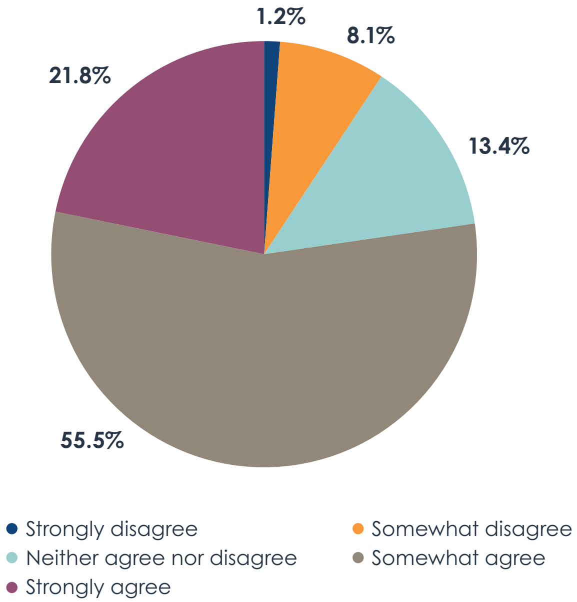

Figure 21. Do you agree or disagree with the following statement? A modern network performance management tool can mitigate the challenges associated with a lack of skilled networking personnel.

Sample Size = 409

Organizations that struggle the least with hiring are also the least convinced that a network performance management solution can help. North Americans are more likely to agree with this idea than Europeans.

# EMA Advice

Companies that struggle with hiring have several distinct priorities for their network operations toolsets. EMA suspects that these organizations are trying to compensate for their lack of personnel by adopting tools with specific capabilities. If you are struggling with hiring, the following list of capabilities may help. These organizations are more likely to require the following from their network operations tool vendors:

- Integrated security insights
- Strong mapping and visualization of data
- Layer 7 (application layer) visibility from packet monitoring tools
- Network usage policy enforcement
- Tools that emphasize proactive problem prevention
- Better features and workflows for
    - Alarms and escalations
    - Problem isolation
    - Root-cause analysis

Finally, here is some advice from a couple of network operations leaders.

- IT operations manager at one of the world's largest government agencies: "It's important to have someone with a decent IQ and a willingness to learn. A good personality is way more important than knowing absolutely everything about technology. You can train someone who is new, give them experience and responsibility. If they want that, then it works out great."
- Network team manager at a Fortune 100 pharmaceutical: "I'm not looking for specific skills. I look for potential. I ask, 'What have you done?' Based on that answer, if he understands technically what he has done on the job, I believe he can learn to work on a new technology. We don't often hire for top-tier skills in a very specific technology. We're just looking for general networking skills."

# Megatrend #2: Multi-Cloud Ubiquity and Network Operations

Nearly 99% of the enterprises in this survey have adopted the public cloud. More significantly, 72% have moved into a multi-cloud strategy, using at least two infrastructure as a service (IaaS) providers, as **Figure 22** demonstrates. The chart also reveals that nearly 88% of companies will be multi-cloud within two years, with more than 47% expecting to have three or more providers. Larger companies (by employee count and revenue) are the most likely to be multi-cloud today, and smaller companies are the most likely to have a single cloud provider.

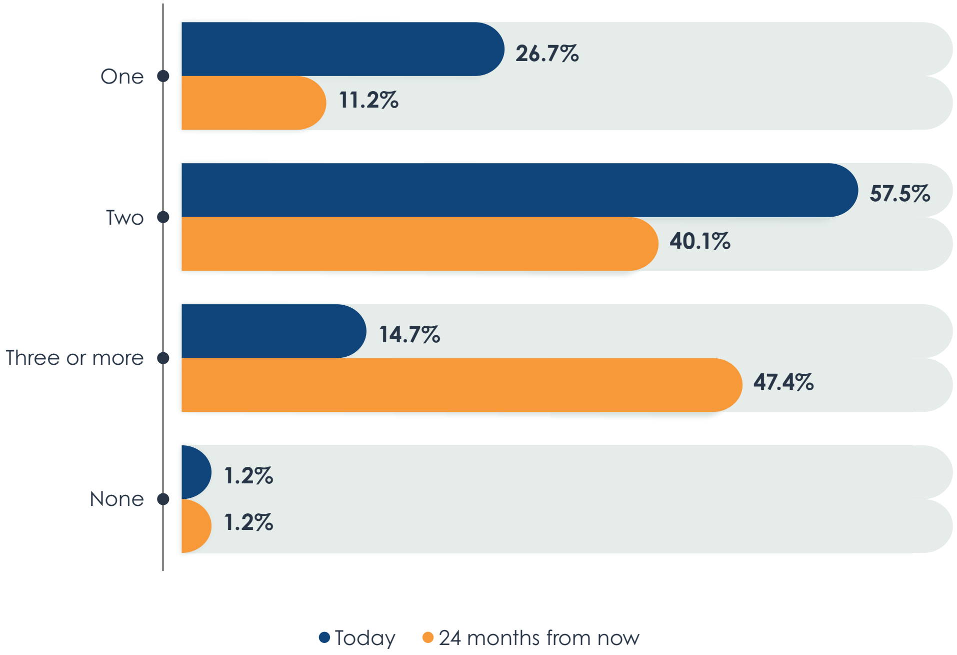

Figure 22. Number of infrastructure as a service (IaaS) cloud providers used today versus in 24 months

Other EMA research recently determined that there are two primary drivers for multi-cloud adoption. IT organizations are trying to optimize performance by distributing cloud workloads closer to end users. They are also trying to establish high-availability architectures so that applications remain available even if a cloud provider or private data center goes down. Data sovereignty, cost optimization, and specific workload requirements are secondary drivers.

Sample Size = 409

# Network Monitoring and the Cloud

**Figure 23** reveals that nearly 91% of network operations teams are using network monitoring tools to monitor public cloud infrastructure. Successful network operations teams are the most likely to monitor the cloud.

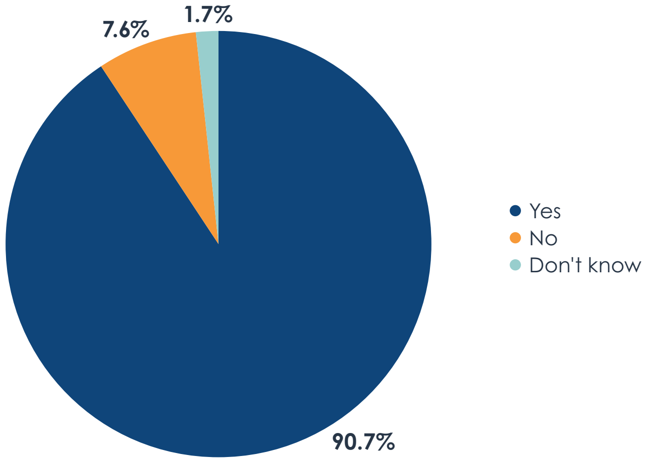

Figure 23. Does your organization use or plan to use its network monitoring tools to monitor its public cloud infrastructure?

"We are monitoring and troubleshooting cloud networks," said a network engineer with a Fortune 100 consumer goods manufacturer. "People always blame the network. If the problem has something to do with the cloud application itself, we're not good at getting that data. Tools need better visibility into the cloud."

Monitoring the cloud will require some adjustments to network operations toolsets. This research found that 38.4% of network operations teams consider cloud provider flow logs to be an essential source of data for network monitoring today. Network managers tasked with monitoring the cloud will need their tool vendors to collect and analyze this data. Not all tool vendors will adequately support cloud visibility. In fact, enterprises with three or more cloud providers are extremely likely to use 21 or more network monitoring and management tools. EMA suspects that these teams are adding new tools to address multi-cloud operations.

Sample Size = 409

*Network operations teams need better cloud visibility. Only 18% described their tools as very effective at monitoring the cloud.*

**Figure 24** reveals that most network operations teams need better cloud visibility. Only 18% described their tools as very effective at monitoring the cloud. Successful network operations teams are twice as likely as less successful teams to have very effective cloud monitoring capabilities. This correlation suggests that cloud visibility can make or break a network operations team in this era of cloud ubiquity. Network teams that use cloud enablement as a measure of their own success are more likely to report very effective cloud visibility.

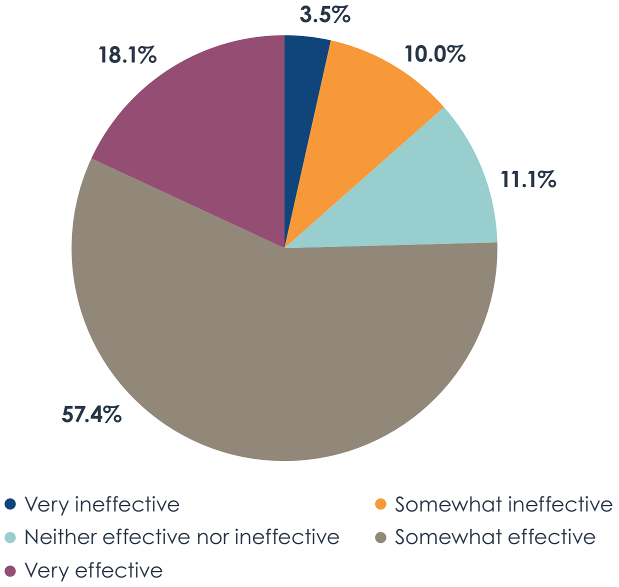

Figure 24. Effectiveness of network monitoring tools at providing visibility into public cloud networks

Enterprises that conduct network operations within a cross-domain operations center are the most likely to have very effective cloud monitoring, whereas companies that maintain a NOC or a distributed approach to network operations are less likely to have good cloud monitoring. EMA suspects that cross-domain operations teams are adopting less network-centric tools for monitoring and troubleshooting, and this is leading to a more optimized toolset for the cloud.

This research also found that network operations teams are more likely to have good cloud visibility if DevOps, application performance optimization, SaaS application adoption, and AIOps adoption heavily influence their overall network management strategy. Network teams that are focused on network performance management tool upgrades and enhancements are also more likely to report effective cloud monitoring.

Network teams that are successful with cloud monitoring prefer fully integrated, multi-function platforms for network monitoring and management tools, rather than best-of-breed tools or loosely integrated best-of-suite tools. They also tend to integrate their network management tools with systems management tools, security monitoring, and IT service management systems.

Finally, effective cloud visibility correlates strongly with use of active, synthetic network monitoring tools and streaming network telemetry.

## EMA Advice

Network operations teams must gain visibility into the cloud. Many network managers tell EMA that they have abdicated responsibility for this domain, and we believe this is a grave mistake. The future of IT is hybrid. While multi-cloud architecture is becoming ubiquitous, private infrastructure will persist. Network operations teams must be able to manage network health and performance across both domains. This will require tools that can collect and analyze data from the cloud. EMA also believes it will require active synthetic monitoring tools that can emulate and reveal how end users are experiencing cloud services.

Sample Size = 371

# Megatrend #3: DevOps Partnerships

DevOps is loosely defined as a set of principles that bring software development and IT operations closer together. It often involves the use of agile development, automation, and observability to improve the time to deployment and quality of applications. DevOps teams often spearhead private and public cloud initiatives. Network operations teams often find themselves on the fringes of DevOps-led transformation. EMA believes it is important for network teams to build strong partnerships with DevOps teams.

This research found that 64% of organizations have the equivalent of a DevOps team today. Another 33% are planning to establish one in the future. DevOps teams were more frequent in enterprises (2,499 employees or more) and high-revenue companies ($1 billion or more). They were also more frequent in North America.

**Figure 25** reveals expectations for the relationship between network operations and DevOps. More than 38% believe these teams will be integrated into a single group. Keep in mind that 29% of these organizations already have a cross-domain operations center, so they are necessarily breaking up a traditional NOC. Also, 21% have informal or distributed network operations teams that already take a flexible approach to organization.

More than half expect network operations and DevOps teams to adopt formalized collaboration, while a much smaller number will go with loose, informal collaboration. The intent is clear. IT organizations want to closely align network operations and DevOps functions. The most successful network operations teams are expecting to be completely integrated into DevOps. Less successful teams expect formalized partnerships between the distinct groups.

“Our network monitoring team has team members who attend all DevOps meetings,” said an IT operations manager for one of the world’s largest government agencies. “It’s going okay. The monitoring team is always hammering the DevOps team, telling them they need to set up more monitoring. It goes over to varying degrees of success. DevOps always says, ‘We have customers to deal with. This can wait.’ It’s not at the top of their list.”

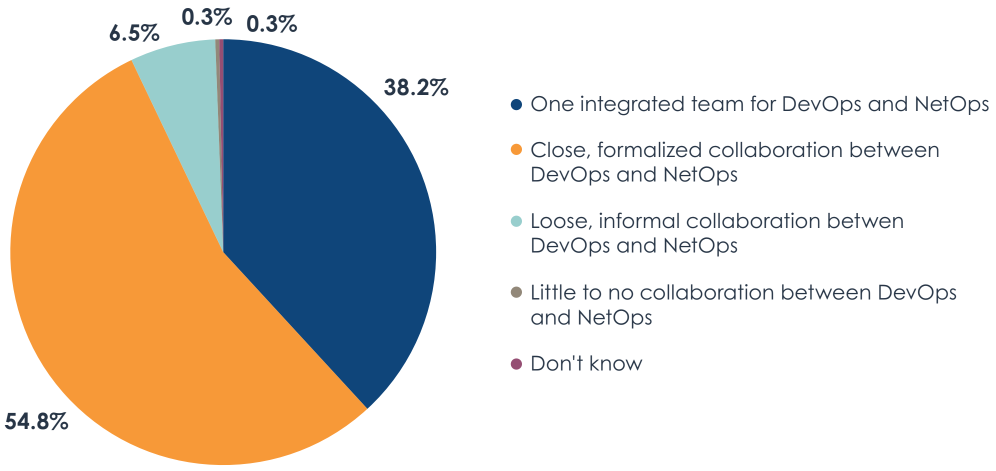

Figure 25. Expected relationship between DevOps and network operations teams

Sample Size = 398

# Where NetOps and DevOps Collaborate

**Figure 26** examines where network operations and DevOps need to focus their collaboration. Security policy design and implementation are clearly essential areas of collaboration between network and DevOps teams. Many also see a good opportunity to work together on application optimization and network capacity planning. Day 2 operations, such as monitoring and troubleshooting, are less of a priority, as is compliance. However, respondents who are actual members of a DevOps team identified operational monitoring as their highest priority. In other words, they need network observability. On the other hand, people who work in a NOC were the most likely to think that troubleshooting is an important collaboration area with DevOps.

Organizations that conduct network operations within a cross-domain operations team were more likely to cite compliance as a collaboration priority. Respondents who work within a cloud architecture and operations team were also more likely to select compliance. Members of the cloud team and the network engineering and architecture team were also more likely to select change management.

*Security policy design and implementation are clearly essential areas of collaboration between network and DevOps teams.*

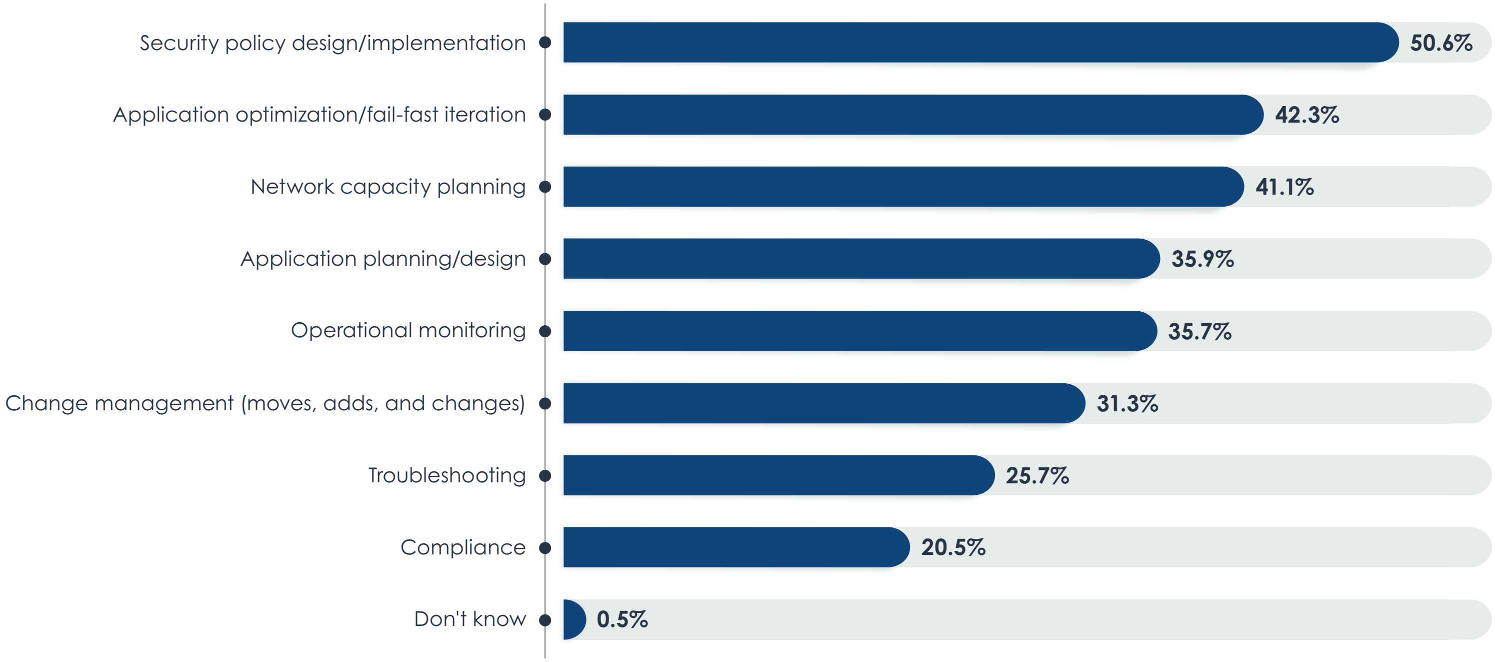

Figure 26. Most important areas of collaboration that should occur between a network team and a DevOps team

Sample Size = 409,
Valid Cases = 409,
Total Mentions = 1,160

# EMA Advice

Given how cloud-driven most network teams are today, EMA believes that it is critical for network operations teams to overcome collaboration barriers and form strong partnerships with the DevOps team. Network operations professionals should identify the barriers that prevent their teams from collaborating with DevOps and break them down. EMA's data shows that network security and network capacity planning knowledge will be immensely valuable to DevOps teams.

*EMA believes that it is critical for network operations teams to overcome collaboration barriers and form strong partnerships with the DevOps team.*

# Megatrend #4: The Internet of Things and Private 5G Engagement

Multiple industries are embracing the Internet of Things (IoT), connecting smart devices and sensors to their corporate networks to support new digital applications for manufacturing, medicine, retail and logistics, smart buildings, and more. At the same time, EMA has observed growing interest in the use of private 5G networks as a supplement to enterprise Wi-Fi, specifically to support IoT connectivity requirements.

**Figure 27** reveals that nearly 96% of the enterprises represented in this research expect IoT devices to connect to their corporate networks. Nearly 30% have such devices on the network today, and another 53% will add them by the end of this year. The larger the network, the more likely it is to have IoT devices connected to it.

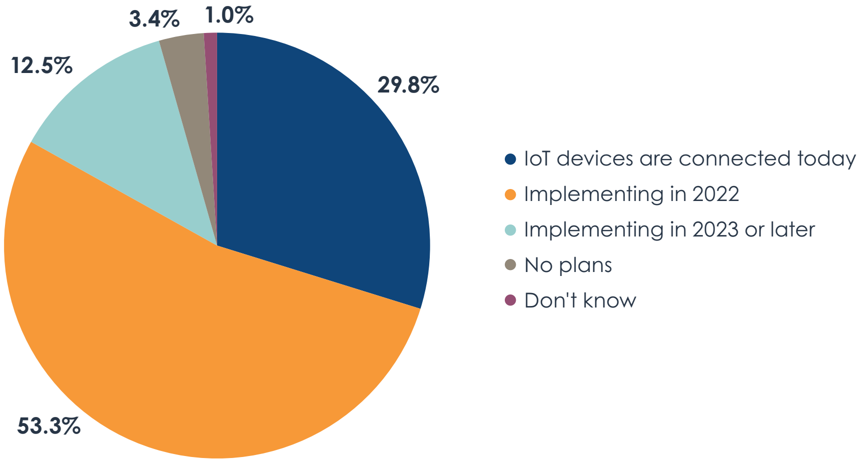

Figure 27. Timeline for connecting Internet of Things devices and sensors to enterprise networks

EMA found that the following industries are the most likely to already have IoT devices on the network:

- Healthcare
- Logistics/Wholesale/Distribution
- Transportation

These industries are most likely to connect IoT devices to the network this year:

- Manufacturing
- Construction/Civil Engineering
- Retail

*Nearly 96% of the enterprises represented in this research expect IoT devices to connect to their corporate networks.*

Sample Size = 409

# IoT-Driven Network Investments

**Figure 28** reveals that nearly 100% of the companies that have connected or plan to connect IoT devices to their networks are investing in networking technologies to support the project. The majority are investing in new network security, network performance monitoring, and network automation solutions to enable IoT. Essentially, they're looking for ways to better secure and manage networks with IoT.

"We have a dedicated team for [IoT connectivity]," said a network team manager with a Fortune 100 pharmaceutical company. "Usually it's under manufacturing. We have complex machines that are monitoring the environment where manufacturing takes place, and we have the manufacturing devices themselves. We're investing in security to support it. There are discussions on how to segment the network to isolate these devices."

Secondarily, these organizations are investing in new infrastructure (Wi-Fi, switching, and routing) and IoT-specific WAN connectivity services, such as low-power WAN. Companies with 500 or more employees were most likely to target IoT-specific WAN connectivity. It's also most common in the energy, manufacturing, and retail industries.

This research also found that 53% of IT organizations intend to use IT management tools to discover and manage IoT devices. This is most common in smaller companies. It was also most common among the companies that are most successful with network operations.

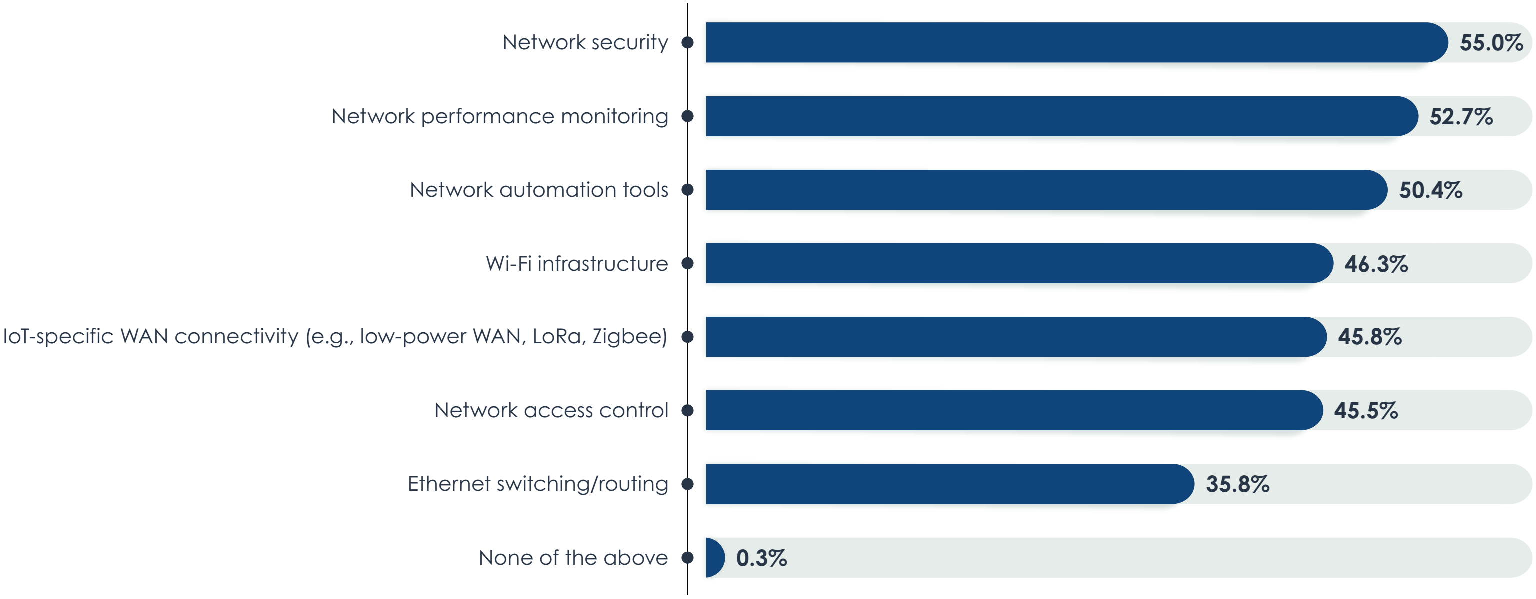

Figure 28. Investments made by the network team to address connectivity requirements of IoT devices and sensors

Sample Size = 391, Valid Cases = 391, Total Mentions = 1,297

# Private 5G Networking Engagement

Private 5G networking is not necessarily new. Many mobile network operators (MNOs) have used network slicing to offer private, dedicated connections to corporate customers over their public mobile networks for years. More recently, a new set of solution providers emerged that would allow enterprises to use dedicated 5G infrastructure for local connectivity. The idea is that private 5G is a better choice than Wi-Fi for connecting certain IoT devices and enabling critical communications. Private 5G is still emerging, with MNOs, cloud providers, and hardware vendors racing to offer DIY and managed solutions.

EMA suspects there is some confusion in the market as to what private 5G is. **Figure 29** reveals the supposed current state of engagement with private 5G solutions. More than one-third of companies claim to be using or implementing private 5G today. This number is much too high. EMA believes many of the respondents are confusing private 5G LAN services with 5G slicing or fixed mobile 5G connections for remote sites and branch offices. Overall, the interest in private 5G networks appears quite high.

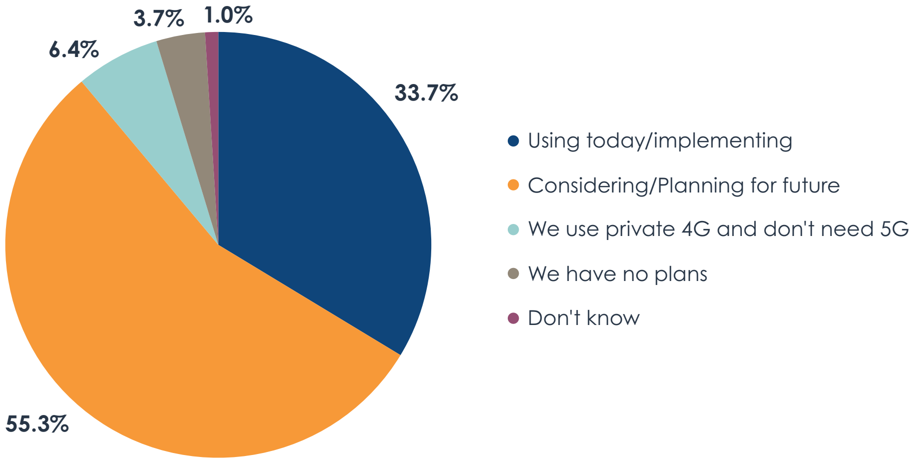

Figure 29. Engagement with private 5G technology (private 5G services or 5G LAN infrastructure)

Sample Size = 409

# EMA Advice

*Network operations teams should invest in security, performance monitoring, and automation tools to support IoT.*

IoT is coming to most enterprise networks over the next year or so. Network teams may be tempted to focus on upgrading or adding network connectivity, such as Wi-Fi and low-power WAN services, to address these requirements. Management tools will be most essential to success. IT operations will be tasked with managing many of these devices. Network operations teams should invest in security, performance monitoring, and automation tools to support IoT. Also, private 5G technology will address some of the unique connectivity needs of IoT devices in some enterprises.

Network teams should familiarize themselves with the emerging market of private 5G solutions and determine whether they want to adopt a DIY product or a managed service. They should look for a trusted vendor that offers a solution if they decide to adopt private 5G. They'll also need to pay special attention to integrating the technology with their end-to-end networks and ensuring that they have sufficient monitoring and troubleshooting tools to empower network operations to support the technology.

# Megatrends #5: Emerging Network Operations Data

# Streaming Telemetry

Streaming telemetry is an emerging technique for collecting metrics and events from network devices. Today, network monitoring tools poll devices at regular intervals, usually via SNMP. Streaming telemetry is a subscription model. Devices push real-time data continuously as it is generated. Tools subscribe to the data types that they need to analyze. Network engineers consider streaming telemetry more efficient, secure, and real-time than polling. The newest switches and routers from leading vendors support some form of it today, but EMA believes that overall adoption is low at this point.

**Figure 30** reveals higher than expected adoption numbers, with nearly 43% claiming to use streaming network telemetry today. EMA believes that some respondents may have conflated streaming network telemetry with streaming telemetry techniques used for collecting metrics, logs, and traces for DevOps-oriented observability solutions. Members of the DevOps group were more likely to say their network operations groups are using it today, but so too were members of the network engineering and network operations groups, who are less likely to conflate streaming network telemetry with DevOps-oriented telemetry.

Regardless, interest in streaming telemetry from network operations teams is high. The most successful network operations teams are the most likely to be using it today. Members of the DevOps group were more likely to say their network operations groups are using it today, but so too were members of the network engineering and network operations groups, who are less likely to conflate streaming network telemetry with DevOps-oriented telemetry.

Cloud-scale companies, like Google, have declared in the past that they intend to eliminate SNMP from their networks through the adoption of streaming telemetry. One of the core missions of the OpenConfig, a consortium of network engineers from hyperscale companies, is to enable that transition by creating a de facto open standard for streaming telemetry. OpenConfig has been successful in getting leading network hardware vendors to support its streaming telemetry implementations in their latest hardware platforms.

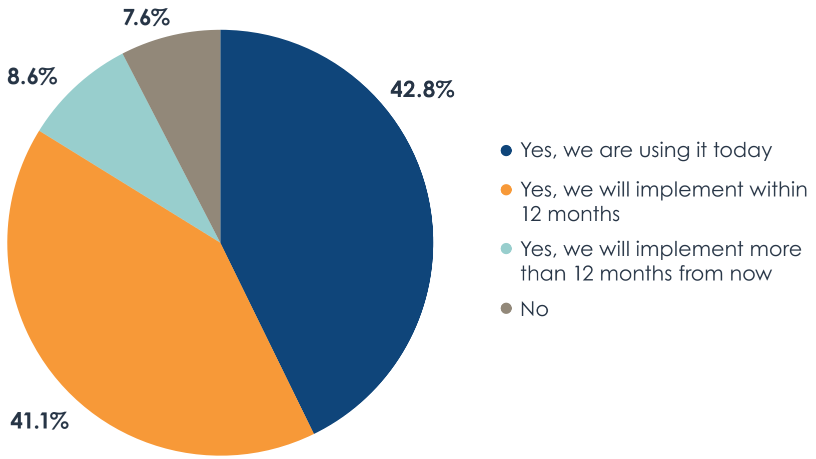

Figure 30. Is your organization interested in using streaming network telemetry?

Sample Size = 409

EMA asked research participants whether they have determined that streaming telemetry will be a requirement in the future to eliminate SNMP from their networks. **Figure 31** reveals that 27% are leaning this way. The rest are exploring the value of streaming telemetry. In the past, most network teams told EMA that they see streaming telemetry as complementary to SNMP, not a replacement. It appears that most of the market is still leaning in that direction.

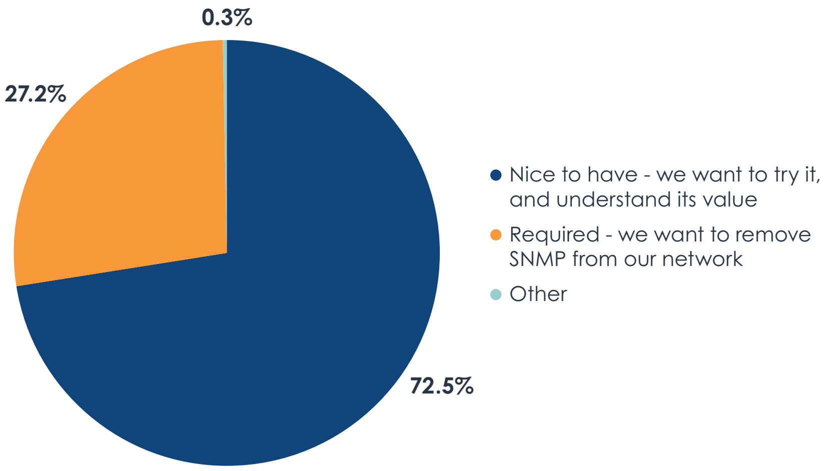

Figure 31. Current goals for using streaming telemetry

**Figure 32** reveals why network teams are interested in using streaming telemetry. First, they like the improved data granularity available through it. Network management tools that poll devices via SNMP and related techniques often struggle to collect data at high intervals. This leads to instances in which brief spikes in metrics are missed.

Second, network managers like the more efficient data transfer of streaming telemetry. SNMP is often derided for adding unnecessary traffic to a network.

Real-time insights are the third benefit. Not only is the data more granular, but it arrives whenever conditions on the network change. When a network manager is reviewing telemetry data, they know that they are reviewing and acting on real-time conditions on the network.

Sample Size = 378

Finally, network managers perceive an opportunity to make data collection more reliable. A device's response to an SNMP poll doesn't always make it to the tool. Streaming telemetry uses a variety of transport protocols, like RESTCONF, NETCONF, and gNMI, to ensure more reliable and efficient data transfers. The most successful network operations teams are more likely to seek this benefit. They are also more likely to value data standardization, which is otherwise an afterthought for most people.

Finally, extensibility of streaming telemetry is not a high priority for most, but the most sophisticated networking experts in EMA's survey (network engineers and network architects) identified this as one of their highest priorities, suggesting that there is an opportunity to customize streaming telemetry with metrics that SNMP cannot support.

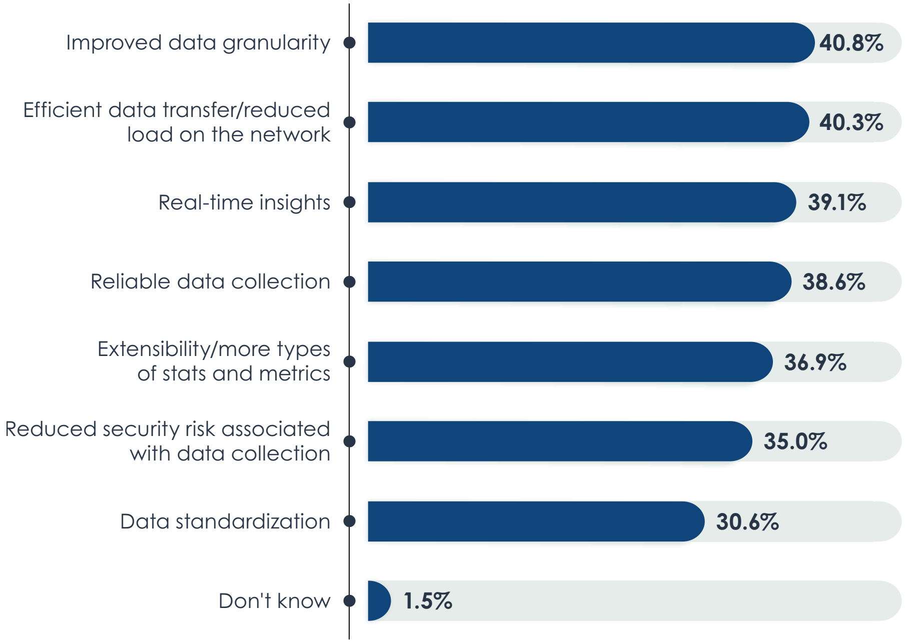

Figure 32. The most valuable benefits of streaming network telemetry

Sample Size = 409, Valid Cases = 409, Total Mentions = 1,075

# Active Synthetic Traffic

Active synthetic traffic is less novel than streaming telemetry, but it has gained traction in network operations teams in recent years because passive monitoring data (network flows, packet data) has become difficult to collect in certain environments. **Figure 33** reveals that interest in using active monitoring tools for network operations is extremely high today.

Successful network operations teams are the most likely to use it today. The disparity of adoption between successful and less successful teams suggests that this class of tools can help many network teams overcome the challenges EMA identified in this report. Both NOCs and cross-domain operations centers are much more likely to use active synthetic monitoring today. Informal and distributed network operations teams are less likely to use it.

Organizations with larger network management toolsets (11 or more) are more likely to use it today, suggesting that active monitoring is contributing to tool sprawl.

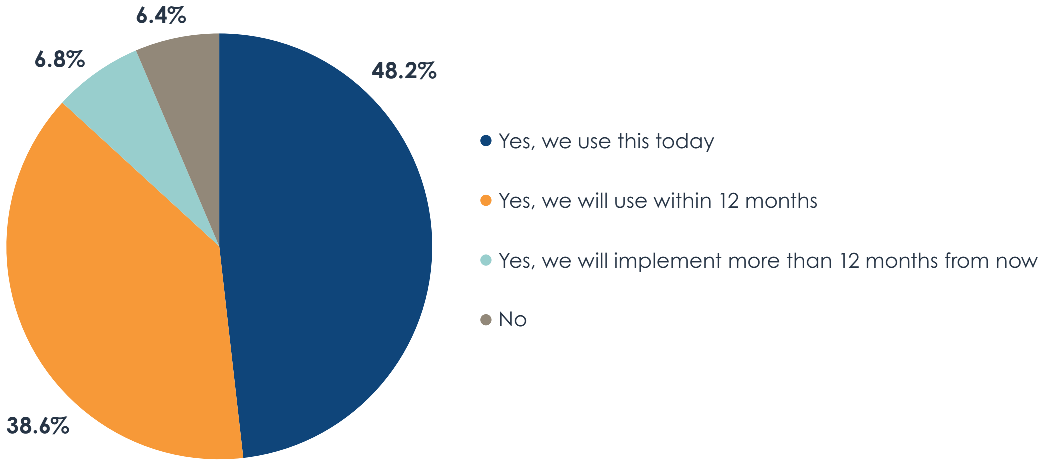

Figure 33. Is your networking team interested in using active, synthetic monitoring tools for network operations?

Sample Size = 409

**Figure 34** identifies why there is so much interest in active monitoring tools. A large majority of network operations teams are trying to gain better visibility into public cloud providers. People who work in network engineering, DevOps, and IT architectures were the most likely to cite public cloud.

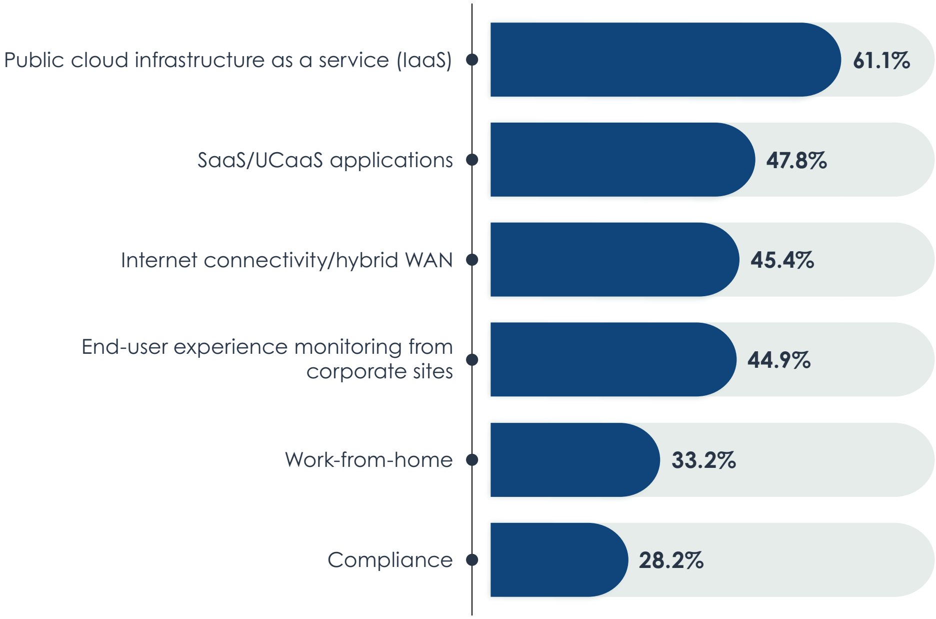

Figure 34. Drivers of network operations team interest in active synthetic monitoring

Sample Size = 383, Valid Cases = 383, Total Mentions = 998

SaaS applications, internet performance, and end-user experience monitoring from corporate sites are secondary drivers. Work-from-home and compliance are the lowest priorities. Successful network operations teams were most likely to cite SaaS and internet connectivity as drivers of active monitoring, suggesting a potential best practice for improving operations.

"We use it for performance monitoring and operations. If the operations team is receiving reports of lowness for the network, they check [the active monitoring tool] to check the performance of circuits. We also use it to measure the [internet] WAN underlay," said a network engineer with a Fortune 100 consumer goods manufacturer.

While work-from-home and compliance are minor drivers overall, organizations with cross-domain operations centers cited both as significant drivers of active monitoring interest. EMA believes that network operations teams that are better integrated into full-stack operations appreciate a broader set of use cases for this technology.

*Successful network operations teams were most likely to cite SaaS and internet connectivity as drivers of active monitoring.*

## EMA Advice

EMA believes that any network operations team that is impacted by cloud and SaaS applications, hybrid WAN, and work-from-home requirements should explore the utility of active synthetic monitoring today. There is a variety of vendors offering products with varying functionality, and at a wide range of price points. Over the last couple years, EMA has spoken with IT managers in within both SMBs and Fortune 50 companies that are making extensive use of such technology.

Streaming network telemetry is still an emergent technology today, but it is a promising solution for network teams that are dissatisfied with SNMP. Network infrastructure and operations teams should evaluate this technology today, especially those who are planning an investment in new network hardware. With more vendors adding support for streaming telemetry in their newest switches and routers, it should be a part of the planning process for management tool investments.

# Conclusion: Network Operations Teams Need to Modernize for the Cloud Era

*Network operations teams are at a cloud crossroads today.*

EMA believes that network operations teams are at a cloud crossroads today. Most are struggling as the public cloud, SaaS applications, and cloud-native application architectures start to drive IT strategy.

Network operations teams have a people problem and a technology problem. They don't have enough skilled personnel and their management tools are not optimized for today's digital world. Network operations leaders need to make it clear that they are essential to cloud transformation and other initiatives, like IoT. They also need to win budget, they need to win support for new hires of technical personnel, and they need to modernize their tools. Today's network management toolsets are bloated, inefficient, and disconnected. These tools are contributing to manual errors that degrade the network, and they are producing too many false alerts.

This report highlights many of the challenges that network operations professionals are struggling with today, but it also points to countless best practices that can help overcome these challenges. Use this report as a guide to optimize your organization.

# Case Study: Fulton Public Schools Optimize and Meet Growth Demands Using Auvik

Serving the city of Fulton, Missouri, the Fulton Public School district is home to 2,000 K-12 students. Over the next few years, the district will conduct intensive planning processes for long-term growth. That includes adding additional IT infrastructure.

The first infrastructure project for this long-term growth initiative was the installation of IP video surveillance equipment to all campuses—a huge undertaking for a four-person IT team. Early on, the IT team identified a need to monitor and manage video surveillance equipment and the entire network from a central position. The team gained visibility by adopting the Auvik network monitoring and management solution, which provides a comprehensive map of all devices for each campus, with real-time network visibility that highlights issues quickly.

For example, when rolling out the new equipment, the team quickly discovered that all on- device data was transmitting through only one NIC instead of distributed between two. With Auvik's advanced topography mapping, the team could quickly see the network connections and the potential issue, and implement a solution. "Auvik is a visual tool that helps me understand where I need to look first, like missing credentials, something is offline, or quickly look up a device IP or the port it is connected to," says Dan Hedgpath, Technology Director.

When considering how to scale to meet growth demands, the IT team at Fulton Public Schools also sought a way to improve network operations and disaster recovery efforts by implementing automated backups and better documentation.

"Developing our Incident Response Plan, it became evident that we didn't have a good way to back up switch configurations or to show any changes to those configs when they occur. Auvik made it very simple to do both," Hedgpath says. Auvik saved the IT team time by eliminating manual processes involved in recording and documenting the network. Physical access to the network is no longer required. The IT team can use Auvik to manage operations remotely, from firmware updates to IP port lookups.

## Automated device configuration backups

Creating manual configuration backups for network devices can be time-consuming. Using Auvik's out-of-the-box configuration backups to automate this process allows the network team to get their time back to focus on other priorities.

## Faster troubleshooting with real-time visibility

Using Auvik's collector to scan and map the topology of the network, the team can now find problems before they become apparent to the end user. They can do this without leaving their desk. "Prior to Auvik, I would have to identify the devices by IP, SSH into the device, and do my work in the CLI. Now, Auvik displays all of that information in the GUI, allows me to run remote commands, and still SSH into the device if I need to. I don't have to remember what a device's IP address is or use the CLI on the device to find the other switches that are connected to it. If I know the MDF switch, I can see all the switches that are connected to it downstream and can even filter by type:switches to see just the switches. Super easy!" says Hedgpath.

## Ease of setup, use, and support

The ease of setup and use was a huge factor for the Fulton Public Schools team, and Auvik stands tall against its competitors in this area. "Support experience is good and Auvik is quick to answer any questions. And there is an extensive knowledgebase, which is helpful getting started."

# Business Benefits

- Auvik has helped the IT team streamline business operations, where it's now easier than ever to find devices, get IPs, update and configure remotely, and back up all device configurations automatically.
- Network visibility through mapping, documentation, and real-time alerts has also helped to increase time savings for the IT team. Being able to access a tool like Auvik means never having to leave the desk to see what's wrong or guess the IP address of the device that may exist across town.
- Resolving network issues before the end-user is aware is imperative to a high-performing network team.
- Getting time back for the IT team, whether that's through better troubleshooting when issues arise or being proactive through monitoring, allows the Fulton Public Schools team to focus on more strategic growth initiatives.

## About Enterprise Management Associates, Inc.

Founded in 1996, Enterprise Management Associates (EMA) is a leading industry analyst firm that provides deep insight across the full spectrum of IT and data management technologies. EMA analysts leverage a unique combination of practical experience, insight into industry best practices, and in-depth knowledge of current and planned vendor solutions to help EMA's clients achieve their goals. Learn more about EMA research, analysis, and consulting services for enterprise line of business users, IT professionals, and IT vendors at **www.enterprisemanagement.com** You can also follow EMA on **Twitter** or **LinkedIn**

1995 North 57th Court, Suite 120, Boulder, CO 80301 +1 303.543.9500 **www.enterprisemanagement.com** 4171.051622