Network Management Megatrends 2020

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

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

SPONSORED BY:

APCON
Solutions for Networks

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

Table of Contents

EXECUTIVE SUMMARY

This is a summary of Enterprise Management Associates' "Network Management Megatrends 2020" report Based on a survey of 350 North American and European IT professionals, the 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.

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

- 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.

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.

Figure 1 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).

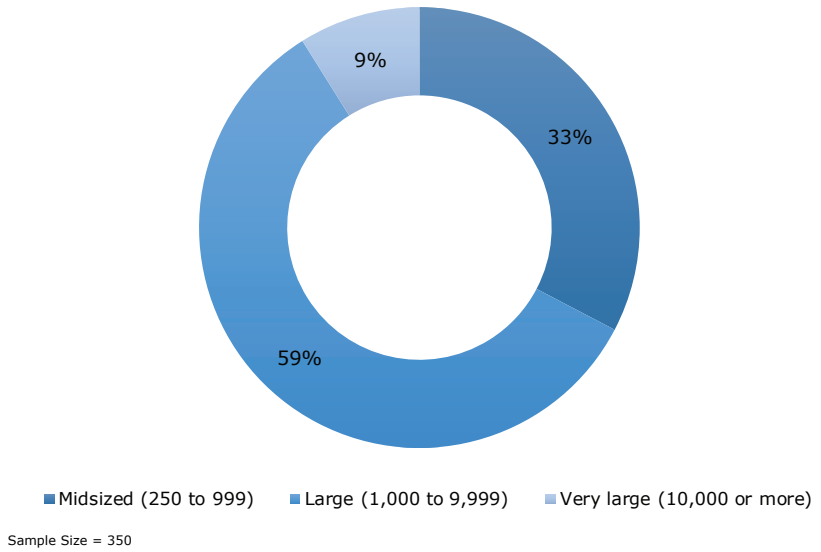


Figure 1. Size of company (by employees)

Figure 2 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.

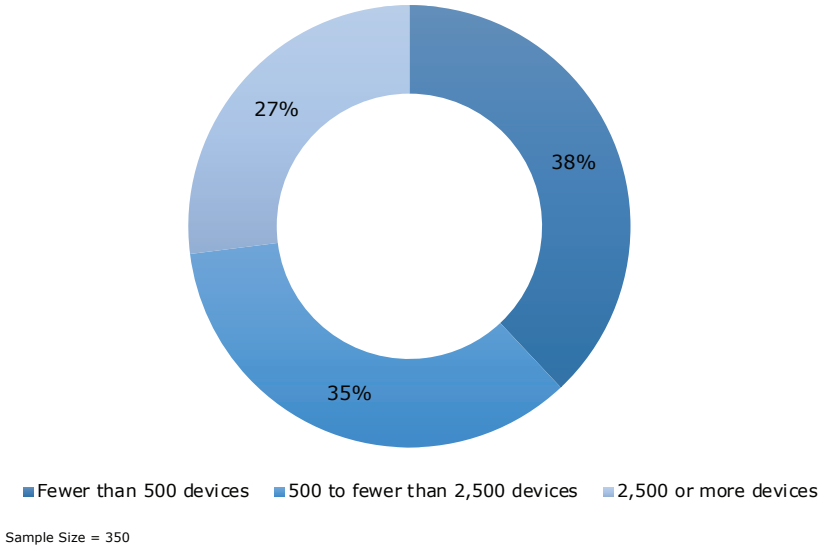


Figure 2. Network size (number of devices)

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 3** 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.

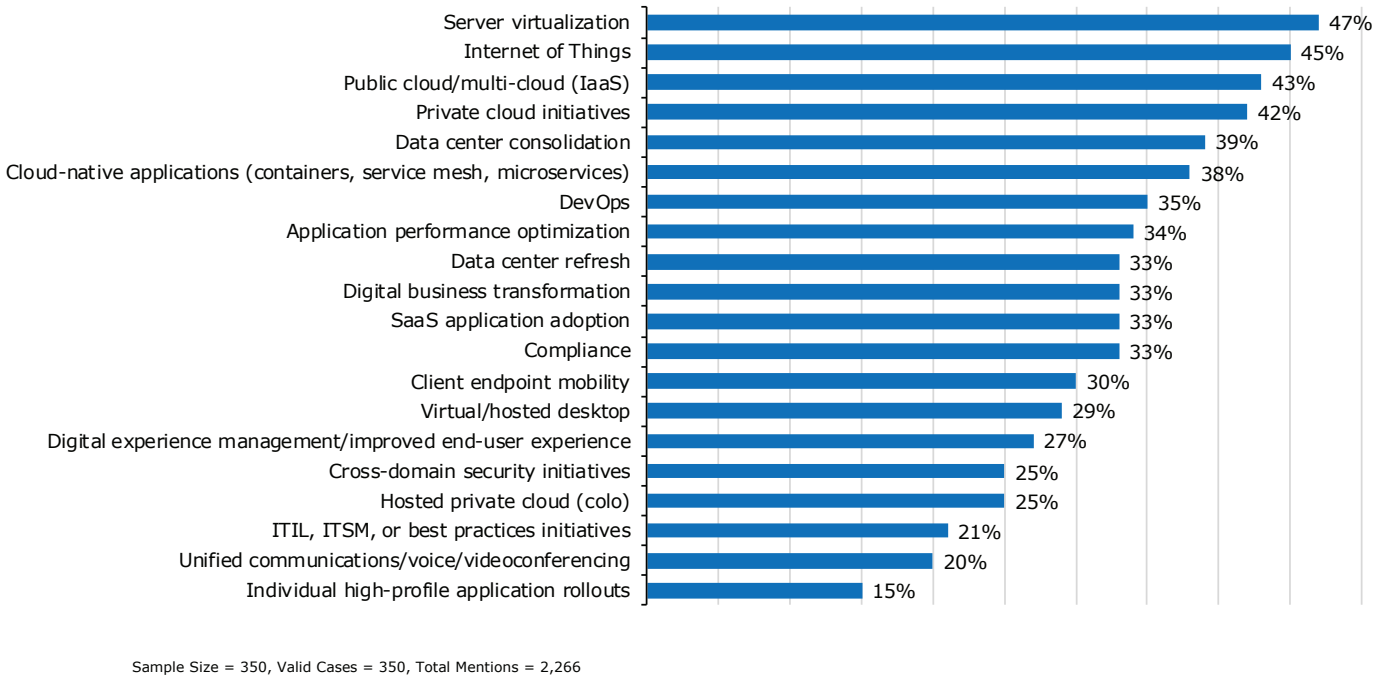


Figure 3. Broad IT initiatives that are driving current priorities in monitoring/managing networks and network application performance

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.

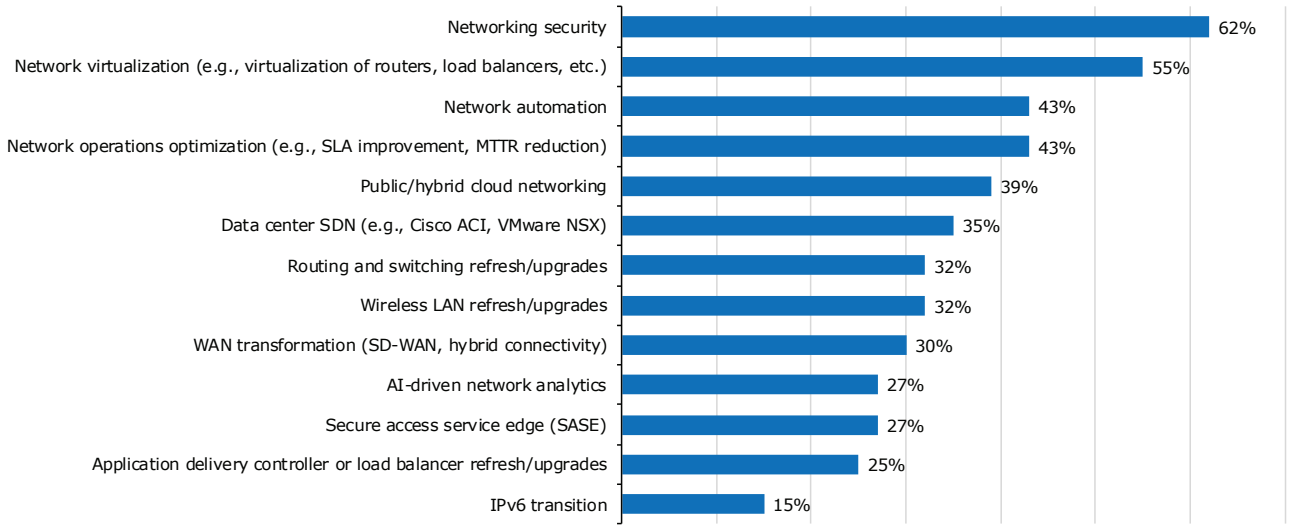
The following IT initiatives are more influential among enterprises that are the most successful with network operations:

- 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 4 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.



Sample Size = 350, Valid Cases = 350, Total Mentions = 1,636

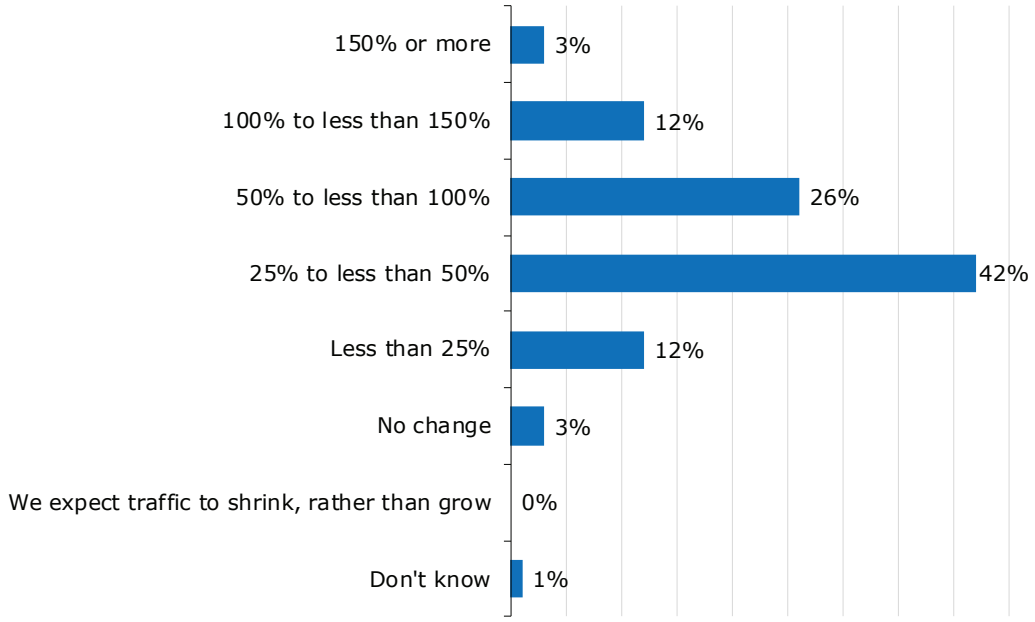
Figure 4. Networking initiatives that are driving current priorities in monitoring/managing networks and network application performance

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

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 5** 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.



Sample Size = 350

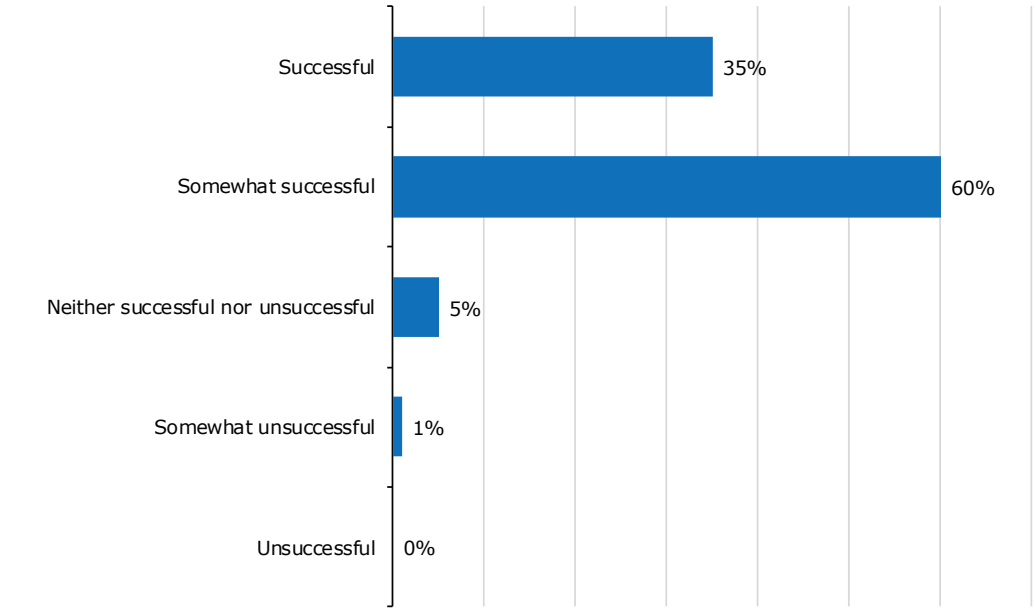
Figure 5. Projected traffic growth over the next 12 months

NETWORK OPERATIONS EFFECTIVENESS

Measuring NetOps Success

Figure 6 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.

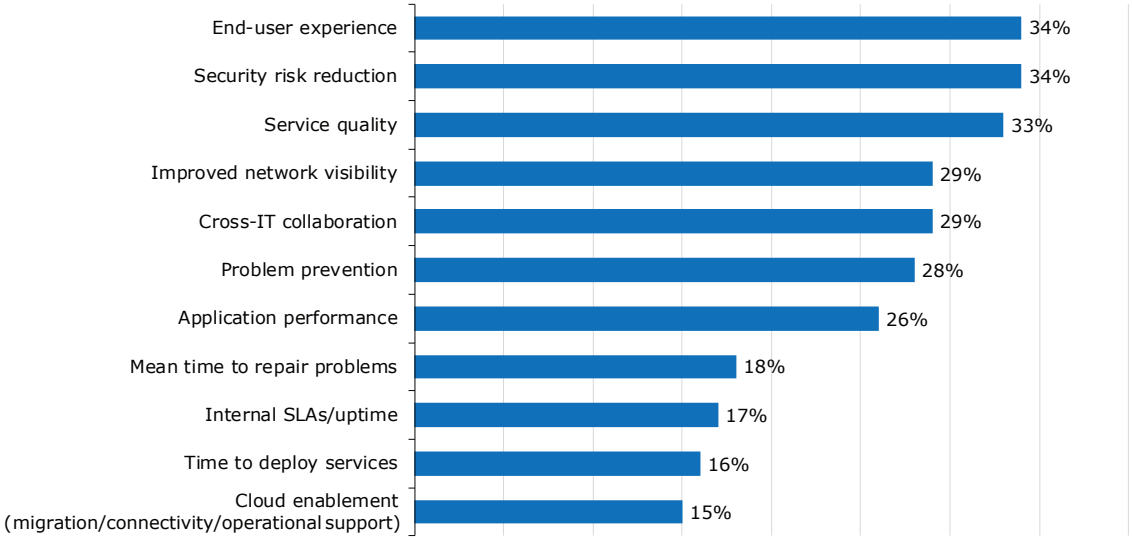
Only 35% rated their network operations efforts as fully successful.



Sample Size = 350

Figure 6. Success with network operations

Figure 7 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 7. 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%).

There is some dissonance between measuring success of NetOps and the business benefits of NetOps, as **Figure 8** 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?

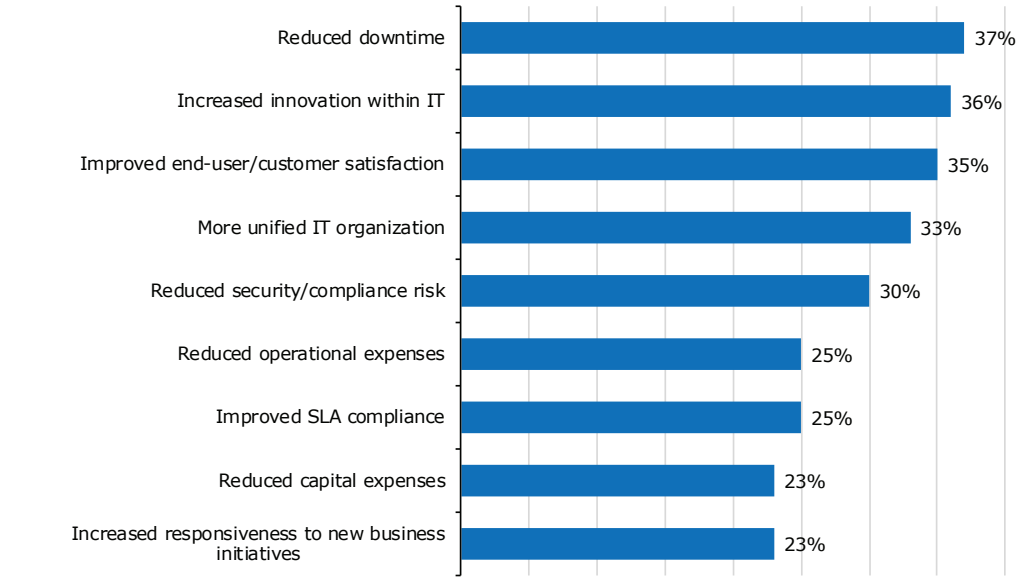


Figure 8. Most important business benefits of network operations success

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.

Network Operations Challenges

Figure 9 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.

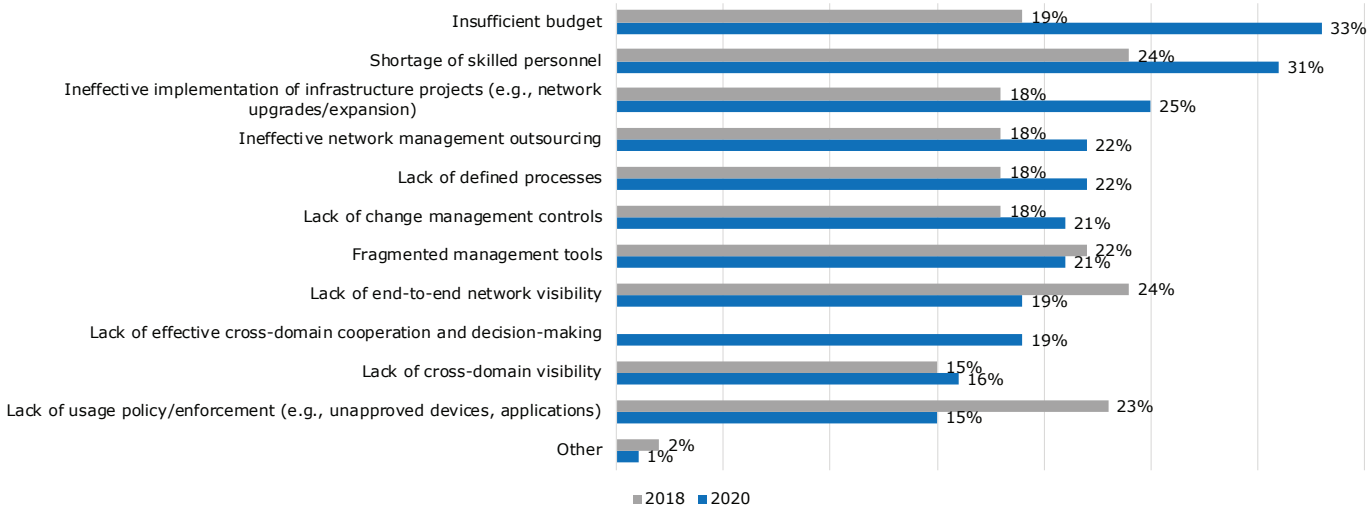


Figure 9. Top challenges to network operations success: 2020 vs. 2018

The shortage of skilled personnel remains prominent, but the rest of 2018's top challenges have subsided.

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.

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

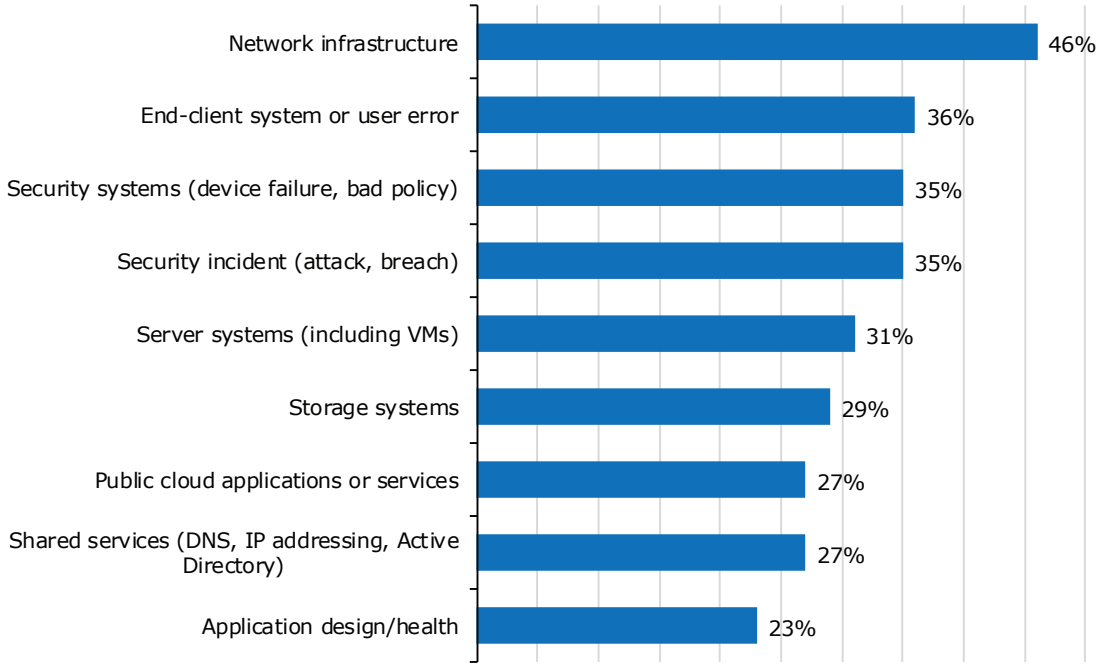
Ineffective implementation of infrastructure projects also emerged from obscurity in previous years to be a major challenge in 2020. A tremendous amount of network transformation occurred over the last few years, such as SD-WAN adoption, data center SDN, multi-cloud and hybrid cloud networks, next-generation 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.

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.

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 10** 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 10. 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.

NETWORK MANAGEMENT TOOLS

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.

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 11** illustrates.

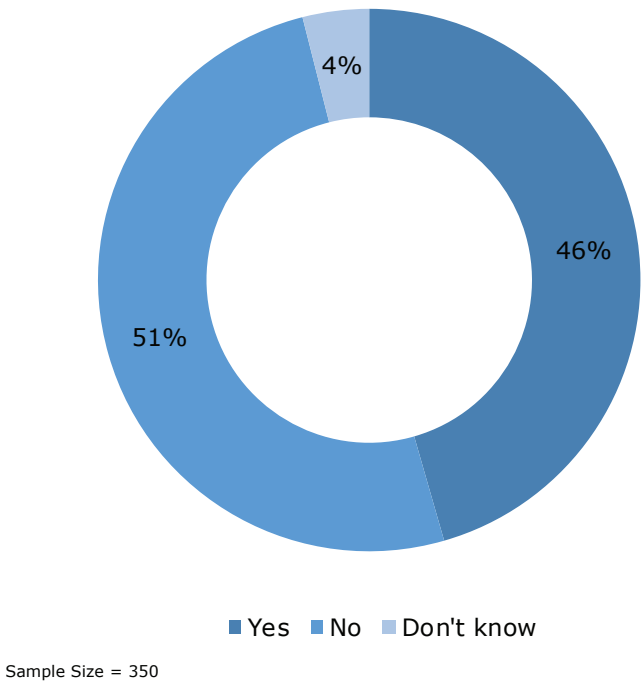


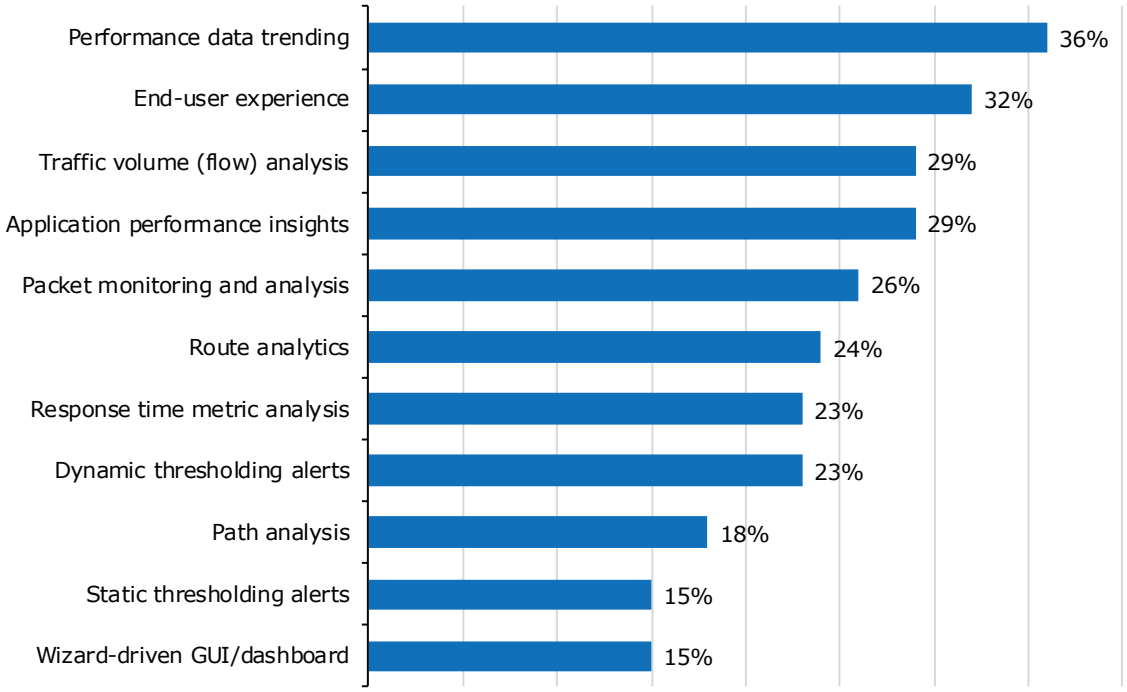
Figure 11. "Does your organization use a network packet broker/network visibility controller to direct traffic to network performance monitoring or diagnostics tools?"

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.

Network Management Tool Requirements

Figure 12 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.



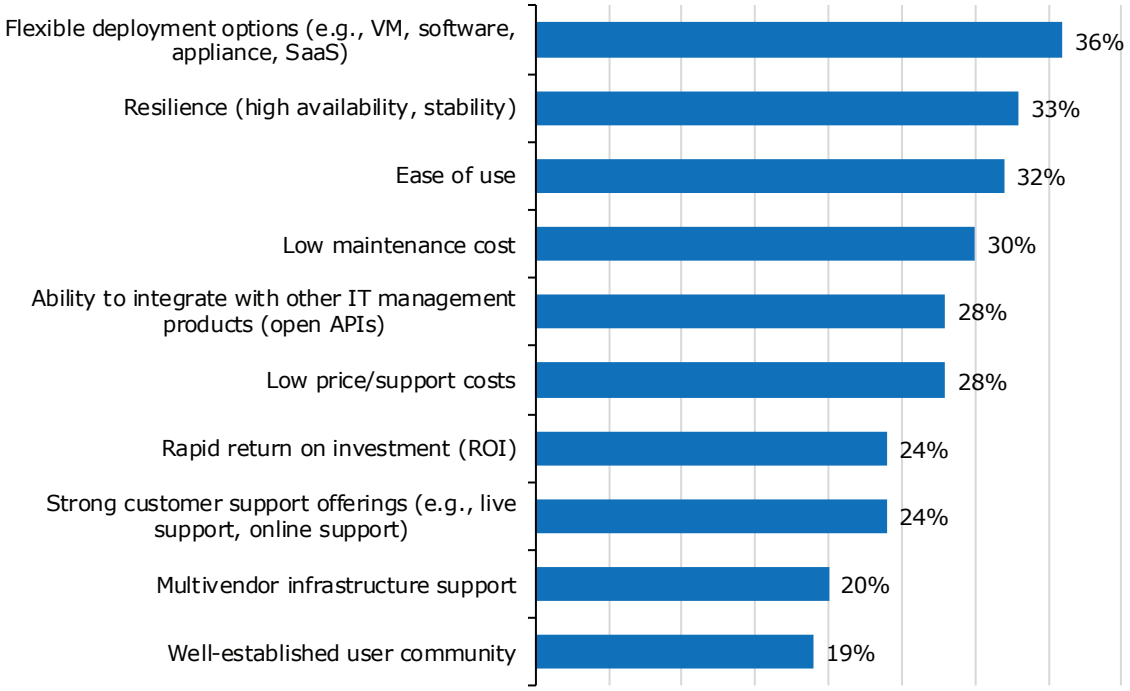
Sample Size = 350, Valid Cases = 350, Total Mentions = 947

Figure 12. 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.

Figure 13 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

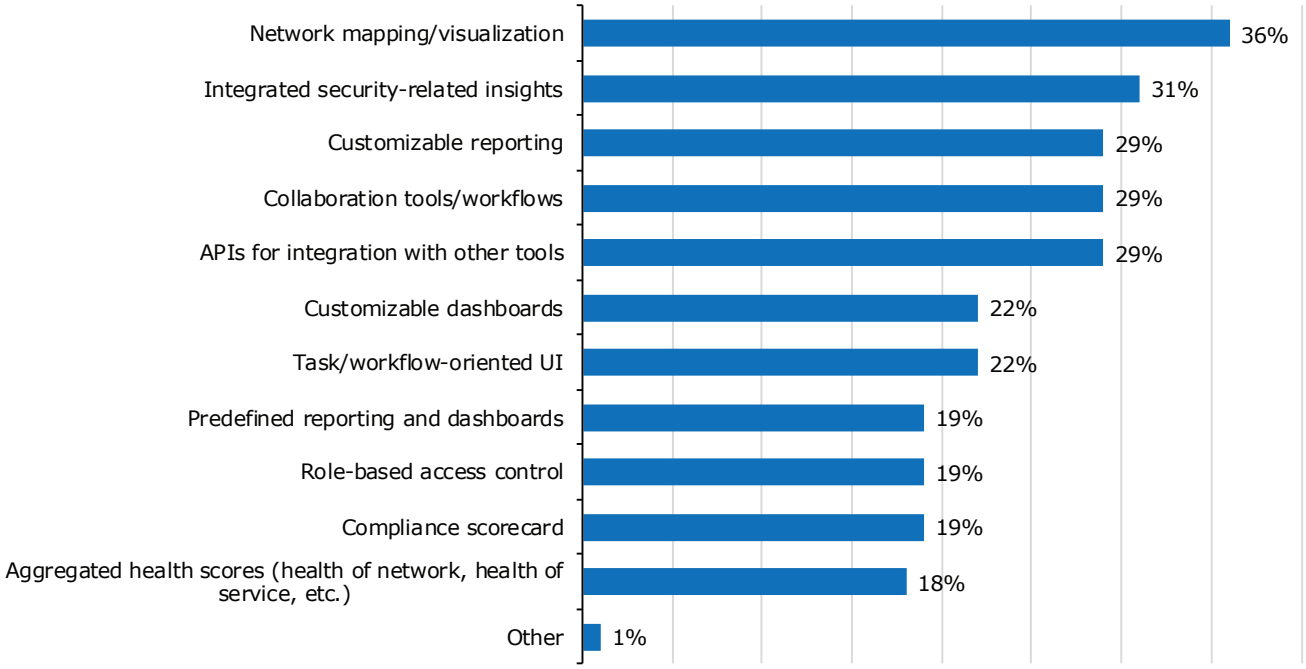
Figure 13. Top business requirements of network management products

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.

Figure 14 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 14. Most valuable general network management product features

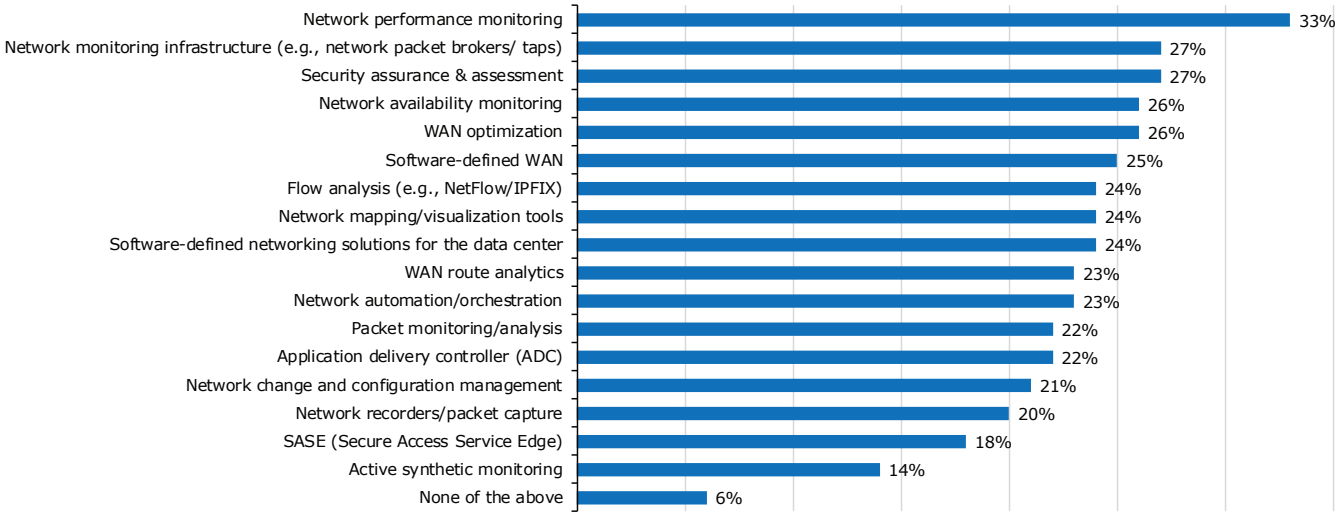
Integrated security insights are the second-most important feature. Midsized companies (38%) are especially more likely to rely on this capability. Customizable reporting, collaboration tools/workflows, and APIs for integration round out the top five tool features. Successful network operations teams 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.

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.

Figure 15 reveals 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 15. 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%).

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 16 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.

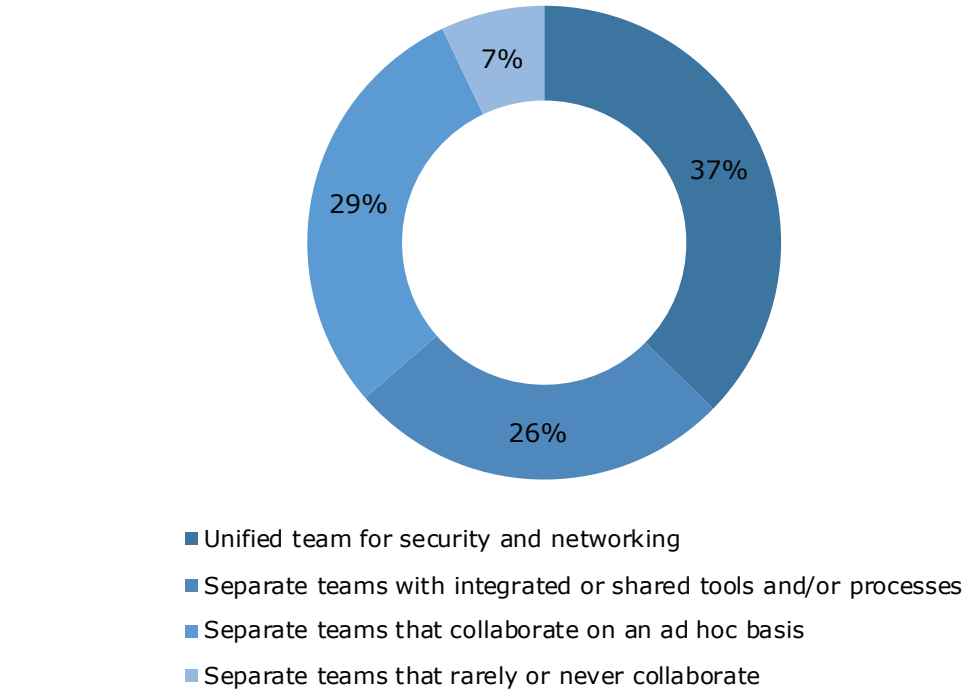
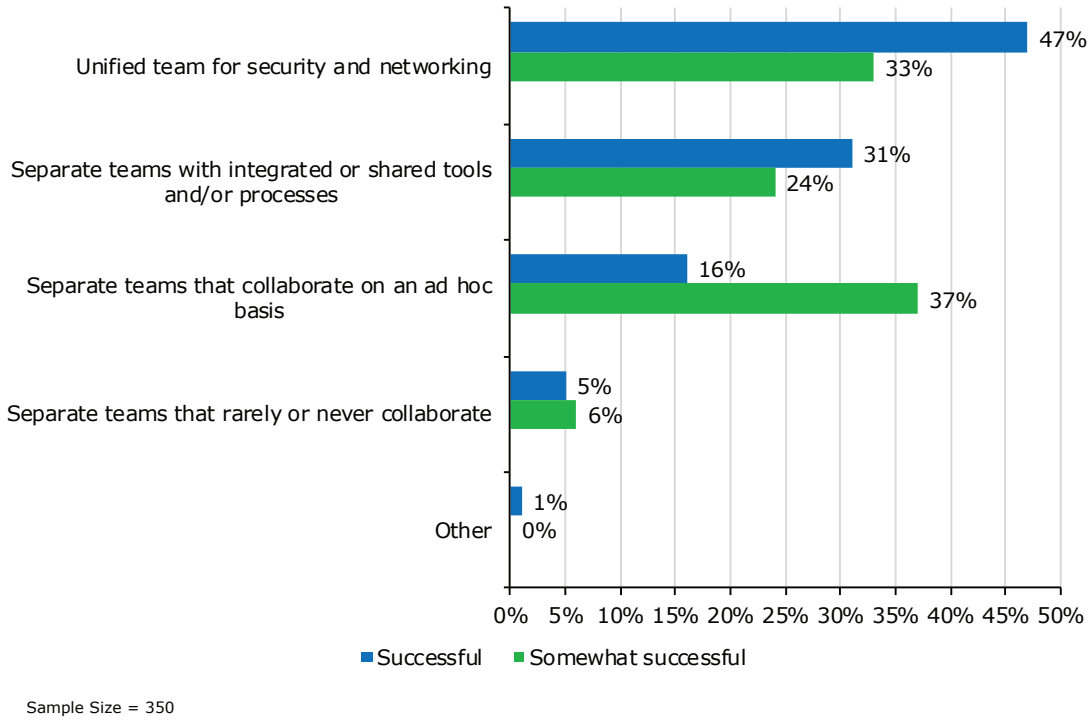


Figure 16. Relationships between today's network management and information security teams

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, as **Figure 17** 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.



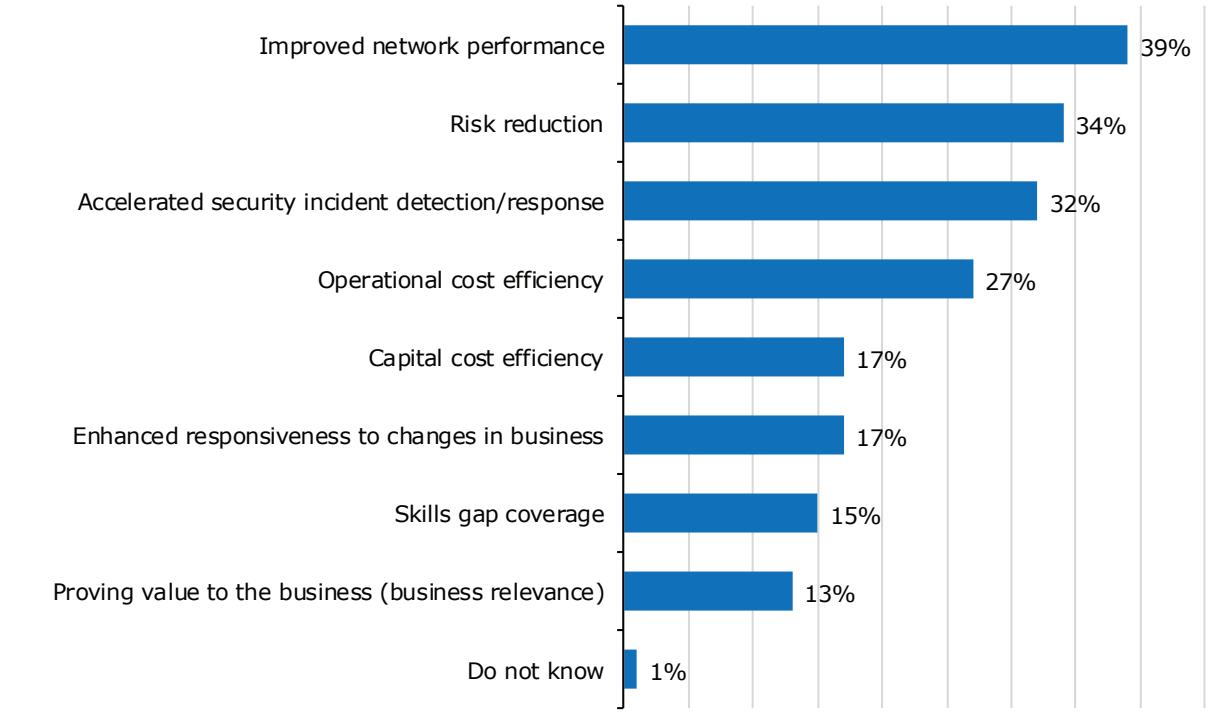
Sample Size = 350

Figure 17. Successful network operations teams have stronger ties to the security group

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

Benefits of NetSecOps Collaboration

Figure 18 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.

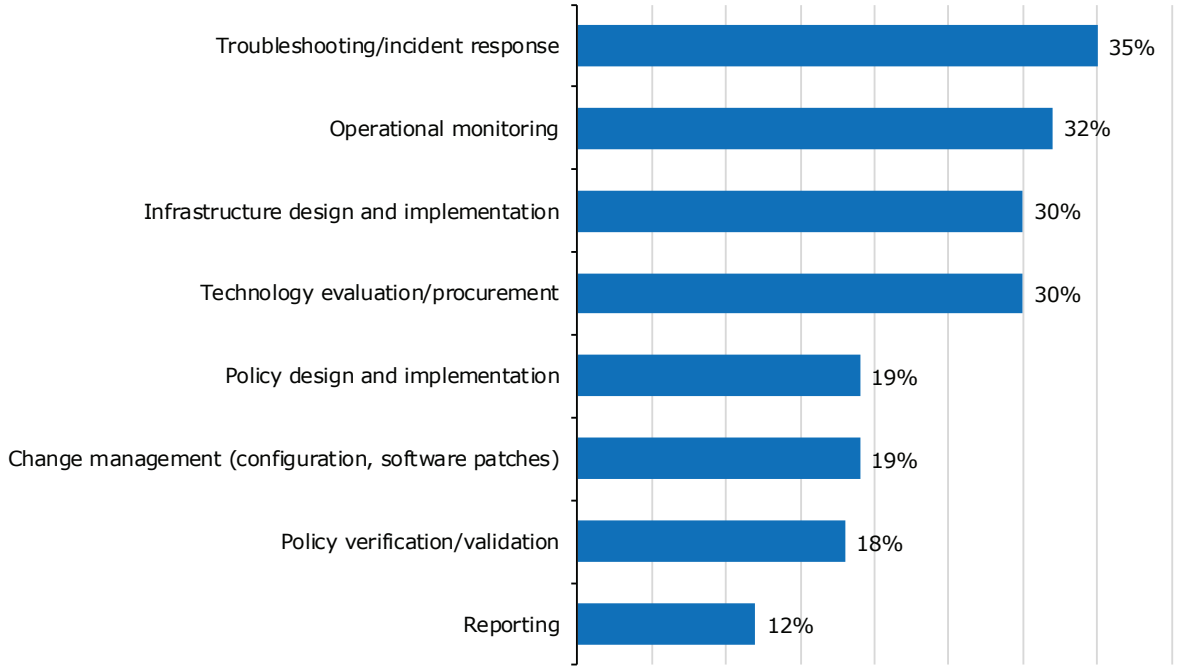


Sample Size = 350, Valid Cases = 350, Total Mentions = 683

Figure 18: Organizational goals of NetSecOps collaboration

How Network and Security Collaborate

EMA identified four aspects of engineering and operations where network and security teams focus their collaboration. **Figure 19** 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 19. Most critical points of collaboration between networking and security teams

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

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 20** 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.

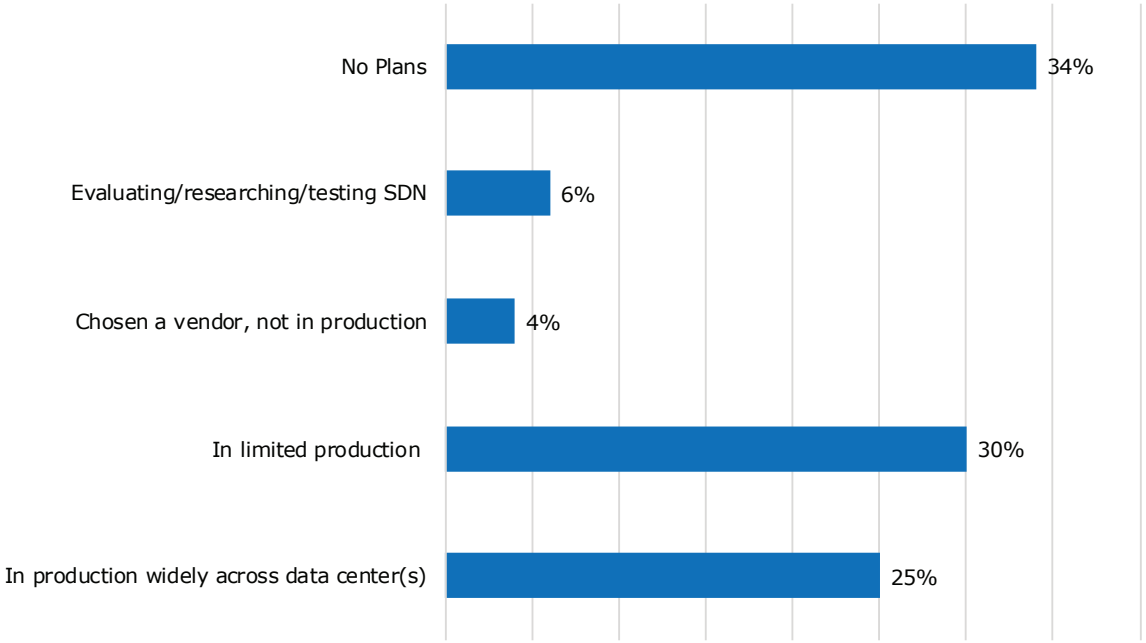
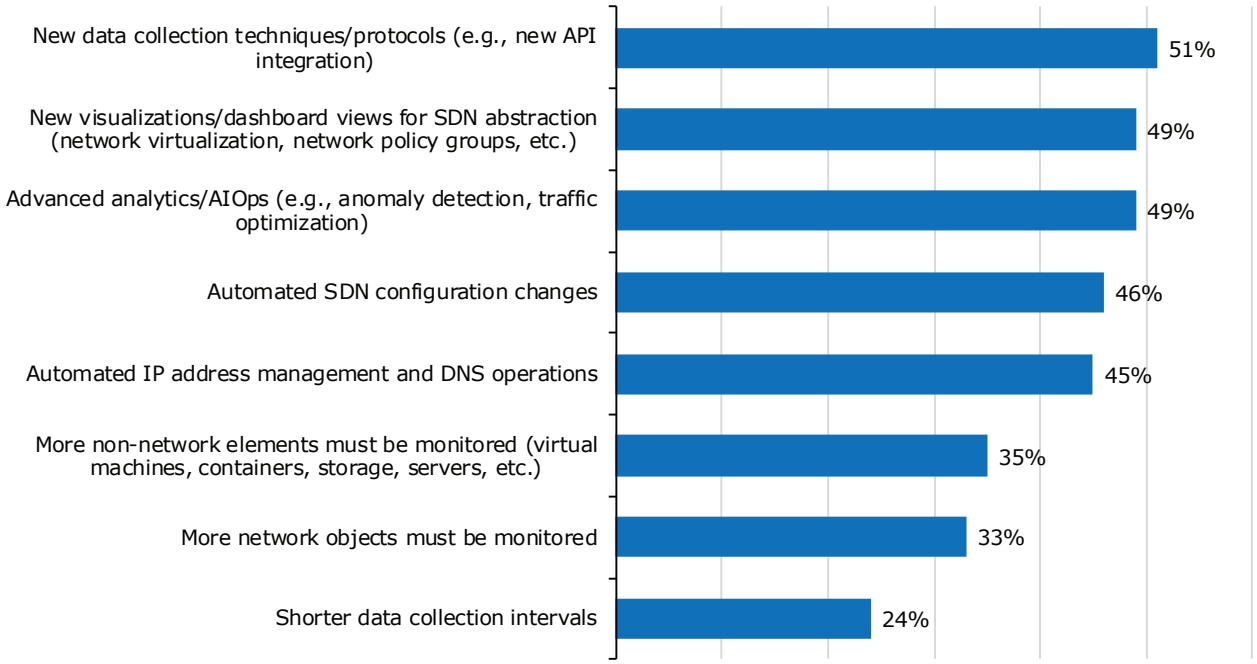


Figure 20. State of data center SDN adoption

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 21** identifies the new requirements SDN imposes on network management tools.



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

Figure 21. Most critical data center SDN-related network management tool requirements

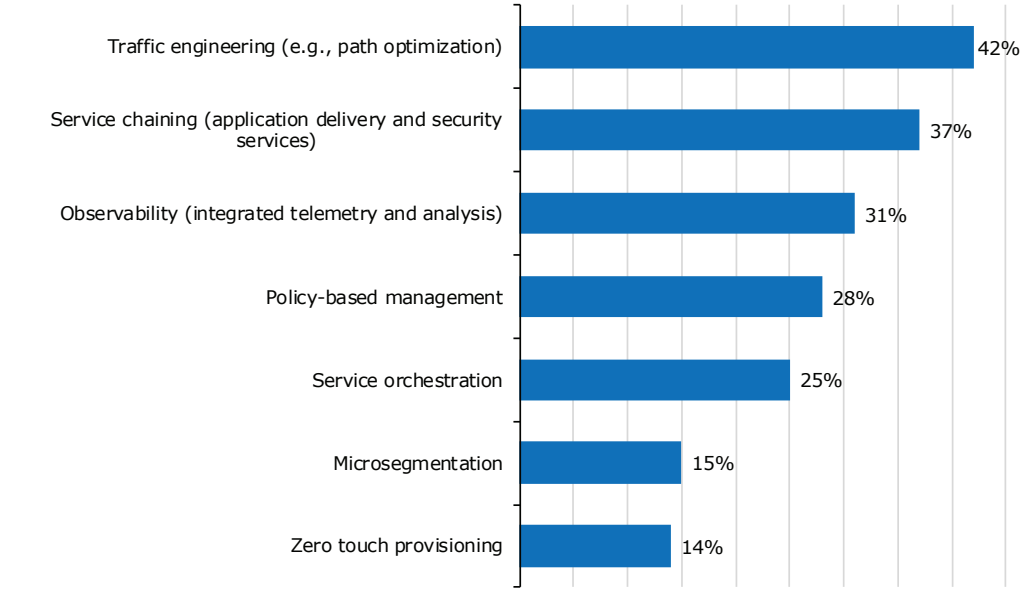
Overall, SDN typically affects network management tool requirements in five ways. It drives a requirement for new data collection techniques and protocols, such as API integration. Network managers also require new visualizations and dashboard views that can account for the abstractions that SDN introduces. 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%).

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 22** reveals that enterprises are primarily interested in traffic engineering and service chaining.



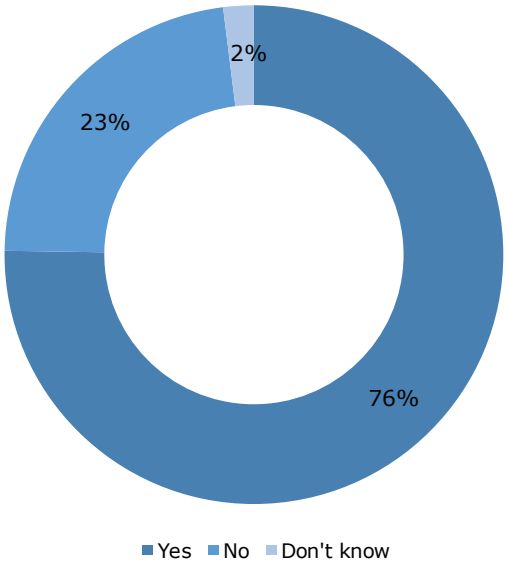
Sample Size = 209, Valid Cases = 209, Total Mentions = 404

Figure 22. 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 23**.



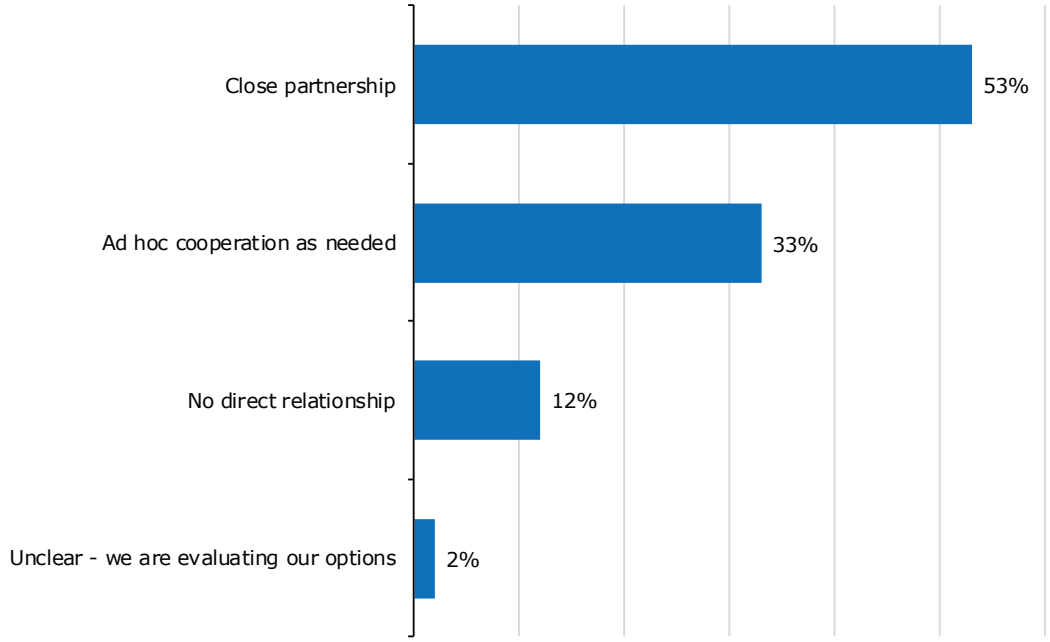
Sample Size = 350

Figure 23. "Are IoT devices connected to your enterprise network?"

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%).

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 24** 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.

IoT is driving closer partnerships with OT groups.



Sample Size = 265

Figure 24. Relationship between network teams and operational technology teams (owners of IoT devices)

IoT-Driven Networking Investments

Figure 25 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%).

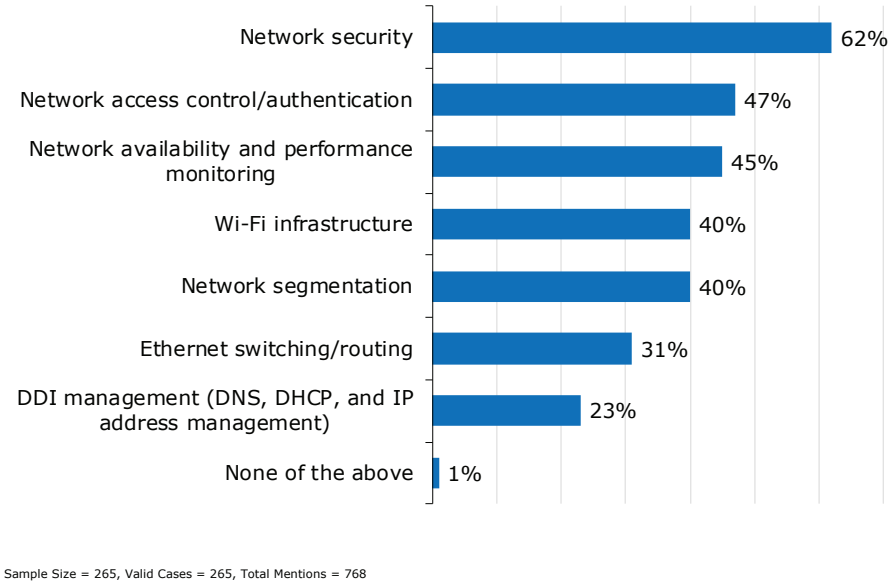


Figure 25. Networking investments driven by IoT connectivity

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%).

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 26** 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%).

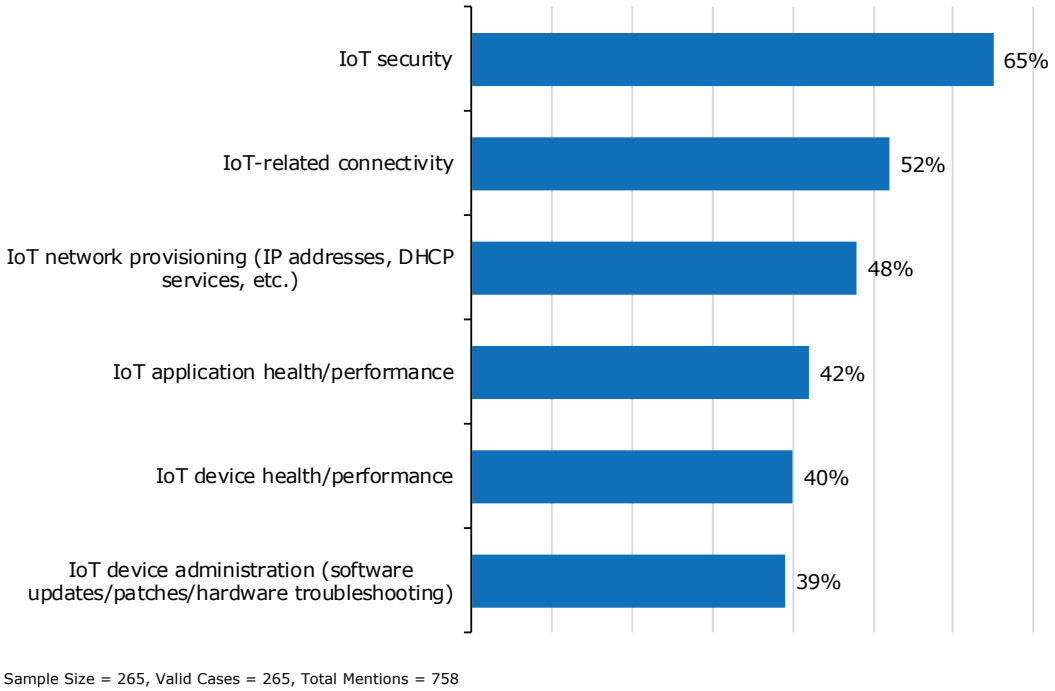


Figure 26. IoT-related responsibilities of the network team

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.

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 27** 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.

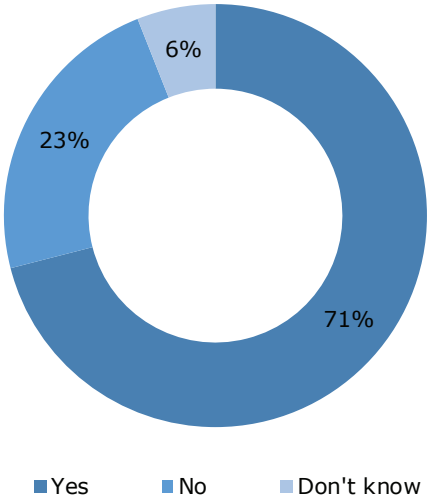


Figure 27. "Are you interested in collecting streaming network telemetry from your infrastructure?"

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 28** 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.

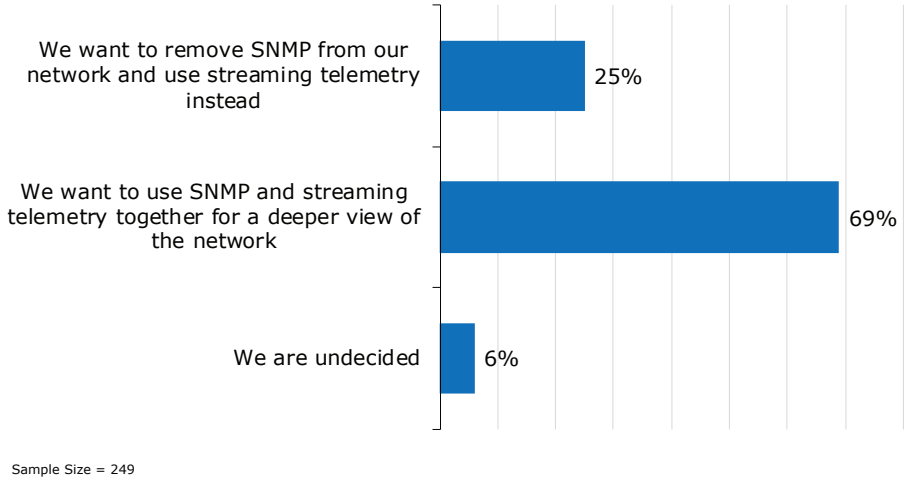


Figure 28. Interest in replacing SNMP with streaming telemetry

EMA asked research participants to identify the single most important driver of their interest in streaming network telemetry. **Figure 29** 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.

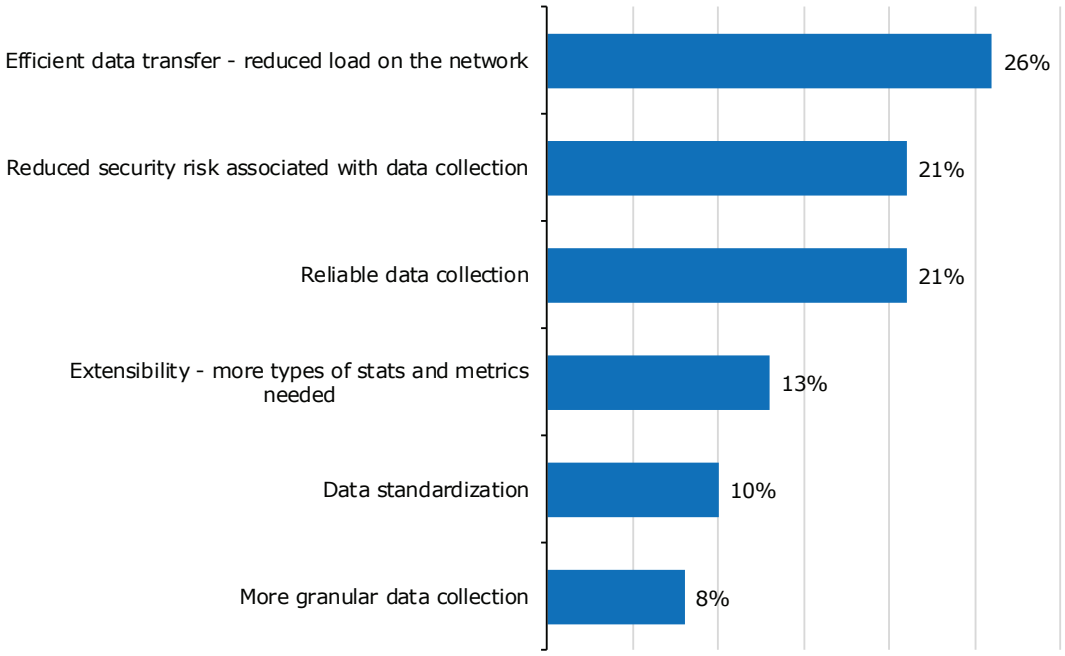


Figure 29. Primary driver of interest in streaming network telemetry

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

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.

This research found that 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.

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 30** 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.

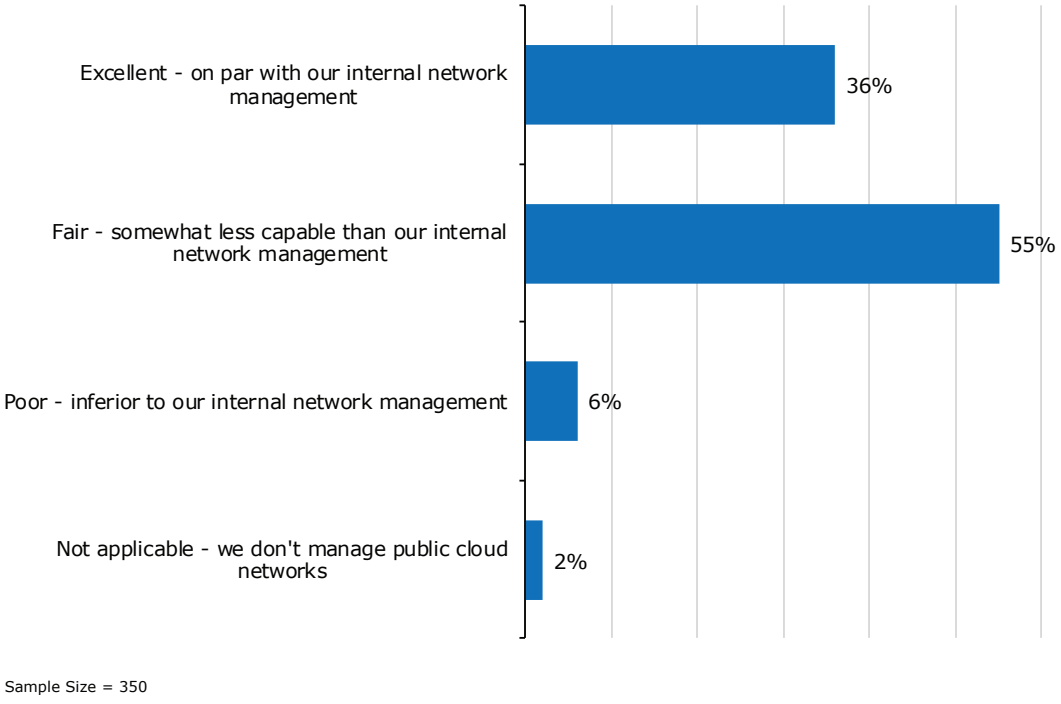


Figure 30. Effectiveness of public cloud support by network management tools

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.

CONCLUSION

EMA was pleased with many of the results in this research.

Network teams are 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.

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.

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

3937.05132020ApconSummary