Network Management Megatrends 2020

Enterprises Embrace NetSecOps, the Internet of Things, and Streaming Network Telemetry

An ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) Research Report
By Shamus McGillicuddy
April 2020

SPONSORED BY:

kentik®

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

Table of Contents

© 2020 Enterprise Management Associates, Inc. | www.enterprisemanagement.com

EXECUTIVE SUMMARY

Enterprise Management Associates' "Network Management Megatrends 2020" report is part of an ongoing biennial study that tracks the evolution of enterprise network engineering and operations. Based on a survey of 350 North American and European IT professionals, the 2020 research reveals that collaboration between network and security teams is essential, the Internet of Things is impacting the majority of networks today, software-defined networking is driving change in the data center, and network managers are turning to streaming network telemetry and cloud provider flow logs to enhance operations.

THE DEFINITIVE BENCHMARK OF NETWORK MANAGEMENT

Since 2008, Enterprise Management Associates (EMA) has conducted biennial research into enterprise network management strategies. This "Network Management Megatrends 2020" research tracks the strategies enterprises adopt for managing their networks and the challenges they encounter. Moreover, this research examines how significant technology and business trends, so-called "megatrends," impact network management strategies.

The result is this report, which tracks evolving network management strategies and challenges over time, while also highlighting how certain megatrends are impacting those strategies and challenges. Please note that this research survey was conducted prior to the World Health Organization's declaration of a coronavirus pandemic. Some of the data uncovered in this research has probably shifted, at least in the short-term. However, many of EMA's findings, such as cloud network management and NetSecOps collaboration, are probably unaffected.

KEY FINDINGS

- Only 35% of enterprises have a fully successful network operations team.
- The top challenges to network operations success are:
  1. Budget gaps
  2. Shortages of skilled personnel
  3. Poor implementation of infrastructure projects
  4. Ineffective network management outsourcing
- More than 33% of all IT service problems are detected and reported by end users before the network operations team is aware of them.
- Enterprises are making progress in reducing fragmented network management toolsets. However, 64% of enterprises still use 4 to 10 tools to monitor and troubleshoot their networks.
- Cloud provider flow logs (e.g., AWS VPC flow or Azure NSG flow logs) have emerged as a critical data source for sustained operational monitoring, troubleshooting, and capacity planning.
- 85% of enterprises plan to adopt 400 Gigabit Ethernet infrastructure, but most are waiting until 2021 or later.
- 51% of enterprises are using commercial tools to manage core network services: DNS, DHCP, and IP address management (DDI).
- 63% of enterprises have formalized collaboration between the network team and the security team.
  - This collaboration focuses primarily on:
    1. Network troubleshooting/security incident response
    2. Operational monitoring
    3. Infrastructure design/implementation
    4. Technology evaluation/procurement
- 66% of enterprises have implemented or plan to implement data center SDN technology, and 25% have completed a production deployment.
- SDN drives the following new requirements in network management tools:
    1. New data collection techniques/protocols
    2. New visualizations and dashboard views for SDN abstractions
    3. AIOps features

© 2020 Enterprise Management Associates, Inc. | www.enterprisemanagement.com

- 76% of enterprises have IoT devices connecting to the corporate network
  - IoT drives close partnerships between network teams and operational technology teams.
  - IoT also prompts the IT organization to invest in more network security, network access control, and network operations monitoring tools.
- 71% of enterprises are interested in collecting streaming network telemetry with their network management tools.
  - Most enterprises view streaming telemetry as a way to enhance SNMP, rather than replace it.
- 61% of enterprises say the cloud networking support offered by their network management tools has room for improvement.

DEMOGRAPHICS OVERVIEW

This research is based on a survey of 350 IT professionals whose job roles focus significantly on their employers' networks. EMA discarded anyone from the survey who had no direct and current interaction with and responsibility for their organization's network.

- 15% say networking is their sole focus
- 72% say networking is a significant part of their overall responsibilities
- 13% say networking is part of their overall focus, but they spend most of their time on other parts of IT

These survey respondents also have direct and current experience with the network management tools used by their organizations, including setting budget and strategy; procuring, implementing and supporting network management tools; and using tools to manage and troubleshoot the network.

Roles Within the IT Organization

In an effort to get insight from subject matter experts in this research, EMA excluded executive-level individuals from its survey. As Figure 1 reveals, 50% of respondents work in middle management, including IT managers and supervisors, directors, and vice presidents. Twelve percent are project managers and the rest are technology specialists, such as administrators, engineers, developers, and architects.

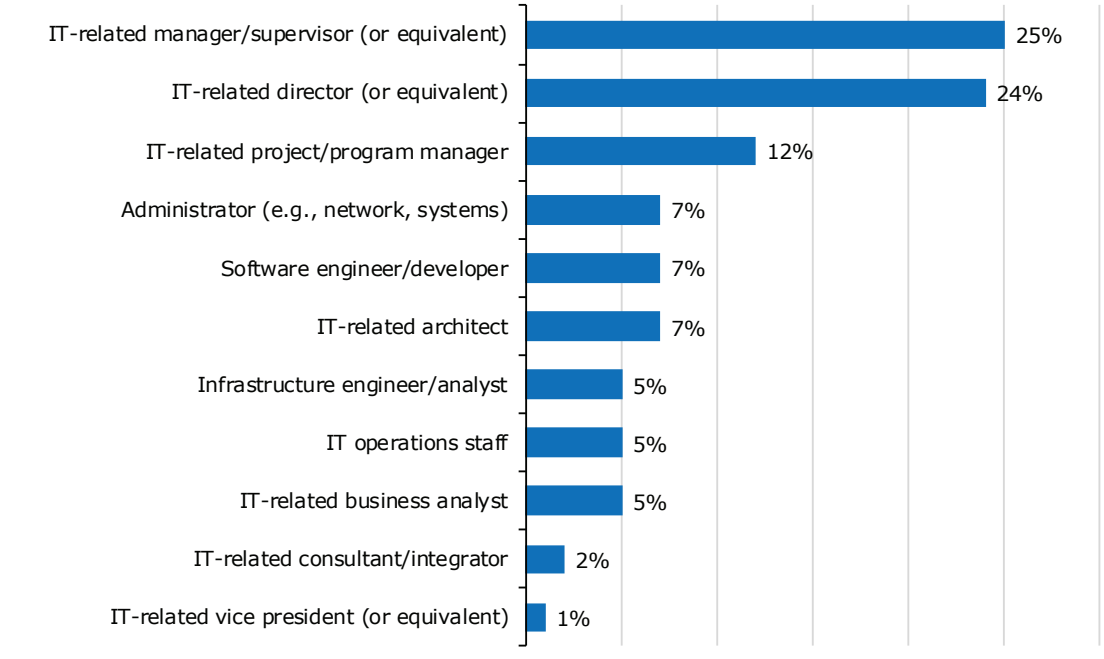


Figure 1. Job titles

© 2020 Enterprise Management Associates, Inc. | www.enterprisemanagement.com

Figure 2 reveals the functional groups survey respondents work within. The IT infrastructure team (planning, design, engineering, architecture) emerged as the most prominent group. They are likely implementers and users of network management tools. IT program/project management, another likely implementer of network management solutions, is the second-most prominent group.

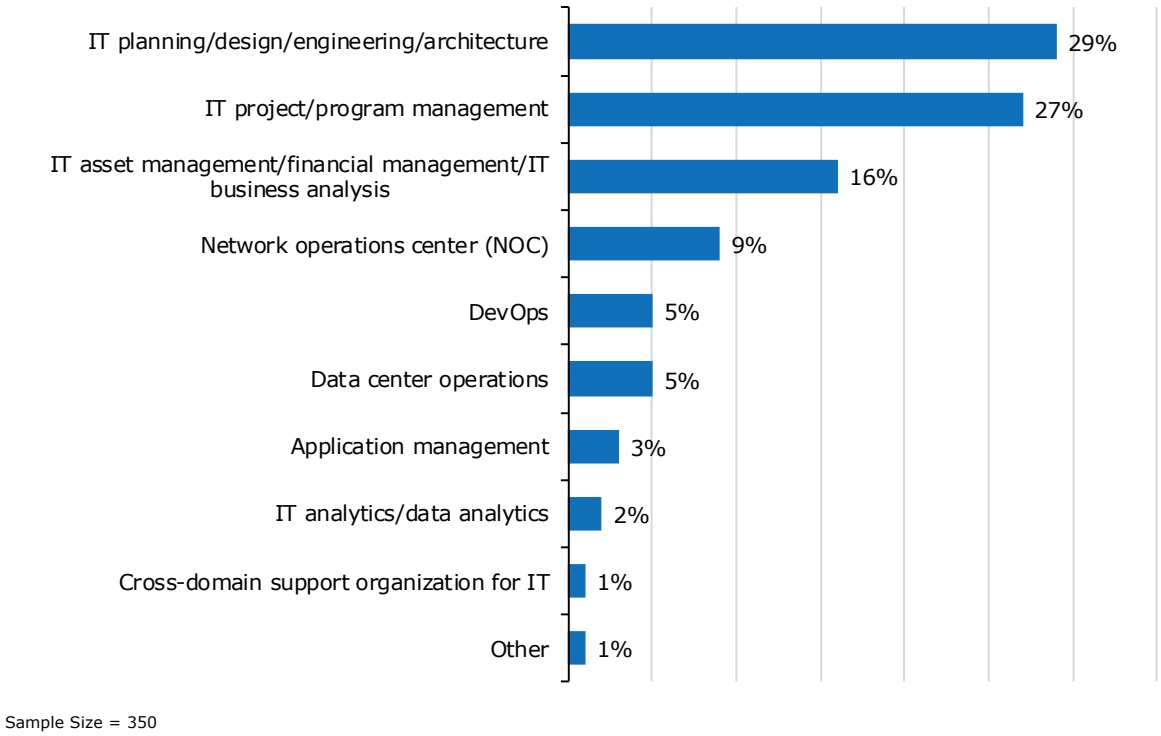


Figure 2. IT groups

IT asset/financial management, the group that controls budget for network infrastructure and network management, is also quite prominent. The rest of the respondents fall into operational groups like the network operations center (NOC), data center operations, DevOps, and application management. To ensure focus on network subject matter experts, EMA excluded several groups, including the "IT executive suite," application development, information security, and IT service management.

© 2020 Enterprise Management Associates, Inc. | www.enterprisemanagement.com

Company Profiles

As usual in this biennial research, EMA sought a transatlantic view of networking. Seventy-seven percent of respondents are from North America. The remaining 23% are from the three largest economies in Europe: Germany, the United Kingdom, and France.

EMA also sought a mix of midsized, large, and very large enterprises. **Figure 3** reveals that the majority of the organizations captured in this survey are large enterprises (1,000 to 9,999 employees). One-third of them are midsized companies (250 to 999 employees). Less than 10% are from very large companies (10,000 or more).

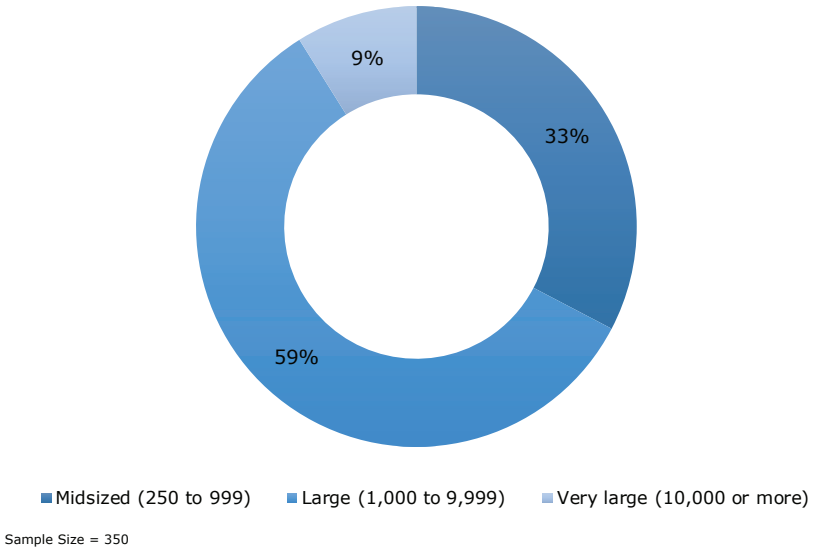


Figure 3. Size of company (by employees)

Obviously, the size of a network will affect a network management strategy. **Figure 4** reveals how many installed network devices are present in the networks represented in this survey. While the majority of respondents have networks with fewer than 2,500 devices, some are extremely large. Three percent of networks had 10,000 to 29,999 devices and 2% had 30,000 or more.

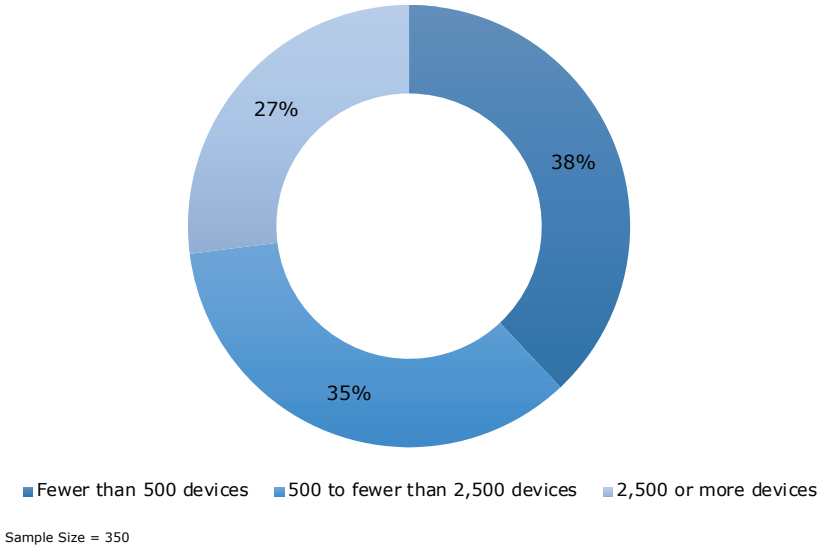


Figure 4. Network size (number of devices)

© 2020 Enterprise Management Associates, Inc. | www.enterprisemanagement.com

At least 21 industries are represented in this survey, as **Figure 5** reveals. The most prevalent are finance/banking/insurance, healthcare/medical/pharmaceutical, manufacturers of goods other than IT equipment, software, hospitality/entertainment/recreation/travel, education, and IT professional services.

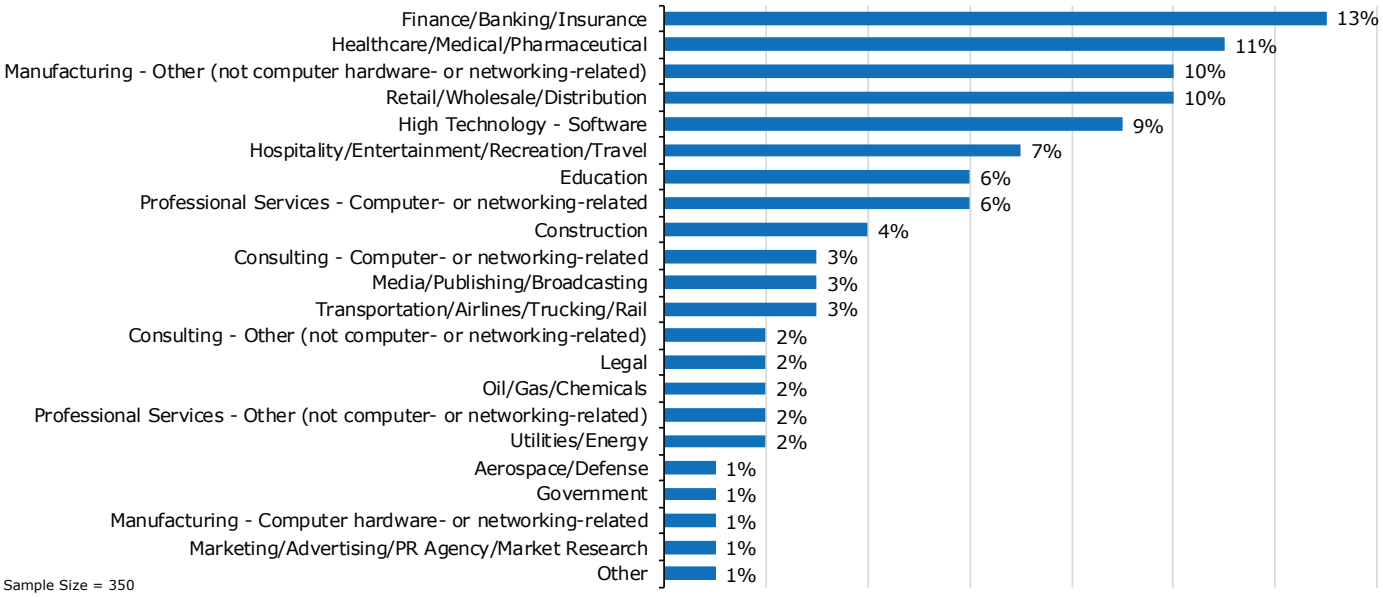


Figure 5. Vertical industries

DRIVERS OF NETWORK MANAGEMENT STRATEGIES

For more than a decade, this biennial research has tracked the broad IT initiatives and networking initiatives that most influence network management strategies. **Figure 6** details the broad IT initiatives that are most influential in 2020. Server virtualization has been at the top of this list every year EMA has conducted this research, since 2008, although it was eclipsed in 2018 by software-defined data centers (SDDCs). This year, EMA consolidated SDDCs with private cloud initiatives as a multiple choice option, and it remains a top driver.

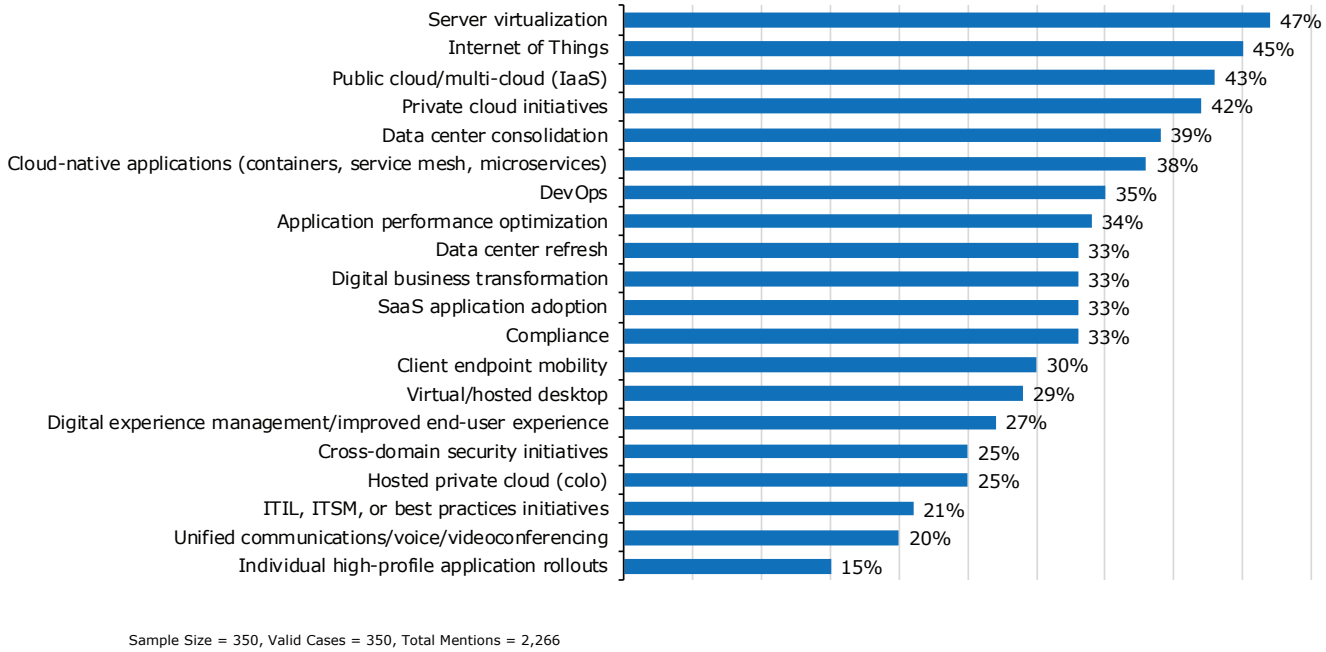


Figure 6. Broad IT initiatives that are driving current priorities in monitoring/managing networks and network application performance

© 2020 Enterprise Management Associates, Inc. | www.enterprisemanagement.com

The Internet of Things (IoT) and DevOps have emerged from obscurity to become highly influential over network management strategies this year. IoT rose from 13th in 2018 to 2nd, and DevOps rose from 16th in 2018 to 7th.

Public/multi-cloud initiatives and data center consolidation have been highly influential in past years, and they remain so. EMA added cloud-native application platforms (e.g., containers, Kubernetes) as a multiple choice option this year, and it immediately emerged as the sixth-most influential initiative.

The following IT initiatives are more influential among enterprises that are the most successful with network operations:

- Digital business transformation
- ITIL/ITSM/best practices
- Cloud-native applications
- Digital experience management
- Private cloud initiatives
- Hosted private cloud
- Unified communications/videoconferencing/voice

The Internet of Things (IoT) and DevOps have emerged from obscurity to become highly influential over network management strategies this year.

Network security has been the most influential networking initiative for more than a decade.

Figure 7 details the networking initiatives that drive network management strategy. Network security and network virtualization are most influential. Network security has been the most influential networking initiative for more than a decade. Network virtualization was the fifth-most influential initiative in 2018.

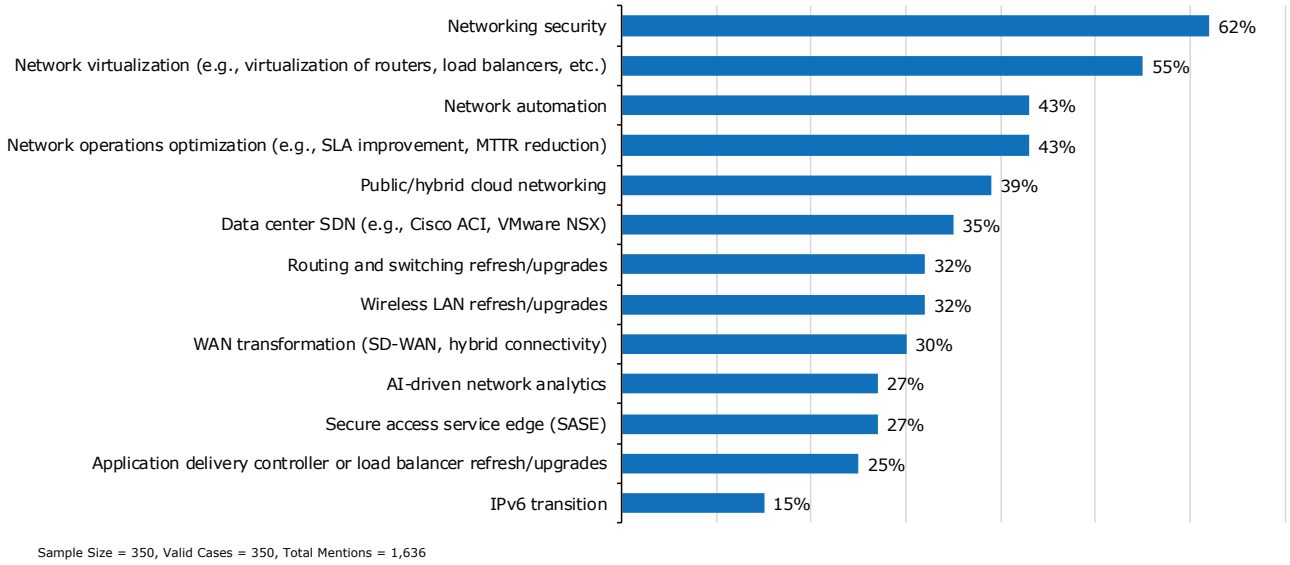


Figure 7. Networking initiatives that are driving current priorities in monitoring/managing networks and network application performance

Network automation and network operations optimization are tied for 3rd. The latter was just as prominent two years ago, but network automation has emerged from relative obscurity to be a top driver this year, suggesting it has become a major focus for enterprises recently. Respondents who work in IT engineering, project management, and the network operations center are all more likely to identify automation as a driver. Also, enterprises that are projecting higher rates of traffic growth over the next year are also more influenced by automation.

© 2020 Enterprise Management Associates, Inc. | www.enterprisemanagement.com

Public/hybrid cloud networking rounds out the top five initiatives. It is more influential among respondents from DevOps teams, but less influential with those in the IT engineering and architecture group.

WAN transformation is relatively low on the list, despite the hype around software-defined WAN technology; however, WAN transformation is more influential with enterprises that are successful with network operations.

Overall, the following networking initiatives are more influential among enterprises that are the most successful with network operations:

- Network virtualization
- Network security
- WAN transformation
- AI-driven network analytics
- Public/hybrid cloud networking
- Data center SDN

Secure access service edge (SASE), a solution conceptualized only in the last year, is one of the least influential initiatives today. SASE was coined by a competing analyst firm last year to describe solutions that combine wide-area network technologies and cloud-based network security services to provide an end-to-end secure access solution for any user in any location to any application. Its relatively low influence is understandable given that the concept is new and somewhat immature. However, North American respondents were three times more likely to cite it as a major influence. Respondents from the following industries also expressed stronger interest: IT consulting, construction, software, hospitality/entertainment, and retail/wholesale/distribution.

Widespread Network Traffic Growth in 2020

EMA asked research respondents if they are projecting traffic growth on their networks over the next 12 months. **Figure 8** indicates that 96% of enterprises are expecting an increase in traffic. Fifteen percent are projecting traffic to grow by 100% or more, essentially doubling the amount of traffic they support. Network monitoring and capacity planning will be critical for managing this growth. EMA believes traffic growth will be a significant influence on network management strategies.

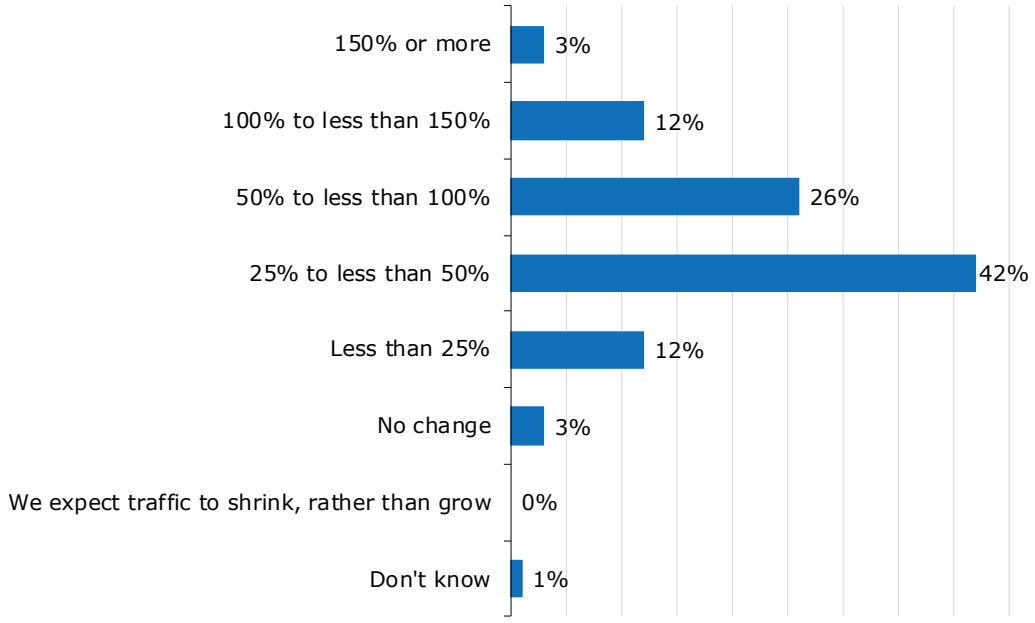


Figure 8: Projected traffic growth over the next 12 months

European respondents are more likely than North Americans to expect significant traffic growth. Very large companies are also more likely to expect significant growth.

© 2020 Enterprise Management Associates, Inc. | www.enterprisemanagement.com

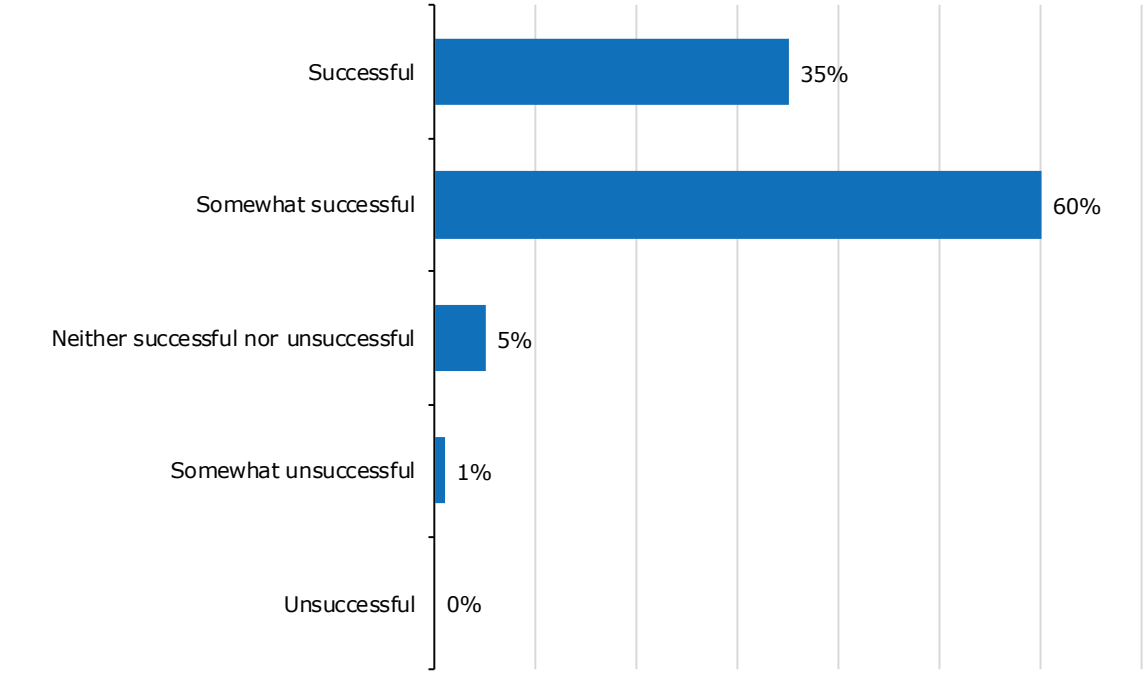
NETWORK OPERATIONS EFFECTIVENESS

Measuring NetOps Success

Historically, EMA has found that very few survey respondents will ever rate themselves as unsuccessful with a technology initiative. Instead, EMA pays careful attention to how respondents from successful and somewhat successful organizations differ in their responses to survey questions. Somewhat successful respondents see room for improvement in their organizations, so EMA looks for indications of possible best practices in its analysis of these two cohorts.

Figure 9 reveals how research respondents rated their organizations' success with overall network operations. Only 35% rated their network operations efforts as fully successful. Instead, a large majority see room for improvement, including 60% who say they are only somewhat successful.

Only 35% rated their network operations efforts as fully successful.

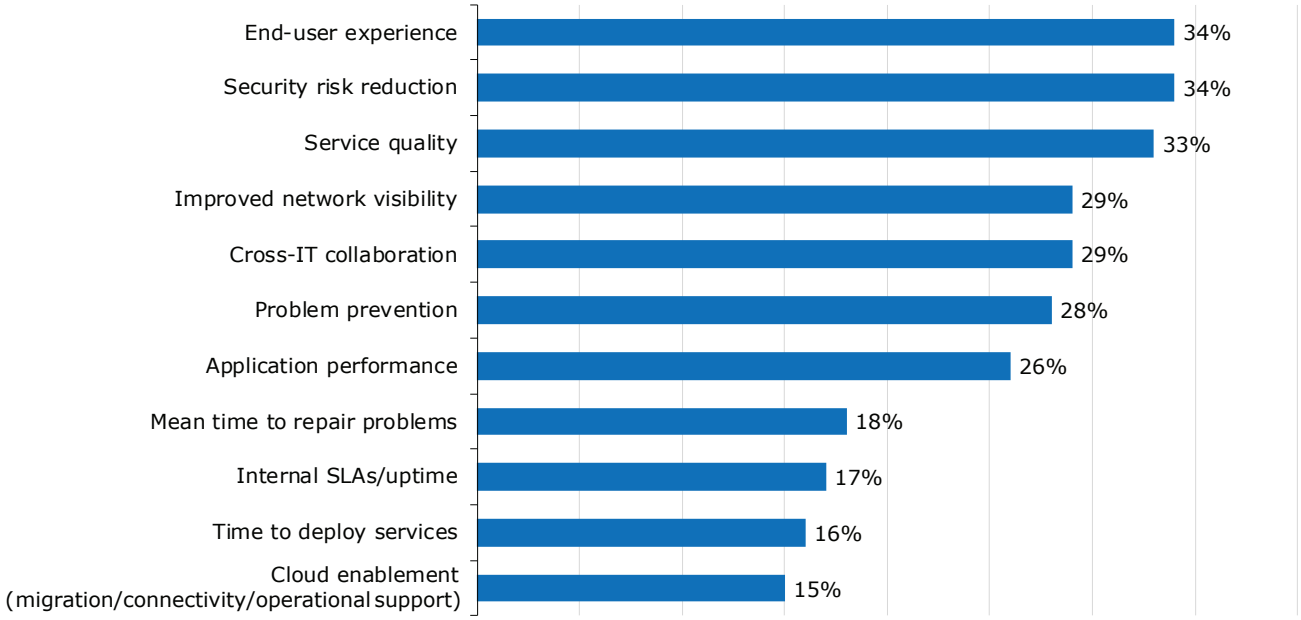


Sample Size = 350

Figure 9. Success with network operations

© 2020 Enterprise Management Associates, Inc. | www.enterprisemanagement.com

Figure 10 reveals how enterprises prefer to measure the success of network operations. End-user experience, security risk reduction, and overall service quality are the most popular means for measuring success. Secondarily, enterprises are also looking at improved network visibility, cross-IT collaboration, problem prevention, and application performance. Large enterprises are more likely to measure with cross-IT collaboration (32%).



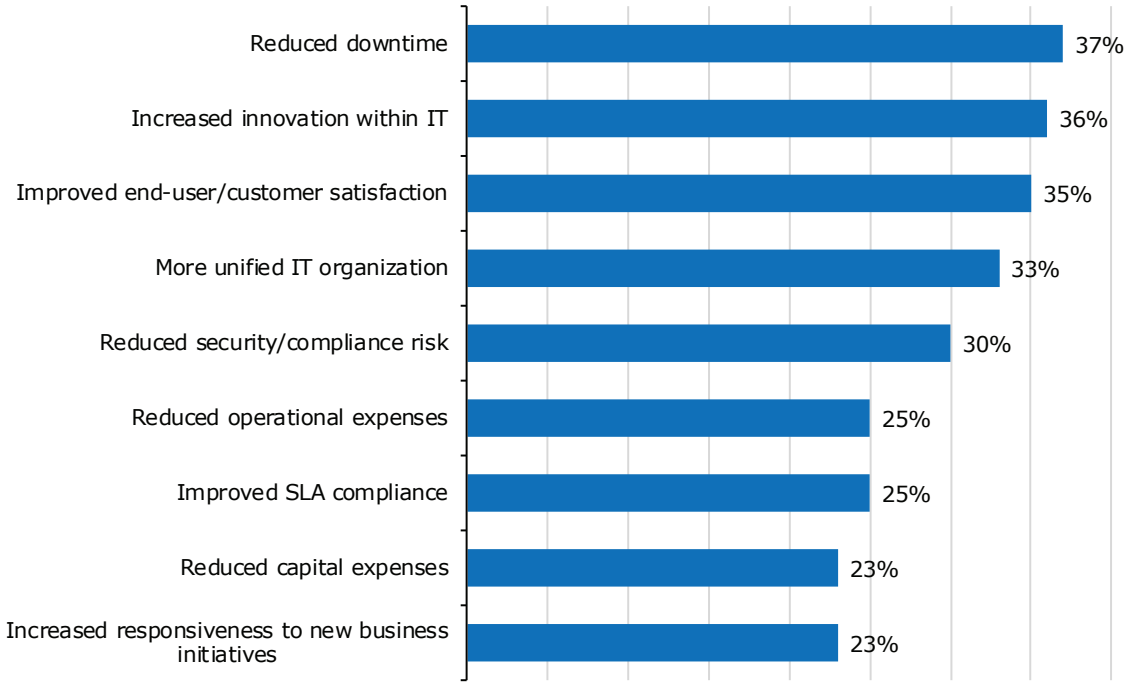
Sample Size = 350, Valid Cases = 350, Total Mentions = 979

Figure 10. Most important measures of network operations of success

Mean time to repair problems, uptime, time to deploy services, and cloud readiness are of least importance. EMA found that successful network operations teams are less likely to use uptime as a measure of success, but they are more likely to consider cloud enablement. Uptime is a top measure of success (35%) for respondents who work within an NOC, which suggests a mismatch of priorities between the NOC and the rest of the business. However, the NOC is also more focused on end-user experience (44%), which is a good sign. Cross-IT collaboration is an important measure for people in application management (50%) and data center operations (47%), but not the NOC (16%).

© 2020 Enterprise Management Associates, Inc. | www.enterprisemanagement.com

There is some dissonance between measuring success of NetOps and the business benefits of NetOps, as **Figure 11** reveals. For instance, the top business benefit is reduced downtime. If uptime is not an important measure of success, why is reduced downtime such an important benefit?



Sample Size = 350, Valid Cases = 350, Total Mentions = 936

Figure 11. Most important business benefits of network operations success

On the other hand, increased innovation within IT, improved end-user experience, unified IT, and reduced security risk are all aligning with expectations. Thus, the dissonance isn't completely problematic. Furthermore, it simply makes sense that a successful network operation is going to deliver a more reliable network with less downtime.

Although increased responsiveness to the business is the least common business benefit, individuals from data center operations (42%), where many business services live, are more focused on it. Increased innovation within IT is a higher priority with DevOps (53%) and the NOC (50%).

European respondents are more likely to perceive the benefits of reduced downtime (48%), reduced security and compliance risk (43%) and increased IT innovation (39%). They are less likely to perceive increased IT responsiveness to the business. Reduced risk is also beneficial more often in financial industries (44%).

© 2020 Enterprise Management Associates, Inc. | www.enterprisemanagement.com

Network Operations Challenges

Figure 12 compares the top network operations challenges that enterprises are facing today, versus what challenged them two years ago. In 2018, network teams were primarily struggling with a lack of end-to-end network visibility, a shortage of skilled personnel, problems with their network usage policy, and fragmented management tools. This year, EMA found a significant shift in networking challenges.

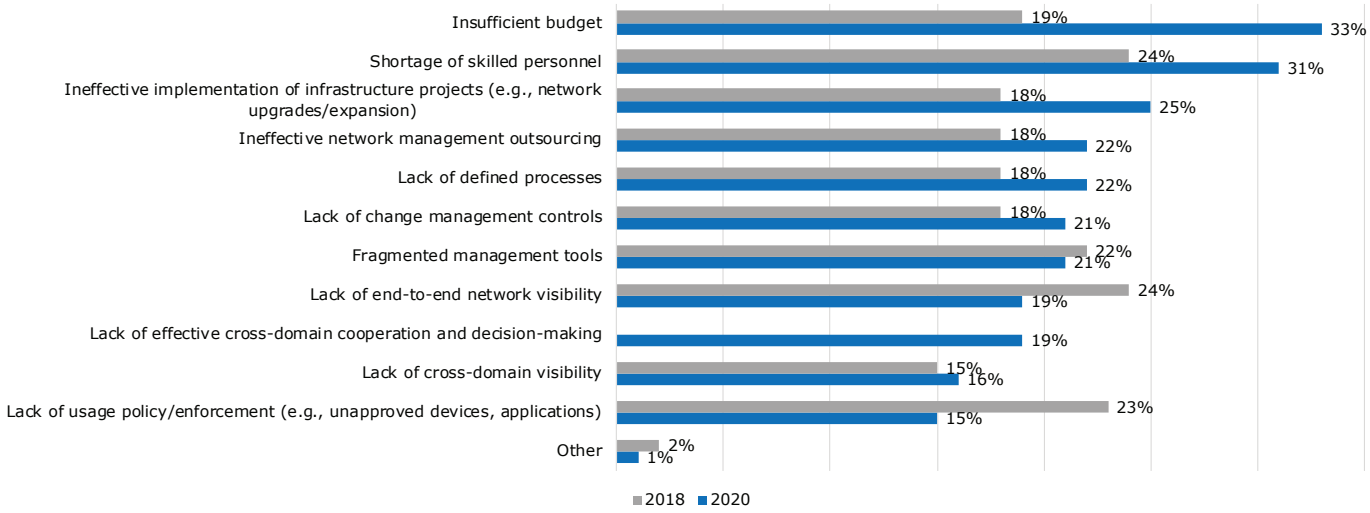


Figure 12. Top challenges to network operations success: 2020 vs. 2018

The shortage of skilled personnel remains prominent, but the rest of 2018's top challenges have subsided. EMA will look at factors that explain the decline of tool fragmentation later in this report. The apparent mitigation of other issues is harder to explain, though shifting business conditions may have caused other challenges to be more pressing.

Insufficient budget is the top challenge to network operations this year.

Insufficient budget is the top challenge to network operations this year, which is a first in EMA's ongoing megatrends research. It ranked as only the 5th leading challenge in 2018. This suggests that new investments in technology, like SDN, SD-WAN, IoT, and cloud, are putting pressure on network management budgets. For instance, this research found that many enterprises buy new tools to manage networking in the public cloud. That's one more tool to purchase and administer.

Ineffective implementation of infrastructure projects also emerged from obscurity in previous years to be a major challenge in 2020. A tremendous amount of network transformation occurred over the last few years, such as SD-WAN adoption, data center SDN, multi-cloud and hybrid cloud networks, next-generation Wi-Fi, and Ethernet upgrades from the core to the edge. It's fair to say that some of these implementations have failed to meet expectations and network operations teams are struggling to mitigate. For instance, EMA research previously found that early adopters of SD-WAN had experienced higher incidences of security breaches at remote sites.

Secondary challenges in 2020 include a lack of defined processes, ineffective outsourcing of network management, tool fragmentation, and a lack of change management controls. Large enterprises struggle more often with a lack of defined processes (26%) and cross-domain visibility (21%), which are issues that become more important with the increased complexity associated with scaled-out networks. Europeans are less likely (9%) to struggle with cross-domain visibility.

Successful network operations teams are more likely (25%) to view poor cross-domain cooperation and decision-making as a major challenge, and they are less likely to struggle with budget problems (22%) or personnel shortages (24%).

© 2020 Enterprise Management Associates, Inc. | www.enterprisemanagement.com

A View From the NetOps Trenches: Problem Detection, Troubleshooting, Remediation

In this section, EMA examines how network operations tasks and processes are functioning by going down a level, from self-assessment of success to the hard details of what's going right and what's going wrong with the network management team.

First are some tooling issues. EMA asked individuals to estimate what percentage of IT service problems are first experienced and reported by end users before network operations teams are aware of them. In other words, do network monitoring tools adequately reveal service problems to IT operations teams in a timely manner?

Figure 13 reveals how the mean response to this question has changed over the last six years. From 2014 to 2018, survey respondents remained quite steady, reporting that end-users were responsible for detecting about 40% of all service problems, which means that 40% of the time, a service problem is already impacting the business before the IT organization can respond. The mean response in 2020 is only 33%, which represents a significant decline from the status quo. Has the industry really improved this much, or is this just a fluke? EMA sees some other changes in the enterprise that could validate this improvement, such as consolidation of network management tools. EMA will review these indicators later in this report.

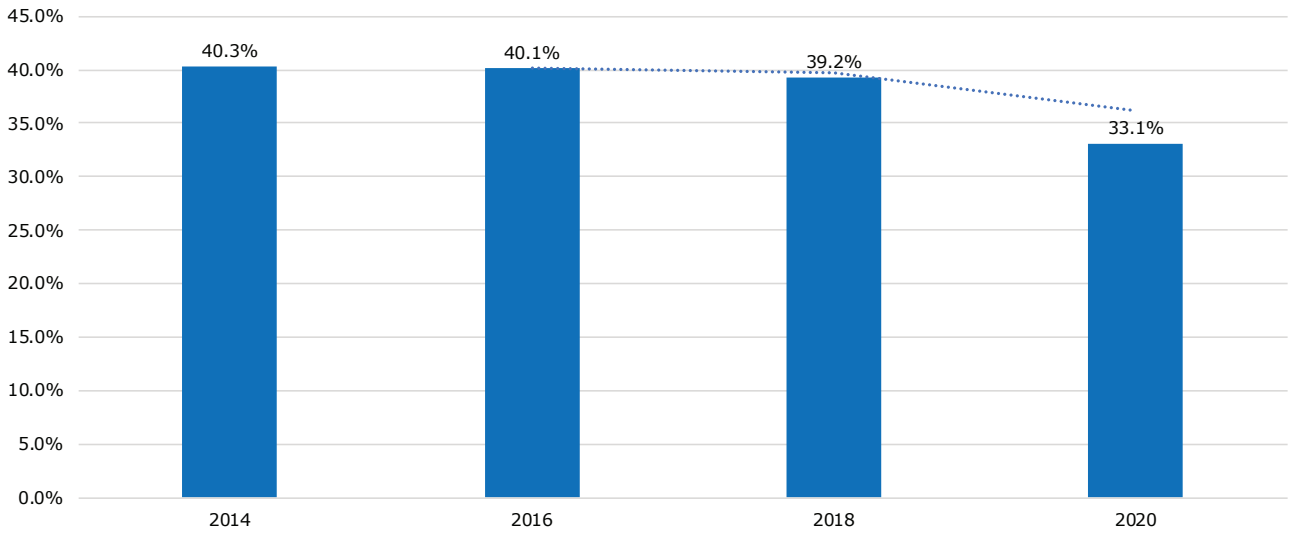


Figure 13. Percentage of IT service problems experienced and reported by end users before NetOps can detect them

Respondents who manage small networks (fewer than 500 devices) reported higher rates of user-based problem detection (39%) this year, versus 30% in networks of 500 to 2,499 devices and 29% in networks of 2,500 or more devices.

© 2020 Enterprise Management Associates, Inc. | www.enterprisemanagement.com

Figure 14 shows that traffic growth will put pressure on a network management team's ability to proactively detect service trouble. Respondents who project 100% or more traffic growth in 2020 rely on end users to detect 41.2% of problems. Effective capacity management tools will be essential to mitigating this operational gap.

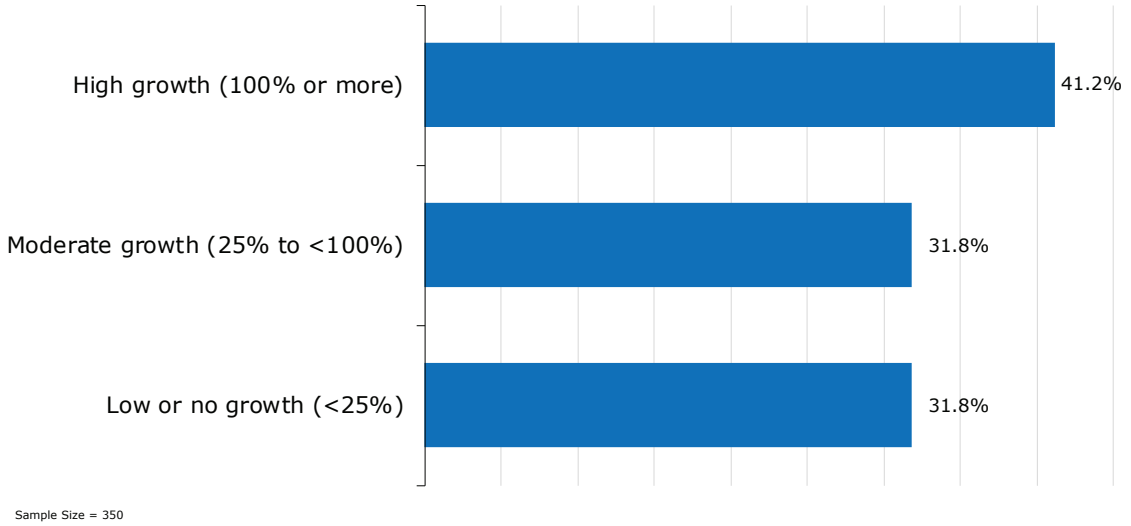


Figure 14: Enterprises with projected high rates of network traffic growth are less effective at IT service problem detection

Figure 15 reveals that the typical network operations professional spends more than half of his or her day keeping the lights on, and most of that time (nearly 30% of the day) in reactive troubleshooting mode. Nearly 27% of the day is spent proactively preventing problems through tasks like operational monitoring and capacity management. That leaves about a quarter of the day to strategic projects, with the least amount of time spent on other tasks (such as keeping up with email, meetings, having lunch).

The typical network operations professional spends more than half of his or her day keeping the lights on.

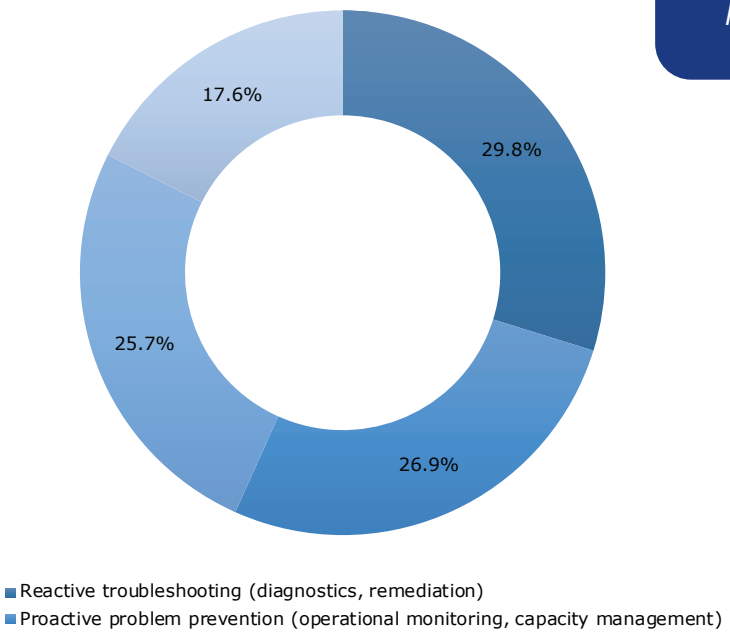


Figure 15. The typical network manager's workday

© 2020 Enterprise Management Associates, Inc. | www.enterprisemanagement.com

In previous years, EMA found that network managers spend about 65% to 70% of their day keeping the lights on; however, in the past this question was asked a little differently by adding "strategic projects" as a multiple choice option. EMA wanted to understand how much time network teams are able to devote to things like cloud enablement and network transformation.

Perceptions of how the workday plays out varies by IT group. Application management said network managers spend only 22.5% of the day on reactive troubleshooting. The cross-domain support organization placed the amount of time spent on reactive troubleshooting at 50%. DevOps said 33.8% of network management time is devoted to proactive problem prevention. Application management sees proactive problem management consuming 38.3% of the day. On the other side of the spectrum, the cross-domain support team estimated 20% devoted to proactive problem prevention, and the IT analytics team put it at 16.2%.

Managers of large networks (2,500+ devices) devote more time to reactive troubleshooting (34%). North Americans also spend more time on reactive troubleshooting (31%) than Europeans.

Figure 16 shows that successful network teams devote a larger part of their day on proactive problem prevention (29.7%) than somewhat successful teams (25.1%). This finding reinforces the importance of establishing network management tools and processes that allow operations to detect and remediate problems before they affect end users and customers.

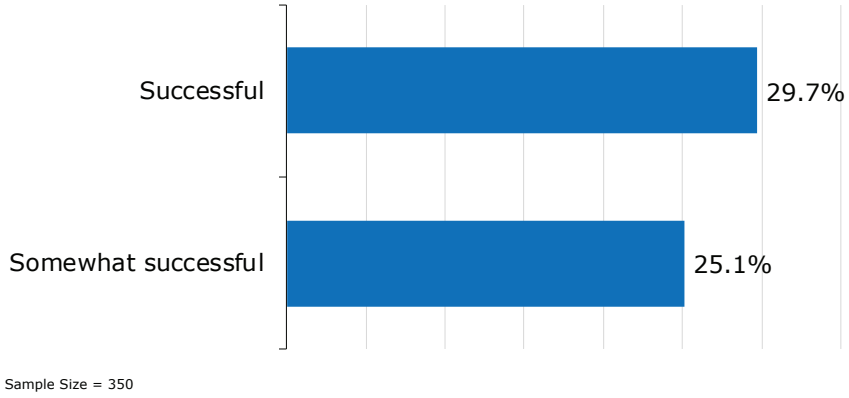


Figure 16. Successful network teams spend a larger percentage of their day on proactive problem prevention

Reactive troubleshooting still consumes much of the network manager's day, in part because tools are inefficient. EMA asked respondents to estimate how many of the alerts generated by their network monitoring tools were actionable and indicative of a real problem. The mean response was 42.7%. This high rate of false alarms will inevitably produce alarm fatigue. Network managers are spending too much time sorting out actionable alerts, which reduces their efficiency.

Figure 17 shows that enterprises with large networks tend to have more efficient tools with fewer false positives.

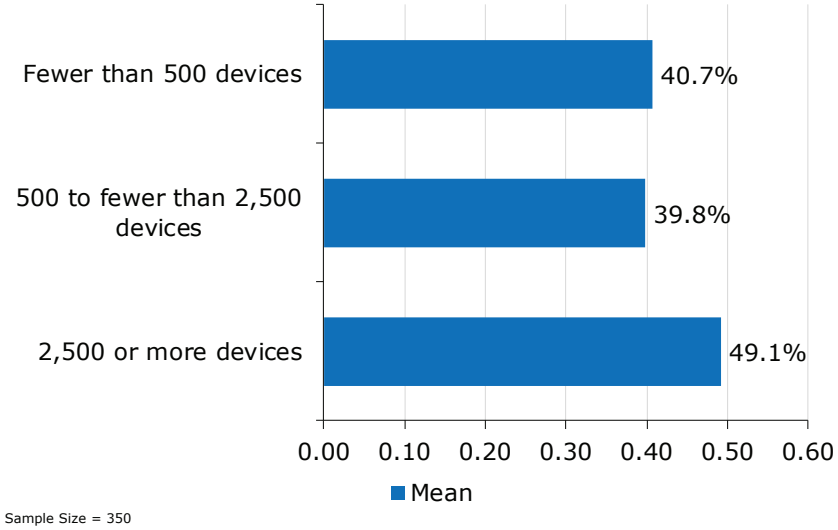
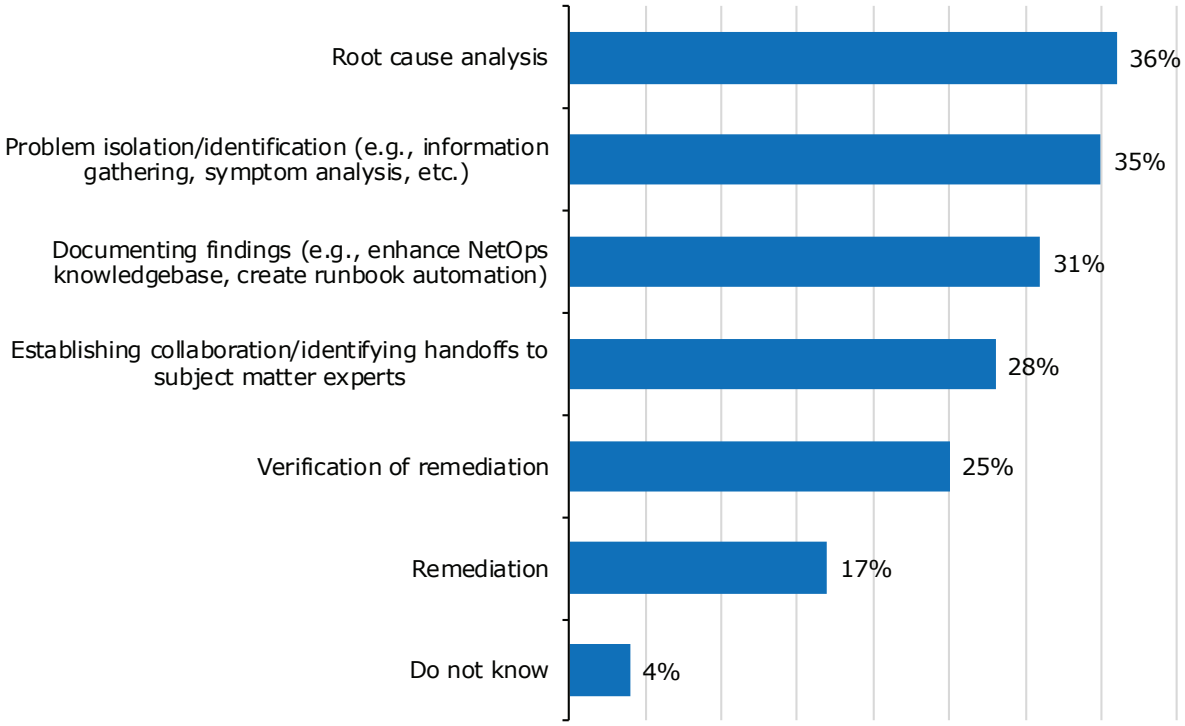


Figure 17. Percentage of alerts generated by network monitoring tools that are actionable and indicative of a real problem—large networks have more efficient tools

© 2020 Enterprise Management Associates, Inc. | www.enterprisemanagement.com

Network management tools are also poor at supporting the processes that IT organizations follow to resolve IT service problems. EMA asked research participants to identify which aspects of network troubleshooting and diagnostics tasks are least supported by their network management tools. **Figure 18** reveals that root-cause analysis and problem isolation/identification are at the top of the list.



Sample Size = 350, Valid Cases = 350, Total Mentions = 614

Figure 18. Network diagnostics and troubleshooting processes least supported by network management tools

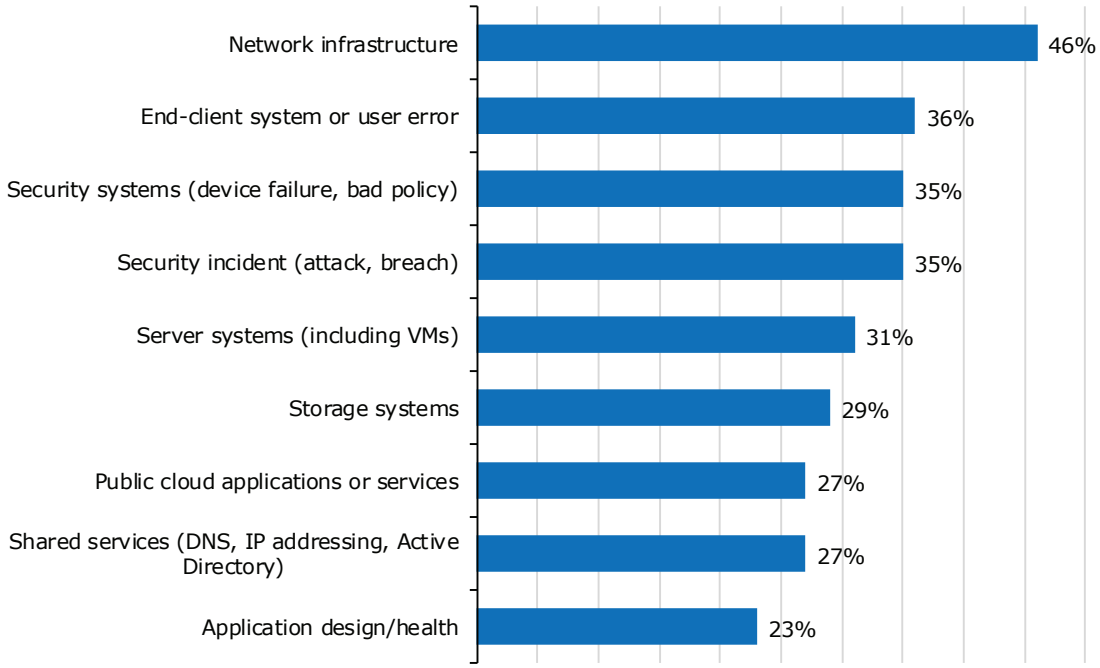
These findings are extremely troubling because these are the two key workflows for finding and diagnosing a problem. This data suggests that network management vendors need to improve their troubleshooting workflow support. Good root-cause analysis support is especially critical in network management tools. Enterprises with successful network operations are less likely (28%) to struggle with this, suggesting that they have the right tools for this task. Europeans (25%) are also less likely to struggle with root-cause analysis.

Problem remediation and verification of remediation are best supported, which makes sense. These are usually a matter of making configuration changes and then monitoring the network to see how those changes play out.

EMA found that enterprises that use 11 or more tools to monitor and troubleshoot their networks are more likely (40%) to struggle with establishing collaboration and identifying handoffs to subject matter experts. On the bright side, they struggle less often (21%) with root-cause analysis.

© 2020 Enterprise Management Associates, Inc. | www.enterprisemanagement.com

Problem isolation and root cause analysis need to be better supported, especially when one thinks about the complexity of many IT service issues. Every two years, EMA asks research participants to identify the root causes of their three most recent complex IT service problems: those which required collaboration across IT domains. **Figure 19** reveals that network infrastructure is the most common problem, but by no means the root cause of the majority of issues. End-user issues, security system problems (bad policies, device failures), and security incidents are also common causes of service trouble. These top four root causes were also in the top in EMA's 2018 megatrends research. However, in 2018, security incidents were significantly more common than security systems and end-user issues.



Sample Size = 350, Valid Cases = 350, Total Mentions = 1,018

Figure 19. Root causes of the three most recent complex service issues that required cross-IT collaboration

Security incidents are a more common problem for enterprises that anticipate high traffic growth this year (45%), versus those with low or no traffic growth (11%). The largest networks represented in this survey are more likely (58%) to identify the network as the root cause. Successful network operations teams are more likely to identify security systems (45%) and server systems (37%) as a root cause of complex issues.

© 2020 Enterprise Management Associates, Inc. | www.enterprisemanagement.com

Network management is typically dominated by manual processes, which explains the prevalence of the network as a frequent root cause of IT service problems. Network management is vulnerable to manual errors that can take down connectivity, create bottlenecks, and introduce vulnerabilities. EMA asked survey respondents to estimate how many of their network problems are caused by these mistakes. As **Figure 20** indicates, EMA found that nearly 26% of all network problems are caused by manual errors.

Nearly 26% of all network problems are caused by manual errors.

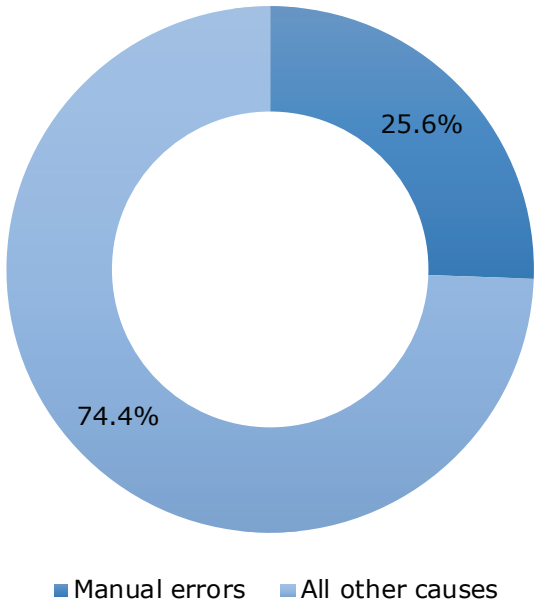


Figure 20: 25.6% of all network-related network problems are caused by manual errors

© 2020 Enterprise Management Associates, Inc. | www.enterprisemanagement.com

THE NETWORK MANAGEMENT ORGANIZATION

This section explores several aspects of how enterprises organize the network operations function. Given that many companies are pursuing digital transformation, the network is increasingly a strategic asset. Its health and performance is critical to digital services. IT leadership should organize the network operations function to meet these requirements.

Cross-Domain Operation Center Replacing the Traditional NOC

Enterprises are shifting toward a multi-disciplinary approach for operational monitoring of infrastructure. As **Figure 21** demonstrates, over the past two years, the number of enterprises that conduct network operations monitoring via a converged, cross-domain operations center has increased significantly, while traditional, independent network operations centers (NOC) have become less common. Also, fewer enterprises are relying on informal, distributed operations.

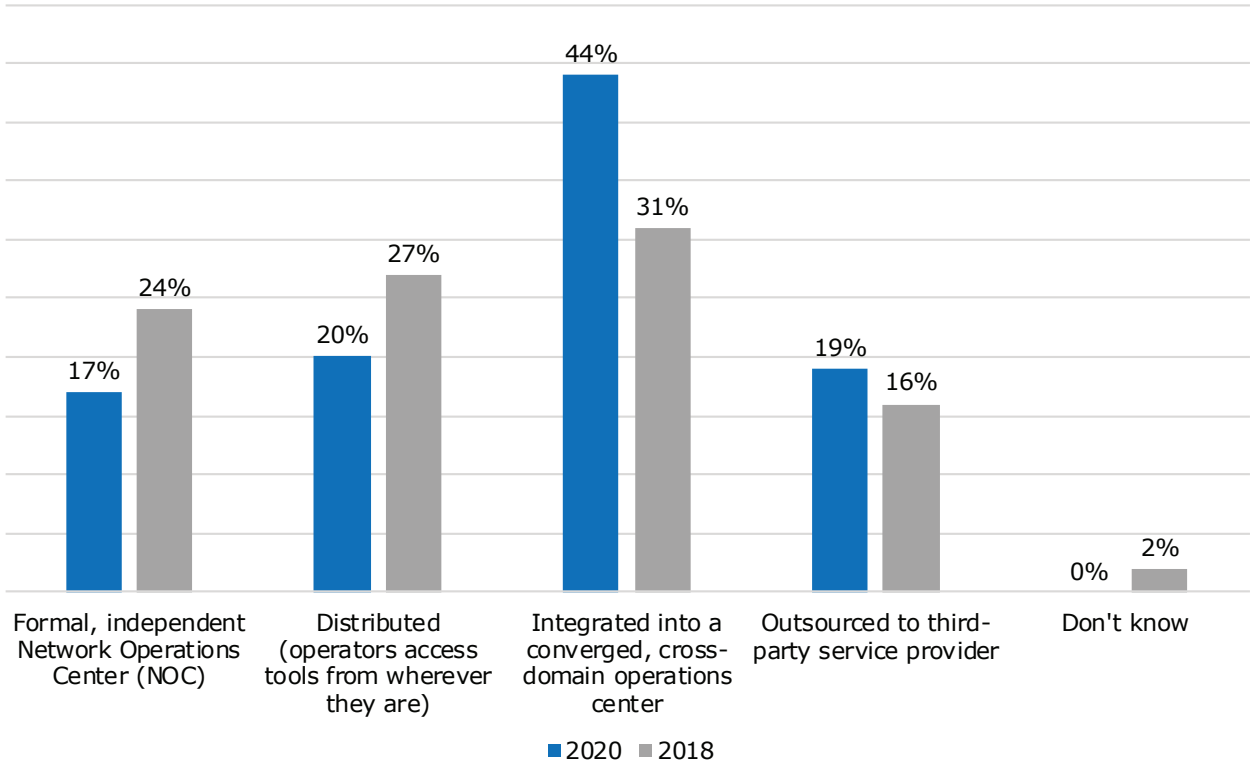


Figure 21. Primary approach to conducting network operations monitoring: 2020 vs. 2018

Collaboration is the touchstone here. EMA recommends that network managers tighten their connections with their peers in other domains of the IT organization. The adoption of cross-domain best practices and shared or integrated tools is a good start. Many teams are pushing toward organizational change to support that collaboration. These measures should streamline IT operations and improve overall IT service delivery.

However, cross-domain IT operations centers are necessarily a best practice. Independent NOCs have existed for years, providing a center of expertise and best practices. Breaking up an NOC to establish a cross-domain operations center can cause disruption. Notably, EMA found that enterprises that are successful with overall network operations are more likely (22%) to have a standalone NOC, versus just 14% of somewhat successful organizations. Clearly, some organizations thrive with a traditional NOC.

© 2020 Enterprise Management Associates, Inc. | www.enterprisemanagement.com

Network Management Outsourcing

Many enterprises will outsource aspects of network operations to a managed services provider to save money, close skills gaps, or improve overall operations. This year's megatrends research found that 49% of enterprises outsource some aspect of network management, as **Figure 22** illustrates. This chart represents a significant decline from 2018, when 58% of enterprises were outsourcing.

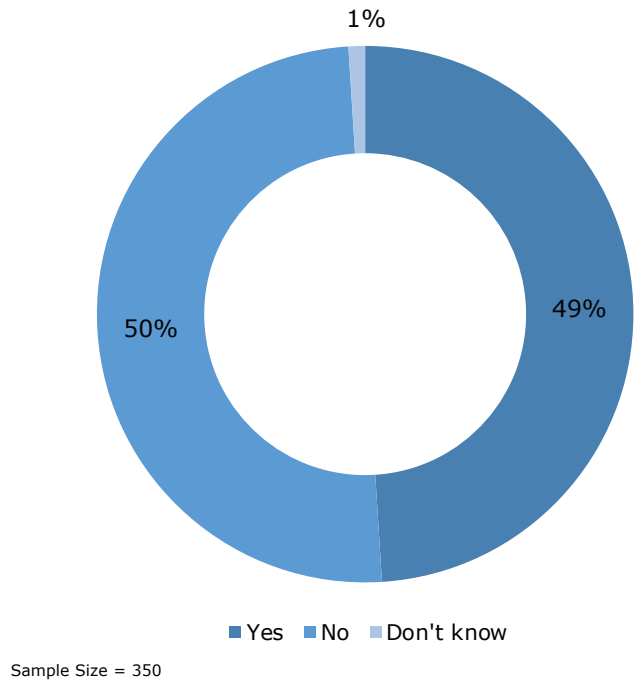


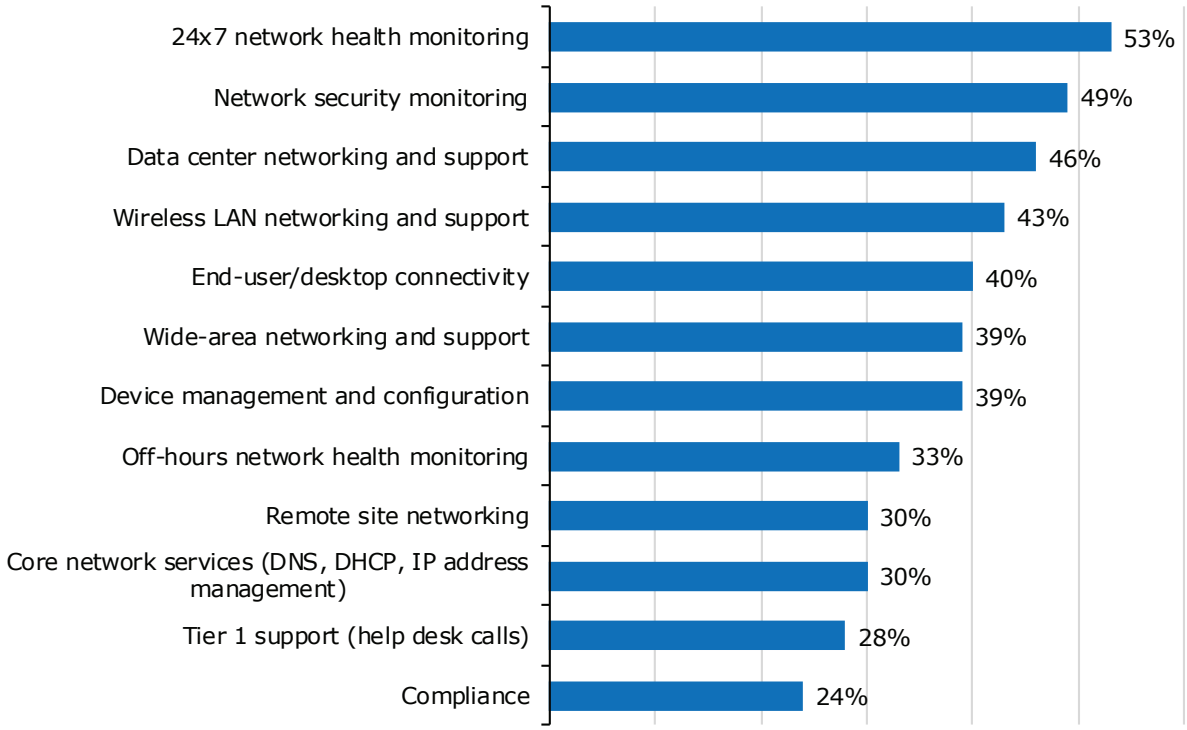
Figure 22. Are any aspects of your organization's network management activities provided by and/or outsourced to a managed services provider (MSP)?

Successful network teams are more likely to outsource aspects of network management (60%), suggesting it's a best practice to outsource functions that aren't strategic to a network team's core capabilities. For instances, if the network team lacks Wi-Fi expertise, it may consider outsourcing some or all of its Wi-Fi management.

Sometimes, the growth of a business can force the network team to outsource in order to keep up with demands on their core expertise. For example, enterprises that project the highest amount of traffic growth on their networks this year are more likely (64%) than those with moderate growth (48%) or low or no growth (43%) to outsource network management.

© 2020 Enterprise Management Associates, Inc. | www.enterprisemanagement.com

Figure 23 reveals the aspects of network management that enterprises are outsourcing. Please note that EMA asked respondents to select management activities that are fully or partially outsourced. Thus, while a majority of enterprises are outsourcing 24x7 network health monitoring, EMA doesn't believe that the majority of them have completely outsourced that activity.



Sample Size = 171, Valid Cases = 171, Total Mentions = 773

Figure 23. Aspects of network management that are fully or partially outsourced

Other top targets for outsourcing are network security monitoring and data center networking and support. Enterprises are least likely to outsource remote site networking, core network services, Tier 1 support (help desk calls), and compliance. However, successful organizations are more likely to outsource Tier 1 support (38%) and compliance (33%), suggesting two potential best practices for outsourcing targets.

© 2020 Enterprise Management Associates, Inc. | www.enterprisemanagement.com

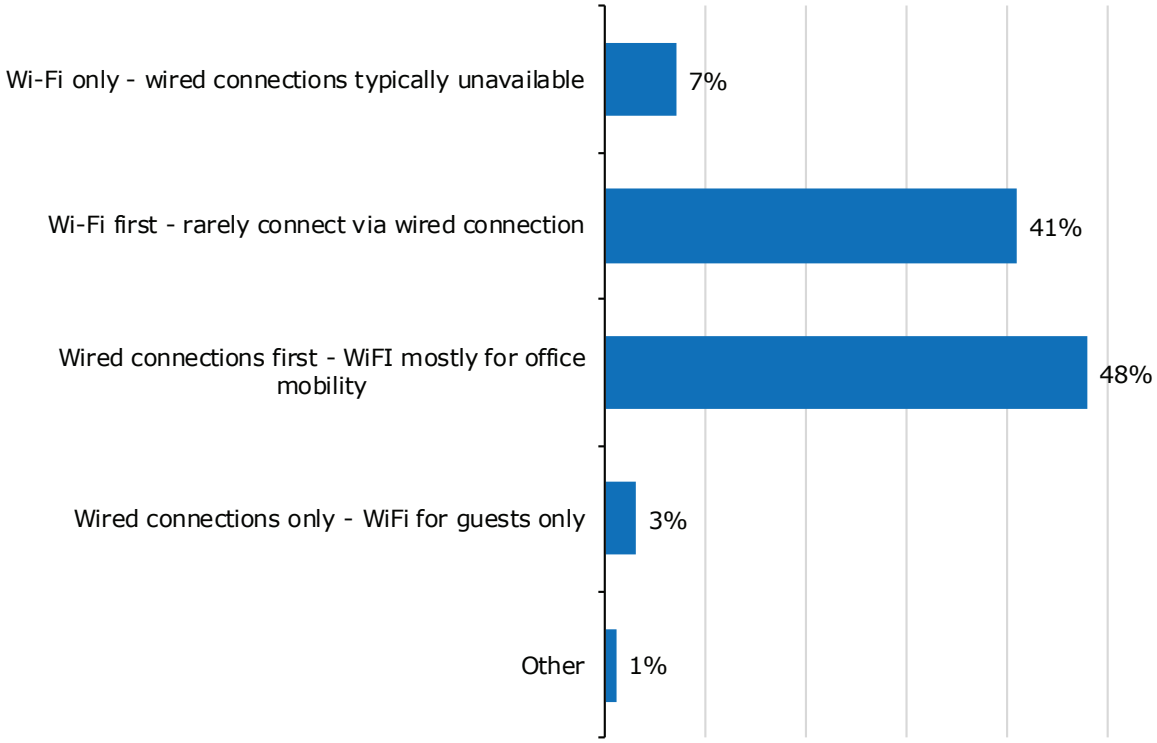
Enterprises that expect the most growth on their networks in the coming year are more likely to outsource 24x7 network health monitoring (65%), wireless LAN networking and support (59%), and network security monitoring (62%).

49% of respondents said their users primarily rely on Wi-Fi to connect to the enterprise network.

Wi-Fi Operations

Wi-Fi technology has advanced significantly over the last decade, making it faster and more reliable. Combined with its convenience, Wi-Fi is rapidly becoming the preferred access technology for enterprise networks. Thus, successful approaches to Wi-Fi operations are becoming more critical.

Figure 24 reveals how critical Wi-Fi connectivity is to businesses today. It shows how users typically connect to the network in campus and branch offices. Overall, 49% of respondents said their users primarily rely on Wi-Fi to connect to the enterprise network. That includes 7% who are "Wi-Fi-only," with wired connections typically unavailable and 41% who are "Wi-Fi first," with wired connections available but rarely used. Successful network operations teams are more likely (11%) than unsuccessful ones to support a Wi-Fi-only network. Europeans (30%) are less likely to adopt a Wi-Fi first approach and more likely to adopt wired-first (56%).



Sample Size = 350

Figure 24. How users typically connect to the enterprise network in campus and branch offices

© 2020 Enterprise Management Associates, Inc. | www.enterprisemanagement.com

More than half of enterprises still primarily rely on wired connections for user access, including 48% who take a "wired-first" approach, with Wi-Fi mostly used for office mobility. These enterprises will typically have less wireless capacity. EMA suspects that as these enterprises upgrade to newer generations of Wi-Fi infrastructure, they will move away from wired connectivity.

EMA also asked respondents to identify the generation of Wi-Fi tech that is most prevalent across their networks. **Figure 25** reveals that legacy technology is quite rare. Only 5% are on 802.11a/b/g or older. At 16%, 802.11n is also relatively uncommon, but it is more prevalent in the government (40%) and utilities/energy (43%) sectors, where infrastructure investment cycles are known to lag.

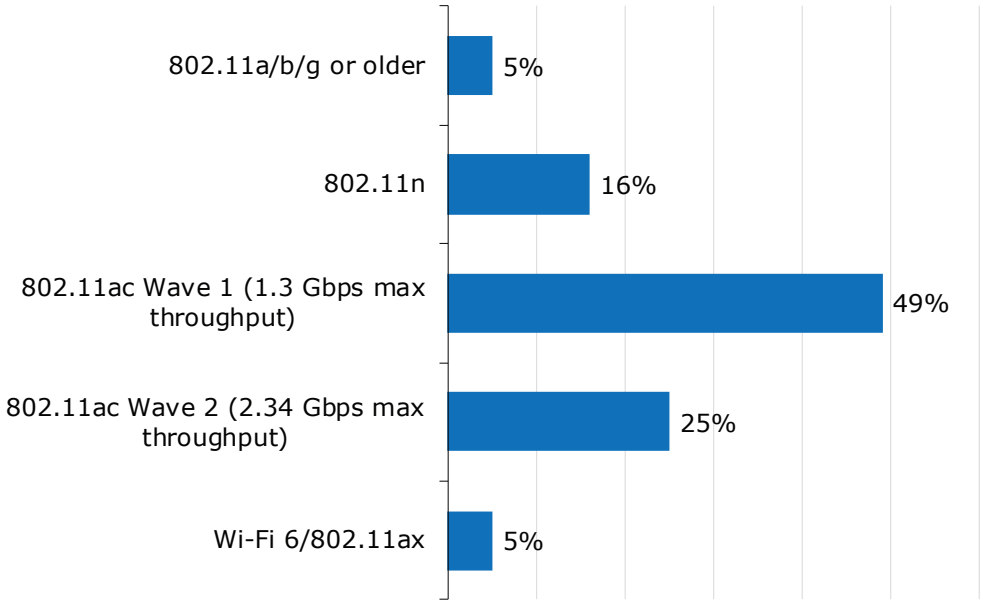


Figure 25: Generation of Wi-Fi technology most prevalent in networks

Nearly three-quarters of companies are primarily using 802.11ac Wi-Fi technology, although the bulk of that cohort is still on the slower Wave 1 generation of 11ac. Wi-Fi 6 technology, which only became commercially available in the last year, is relatively rare.

EMA found that successful network teams tend to be more advanced with Wi-Fi. For instance, 35% of them are primarily using 802.11ac Wave 2 and 12% of them are primarily at Wi-Fi 6. Projected network traffic growth also correlates with more advanced Wi-Fi. Thirty-eight percent of enterprises that are projecting the highest growth in traffic are on 11ac Wave 2. On the other hand, enterprises that are projecting the least growth in traffic are more likely (15%) to be primarily using 802.11a/b/g or older.

Wi-Fi management is very different from wired LAN and WAN management. Obviously, the physical layer is extremely different. Radio frequency (RF) spectrum is a major consideration. Also, Wi-Fi has its own set of network protocols that require specific analysis. As a consequence, many enterprises may treat Wi-Fi operations differently from the rest of network operations, because Wi-Fi requires unique tools and specific expertise.

© 2020 Enterprise Management Associates, Inc. | www.enterprisemanagement.com

Figure 26 reveals how enterprises primarily address Wi-Fi management. The majority have a unified team that manages both wired and wireless networking. Less than one-quarter have separate specialized teams, and an equal number primarily outsource wireless management to an MSP.

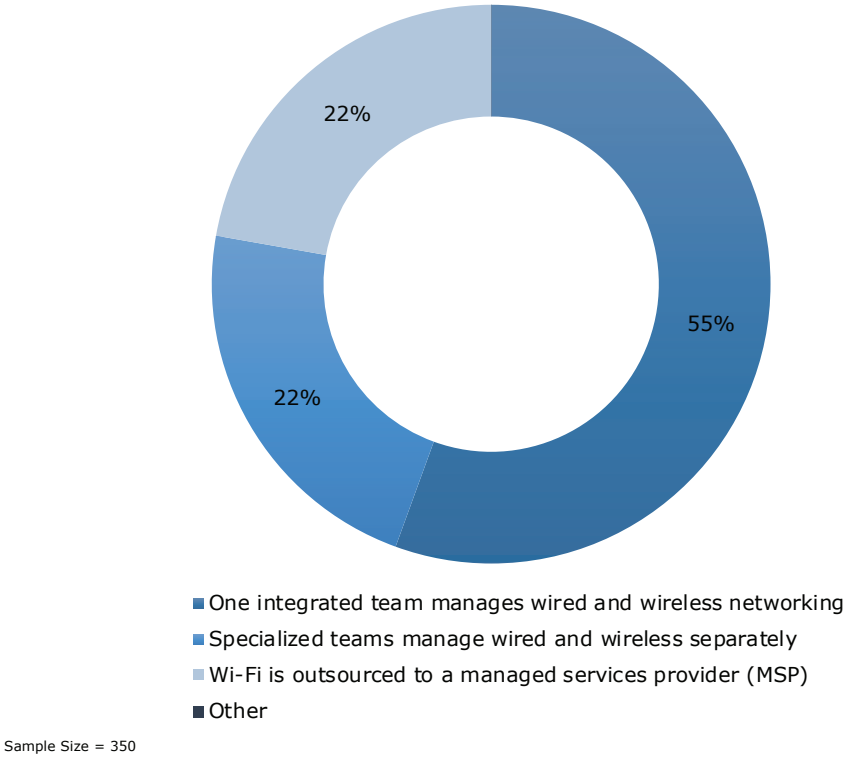


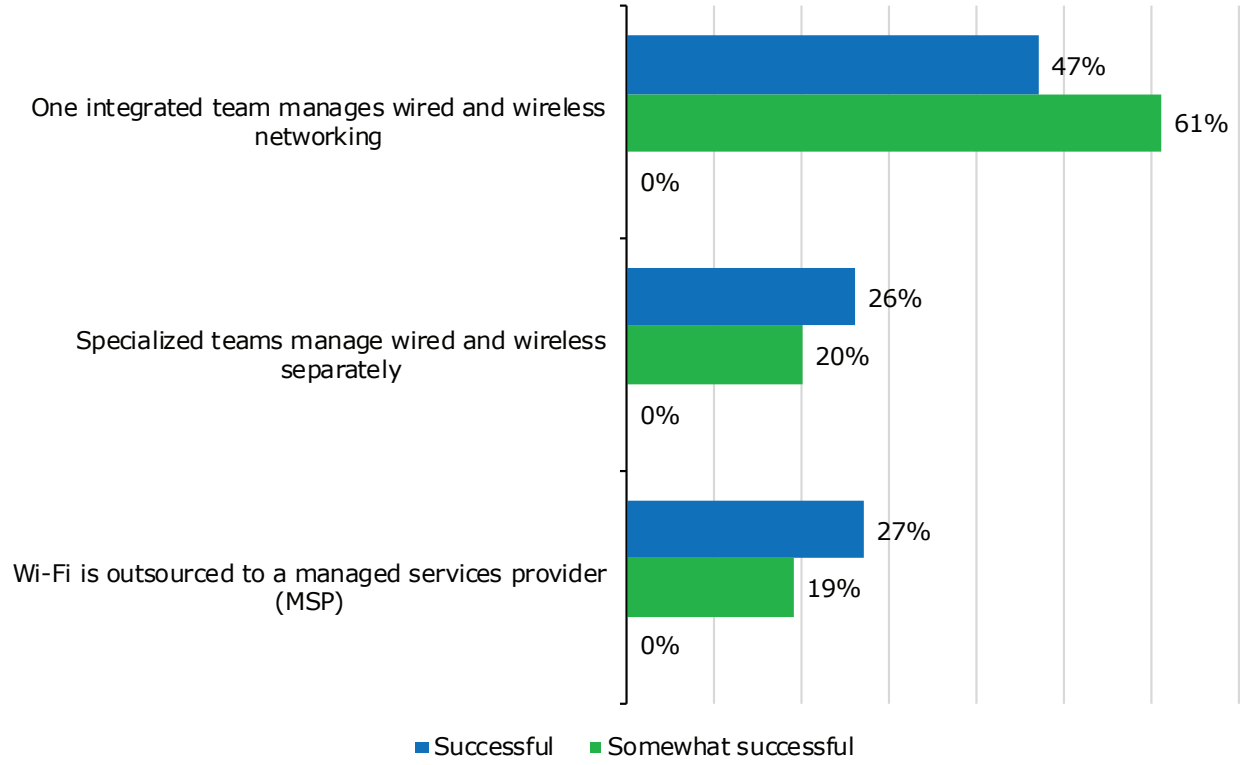
Figure 26. Organizational approaches to managing Wi-Fi wireless LAN infrastructure

Europeans are less likely (9%) to have separate teams and more likely (34%) to outsource. Midsized enterprises are more likely (30%) to have separate teams.

Vendors have evangelized the value of having a unified approach to wired and wireless network management. However, this research suggests that unified management isn't necessarily a best practice.

© 2020 Enterprise Management Associates, Inc. | www.enterprisemanagement.com

Vendors have evangelized the value of having a unified approach to wired and wireless network management. However, this research suggests that unified management isn't necessarily a best practice. **Figure 27** illustrates that successful network teams are less likely to consolidate management. Instead, they silo wired and wireless management.



Sample Size = 350

Figure 27. Successful network teams are less likely to consolidate wired and wireless network operations

EMA doesn't believe that a siloed approach to wireless management is a best practice, but this data does suggest that unified operations may be overrated. For instance, EMA's survey found that consolidated wired and wireless management correlates with a more reactive network operations approach. Enterprises with unified wired and wireless teams spend a higher percentage of their workday (32%) on reactive troubleshooting than siloed, specialized teams (28%). This latter finding suggests operational inefficiency.

© 2020 Enterprise Management Associates, Inc. | www.enterprisemanagement.com

NETWORK MANAGEMENT TOOLS

Overall Tool Strategy: Consolidation and Integration

Regardless of how an enterprise organizes the network operations function, EMA believes that IT organizations need to consolidate their network toolsets. For years, many enterprises had too many tools, leading to fragmented workflows, inefficient data collection and sharing, difficulty in escalating problems to subject matter experts, and more.

Enterprises reduced the number of network management tools they rely on from 2018 to 2020.

EMA always asks megatrends research respondents to estimate how many tools their organizations use to monitor and troubleshoot their networks. Every year, enterprises indicate an interest in reducing the number of tools they use, but until now, EMA has not seen progress. **Figure 28** reveals that enterprises reduced the number of network management tools they rely on from 2018 to 2020. This consolidation is the first significant improvement EMA has observed. The number that use 11 or more tools has declined since 2018, while the number that use only 4 or 5 tools has increased significantly.

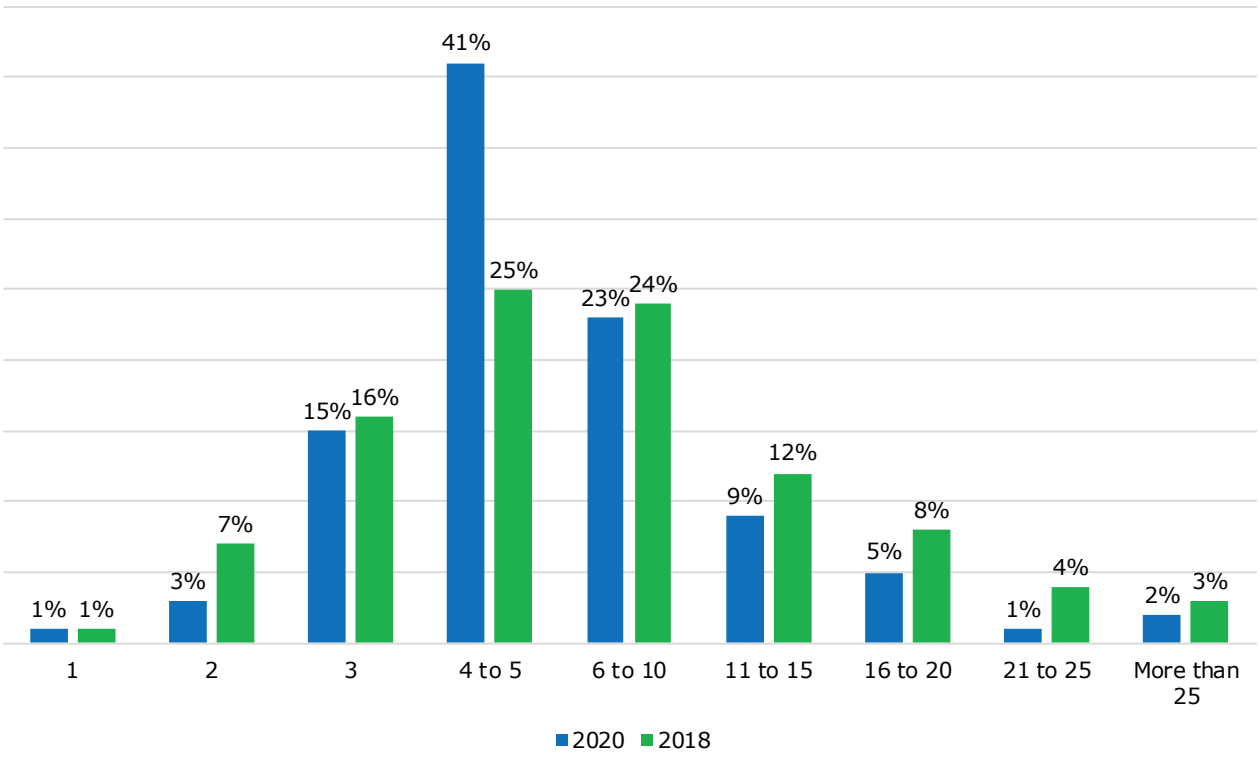


Figure 28. Number of tools used to monitor and troubleshoot the network

Size of toolset has always had some correlation to size of company, and 2020 is no exception. For instance, 50% of all organizations with 1 to 3 tools are midmarket companies. EMA observed something similar with size of network. For instance, 47% of organizations that use only 1 to 3 tools have smaller networks (less than 250 network devices), and no organization with such a small network had 11 or more tools.

However, very large enterprises and very large networks aren't necessarily predictive of a large toolset. For instance, only 18% of organizations with 11 or more tools were very large enterprises, and 25% of enterprises with 11 or more tools had between 500 and 1,000 devices, which is a rather small network for such a large toolset.

© 2020 Enterprise Management Associates, Inc. | www.enterprisemanagement.com

Large Toolsets are not Necessarily a Bad Practice

Enterprises with 11 or more network management tools are most likely (54%) to say they are successful with network operations, versus 28% of those with 1-3 tools and 29% of those with 4-5 tools. These companies with large toolsets are also the most likely (47%) to say that network operations success leads to more IT innovation. While EMA advises a consolidated approach to network management, large toolsets aren't necessarily a harbinger of doom. However, EMA believes that enterprises with large toolsets should find opportunities to integrate those tools for unified workflows and better correlation.

EMA also found that companies with 11 or more tools tend to spend more of their day on proactive problem prevention (30%) than those with 1-3 tools (25%) and 4-5 tools (26%). This finding implies increased effectiveness of the network management team.

The public cloud is a prime example of why enterprises struggle to consolidate network management tools. Fifty-seven percent of the enterprises in this survey have acquired new tools to address their cloud networking monitoring and management requirements. Also, EMA found that organizations with 11 or more network management tools are more likely (33%) to use cloud enablement as a measure of overall network operations success, versus just 10% of those who have 1-3 tools and 8% of those with 4-5.

Regardless of these correlations, network management tool sprawl must be managed carefully. A large collection of siloed tools with no integration will disrupt network operations processes. IT organizations with 11 or more tools are more likely to cite fragmented toolsets (30%) and a lack of cross-domain cooperation and decision-making (28%) as major network operations challenges. Also, teams with 6-10 tools are more likely (32%) to struggle with a lack of defined processes.

Figure 29 examines how enterprises think about these issues when they procure and implement network management tools. EMA has asked this question every two years since 2008. As always, most enterprises prefer unified, multifunction platforms or integrated suites of tools. The most popular procurement strategy is the use of fully integrated, multifunction platforms.

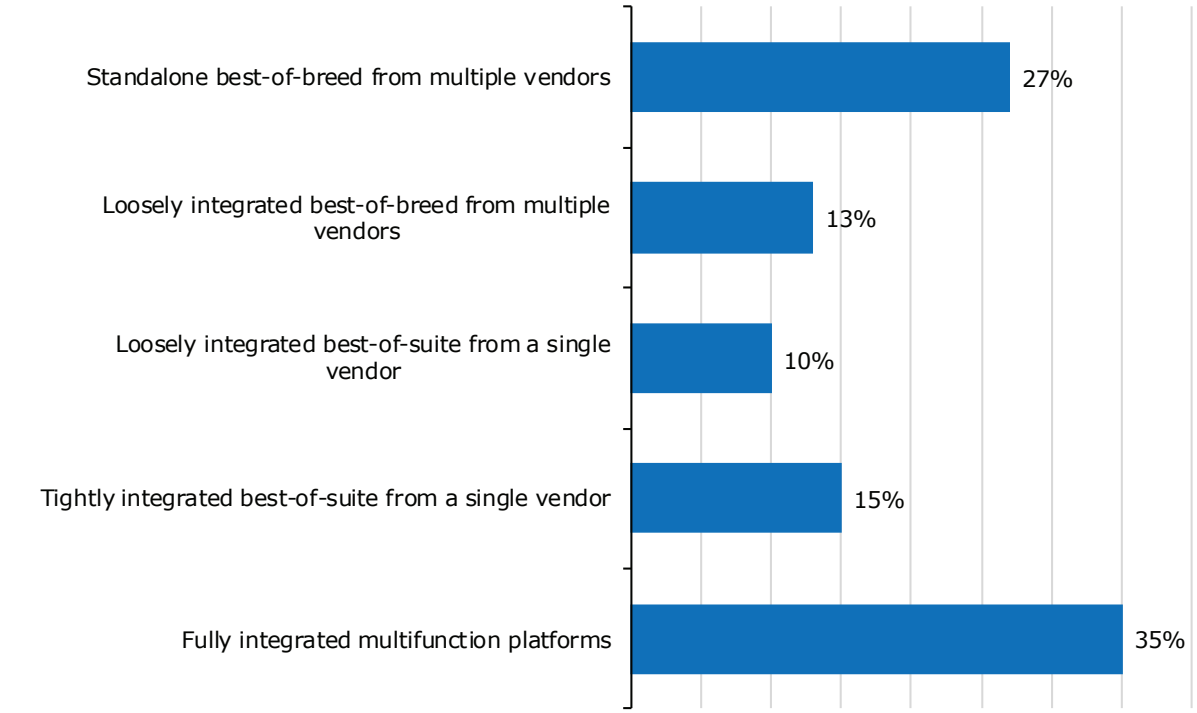


Figure 29. Strategy used when acquiring and deploying network management products

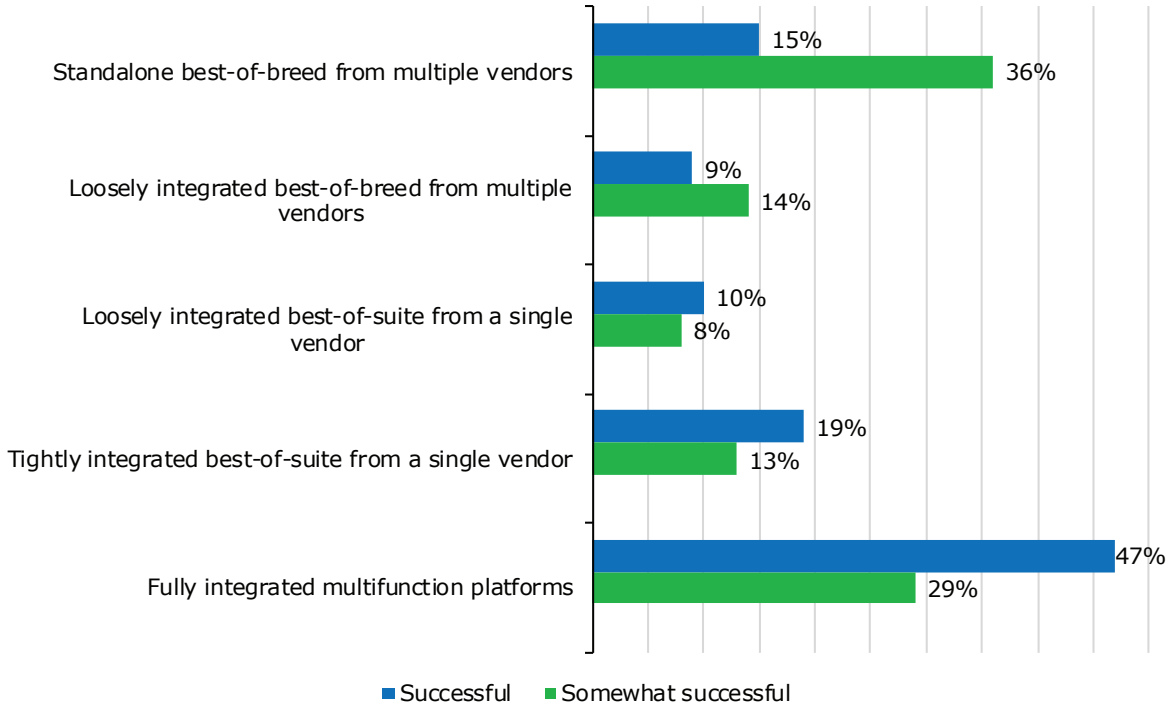
However, the percentage of enterprises that prefer standalone, best of breed tools spiked from 17% in 2018 to 27% this year. EMA believes this is a worst-practice approach to network management tool procurement. While this looks like a shift in the wrong direction for IT organizations, EMA believes this standalone tool strategy has been underreported for years. EMA has always found tool sprawl in this research, and those with the largest toolsets have always processed a unified tool procurement strategy. EMA believes that for many companies, a unified tool strategy is an aspiration, but never a reality.

© 2020 Enterprise Management Associates, Inc. | www.enterprisemanagement.com

There is a very strong correlation between network operations success and an integrated approach to network management tool procurement.

Certain groups in the IT organization have different preferences. For instance, individuals from the IT engineering and architecture group are more likely (37%) to prefer standalone, best of breed tools. DevOps professionals are more likely to procure loosely integrated best of suite tools (26%). The NOC is more likely (28%) to look for tightly integrated, best of suite tools.

Figure 30 reveals that there is a very strong correlation between network operations success and an integrated approach to network management tool procurement. Successful network teams have a clear preference for procuring integrated, multifunction network management tools, but somewhat successful teams are more likely to adopt standalone, best of breed tools. EMA is comfortable in asserting that multifunction platforms and tightly integrated suites of tools are best practice strategies.



Sample Size = 350

Figure 30. Successful network teams prefer tightly integrated network management tools; somewhat successful teams prefer standalone, best of breed tools

© 2020 Enterprise Management Associates, Inc. | www.enterprisemanagement.com

Speaking of integration, **Figure 31** shows that 97% of enterprises require that their network management tools integrate with IT operations management tools inside the organization.

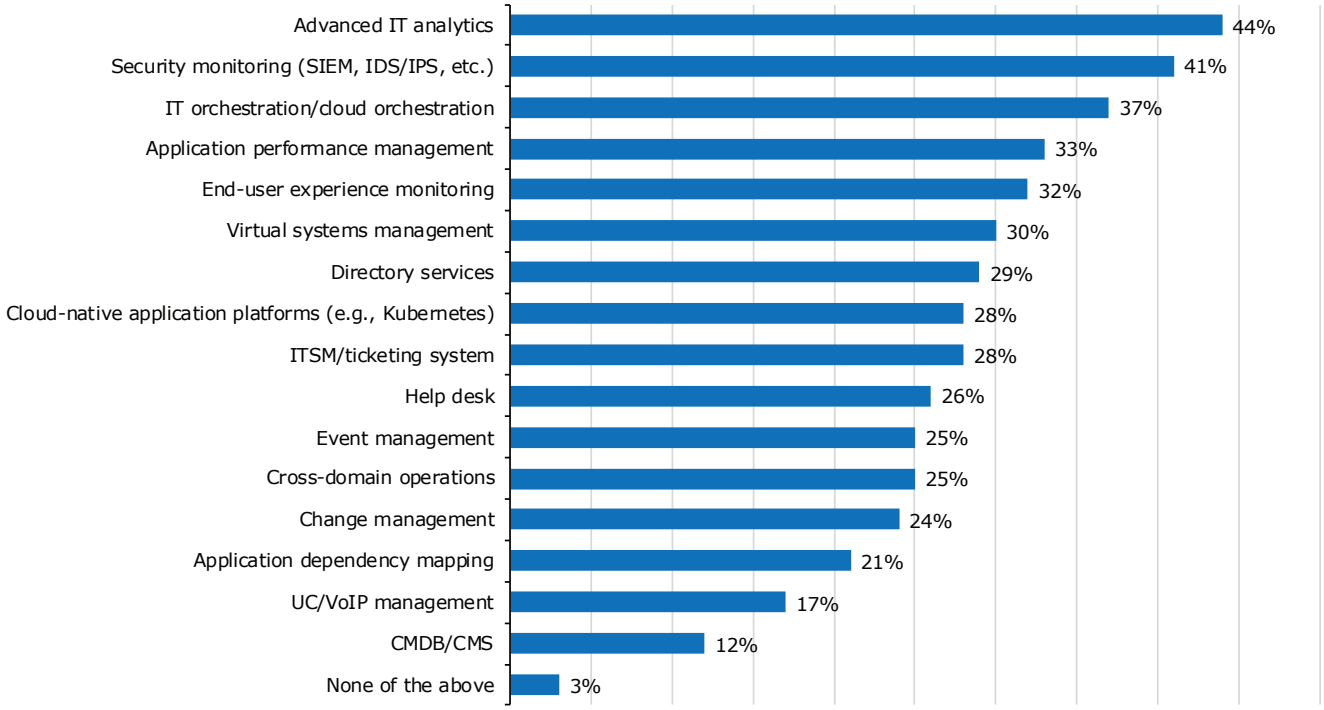


Figure 31. Integration requirements for network management tools

The top three integration requirements are advanced IT analytics (AKA AIOps), security monitoring, and IT orchestration/cloud orchestration tools. These three were the top integration requirements in 2018, too, although in a different order: IT orchestration, security monitoring, analytics.

EMA observed some shifts in other priorities. IT service management, which has been a top integration requirement for years, slipped from 4th in 2018 to 9th this year. Meanwhile, application performance management jumped from 7th to 4th. Cloud-native application platforms (such as Kubernetes) have gone mainstream since EMA's last megatrends study, so this technology was added as a multiple choice option in 2020. Already, 28% of enterprises require that their network management tools integrate with it.

Successful network teams generally are more likely to have the following integration requirements for their network management tools:

- Event management
- Cloud-native application platform management/orchestration
- Security monitoring
- Cross-domain operations consoles
- Help desk
- IT service management

Enterprises that are projecting the highest network traffic growth this year are more likely to require integration with virtual systems management, end-user experience monitoring, and change management.

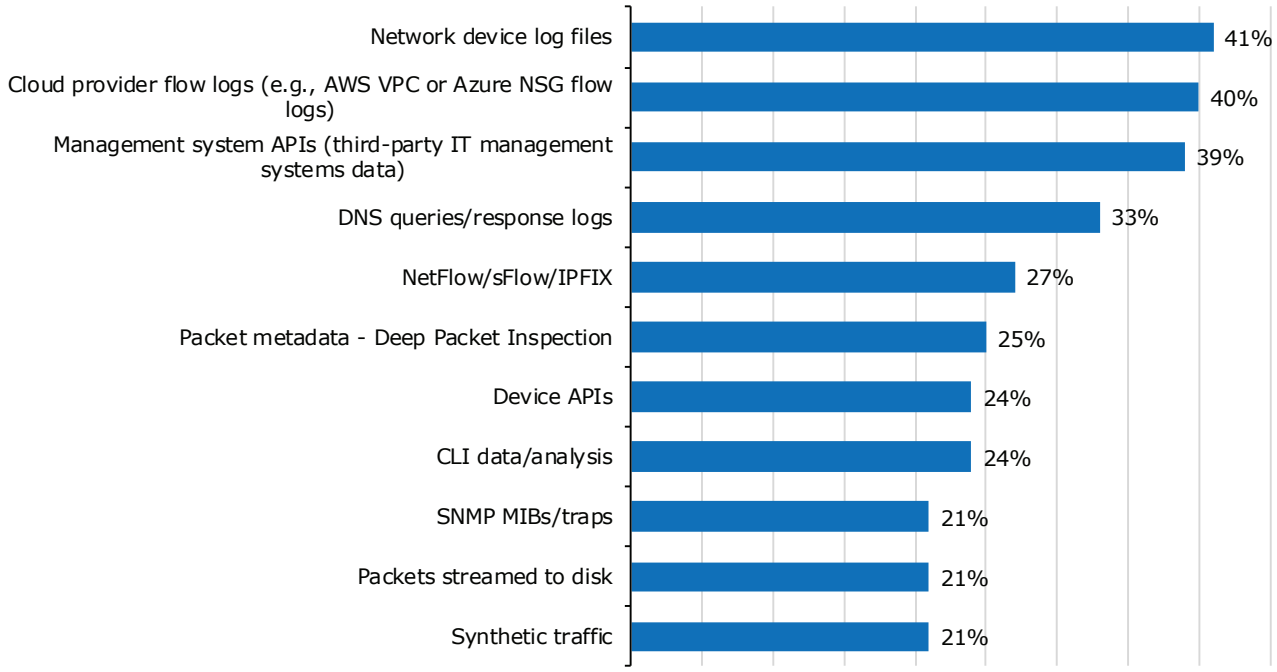
© 2020 Enterprise Management Associates, Inc. | www.enterprisemanagement.com

Network Management Tool Data Sources

EMA's megatrends research asks enterprises on a biennial basis to identify the data they use to support different network management tasks. The responses should not be viewed as accurate adoption numbers. Instead, these responses are reflective of the data sources that are top-of-mind for network managers. They tend to reflect current trends in network operations.

For instance, in 2014, EMA saw rising interested in log files (e.g., switch syslogs). In 2016, network flow records were hot. In 2018, EMA found strong interest in active synthetic traffic. In 2020, EMA is seeing something new.

Figure 32 reveals preferred data sources for sustained network availability and performance monitoring. Enterprises showed renewed interest in device logs this year, after EMA had observed declining interest in them over the last half-decade. Management system APIs (third-party IT management system data) was a priority in 2018 and remains a priority today.



Sample Size = 350, Valid Cases = 350, Total Mentions = 1,112

Figure 32. Popular data sources for supporting sustained network availability and performance monitoring

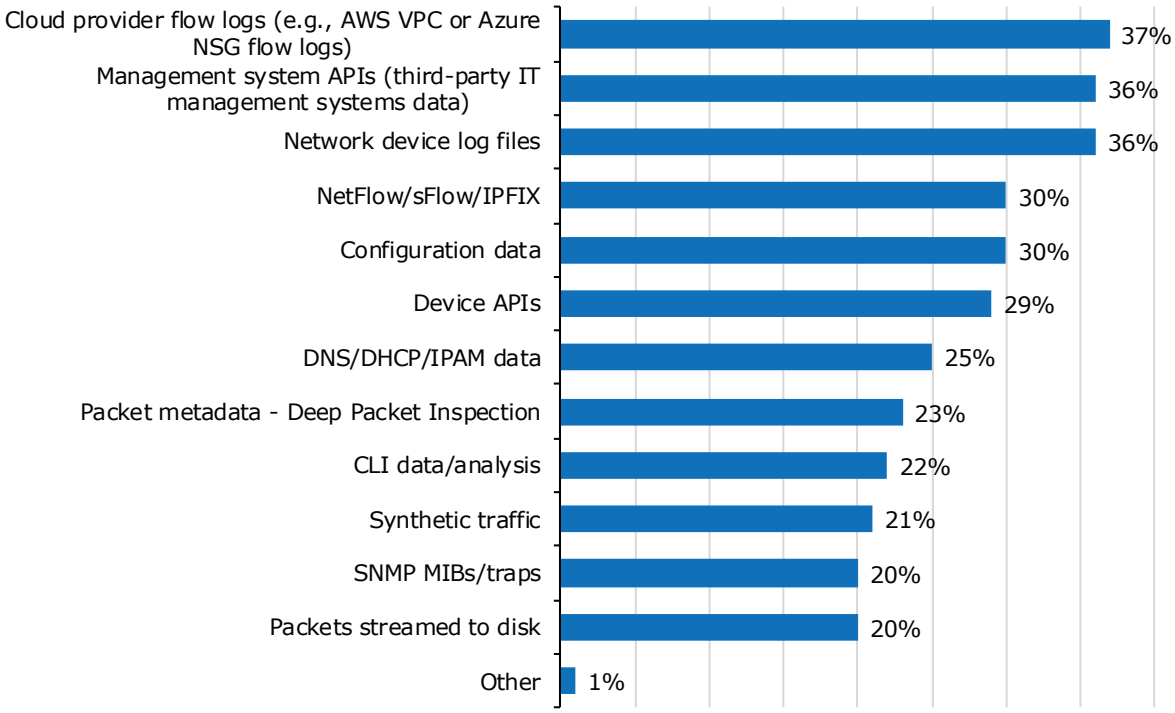
For the first time ever, EMA added cloud provider flow logs, such as AWS VPCs or Azure NSG flow logs, as a multiple choice option to these data questions. It immediately emerged as the number-two priority for sustained network monitoring data. This reflects the growing importance of incorporating public cloud visibility into network management tools and processes.

Successful network operations teams are more likely to value cloud provider flow logs (48%) and management system APIs (50%), which drives home the point that both of these data sources are important to sustained monitoring.

DNS queries and response logs are also quite important to network monitoring. Synthetic traffic, which had been one of the most popular data sources in 2018, dropped to the bottom of the list. However, North Americans (24%) remain more interested than Europeans (13%) in synthetic data. Midsized enterprises are more focused on packets, including packets streamed to disk (33%) and packet metadata for real-time analysis (37%).

© 2020 Enterprise Management Associates, Inc. | www.enterprisemanagement.com

Figure 33 identifies data sources that are popular for network capacity planning and engineering. The top three data sources are the same as they are for sustained monitoring, only in a different order. Network flow data, configuration data, and device APIs are more valuable than they were for monitoring. Synthetic traffic, SNMP MIBs/traps, and packet captures are least popular.



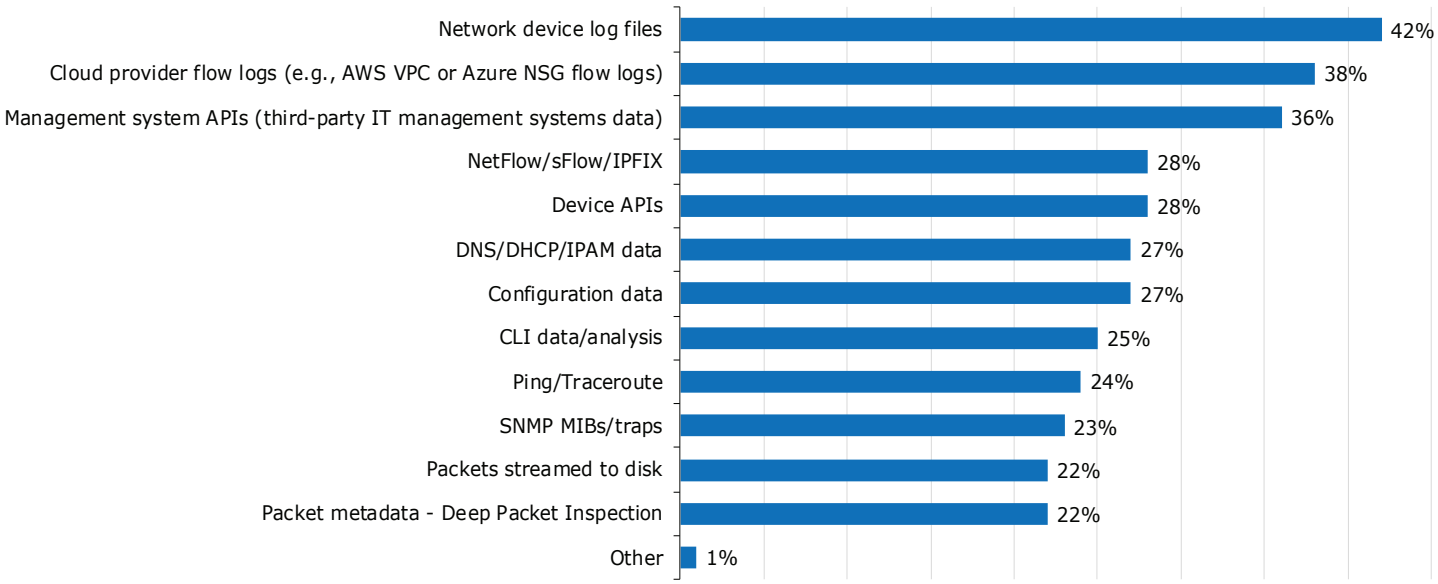
Sample Size = 350, Valid Cases = 350, Total Mentions = 1,152

Figure 33. Popular data sources for supporting capacity planning and engineering

Successful teams are more likely to use Netflow/sFlow/IPFIX (39%) and management system APIs (45%). Midsized companies are more likely to use packet metadata (31%), synthetic traffic (31%), and network device logs (43%).

© 2020 Enterprise Management Associates, Inc. | www.enterprisemanagement.com

Finally, **Figure 34** identifies the data sources that enterprises are focused on for supporting network troubleshooting. Again, the top three data sources are the same as on the previous two charts, only in a different order. Everything else is clearly a secondary data priority, with very little separation between NetFlow at 4th and packet metadata at 12th.



Sample Size = 350, Valid Cases = 350, Total Mentions = 1,201

Figure 34. Popular data sources for supporting network troubleshooting

Large enterprises expressed more interest in using cloud provider flow logs (42%) and DNS/DHCP/IPAM data (31%). Midsized companies expressed more interest in network device logs (51%).

Regardless of what the previous chart revealed, packets remain a critical data source for network operations. To access packets for network management purposes, enterprises typically mirror traffic from multiple points on the network. Depending on the size and complexity of that network, the IT organization may also need to aggregate and groom these mirrored packet flows before delivering them to network operations tools. This is where a network packet broker (NPB) comes in. It aggregates, grooms, and load balances packets that have been mirrored from the network.

© 2020 Enterprise Management Associates, Inc. | www.enterprisemanagement.com

NPBs aren't cheap, so many enterprises will instead plug their tools directly into a mirrored port, rather than add a layer of infrastructure. Despite the potential expense, EMA found that 46% of enterprises are using NPBs today, as **Figure 35** illustrates.

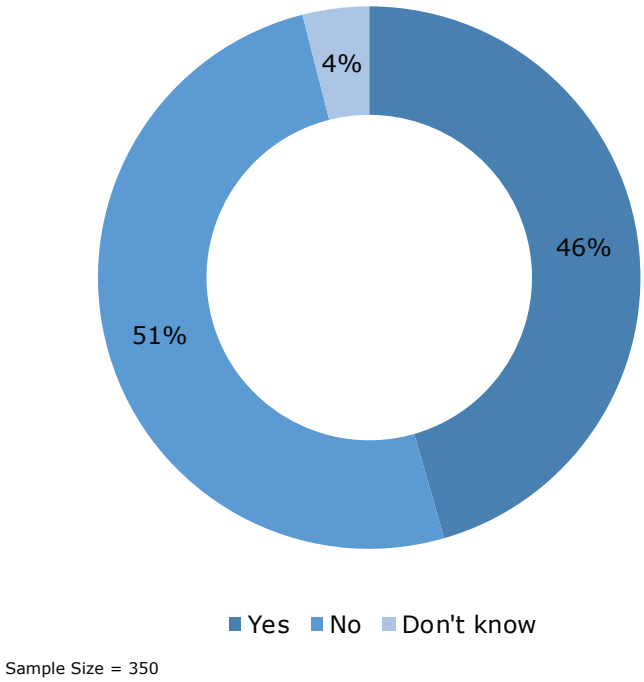


Figure 35. "Does your organization use a network packet broker/network visibility controller to direct traffic to network performance monitoring or diagnostics tools?"

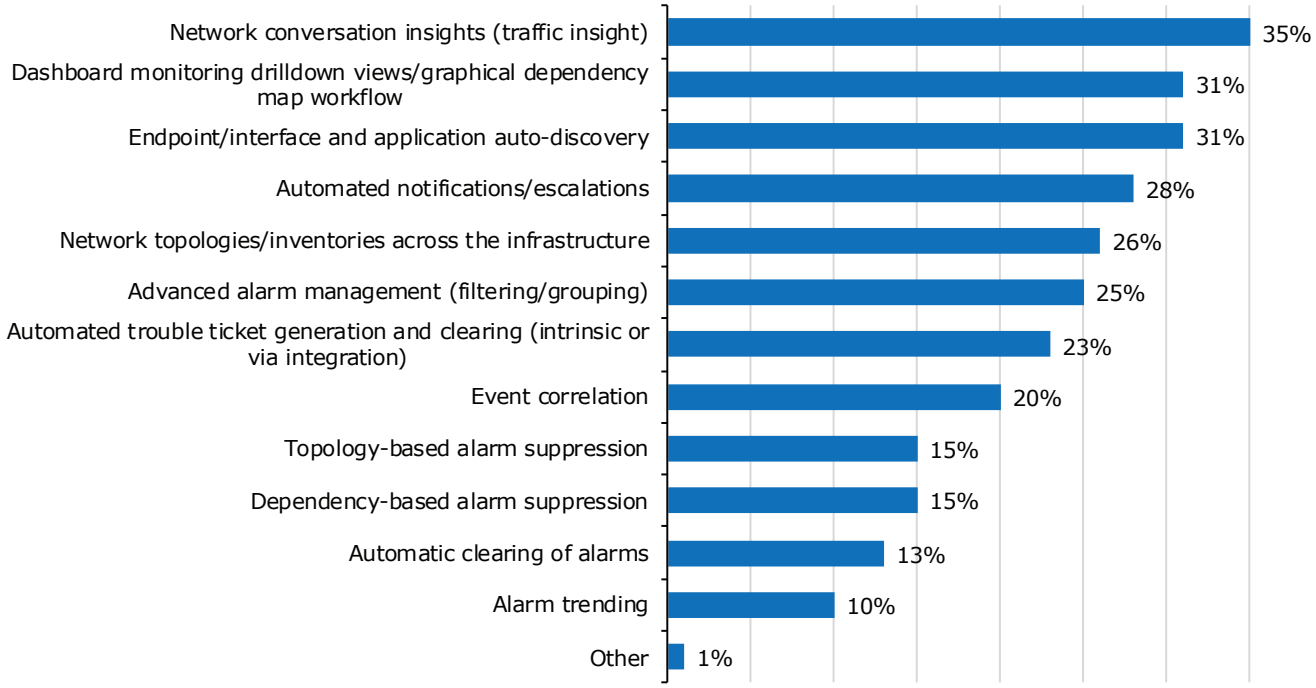
Successful network operations teams are more likely (54%) than somewhat successful teams (42%) to have an NPB deployed, suggesting two things: packets are a valuable source of network operations data and NPBs are essential to packet-based tools. EMA also found that NPB adoption is more common among enterprises projecting high traffic growth this year (62%) versus 28% of those projecting low or no growth.

Successful network operations teams are more likely (54%) than somewhat successful teams (42%) to have an NPB deployed, suggesting two things: packets are a valuable source of network operations data and NPBs are essential to packet-based tools.

© 2020 Enterprise Management Associates, Inc. | www.enterprisemanagement.com

Network Management Tool Requirements

This section reviews the technical and business requirements enterprises have for their network management tools. **Figure 36** reveals which technical features research participants identified as most valuable in their network availability monitoring tools. Network conversation insights (e.g., insights into the network conversations between hosts that are generating traffic) is at the top of the list. This helps a network manager understand where communication faults might be occurring.



Sample Size = 350, Valid Cases = 350, Total Mentions = 955

Figure 36. Most valuable network availability monitoring tool features

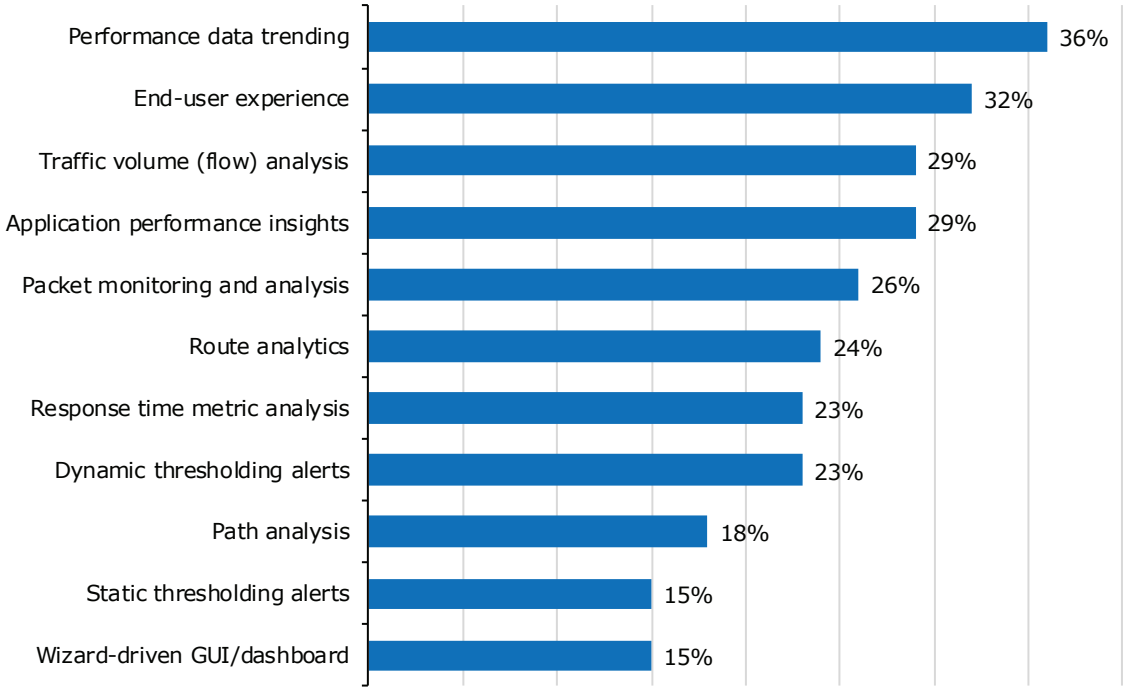
Dashboard monitoring drilldown views and graphical dependency map workflows tied with endpoint/interface and application auto-discovery as the next-most valuable features. Successful network teams are less likely (22%) to value endpoint/interface and application auto-discovery, suggesting that this feature might be overrated in an availability monitoring tool.

Automated notifications and escalations, network topologies/inventories across infrastructure, advanced alarm management, and automatic trouble ticket management are all of middling value. Of least importance are topology-based alarm suppression, dependency-based alarm suppression, auto-clearing of alarms, and alarm trending. Individuals from the DevOps team were more likely to value dependency-based alarm suppression (32%). Application management team member were more likely to select event correlation (42%).

Very large enterprises expressed more interest in automated notifications/escalations (50%). Large (29%) and very large (33%) are very interested in advanced alarm management. Midmarket companies are more interested in endpoint/interface and application auto-discovery (37%).

© 2020 Enterprise Management Associates, Inc. | www.enterprisemanagement.com

Figure 37 reviews the most valuable features in network performance monitoring tools. Performance data trending is the top feature, followed by end-user experience monitoring. Very large enterprises are less likely to recognize the value of either these features (both 17%). Lack of interest in an end-user experience feature suggests that very large companies are relying on standalone tools for that insight.



Sample Size = 350, Valid Cases = 350, Total Mentions = 947

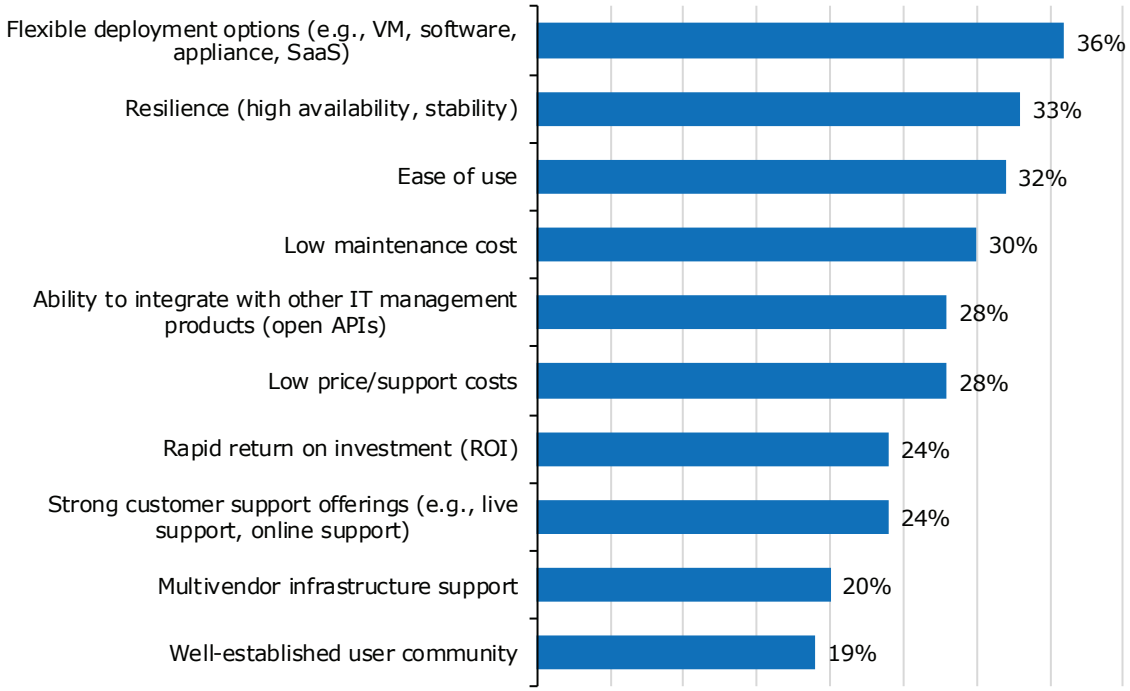
Figure 37. Most valuable network performance monitoring features

Path analysis, static thresholding alerts, and wizard-driven GUIs and dashboards are least valuable. Successful network teams are particularly less interested in path analysis (12%). Europeans are less likely to recognize the value of path analysis (10%) or performance data trending (25%). Very large enterprises are more likely to select wizard-driven GUIs and dashboards as valuable (37%). They are also more interested in traffic volume analysis (43%).

Enterprises that are projecting high traffic growth this year place more value on packet monitoring/analysis (43%). Those with only moderate growth are more likely (27%) to value route analytics.

© 2020 Enterprise Management Associates, Inc. | www.enterprisemanagement.com

Figure 38 identifies the most important business requirements enterprises set for their network management tools. Flexible deployment options have emerged as a top priority this year, after being only the sixth-most important business requirement in 2018. Tool resilience is a new multiple choice option this year, and it immediately emerged as the number-two priority. Ease of use is the number-three priority. It was number-two in 2018, so it remains a high priority.



Sample Size = 350, Valid Cases = 350, Total Mentions = 963

Figure 38. Top business requirements of network management products

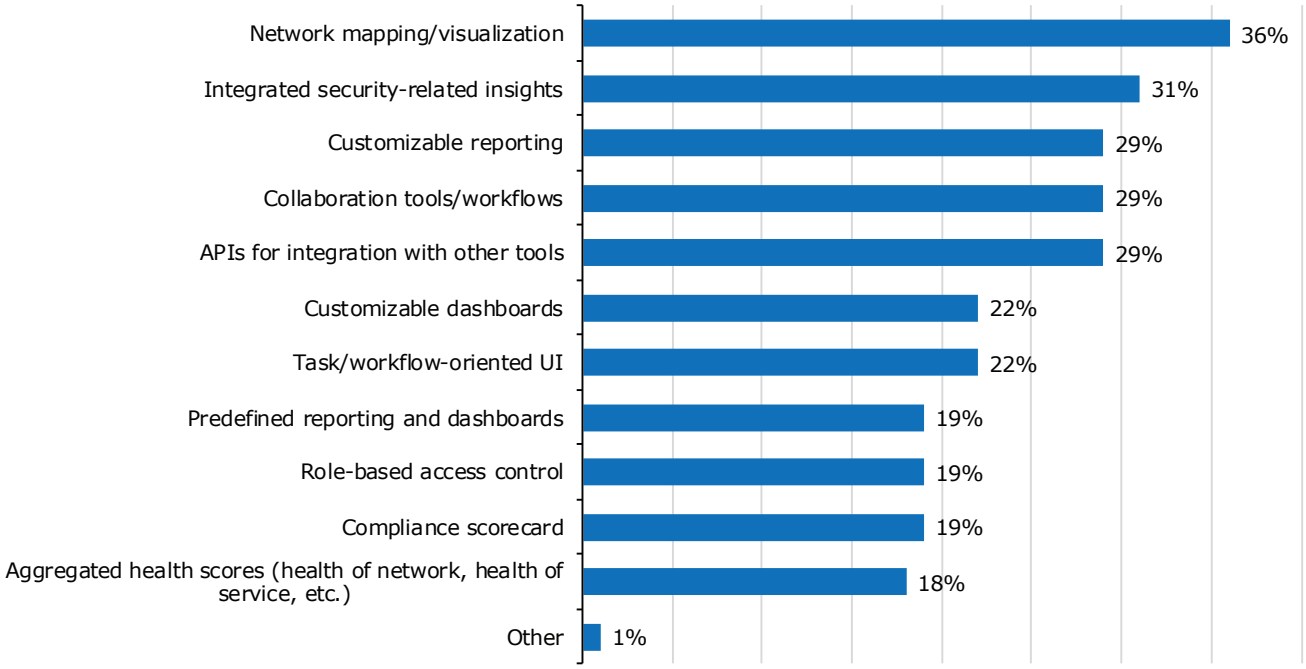
Rapid return on investment (ROI) was the top business requirement of network management tools in 2018, but now it has slipped to the 7th spot. EMA has observed in its research over the last two years a reduced focus on earning an ROI with technology investments.

Although a well-established user community is the least important business requirement, very large enterprises have more interest in it (40%). Large enterprises are more interested in multi-vendor support (26%). Europeans are more likely (41%) to seek solutions with low maintenance costs.

Rapid return on investment (ROI) was the top business requirement of network management tools in 2018, but now it has slipped to the 7th spot.

© 2020 Enterprise Management Associates, Inc. | www.enterprisemanagement.com

Figure 39 reviews the general network management product features that enterprises consider the most important to their operations. Research participants clearly singled out network mapping and visualization as the top priority. Respondents from the IT engineering and architecture group (45%) and the NOC (47%) are especially focused on this feature.



Sample Size = 350, Valid Cases = 350, Total Mentions = 955

Figure 39. Most valuable general network management product features

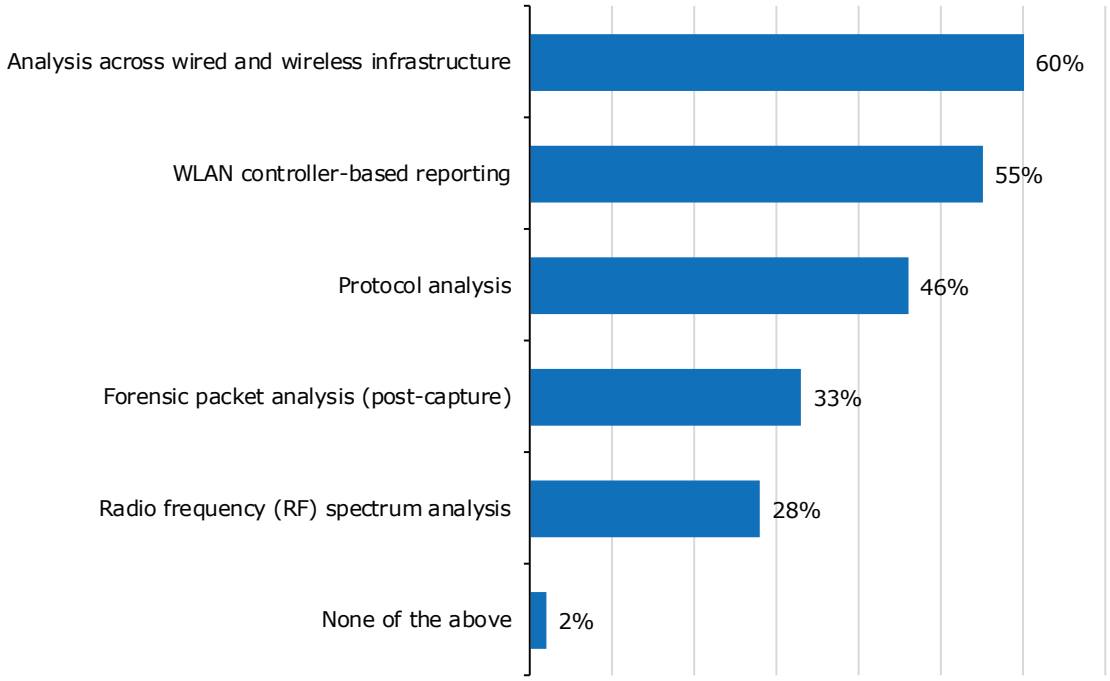
Integrated security insights are the second-most important feature. Midsized companies (38%) are especially more likely to rely on this capability. Customizable reporting, collaboration tools/workflows, and APIs for integration round out the top five tool features. Successful network operations teams are especially interested in APIs for integration (38%), which emphasizes the overall importance of integrated and consolidated IT operations toolsets. DevOps professionals (47%) are also very focused on APIs.

Canned reports/dashboards, role-based access control, compliance scorecards, and aggregated health scores were all at the bottom of the list.

© 2020 Enterprise Management Associates, Inc. | www.enterprisemanagement.com

Wi-Fi Management Tools

Given the specialized nature of Wi-Fi management, EMA asked several questions specific to the task. **Figure 40** identifies the Wi-Fi availability and performance management capabilities that enterprises reply upon the most.



Sample Size = 350, Valid Cases = 350, Total Mentions = 783

Figure 40. Wi-Fi availability and performance management capabilities enterprise most rely upon

Enterprises singled out the ability to conduct analysis across wired and wireless infrastructure as the most important capability. A majority also rely on wireless LAN controller reporting. Successful network operations teams are more likely (64%) to emphasize wireless LAN controller reporting.

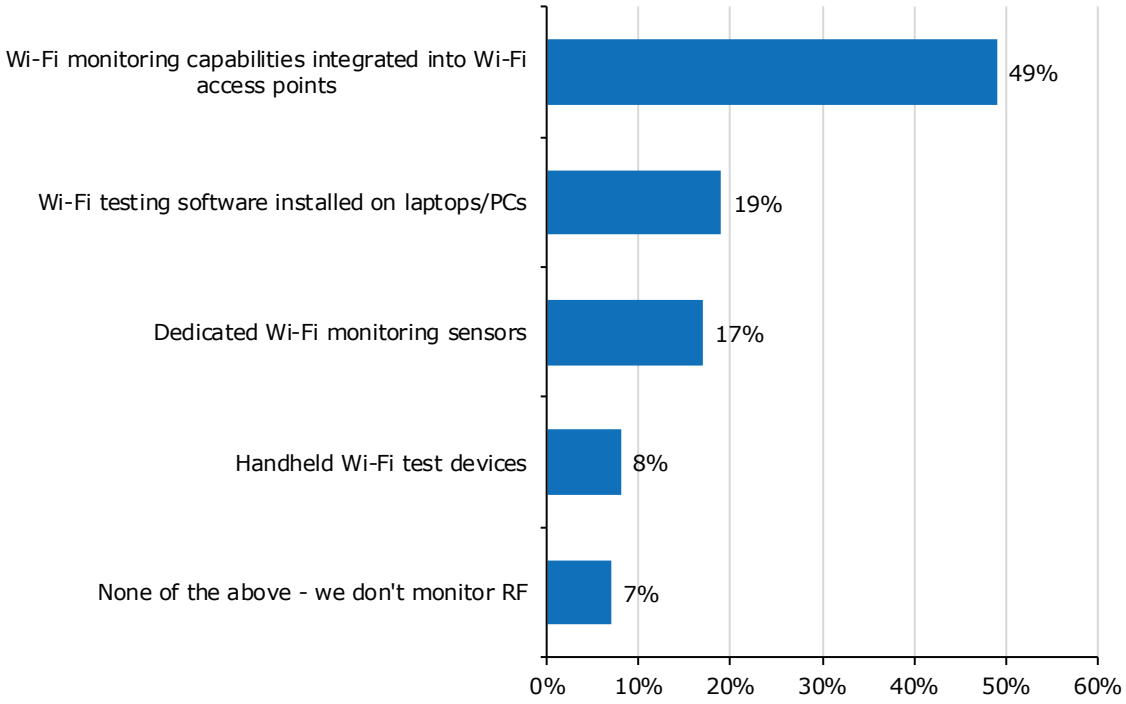
Less than half use protocol analysis. Individuals who work in an NOC were the least likely (22%) to rely on protocol analysis, while IT engineering/architecture (52%) were more likely, suggesting this is a capability for Tier 2 and 3 support.

Forensic packet analysis and RF spectrum analysis are used least often. IT engineering/architecture (45%) and DevOps (53%) are more likely to rely on forensic packet analyses.

Network teams that have an operations team dedicated solely to Wi-Fi are more likely (41%) to rely on RF spectrum analysis, versus 22% of enterprises that have a unified wired and wireless network operations approach. This suggests that specialized teams are more likely to have RF engineering experts, or more likely to budget for RF management tools.

© 2020 Enterprise Management Associates, Inc. | www.enterprisemanagement.com

RF management requires dedicated tools and specific engineering skills. Unlike packet analysis, controller reporting, and other techniques, RF management isn't something that is pulled off the wire. It requires a radio that collect wireless signals for analysis. EMA asked research participants how they primarily perform this function. Overall, 93% of enterprises do some form of RF management, as seen in **Figure 41.**



Sample Size = 350

Figure 41. Primary approach to monitoring and managing Wi-Fi radio frequency spectrum

Nearly half of enterprises (49%) primarily rely on integrated capabilities in their Wi-Fi access points (APs). This approach allows broad coverage of the network but it is limited since most APs use their radios primarily for production traffic. Repurposing a radio to RF monitoring will reduce the overall capacity and performance of the AP. Some premium Wi-Fi APs have an extra dedicated radio for RF monitoring and analysis, but the majority of installed devices do not. Thus, it's hard to continuously monitor the RF spectrum with this technique. This is the most popular technique among enterprises that have a specialized team dedicated just to Wi-Fi operations (60%).

Dedicated Wi-Fi mentoring sensors is the preferred technique for 17% of enterprises. This is the most comprehensive approach to RF management, but it's also the most expensive. It requires enterprises to procure, deploy, and manage Wi-Fi sensors throughout their environment.

Nearly 20% of enterprises mostly rely on Wi-Fi testing software deployed on a laptop or PC, and 8% rely on handheld Wi-Fi testing devices. Both of these techniques are more suited for troubleshooting than operational monitoring, since these tools are usually employed by engineers roaming the office on the hunt for the root cause of a network problem.

© 2020 Enterprise Management Associates, Inc. | www.enterprisemanagement.com

DDI Management (DNS, DHCP, and IPAM)

Management of core network services like DNS, DHCP, and IP addresses (DDI) are often overlooked by IT organizations. EMA has seen many examples of enterprises taking an informal approach using open-source tools and spreadsheets, rather than enterprise-grade tools that can scale infrastructure and automate operations.

Figure 42 reveals how enterprises are approaching DDI management today. Overall, there is no mainstream approach. Only a quarter of enterprises have a unified DDI management suite from a single vendor, while slightly more have multiple commercial management tools from different vendors. The rest, nearly half of all enterprises, don't use commercial DDI management tools at all. Many use open-source tools, homegrown tools, and spreadsheets. Others use ad hoc solutions without centralized management, such as Microsoft DNS.

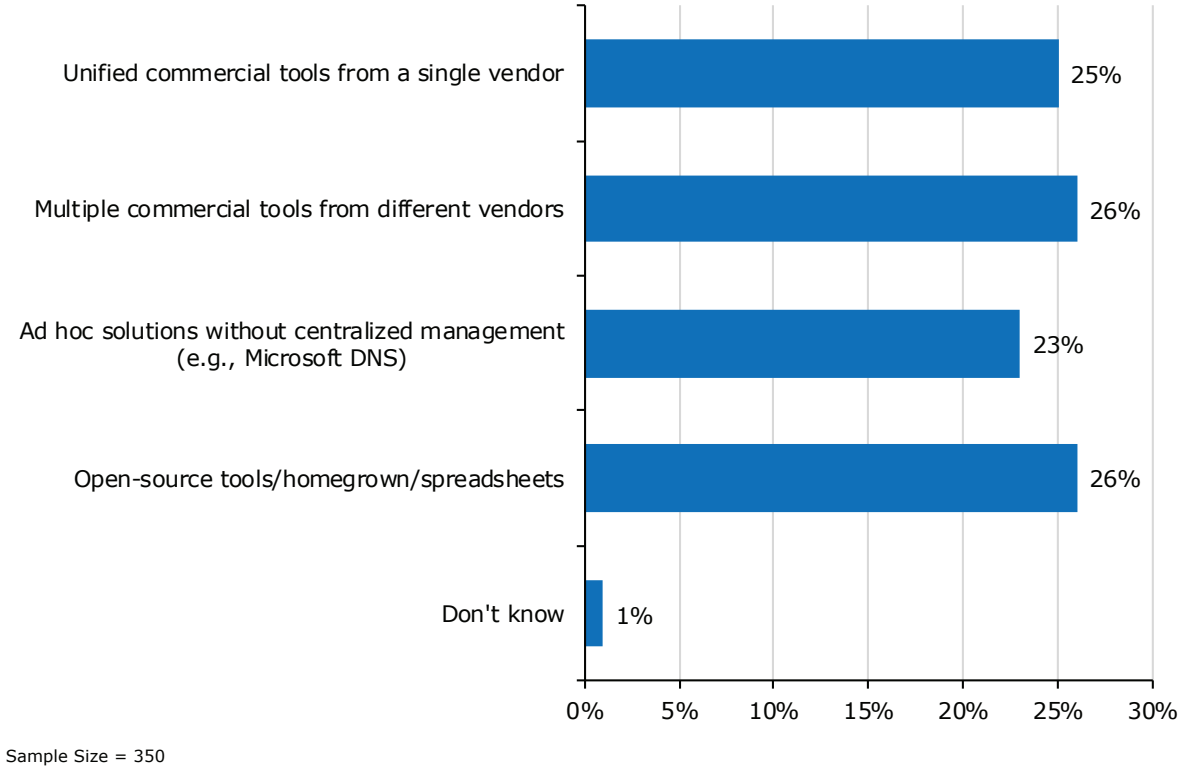


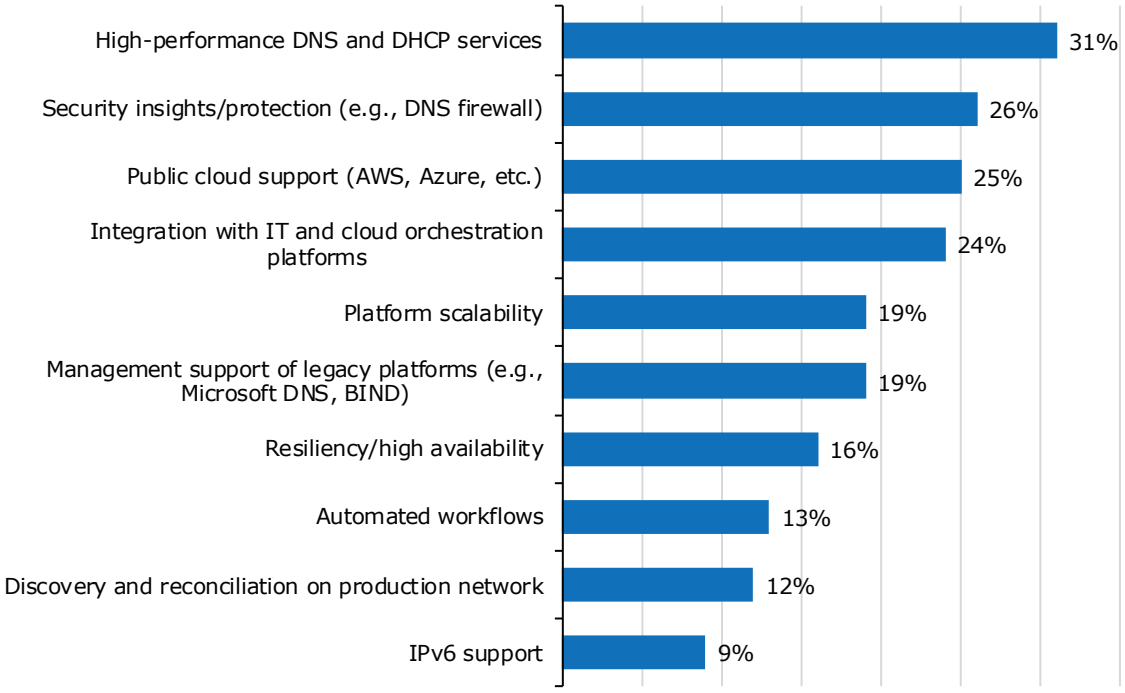
Figure 42. Overall approach to DDI management (DNS, DHCP, IP address management)

Successful network operations teams are more likely to use commercial DDI tools. Thirty-one percent use commercial tools from multiple vendors and 29% use unified DDI tools. Somewhat successful teams are more likely to use open-source and homegrown tools (32%). Data center operations (47%) is especially likely to say they use ad hoc solutions without centralized management.

Successful network operations teams are more likely to use commercial DDI tools.

© 2020 Enterprise Management Associates, Inc. | www.enterprisemanagement.com

Figure 43 reviews the capabilities that enterprises consider most important in their DDI tools. First, they want high-performance DNS and DHCP services. They don't want DNS infrastructure that takes too long to respond to queries or crashes during peak volumes. They also don't want client devices to wait too long to get an IP address from a DHCP service.



Sample Size = 350, Valid Cases = 350, Total Mentions = 683

Figure 43. Most important capabilities of DDI solutions

Second, enterprises want security insights or protection. DNS is often targeted by malicious actors, and DNS security capabilities can act as a firewall to protect against DNS poisoning and hijacking. They can alert on suspicious DNS activity.

The other two most important DDI capabilities are public cloud support and integration with IT and cloud orchestration platforms. These latter findings are unsurprising, given that public and private cloud initiatives and cloud-native platforms are currently driving many network management priorities. Public cloud support is particularly important to successful network operations teams (32%). Cloud support is also more important to software companies (36%) and retailers (35%). Europeans are less likely (15%) to emphasize integration with orchestration tools.

Platform scalability and management support of legacy platforms like BIND servers are secondary requirements. Automated workflows, discovery and reconciliation on the production network, and IPv6 support are of least interest. Data center operations professionals are more likely (42%) to emphasize resiliency and high availability. DevOps professionals are more likely (42%) to emphasize management support of legacy platforms.

© 2020 Enterprise Management Associates, Inc. | www.enterprisemanagement.com

NETWORKING SPENDING PLANS

This section reviews network spending plans for the enterprises represented in this survey-based research. Please note that this data was collected before the COVID-19 pandemic crisis. Investment priorities may have shifted.

Investment in 400 GbE infrastructure will truly ramp up in 2021.

Last year, network infrastructure vendors started announcing their first 400 Gigabit Ethernet (GbE) switches and routers for the enterprise. These new products represent the first major leap forward in hardware speeds since vendors introduced 40 GbE and 100 GbE devices a decade ago.

The adoption of 400 GbE will obviously impact network management. For one thing, the higher speeds will challenge packet-based analysis tools. It's still too early to gauge that impact, but EMA did ask research participants to reveal their investment plans. **Figure 44** shows that mainstream adoption will take some time. Only 18% of enterprises plan to install 400 GbE devices in 2020.

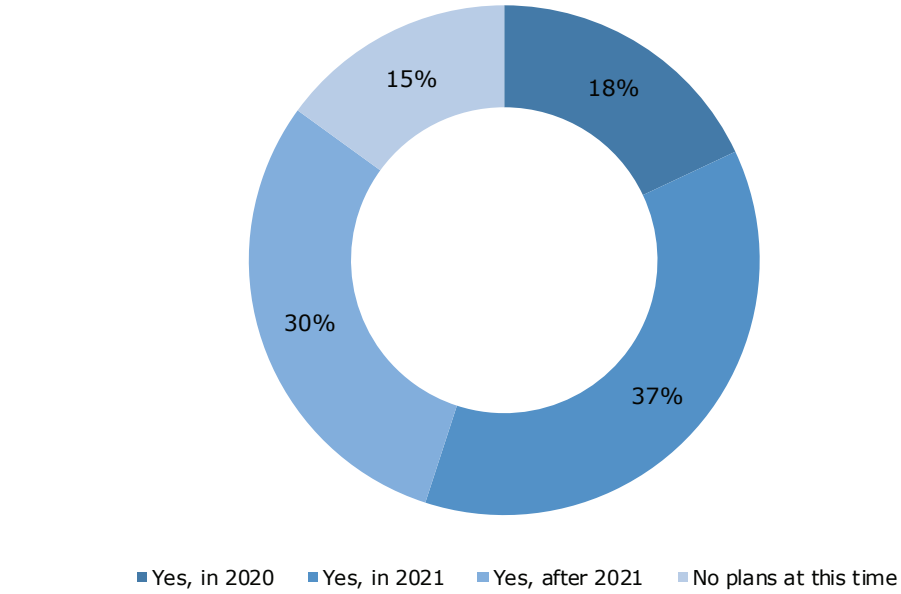


Figure 44. 400 Gigabit Ethernet infrastructure investment plans

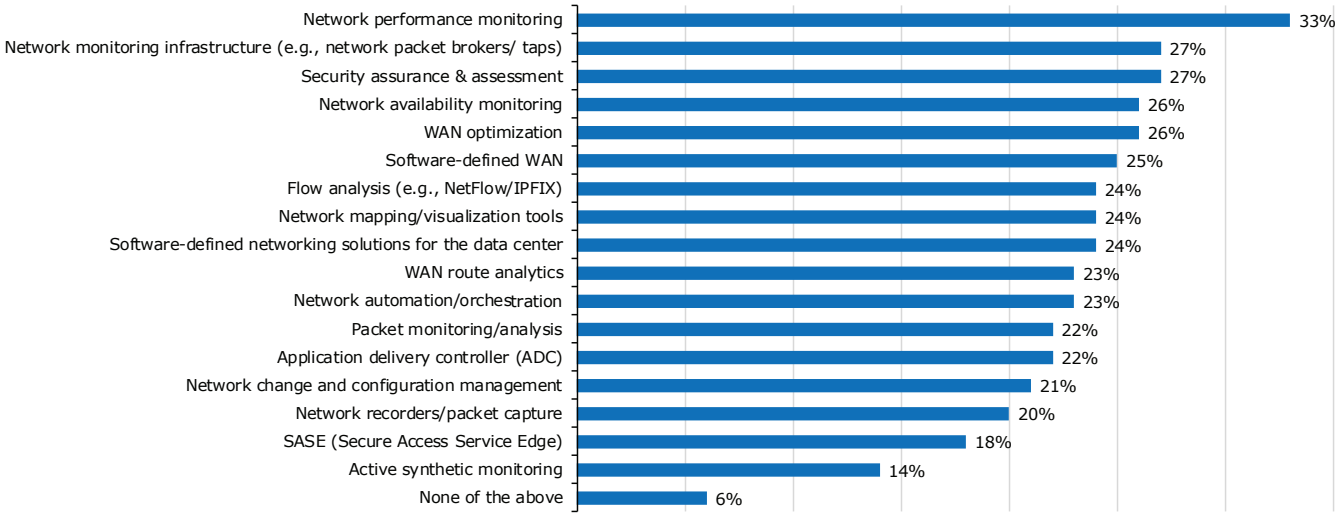
Investment in 400 GbE infrastructure will truly ramp up in 2021, when 37% of respondents have plans to buy the devices. However, 15% of companies still have no specific plans, and 30% are holding off until 2022 or later. Enterprises with successful network operations teams are more likely (30%) to invest in 400 GbE in 2020. Somewhat successful teams are more likely to expect 400 GbE in 2022 or later (38%).

Very large enterprises are more likely (50%) to be deploying 400 GbE in 2021, versus 32% of large enterprises. Instead, large enterprises are more likely to be looking at 2022 and later (35%), versus 13% of very large enterprises.

EMA also found that enterprises are more likely to have immediate 400 GbE investment plans if they are projecting higher traffic growth, which makes perfect sense. For instance, 53% of enterprises expecting high traffic growth will install 400 GbE in 2021, versus only 19% of enterprises that project little to no traffic growth. On the flip side, 36% of enterprises with little to no projected traffic growth have no 400 GbE investment plans at all, versus only 9% of those with high traffic growth.

© 2020 Enterprise Management Associates, Inc. | www.enterprisemanagement.com

Figure 45 reveals other network-related spending plans that enterprises have over the next 12 months. Network performance monitoring tools are the biggest spending priority. Several industries are more likely to be investing in these tools this year, including enterprises in construction (50%), education (45%), finance/banking/insurance (40%), and hospitality/entertainment (42%).



Sample Size = 350, Valid Cases = 350, Total Mentions = 1,416

Figure 45. Network-related spending plans over the next 12 months

Network monitoring infrastructure (e.g., NPBs, taps), security assurance and assessment tolls, network availability monitoring, WAN optimization, and SD-WAN are leading secondary spending priorities. Individuals who work within a NOC were more likely (44%) to report spending plans for security assurance, as were individuals who work for midsized enterprises (34%). Midsized enterprises are more likely (41%) to have plans to buy network monitoring infrastructure. SASE services and active synthetic monitoring tools are the two least likely solutions in the budget for this year.

Midsized companies are also more likely to be investing in network availability monitoring (38%), flow analysis (31%), network mapping/ visualization (32%), and data center SDN (31%). Very large enterprises are more likely to buy WAN optimization (40%) and network automation (37%).

© 2020 Enterprise Management Associates, Inc. | www.enterprisemanagement.com

MEGATREND #1: NETSECOPS: THE PARTNERSHIP BETWEEN NETWORK AND SECURITY TEAMS

EMA has found strong evidence over the last few years that network operations teams are working more closely with information security teams. In EMA's 2018 megatrends research, the majority of enterprises had some form of formal collaboration between the two groups. In 2020, EMA's research found ongoing and expanding partnerships.

Figure 46 shows that 37% of enterprises claim to have fully converged network and security teams. This is more common in Europe (54%). More than a quarter of enterprises have maintained separate groups, but they have deployed shared tools and processes to facilitate collaboration.

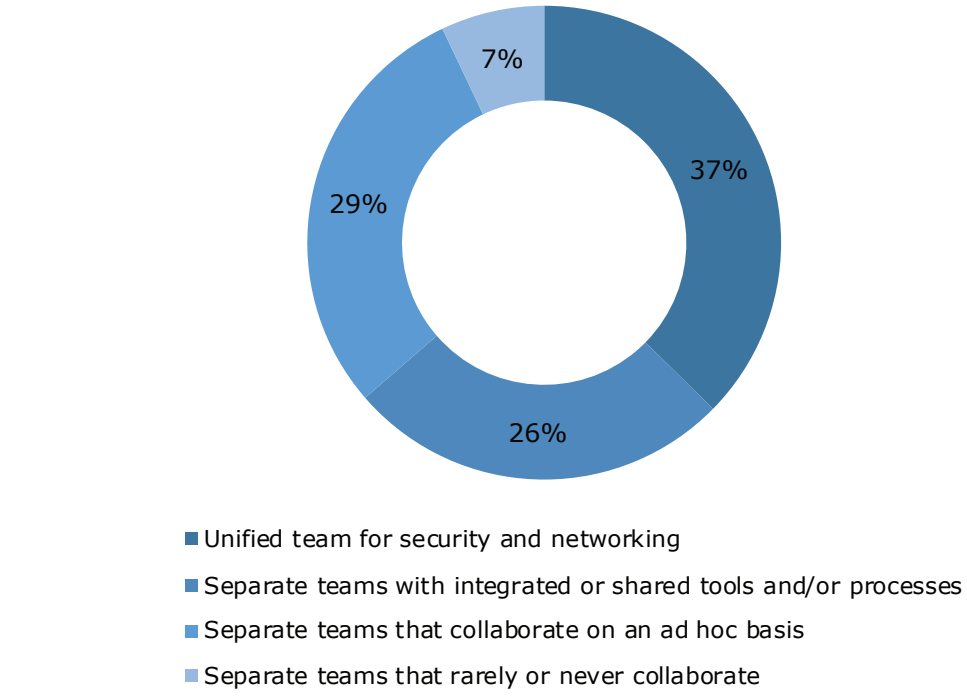


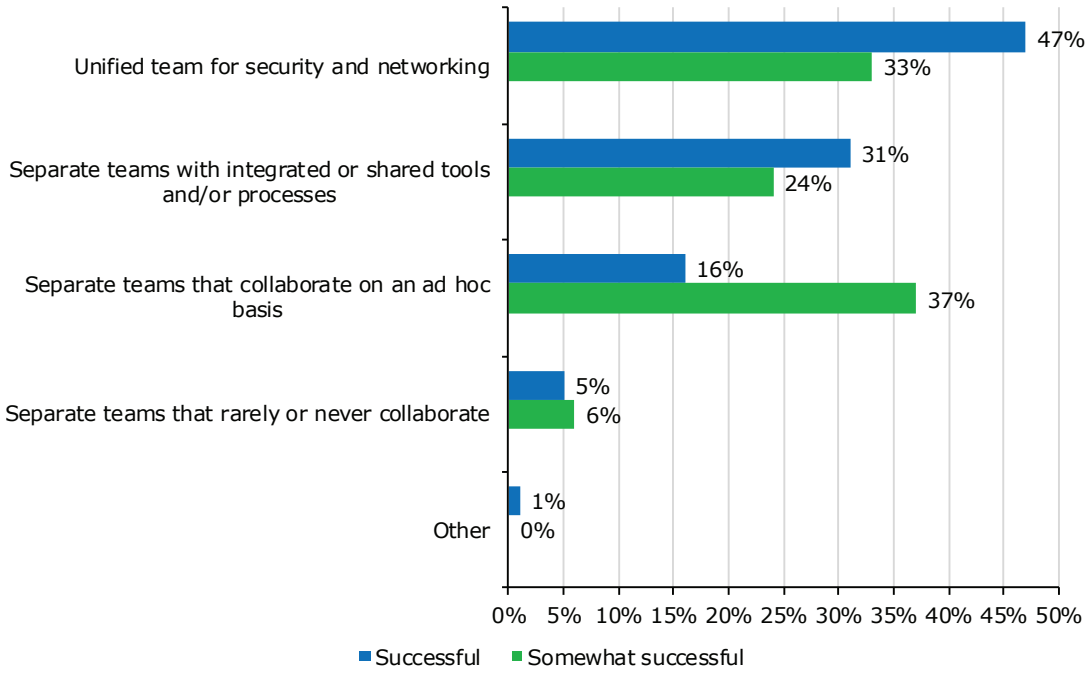
Figure 46. Relationships between today's network management and information security teams

A significant percentage have only ad hoc collaboration between the groups, and a small number claim to have no collaboration at all. North Americans are more likely (34%) to rely on ad hoc collaboration, versus only 14% of Europeans. Ad hoc collaboration is also more common in large enterprises (34%), but rare in very large enterprises (10%).

EMA found a very strong correlation between close NetSecOps collaboration and overall network operations success.

© 2020 Enterprise Management Associates, Inc. | www.enterprisemanagement.com

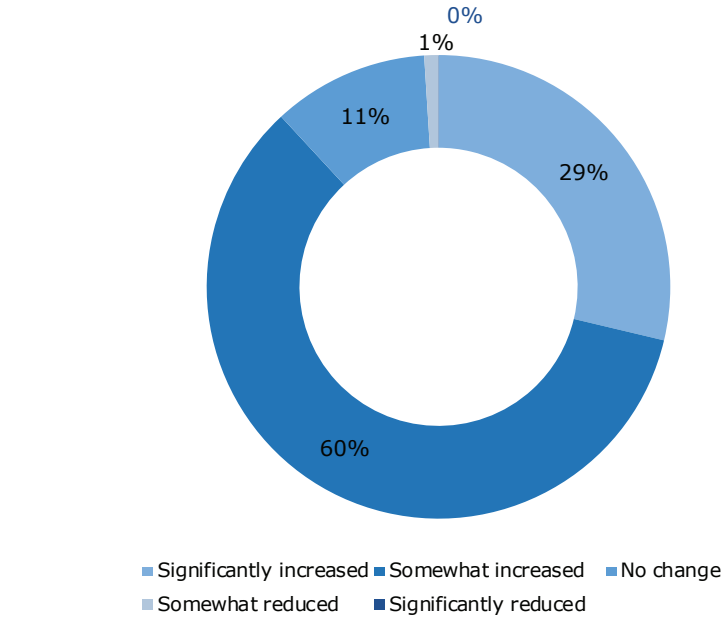
EMA found a very strong correlation between close NetSecOps collaboration and overall network operations success, as **Figure 47** illustrates. Successful teams are very likely to have converged groups or integrated tools and processes between the two groups. Less successful network teams are more likely to rely on ad hoc collaboration.



Sample Size = 350

Figure 47. Successful network operations teams have stronger ties to the security group

EMA found that 89% of network teams have increased their collaboration with security teams over the last two years, as **Figure 48** details. Twenty-nine percent described that increased collaboration as significant. Only a handful of research participants (1% overall) reported a reduction in collaboration.



Sample Size = 350

Figure 48. Changes in the amount of collaboration between network and security teams over the last two years

© 2020 Enterprise Management Associates, Inc. | www.enterprisemanagement.com

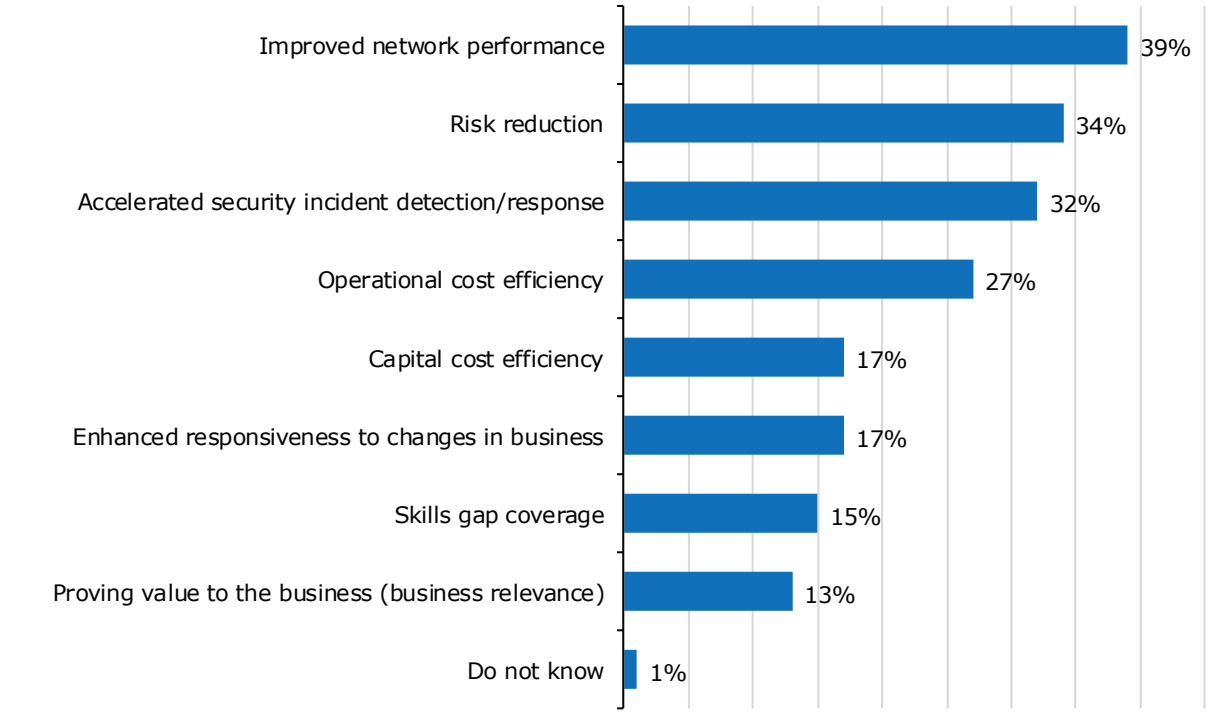
Perceptions of this change vary across IT groups. For instance, DevOps professionals are more likely (47%) to report significantly increased collaboration. Data center operations professionals are more likely (32%) to report no change. Midmarket companies are also segmented where a significant increase in NetSecOps collaboration is more concentrated (39%).

Traffic growth appears to be a possible driver of this collaboration. Enterprises that project the highest rates of traffic growth this year are the most likely to perceive significantly increased collaboration (52%), in stark contrast to those who perceive low or no growth (4%).

Finally, increased collaboration looks like an industry best practice. Successful network operations teams are more likely to report significant increases in NetSecOps collaboration (45%), versus just 21% of less successful teams.

Benefits of NetSecOps Collaboration

Figure 49 reveals the benefits that IT organizations target with their network and security team collaboration. The top goal is improved network performance. Europeans are particularly focused on this goal (51%). This research already established that security system problems and security incidents are common root causes of IT service problems. Improved collaboration can help IT organizations accelerate the detection and remediation of these problems.



Sample Size = 350, Valid Cases = 350, Total Mentions = 683

Figure 49: Organizational goals of NetSecOps collaboration

© 2020 Enterprise Management Associates, Inc. | www.enterprisemanagement.com

EMA sees hard evidence of this in the research data. Enterprises with formal collaboration between the two groups tend to spend less time on reactive network troubleshooting and more time on proactive problem prevention, as this table illustrates:

LEVEL OF NETSECOPS COLLABORATION	PERCENTAGE OF WORKDAY	
	REACTIVE TROUBLESHOOTING	PROACTIVE PROBLEM PREVENTION
UNIFIED TEAMS	26%	27%
TEAMS WITH SHARED TOOLS AND PROCESSES	29%	29%
AD HOC COLLABORATION	35%	24%

The nature of NetSecOps collaboration has some association with the goals of that collaboration. For instance, enterprises that have unified their network and security teams are more likely to pursue improved network performance (48%). Unified teams (36%) and teams that have shared tools and processes (39%) are focused more often on accelerating security incident detection and response. Unified teams are less often focused on skills gap coverage (10%), but it is more likely a priority for teams with shared tools and processes (21%).

Risk reduction is the second benefit that enterprises focus on, followed by faster security incident detection and response. Finally, operational cost efficiency round out the top four benefits. Risk reduction is particularly popular among enterprises that predict little or no network traffic growth this year (47%).

Capital expense efficiency, responsiveness to business change, skills gap coverage, and demonstrating value to the business are lower priorities for this collaboration. These findings suggest that enterprises primarily encourage this collaboration to improve the effectiveness of network and security operations, rather than enhancing IT agility.

Successful network operations teams are more likely to target accelerated security incident detection/response (40%), but somewhat successful teams are more likely to target risk reduction (39%).

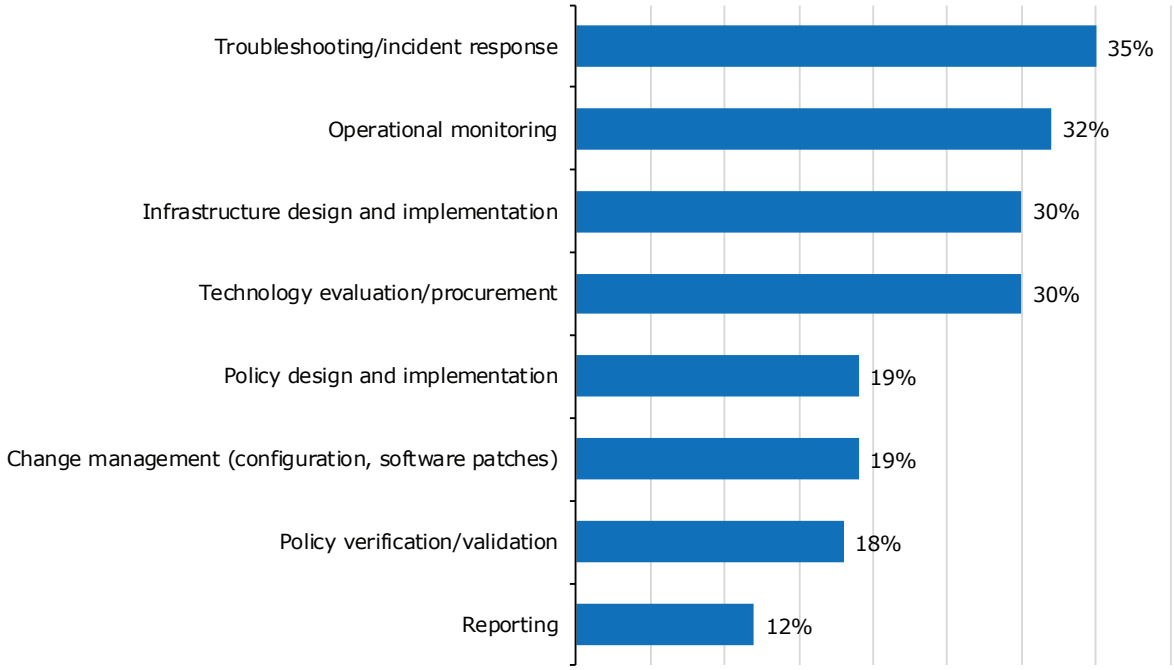
DevOps professionals are focused more on closing skills gaps (32%). Members of the IT asset and financial management team are more likely to look at NetSecOps as a source of improved business relevance (22%).

© 2020 Enterprise Management Associates, Inc. | www.enterprisemanagement.com

Network troubleshooting and security incident response are the primary areas of collaboration between network and security teams.

How Network and Security Collaborate

EMA identified four aspects of engineering and operations where network and security teams focus their collaboration. **Figure 50** reveals that network troubleshooting and security incident response are the primary areas of collaboration between network and security teams. IT engineering and architecture professionals are more likely (47%) to focus on this, while individuals from the NOC are not (25%). This contrast makes sense, since engineers and architects are more likely to provide Tier 2 and 3 support during an event.



Sample Size = 350, Valid Cases = 350, Total Mentions = 681

Figure 50. Most critical points of collaboration between networking and security teams

The other three priorities are operational monitoring, infrastructure design and implementation, and technology evaluation and procurement. DevOps team members (47%) and NOC professionals (44%) are more likely to focus on infrastructure.

These findings contrast somewhat with EMA's 2018 research, when infrastructure design and implementation were the top targets by a significant margin, followed by operational monitoring and troubleshooting/incident response. Technology evaluation and procurement wasn't a multiple choice option in 2018.

Reporting is the least important opportunity for collaboration, although members of the NOC team (22%) are more likely to see value in it. Policy design and implementation are a higher priority for collaboration in midsized enterprises (25%). Change management is a surprisingly low priority, and is especially so for successful network operations teams (12%), suggesting that there are limited opportunities to improve overall change management practices through NetSecOps collaboration.

The network and security teams aren't necessarily natural partners. Their fundamental missions are divergent. The network team focuses on connectivity by providing employees, partners, and customers access to applications, data, and services. The security team is fundamentally focused on the opposite. They lock down data and limit connectivity. Thus, it's important to examine the challenges that IT organizations experience when these teams try to come together.

© 2020 Enterprise Management Associates, Inc. | www.enterprisemanagement.com

Figure 51 reveals the top challenges to successful NetSecOps collaboration. Only 8% claim to have no significant challenges, but successful network operations teams are more likely to make this claim (15%). The top problem is that the two groups have different goals for this collaboration.

Sample Size = 350, Valid Cases = 350, Total Mentions = 871

Figure 51. Challenges to NetSecOps collaboration

Cross-team skills gaps and a lack of tool support for collaboration are only slightly less challenging than the issue of conflicting goals. DevOps (53%) and application management professionals (59%) are more likely to say the cross-team skills gaps are a problem. Successful network operations teams are less likely to struggle with these skills gaps (21%). However, it's common for individuals to lack the skills and experience required to use the technology, tools, and processes that their peers in the other team rely upon. They will require some training. Moreover, to address the lack of collaboration support, network management tools will need workflows and features that facilitate collaboration and provide security-related insights.

Data issues round out the top five challenges of NetSecOps collaboration. First, many enterprises are struggling with conflicts about the control of data. Individual teams can be very protective of the data they extract from the network, both on the security side and the network side of the business. In interactions with the industry, EMA has observed that this reticence to share data with others causes conflicts. This is an issue that IT leadership needs to address by setting an agenda of cooperation.

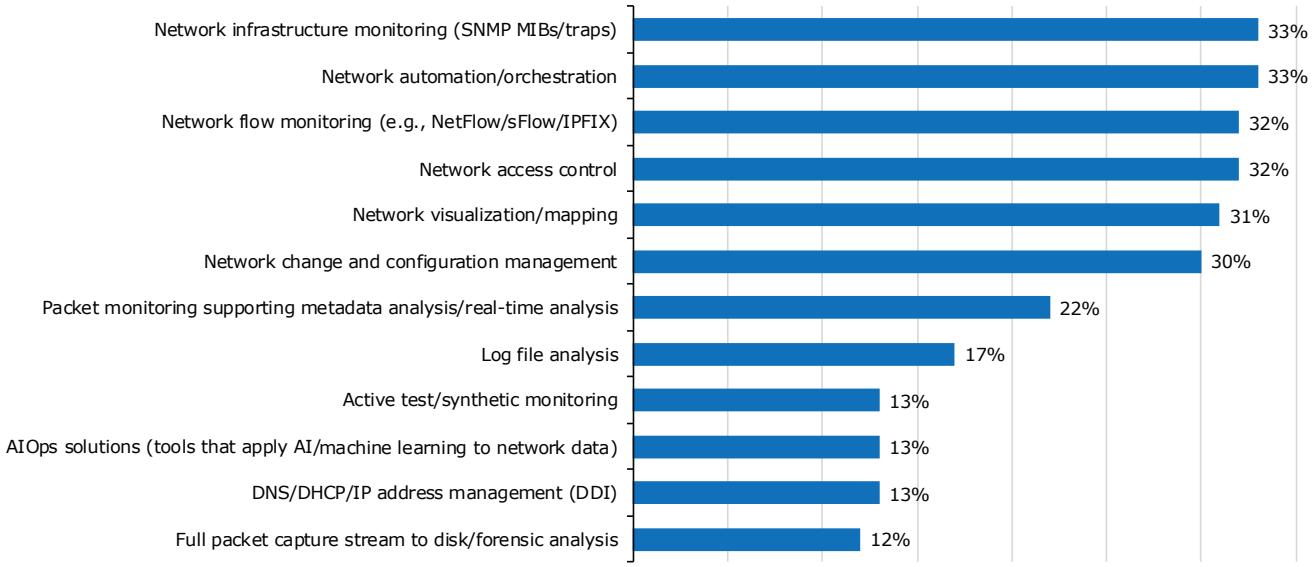
In other cases, the data that teams do share for collaboration can be inconsistent, irrelevant, or out-of-date. For example, a security team might detect a breach and request a forensic analysis from network operations. Unfortunately, that network team might be continuously capturing packets. Thus, it can only offer packets collected after the event ended in the hopes that they can trace something or recreate the incident after it is over. To ensure that these teams have the right shared data, network and security teams should find ways to unify their data collection and the tools they use for analysis wherever possible.

Cultural resistance is the least problematic challenge, which is good. It suggests that both teams are open to collaboration. A lack of defined processes and best practices is also a somewhat uncommon challenge, but enterprises that project high traffic growth in the next year are struggling with it significantly more often (34%). Application management professionals also perceive this challenge more often (42%).

While silos created by architectural limitations are a less prominent challenge, individuals who work in an NOC complained of it the most (31%).

© 2020 Enterprise Management Associates, Inc. | www.enterprisemanagement.com

EMA asked respondents to identify the tools that best equip them for collaboration with security. Six tools emerged as most useful, as **Figure 52** illustrates. Basic network infrastructure monitoring tools collect device metrics via SNMP, device APIs, etc., and network automation tools are slightly more useful for collaboration than other tools. Infrastructure monitoring tools can detect unusual activity on a network device, such as saturation of an interface by an attack. Network automation tools allow enterprises to make quick changes to the network in response to a security event. Network infrastructure monitoring is a more popular enabler of collaboration for network teams that have fully unified with security teams (40%), but less popular for teams that collaborate on an ad hoc basis (26%).



Sample Size = 350, Valid Cases = 350, Total Mentions = 987

Figure 52. Network management solutions that best support NetSecOps collaboration

Network flow monitoring (e.g., NetFlow) and network access control (NAC) are also important. Flow monitoring can show high-level views of network traffic patterns and activity. Sophisticated analysis of flows can reveal patterns of suspicious behavior, even signature behavior of known threats. NAC, naturally, controls access to the network, which is a key tool for securing the network. Europeans are more likely to identify NAC as an essential enabler of collaboration (43%).

Network visualization/mapping and network change and configuration management (NCCM) round out the group of six tools that are clearly more valuable for this collaboration. Individuals from the IT engineering (39%) and data center operations teams (42%) are more likely to value visualization tools. Visualization tools can help network managers understand where a threat might be and which assets are affected. NCCM tools can reduce risk through change management, but they can also facilitate quick remediation of a security incident through configuration changes.

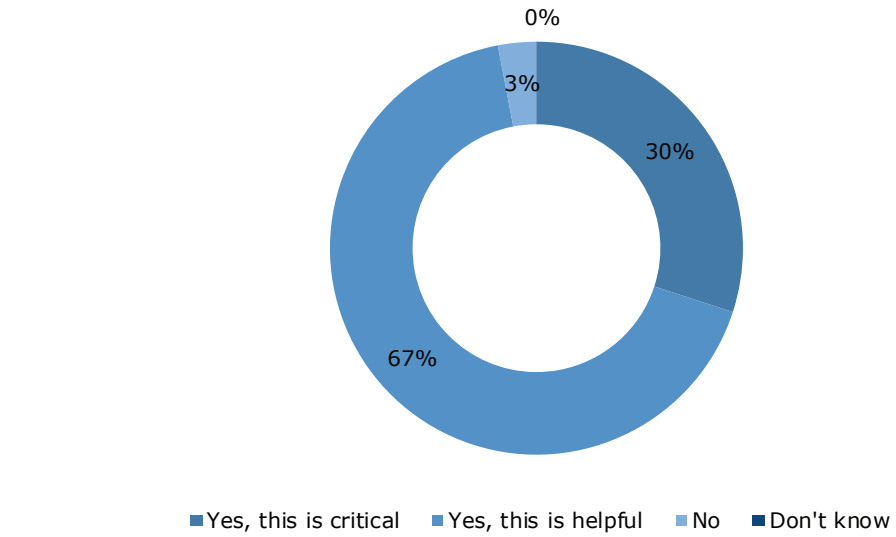
Real-time packet monitoring and log file analysis are less prominent enablers of collaboration. However, enterprises with fully unified network and security teams are more likely to recognize the value of real-time packet monitoring (18%). Log file analysis, on the other hand, offers more value to enterprises that collaborate only on an ad hoc basis (22%).

DDI management tools aren't high on this list, but DevOps professionals perceive their collaborative value tremendously (39%). AIOps solutions are a low priority, but large enterprises (18%) are more likely to recognize their value.

97% of network teams are interested in using security capabilities provided by their network management vendors. Thirty percent say this is critical to their efforts to collaborate with the security group.

To support collaboration, 97% of network teams are interested in using security capabilities provided by their network management vendors and **Figure 53** reveals that 30% say this is critical to their efforts to collaborate with the security group. Such capabilities include security insights, features, or dedicated products. Individuals from DevOps (47%), IT asset management (38%), and project management (35%) are more likely to say this is critical, while people from the NOC (16%) and IT engineering (23%) are less so.

© 2020 Enterprise Management Associates, Inc. | www.enterprisemanagement.com



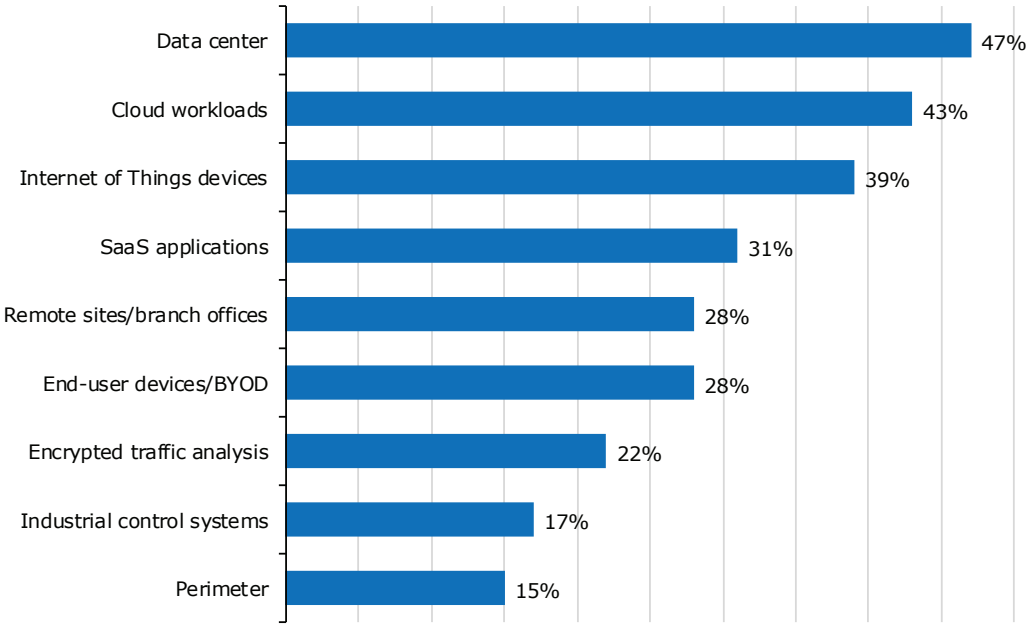
Sample Size = 350

Figure 53. "Are you interested in security-related insights, features, or products from your traditional network management vendors to support collaboration with the security group?"

Security-related capabilities from network management tools are a potential best practice approach to NetSecOps collaboration. Successful network operations teams are the most likely to say they have a critical need for these capabilities (40%), versus only 25% of somewhat successful teams. Very large enterprises (53%) and enterprises with fully unified NetSecOps teams (43%) are also more likely to have a critical need.

Enterprises should make sure that these security capabilities offer some integration with the data and workflows in their network management tools, even if they adopt separate security products from that network management vendor.

EMA asked individuals who want security-related capabilities from their network management solutions to identify the aspects of their digital environments where they would like to apply these capabilities. **Figure 54** reveals that data center, cloud workloads, and IoT devices are the priorities. SaaS applications, remote sites, and end-user devices are secondary priorities.



Sample Size = 341, Valid Cases = 341, Total Mentions = 919

Figure 54. Aspects of the digital environment where network managers need to apply security capabilities

© 2020 Enterprise Management Associates, Inc. | www.enterprisemanagement.com

The perimeter was the lowest priority, which suggests many of these network teams have embraced zero trust security models as part of their collaboration efforts with security. In fact, successful network operations teams are the least likely (7%) to focus their efforts on the perimeter. Instead, successful teams are more likely to focus on SaaS applications (42%).

The perimeter is also less of a focus for fully unified NetSecOps teams (6%), and separate teams that share tools and processes (13%). However, ad hoc collaborators tend to be very focused on the perimeter (30%).

Data center operations professionals are especially interested (74%) in applying these capabilities to the data center, which is no surprise. Application management (45%), IT asset management (38%), NOC (35%), and data center operations (53%) are all more likely to focus these capabilities on remote sites. The NOC is also more interested in end-user devices and BYOD (48%). DevOps teams are more focused on SaaS applications (63%).

Large enterprises are more likely to apply these security capabilities from their network management tool vendors to the perimeter (19%). Very large enterprises are more likely to look at remote sites (43%).

Finally, this research has revealed that NetSecOps collaboration is often challenged by issues around sharing data and data quality. Consolidating critical data, like logs and events, can help overcome this problem. EMA asked research participants if they were taking steps to consolidate. **Figure 55** reveals that 90% are doing this or planning to do so.

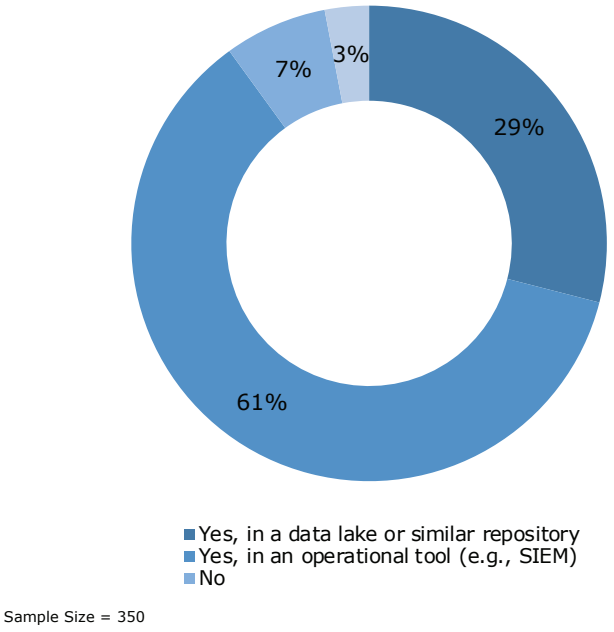


Figure 55. "Are you consolidating or planning to consolidate logs, events, and other critical data to facilitate data sharing between the network and security teams?"

Most plan to consolidate data in an operational tool, like a SIEM solution, but some are consolidating in a data lake or similar repository, which can be accessed by big data and advanced analytics tools. DevOps professionals (47%), large enterprises (43%), and enterprises with fully unified NetSecOps teams (35%) are more likely to use a data lake. Successful network operations teams are also likely (46%) to consolidate in a data lake, but just as many (45%) use an operational tool.

© 2020 Enterprise Management Associates, Inc. | www.enterprisemanagement.com

The majority of enterprises are adopting or planning to adopt data center SDN, but 34% still have no intention of doing so.

MEGATREND #2: DATA CENTER SDN DRIVES NEW NETWORK MANAGEMENT REQUIREMENTS

Traditional software-defined networking (SDN) solutions, in which the control plane of network devices are separated from the data plane and centralized in a controller, never achieved significant adoption in enterprise networks. However, vendors did respond to the potential disruption of SDN by developing products that leveraged innovations in network management, network automation, network virtualization, and other areas to create new solutions that carry the SDN label but aren't necessarily true SDN products. They include Cisco Application-Centric Infrastructure (ACI) and VMware NSX.

These second-generation "SDN" solutions are gaining significant adoption in data center networks. **Figure 56** reveals that the majority of enterprises are adopting or planning to adopt data center SDN, but 34% still have no intention of doing so. A quarter of enterprises have full production deployments, but limited pilot deployments are more common.

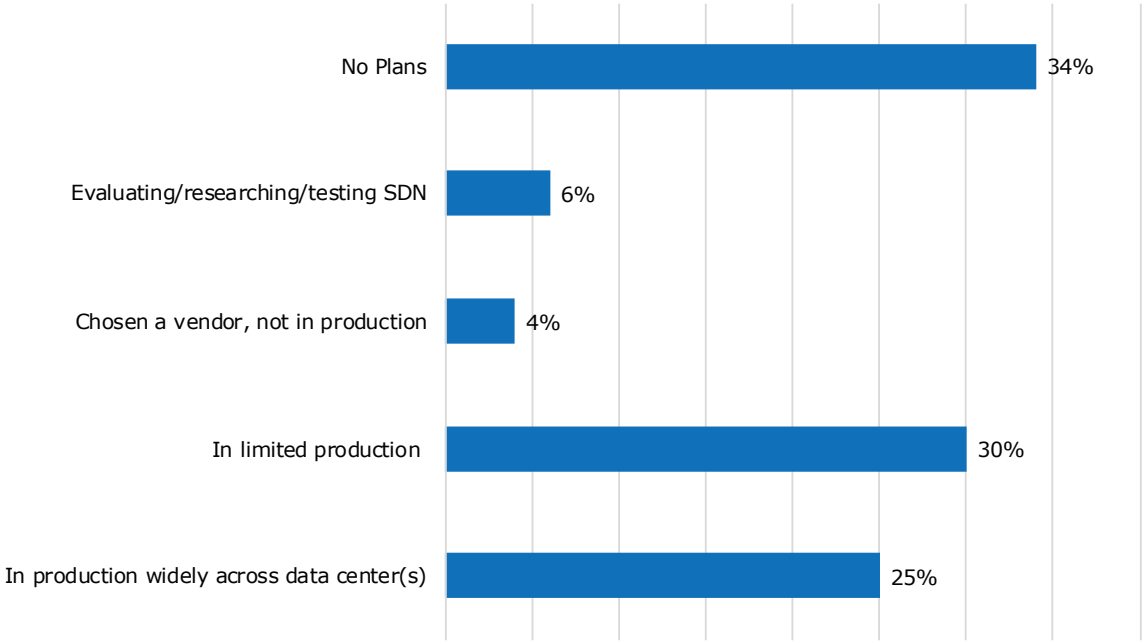
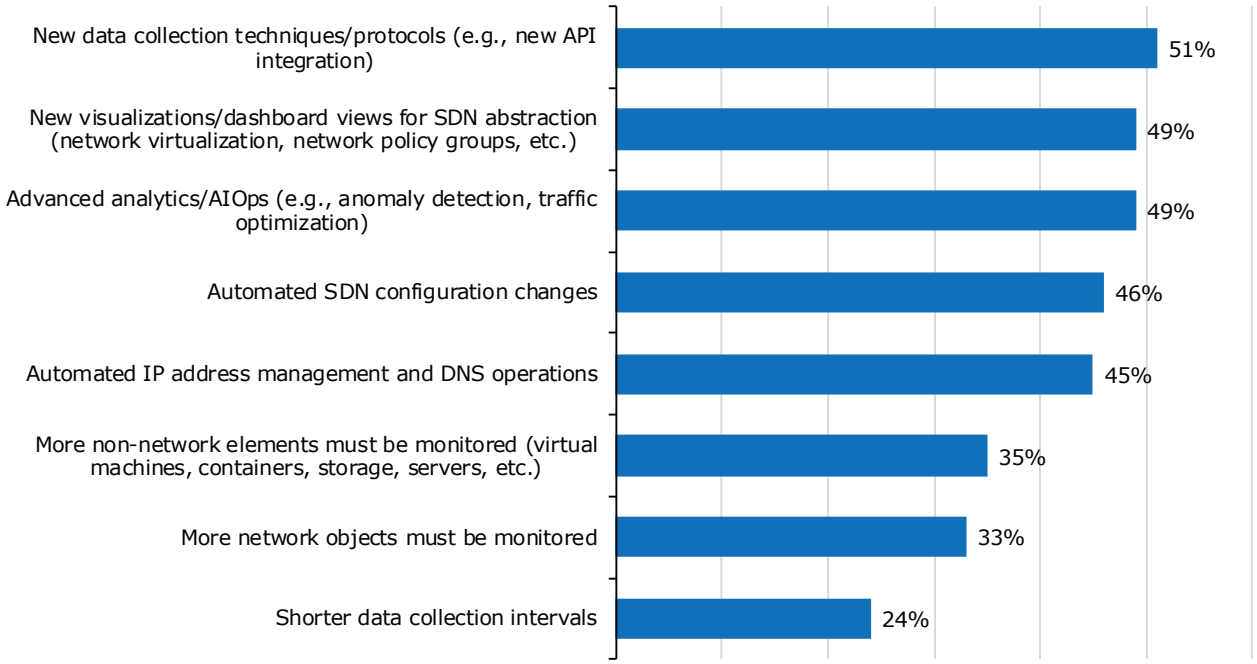


Figure 56. State of data center SDN adoption

© 2020 Enterprise Management Associates, Inc. | www.enterprisemanagement.com

Data center SDN solutions can be disruptive. Network engineers may find themselves working more with software elements than hardware, which will be an adjustment. Additionally, these solutions can generate new types of data and telemetry that need to be collected and analyzed. Overall, many enterprises find that they need new capabilities in their network management tools. **Figure 57** identifies the new requirements SDN imposes on network management tools.



Sample Size = 209, Valid Cases = 209, Total Mentions = 695

Figure 57. Most critical data center SDN-related network management tool requirements

Overall, SDN typically affects network management tool requirements in five ways. It drives a requirement for new data collection techniques and protocols, such as API integration. Network managers also require new visualizations and dashboard views that can account for the abstractions that SDN introduces. This is particularly of interest to people in the IT engineering group (63%).

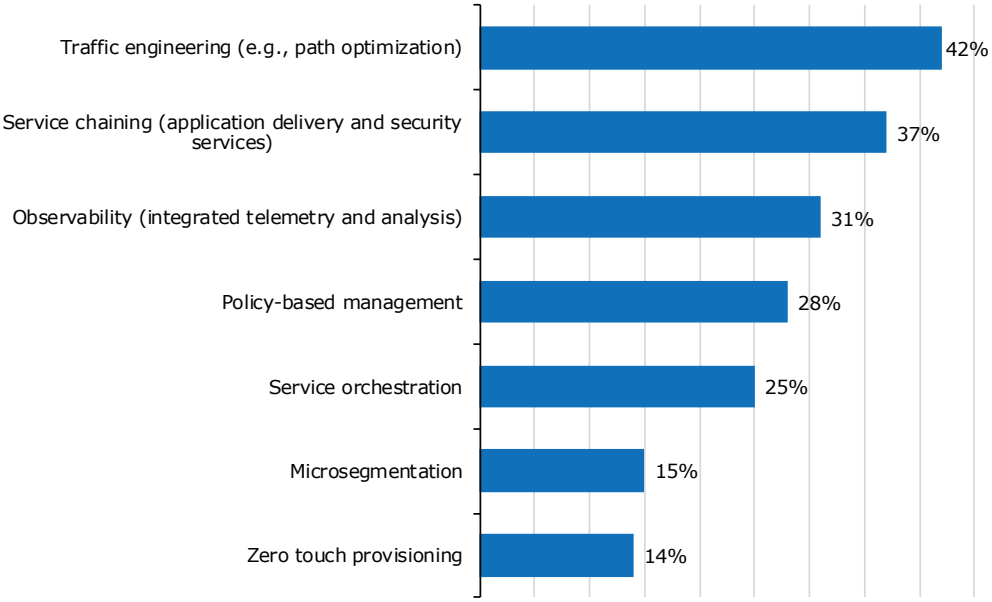
The AIOps capability for addressing needs like anomaly detection and traffic optimization is another top requirement, and it is also more appealing to IT engineering teams (58%). Successful network teams are also more interested in AIOps (60%).

Automated SDN changes and automated DNS and IP address management are the last two significant requirements for SDN network management. Successful network teams are more likely to seek automated configuration changes (57%), as are large enterprises (57%).

Enterprises are least likely to need increased monitoring of non-network elements, monitoring of a larger number of network elements, or shorter data collection intervals. However, DevOps professionals do see the value of monitoring non-network elements (58%), and so do North American enterprises (40%).

© 2020 Enterprise Management Associates, Inc. | www.enterprisemanagement.com

EMA also asked enterprises that have adopted or plan to adopt data SDN to identify the most important features and functionality that those technologies offer. **Figure 58** reveals that enterprises are primarily interested in traffic engineering and service chaining.



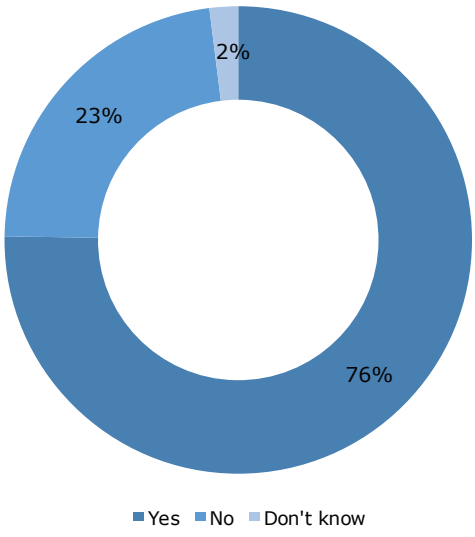
Sample Size = 209, Valid Cases = 209, Total Mentions = 404

Figure 58. Critical SDN capabilities

Improved observability, policy-based management, and IT service orchestration are secondary priorities. Service orchestration is particularly important to data center operations professionals (50%). Microsegmentation and zero-touch provisioning are the least critical. EMA suspects that microsegmentation might have received more interest if EMA had included IT security professionals in the survey.

MEGATREND #3: THE INTERNET OF THINGS IS DRIVING IT/OT PARTNERSHIPS

Previous research found that many enterprises are connecting IoT devices to their corporate networks. This year, that trend continues to hold, with more than three-quarters of enterprises reporting IoT devices on their networks, as revealed in **Figure 59**.



Sample Size = 350

Figure 59. "Are IoT devices connected to your enterprise network?"

© 2020 Enterprise Management Associates, Inc. | www.enterprisemanagement.com

IoT appears to be a driver of traffic growth, which is no surprise. Enterprises that project high (82%) or moderate (81%) network traffic growth over the next year are more likely to have IoT devices on the network, while enterprises with little or no project traffic growth are less likely (51%).

IoT is driving closer partnerships with OT groups.

EMA asked research participants to describe how the prevalence of IoT devices on the network is influencing their partnership with the operational technology (OT) group, the organization that typically has ownership of IoT devices. As **Figure 60** reveals, IoT is driving closer partnerships with OT groups. Among network teams with IoT on the network, 53% have close partnerships between the network team and the OT team already. Only 12% say there is no relationship between the two groups. Europeans are more likely (65%) to have a close partnership between the groups.

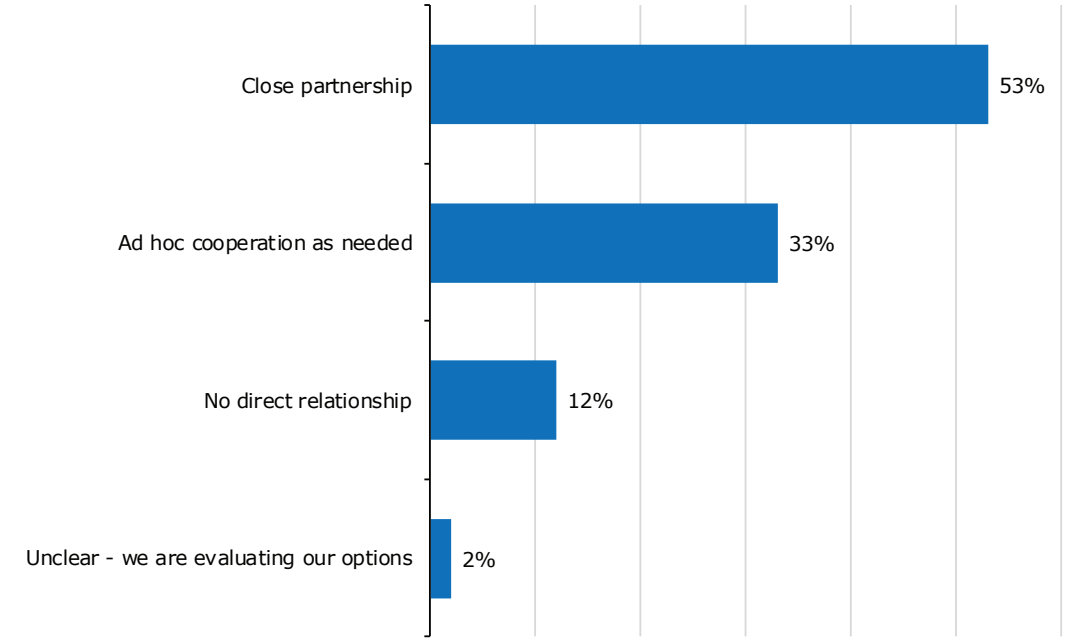


Figure 60. Relationship between network teams and operational technology teams (owners of IoT devices)

EMA found that close IT/OT partnerships are more likely within software companies, manufacturers, professional services firms, and retail/distribution/wholesale companies. Ad hoc collaboration is likely in financial companies, hospitality and entertainment, and legal firms.

© 2020 Enterprise Management Associates, Inc. | www.enterprisemanagement.com

IoT-Driven Networking Investments

Figure 61 reveals that IoT initiatives lead the majority of enterprises to make additional investments in network security. Secondarily, many IT organizations invest in network access control and network availability and performance monitoring. Wi-Fi and network segmentation investments are somewhat common. Wi-Fi investments are more common in enterprises that are projecting high overall network traffic growth this year (56%).

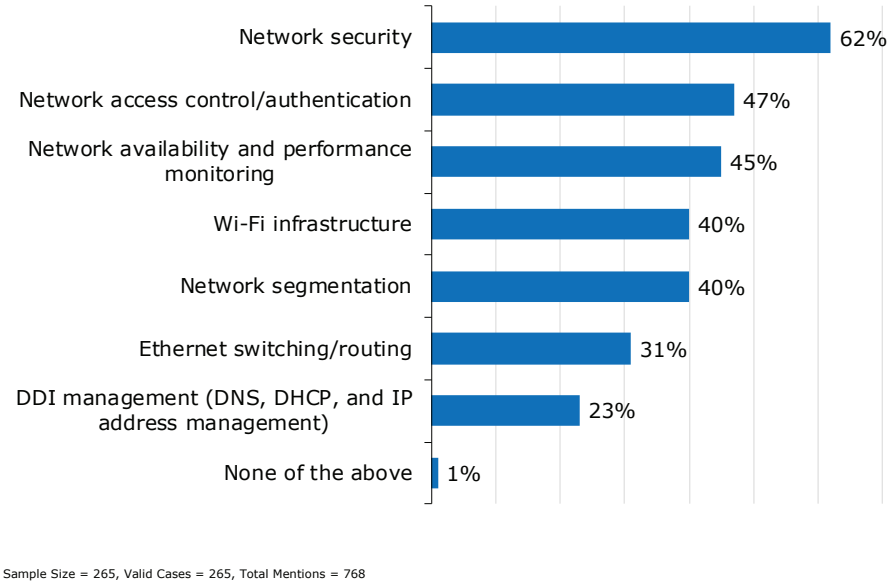


Figure 61. Networking investments driven by IoT connectivity

IoT initiatives are least likely to spur investment in DDI solutions. However, successful network teams are more likely (35%) than less successful teams (18%) to make IoT-related DDI investments. Successful teams are also making more investments in network monitoring tools (57%).

EMA also examined activity around edge computing. Edge computing is a distributed architecture concept that brings computing and data storage closer to the location where it is needed, reducing latency, bandwidth demand, and security risk for certain edge applications. IoT is a potential driver of edge computing adoption. **Figure 62** reveals that 23% of enterprises already have some form of edge computing in production, and only 5% claim to have no activity at all. Midsized enterprises are less likely (12%) to have edge computing in production However, the vast majority are either researching, evaluating, or implementing solutions.

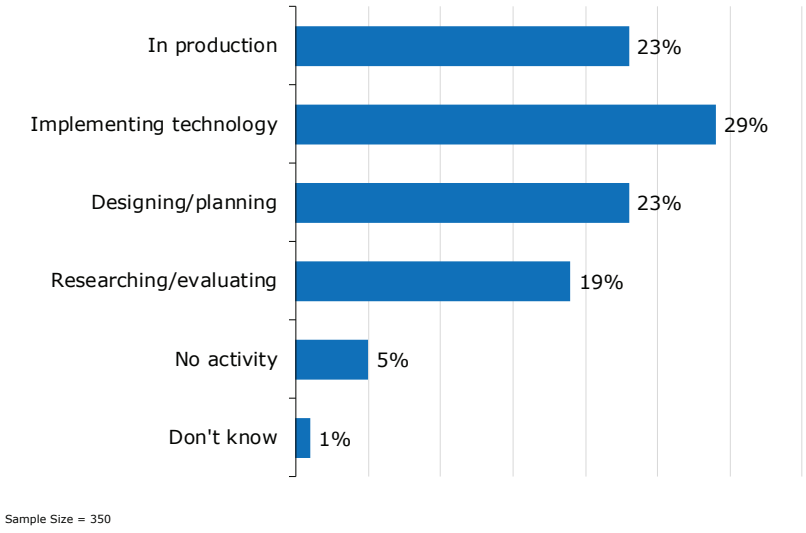
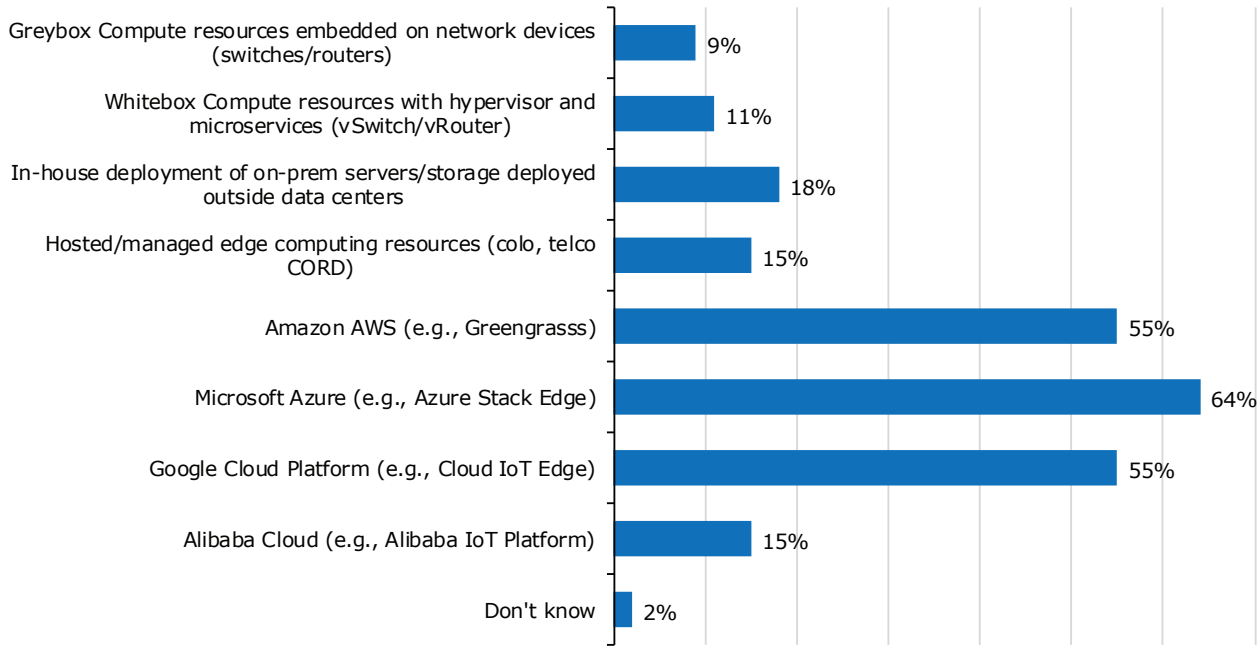


Figure 62. Edge computing adoption

© 2020 Enterprise Management Associates, Inc. | www.enterprisemanagement.com

Figure 63 reveals the edge computing solutions enterprises are using or considering for use. Edge computing solutions from the big three cloud providers (AWS Greengrass, Azure Stack Edge, and Google Cloud IoT Edge) are drawing the majority of interest from enterprises. Nothing else has captured much interest.



Sample Size = 350, Valid Cases = 350, Total Mentions = 853

Figure 63. Edge computing solutions that enterprises are considering/adopting

Successful network teams expressed more interest in Azure solutions (74%), but also in some of the less popular options, such as hosted or managed edge computing (e.g., colocation provider) (21%), white-box resources (19%), and grey-box resources on a network device (14%).

© 2020 Enterprise Management Associates, Inc. | www.enterprisemanagement.com

A large majority of network teams take on added responsibility for the security of IoT devices and services.

IoT Responsibilities of the Network Team

With so many enterprises connecting operational technology devices to the network, EMA wanted to measure how this impacts the responsibilities of the network team. **Figure 64** shows that a large majority of network teams take on added responsibility for the security of IoT devices and services. Security is an especially common responsibility for network teams in the healthcare industry (79%).

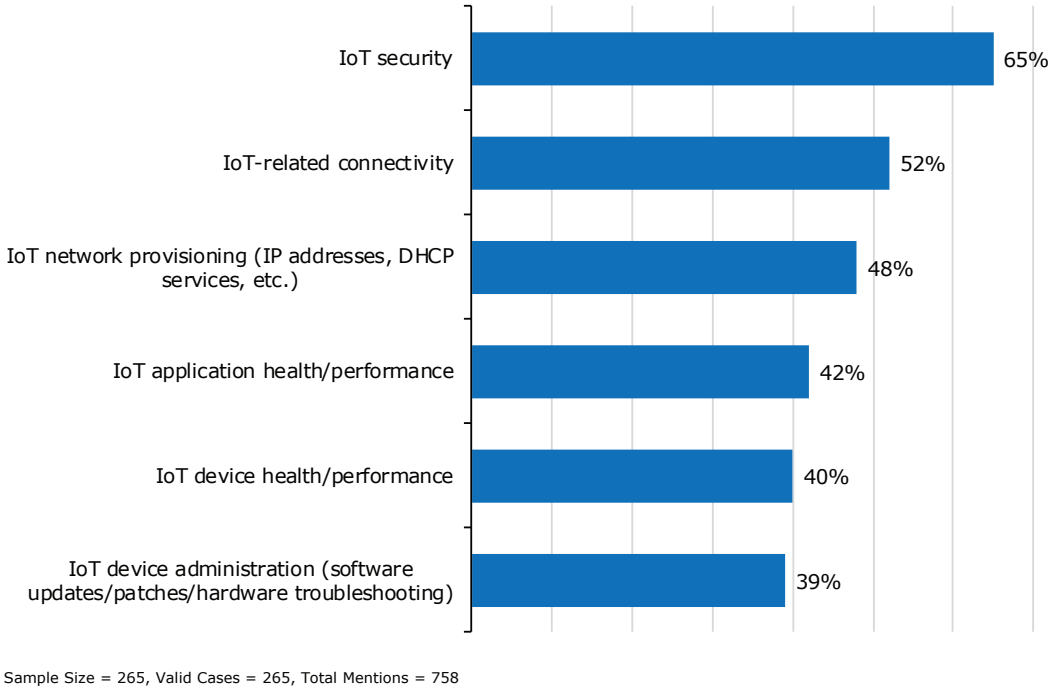


Figure 64. IoT-related responsibilities of the network team

The majority of network teams are also responsible for managing IoT-related connectivity (obviously) and nearly half are responsible for IoT network provisioning (IP addresses, DHCP). A significant minority are also responsible for IoT app health/performance and IoT device health/performance. The least common responsibility shouldered by the network team is IoT device administration. Network teams in midmarket enterprises are more likely (48%) to take on device administration, possibly because these smaller companies often lack a formal OT organization that is dedicated to the task.

EMA found that successful network teams take on more IoT responsibility in general. They are more likely to shoulder IoT-related connectivity, IoT network provisioning, device administration, and the health and performance of both IoT applications and devices.

© 2020 Enterprise Management Associates, Inc. | www.enterprisemanagement.com

MEGATREND #4: STREAMING NETWORK TELEMETRY POISED TO ENRICH MONITORING

Streaming network telemetry is an emerging option for gathering network statistics and metrics. Management plane streaming telemetry is a leading example. Rather than pull data via the Simple Network Management Protocol (SNMP) polling, network monitoring tools can subscribe to telemetry streams generated by network devices via mechanisms like NETCONF/Yang Push or gRPC Network Management Interface.

Streaming telemetry can be a more efficient, reliable, and secure mechanism for data collection. **Figure 65** reveals that 71% of network teams are interested in using this emerging technology. Somewhat successful network teams (76%) are particularly inclined to adopt it, whereas interest from successful teams is a bit softer (64%). This disparity suggests that enterprises that are struggling with network operations are more likely to look to new technologies to optimize management.

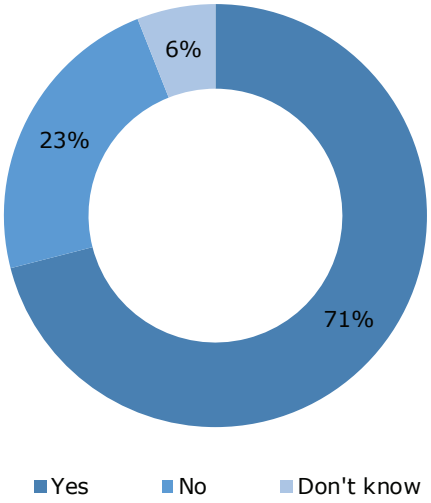


Figure 65. "Are you interested in collecting streaming network telemetry from your infrastructure?"

Enterprises that project high (77%) and moderate network traffic growth (77%) are more likely to be interested in streaming telemetry than companies that expect little or no growth (49%). North Americans (76%) also expressed more interest than Europeans (56%).

Streaming telemetry is often discussed as a potential replacement for SNMP in network management tools. IT organizations often complain that SNMP is resource-intensive, insecure, and lacks granularity and extensibility, and some prominent companies have proclaimed publicly their intent to remove SNMP from their networks altogether. However, **Figure 66** makes it clear that most enterprises have no plans to eliminate SNMP. Instead, they want to combine streaming telemetry with SNMP to get a deeper view of the network.

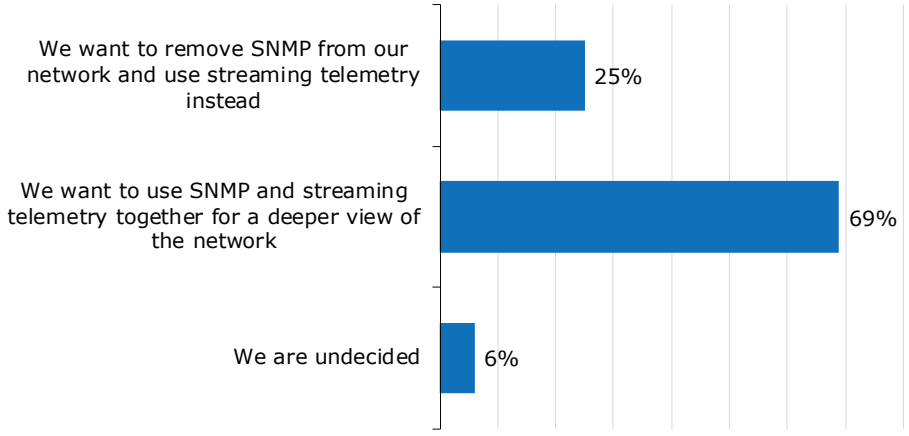


Figure 66. Interest in replacing SNMP with streaming telemetry

© 2020 Enterprise Management Associates, Inc. | www.enterprisemanagement.com

Enterprises that project the highest rates of network traffic growth are the most likely (39%) to want to remove SNMP from their network. Although they have less interest in streaming telemetry overall, Europeans are more likely (39%) than North Americans (22%) to look at it as a way to eliminate SNMP on the network.

EMA asked research participants to identify the single most important driver of their interest in streaming network telemetry. **Figure 67** reveals that efficient data transfer on the network is the most prominent driver, but not by a huge margin. Europeans (39%) are more interested in this benefit.

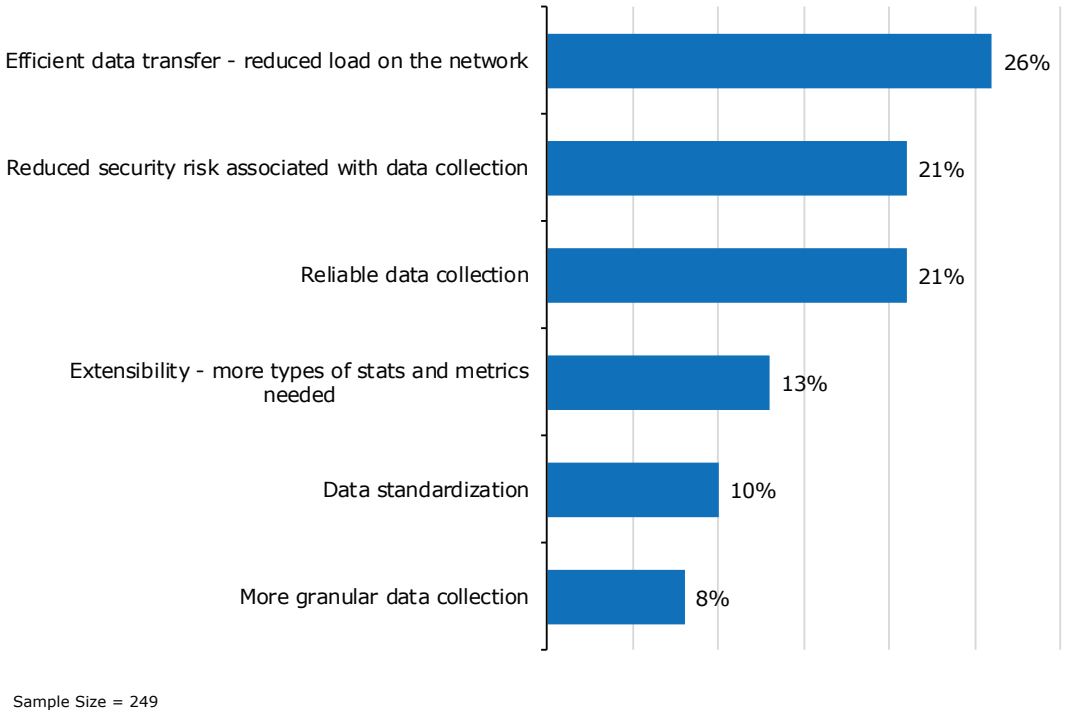


Figure 67. Primary driver of interest in streaming network telemetry

The chief secondary drivers are reduced security risk and the reliability of data collection. Extensibility was less important, and data standardization and data collection granularity were of least interest. Data center operations professionals expressed extremely strong interest in data standardization (44%). Enterprises that are expecting little or no traffic growth on their networks expressed strong interested in reduced security risk (38%).

MEGATREND #5: CLOUD PROVIDER FLOW LOGS ESSENTIAL TO NETOPS

This year, the average enterprise in this research estimates that 40% of all traffic on its network is attributable to external cloud applications, such as SaaS and IaaS-based services. This mean response represents a decline from 45% in 2018 and 44% in 2016. This reduction doesn't mean enterprises are necessarily pulling back from the cloud. It might just be a fluke, or traffic generated by non-cloud assets may be increasing significantly, driving down the share of traffic from the cloud. After all, 96% of enterprises expect overall traffic to increase this year.

The average enterprise in this research estimates that 40% of all traffic on its network is attributable to external cloud applications.

Given this prominence of cloud traffic, EMA has been paying close attention to how network operations teams incorporate cloud networking management into their overall tools and processes. One thing has become abundantly clear. Cloud provider flow logs are an essential data source for network management.

Earlier in this research, EMA described how cloud provider flow logs are the number-one data source for network capacity planning and the number-two data source for both sustained operational monitoring and network troubleshooting.

© 2020 Enterprise Management Associates, Inc. | www.enterprisemanagement.com

EMA's interactions with the industry have confirmed that cloud provider flow logs are a significant focus for network management vendors that are serving the needs of cloud-forward enterprises. While it is possible to collect other types from the cloud with network management tools, flow logs are clearly delivering tremendous value.

With that said, enterprises still need help with cloud network management. **Figure 68** reveals that only 36% of network teams believe that their ability to managing cloud networking with their current toolset is on par with their ability to manage their corporate networks.

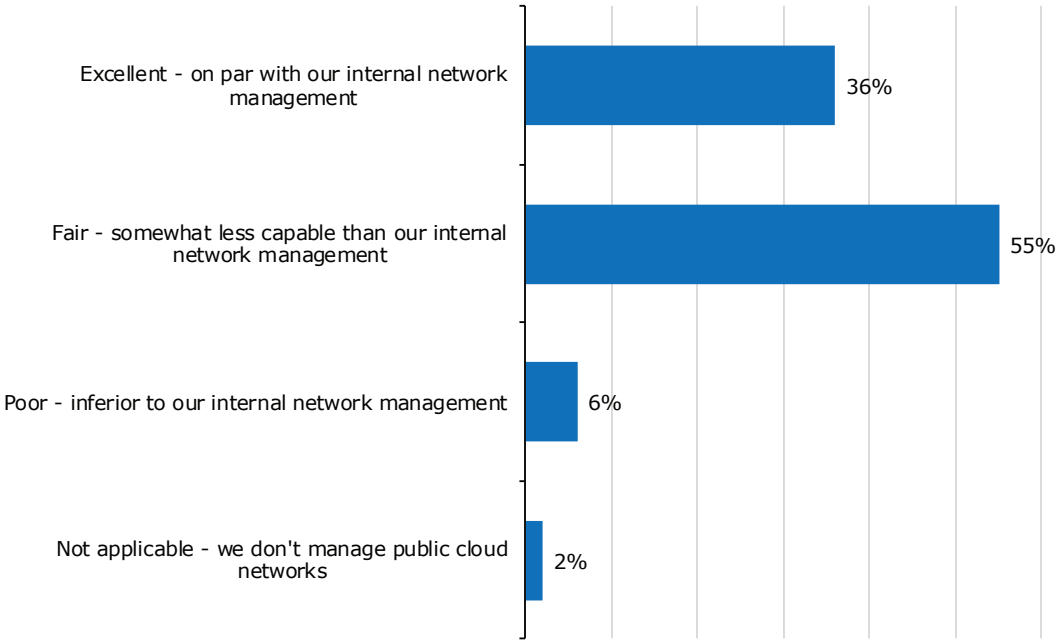


Figure 68. Effectiveness of public cloud support by network management tools

The majority of enterprises say their ability to manage public cloud networks is inferior to their management of internal network assets.

The majority of enterprises say their ability to manage public cloud networks is inferior to their management of internal network assets. This suggest that a great many network management vendors need to improve their public cloud support.

Naturally, successful network teams reported a higher rate of excellence with cloud networking management (63%), while only 22% of somewhat successful teams could say the same. In other words, successful network teams are three times more likely to have excellent cloud support from their network management toolsets.

Enterprises with 11+ network management tools are also more likely (61%) to have excellent cloud support, which reinforces EMA's belief that network operations teams close cloud gaps through new tool procurement.

© 2020 Enterprise Management Associates, Inc. | www.enterprisemanagement.com

CONCLUSION

EMA was pleased with many of the results in this research. For years, EMA has urged enterprises to take a consolidated approach to network management tool procurement. For the first time since 2008, enterprises showed progress on that front. Network teams also improved their ability to proactively detect IT service problems, which bodes well.

Network teams are also making progress in their partnerships with their peers in the security group. These two organizations need to collaborate because network performance and security are inextricably linked. The network is the gateway into the enterprise, a natural point of vulnerability. At the same time, security problems are often the root cause of network performance. Working together, these two teams can ensure the enterprise has a high-performing and secure network.

However, many challenges lay ahead. Network teams continue to struggle with cloud networking management. Their existing tools simply aren't as effective in that domain. This research did reveal significant interest in cloud provider flow logs, which suggests a path forward to improved cloud operations. Enterprises will need to push vendors to deliver parity between internal network management and external cloud network management.

IoT and data center SDN are also impacting many network teams, and they will need to adjust their tools and processes accordingly.

Finally, at the time of this publication, there is a great deal of uncertainty due to the COVID-19 virus. As the world responds to this crisis, the network is essential. Governments and businesses everywhere are relying on networks to respond to the crisis. Individuals need networks to continue working so they can connect with family and friends and distract themselves in uncertain times. Network managers are needed now more than ever. EMA's research will continue to explore how networks and network management evolve through this crisis and beyond in a better future.

© 2020 Enterprise Management Associates, Inc. | www.enterprisemanagement.com

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 or blog.enterprisemanagement.com. You can also follow EMA on Twitter, Facebook, or LinkedIn.

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

©2020 Enterprise Management Associates, Inc. All Rights Reserved. EMA™, ENTERPRISE MANAGEMENT ASSOCIATES®, and the mobius symbol are registered trademarks or common-law trademarks of Enterprise Management Associates, Inc.

Corporate Headquarters:
1995 North 57th Court, Suite 120
Boulder, CO 80301
Phone: +1 303.543.9500
www.enterprisemanagement.com

3937.03112020