IT & DATA MANAGEMENT RESEARCH, INDUSTRY ANALYSIS & CONSULTING

Sponsored by:

Post-Pandemic Networking: Enabling the Work-From-Anywhere Enterprise

July 2021 EMA Research Report Summary

By Shamus McGillicuddy

Table of Contents

Executive Summary

The COVID-19 pandemic forced hundreds of thousands of companies to send their employees home indefinitely. As the world starts inching toward a post-pandemic future, it's clear that most companies will allow many employees to work from home forever. This summary of new research by Enterprise Management Associates explores how enterprise IT organizations are adjusting their network infrastructure and operations to the massive and permanent increase in people who are working from home. It also explores the ripple effects this paradigm shift is having on on-premises network infrastructure.

The Work-From-Anywhere Revolution

The COVID-19 pandemic fundamentally changed the nature of work. Social distancing requirements across the world prompted thousands of companies and millions of employees to discover the benefits of a flexible work environment. Working from anywhere can enhance quality of life and productivity. For many, working from anywhere means working from home.

When the pandemic ends, millions of people will not return to working in corporate offices full-time. As **Figure 1** reveals, more than 85% of companies believe that the pandemic has permanently increased the number of their employees who work from home (WFH) on at least a part-time basis. Technology companies are especially likely to embrace this shift. For instance, 97% of IT equipment manufacturers and 93.3% of IT services and consulting companies reported permanent expansions of WFH employees.

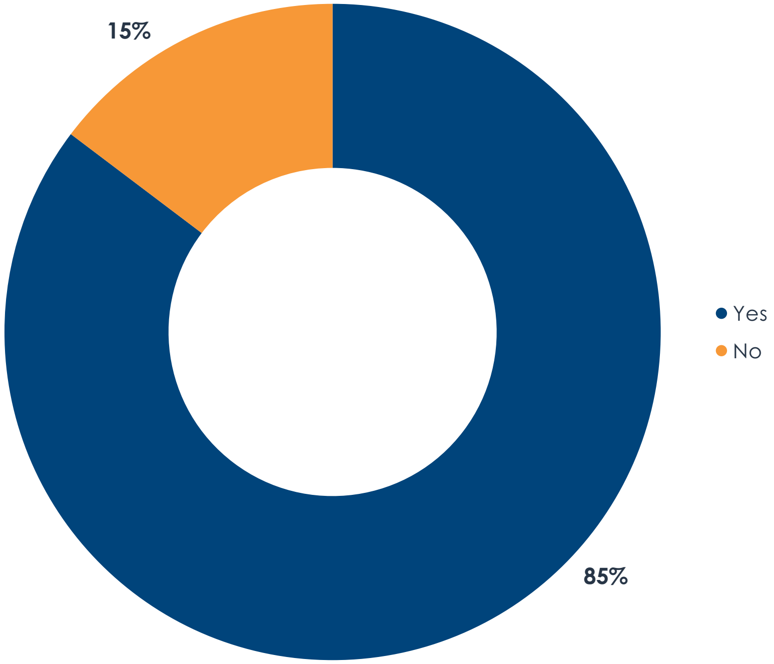

Figure 1. Has the COVID-19 pandemic permanently increased the number of employees in your company who work from home on a full-time or part-time basis?

Figure 2 shows the extent of the work-from-home impact in the average enterprise. Before 2020, less than 20% of employees worked from home on a part-time or full-time basis. After the pandemic, more than half of employees will be working from home. Even some industries that one might consider ill-suited to working from home are being impacted:

- Transportation from 11.2% to 30.1%
- Retail/Wholesale/Distribution from 16.7% to 40.1%
- Construction from 15.0% to 48.8%
- Oil/Gas/Chemical from 19.4% to 55.0%

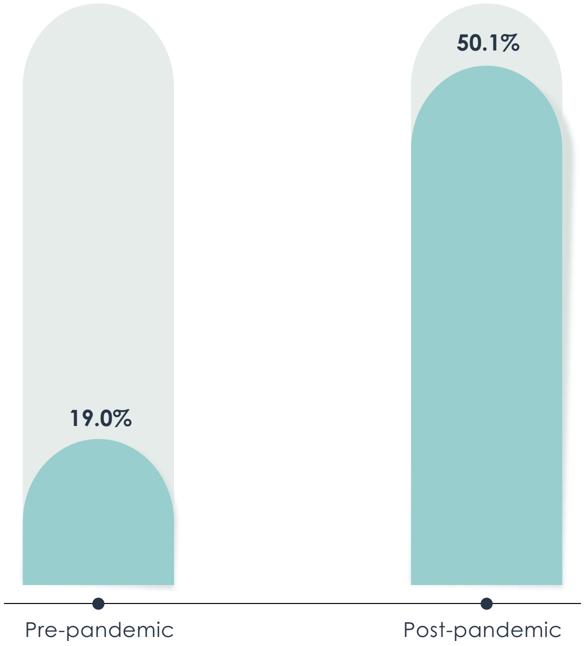

Figure 2. Estimated percentage of employees who work from home on at least a part-time basis, before and after pandemic

Sample Size = 312

"After the pandemic, we expect about 70% of people to go into the office only two or three days a week. Another 15% will never go back ever, and they will just do their jobs at home," said a network engineer with a large insurance company.

With this massive shift in the nature of work, network infrastructure and operations teams must adapt. For years, working from home was a perk, not a way of doing business. IT organizations often took an ad hoc approach to supporting remote employees. They operated a remote VPN to ensure secure access, but user experience was not a priority.

Now, the WFH end user is the future of business. Network teams need to embrace the home office as a part of the corporate network. They need to deliver secure connectivity with a consistent user experience. At the same time, they must understand how the on-premises network will change in the wake of this WFH revolution.

This research project explores how IT organizations will adapt their networks to this new reality. EMA believes that this shift toward remote work will force organizations to take a more systematic and strategic approach to connecting remote end users to applications and data. In the industrialized world, the typical home has a decent internet connection and a fine consumer-grade Wi-Fi setup for local connectivity. This setup has been mostly good enough for companies with small remote workforces. However, one's definition of "good enough" might change when a company goes from 80% of work taking place in corporate offices to 80% of work taking place in employees' homes. When that shift happens, the IT organization will lose control and struggle with observability and security.

This research summary explores how enterprises are reacting to this shift in working. It examines how network infrastructure and operations teams are changing their approach to the home office. It also explores ripple effects that this trend might be having on on-premises networks. This research is based on an April 2021 survey of 312 North American and European IT professionals with direct knowledge of how network infrastructure and operations will evolve in a post-pandemic world. EMA supplemented with survey data by conducting one-on-one interviews with several network infrastructure and operations professionals, who will quoted throughout this report.

This research is based on an April 2021 survey of 312 North American and European IT professionals.

Key Findings

- Only 31% of IT organizations are fully successful with supporting the networking requirements of users who work from home
    - Budget issues and infrastructure complexity are their biggest challenges
- 75% of IT organizations are installing network hardware in the homes of some end users
    - Network security and Wi-Fi are the most typical network functions running on this hardware
- 72% of IT organizations are installing wireless WAN connectivity (4G and 5G) in the homes of some end users
- 78% of IT organizations are deploying SD-WAN in the homes of end users
    - 16% take a software-only approach to deploying SD-WAN in homes
- The pandemic prompted 81% of IT organizations to launch or accelerate their engagement with secure access service edge (SASE) technology
- 96% of IT organizations are allocating budget for enabling network monitoring and troubleshooting toolsets to support end users who work from home
- Network operations teams need tools that offer security-related insights, dashboards, and reporting on home office networks, and more scalability
- Despite the expansion of remote work, 61% of enterprises are increasing their investments in on-premises local network infrastructures
    - This expanded investment is primarily driven by new security requirements, bandwidth demand, and office mobility requirements
- Nearly 85% of IT organizations say the pandemic has led to interest in the long-term use of location-based services on their wireless LAN infrastructures, particularly:
    - Productivity optimization, such as floating desk and conference room availability management
    - Room occupancy enforcement
    - Smart HVAC
- 59% of IT organizations have increased their investment plans for SD-WAN installed in corporate offices, despite the work-from-home surge
    - These investments are primarily driven by new security requirements and cloud access requirements
- 91% of network teams permanently expanded their use of network automation during the pandemic

Adapting Network Infrastructure and Operations to Work-From-Anywhere

Connecting and Securing the Home Office

IT organizations have not traditionally deployed network hardware in the homes of end users, unless those users were very important people, such as a CEO who likes to hold HD video conferences with important customers from his mansion. IT organizations were surrendering a good deal of control and visibility with this lack of hardware, and they were fine with that in the past. However, things have changed.

The Home Internet Connection

Across Europe and the United States, broadband infrastructure has still not reached all rural areas. It's hard for an employee to be productive while relying on a tier 3 ISP with limited bandwidth and unreliable performance. Enterprises avoid this problem by placing corporate offices in locations with robust telecommunications infrastructure. When people start working from home, the rural broadband gap becomes a problem.

"Our biggest issue is West Virginia, where we have a big call center. There aren't any big cable companies. It's all very low-quality ISPs. People are having issues out there," said a network engineer with a large insurance company.

In areas where terrestrial ISPs are inferior, fixed mobile broadband services like 4G and 5G can remediate the problem. **Figure 3** reveals that 72% of IT organizations are deploying these wireless services to the homes of some employees. Small enterprises (fewer than 1,000 employees) and midsized enterprises (1,000 to 10,000) are more likely to be moving in this direction. Best-in-class companies are less likely to be deploying wireless to homes, suggesting that a good chunk of IT organizations that are successful with supporting WFH initiatives are not confronted by poor ISP quality.

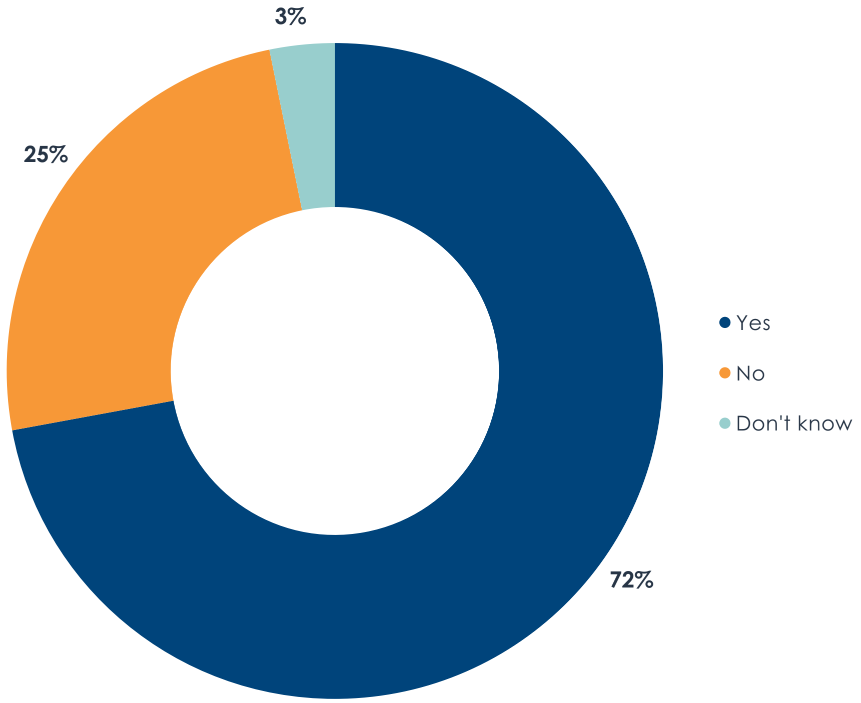

Figure 3. Has your IT organization installed or does it plan to install wireless WAN connectivity (e.g., fixed 4G or 5G) in the homes of any of its remote workers?

Installing Enterprise Network Hardware in Home Offices

Figure 4 reveals that 75% of IT organizations are planning to deploy network hardware in the homes of at least some remote employees. This is more common in North America (81.9%) than Europe (67.4%). It's also more common among manufacturers of IT equipment (89.5%), IT services and consulting firms (80%), professional services and consulting firms (100%), and retailers (86.4%). It's less common among government organizations (50%), nonprofits (40%), oil and gas companies (37.5%), and transportation enterprises (57.1%).

"I think we need a home office network-in-a-box. You can send them an access point, possibly a little switch, and a security gateway. The footprint would be really small. It could be one device or a modular system. It can get expensive if you have 10,000 users, but I think it would give home users an in-office experience. It would probably still be cheaper than paying for real estate," said a network engineer with a large regional bank.

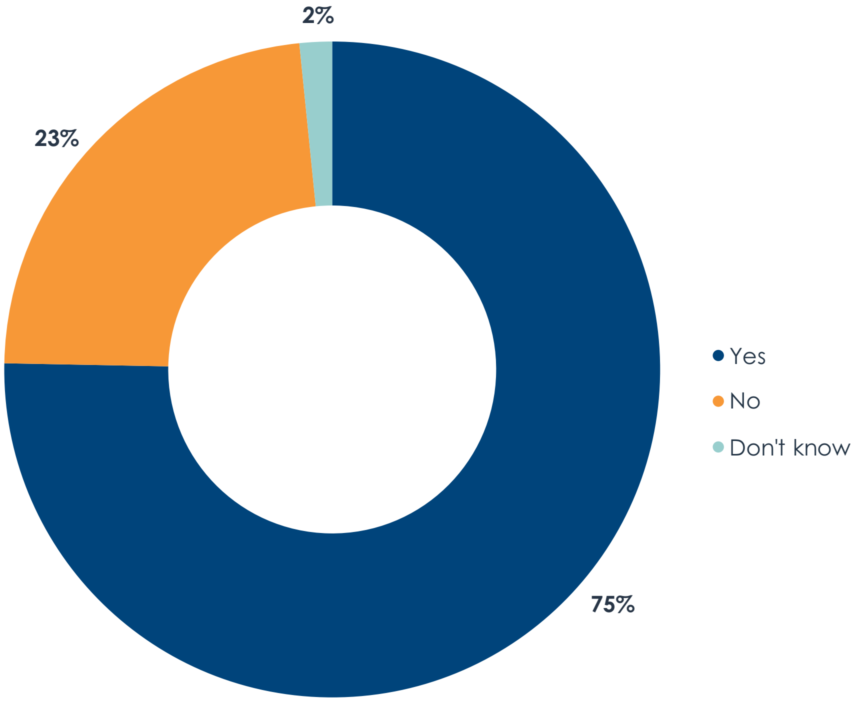

Figure 4. Has your IT organization installed, or does it plan to install, network hardware of any kind in the homes of remote employees?

Figure 5 reveals the kind of network functions and services IT organizations will run on the hardware that they deploy to homes.

Top reasons for deploying network hardware in home offices

1. Network security
2. Wi-Fi connectivity

Network security will reduce the risk associated with the growth in remote work. As more people work from home, more data is exposed. Secure remote access technology, like a VPN tunnel, can secure data as it traverses the internet, but a UTM or firewall can protect all of the IT assets that reside in an employee's home. Consumer Wi-Fi is susceptible to interference and coverage issues in a home. Many companies also struggle with employees who live in apartment complexes with shared Wi-Fi. They may elect to install a dedicated access point in an apartment with a mobile broadband router to ensure consistent network performance.

IT organizations also have significant plans for installing WAN routing, software-defined WAN (SD-WAN) gateways, and switches in some homes. Larger enterprises are more likely to have plans for installing SD-WAN gateways and switches.

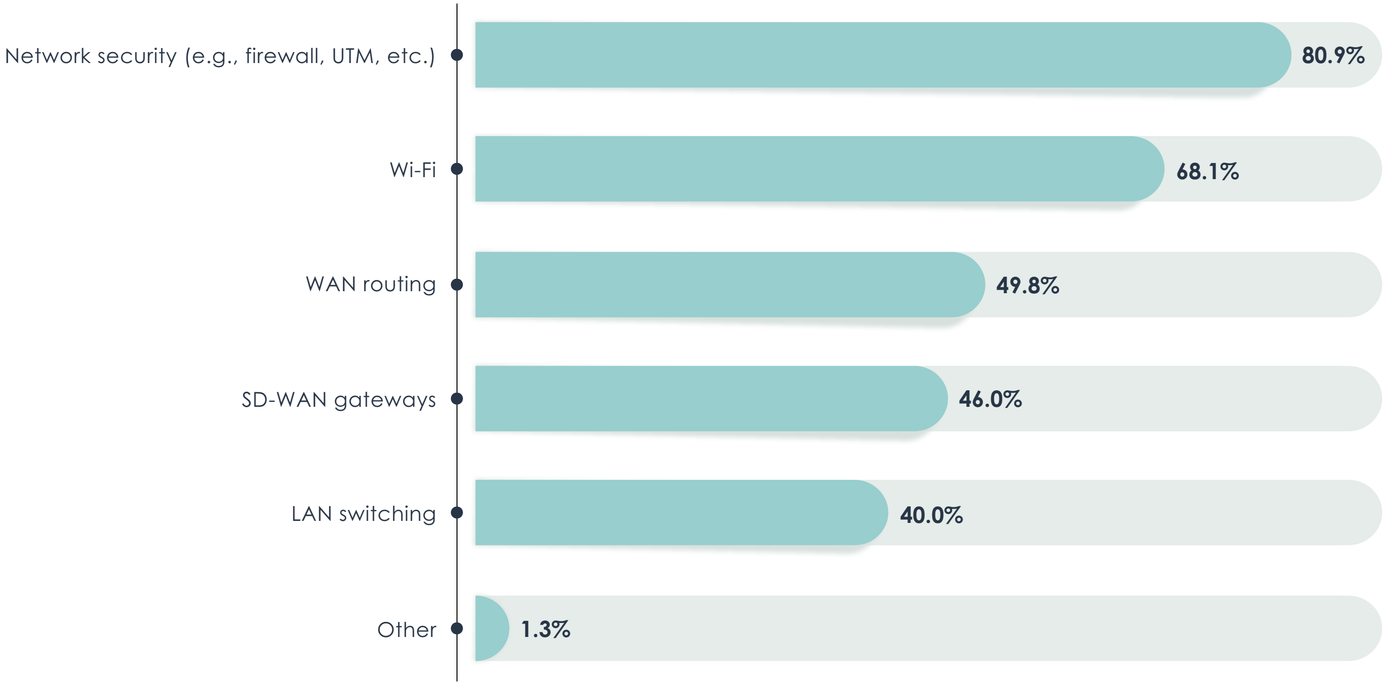

Figure 5. Network capabilities that IT organizations will deploy on enterprise hardware installed in the home offices of remote employees

SD-WAN and SASE for Work-From-Home Networks

78% of IT organizations are planning to deploy SD-WAN capabilities in at least some home offices.

Figure 6 reveals that 78% of IT organizations are planning to deploy SD-WAN capabilities in at least some home offices. North Americans are more likely (83.6%) to deploy SD-WAN to home offices than Europeans (70.2%). Finance, healthcare, manufacturing, and retail companies all have stronger interest in this use case for SD-WAN.

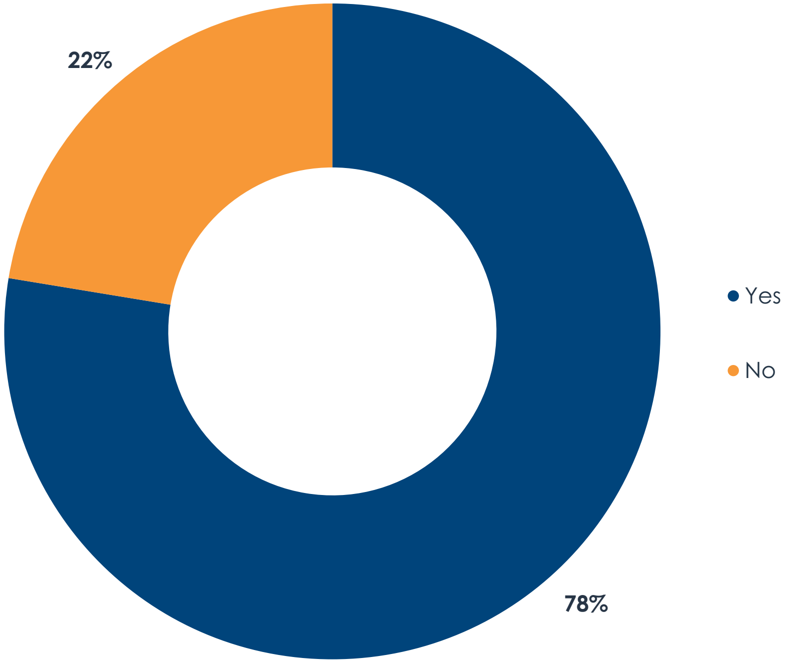

Figure 6. Has your company installed or does it plan to install SD-WAN capabilities to any home offices?

Figure 7 reveals that 16% of IT organizations prefer to install software agents on client devices to bring SD-WAN functionality to home offices. Only 22% prefer a dedicated SD-WAN appliance. The majority wish to install SD-WAN on a multifunction network hardware device in the home, which is something that might also support the Wi-Fi and network security functions that so many companies are implementing in home offices.

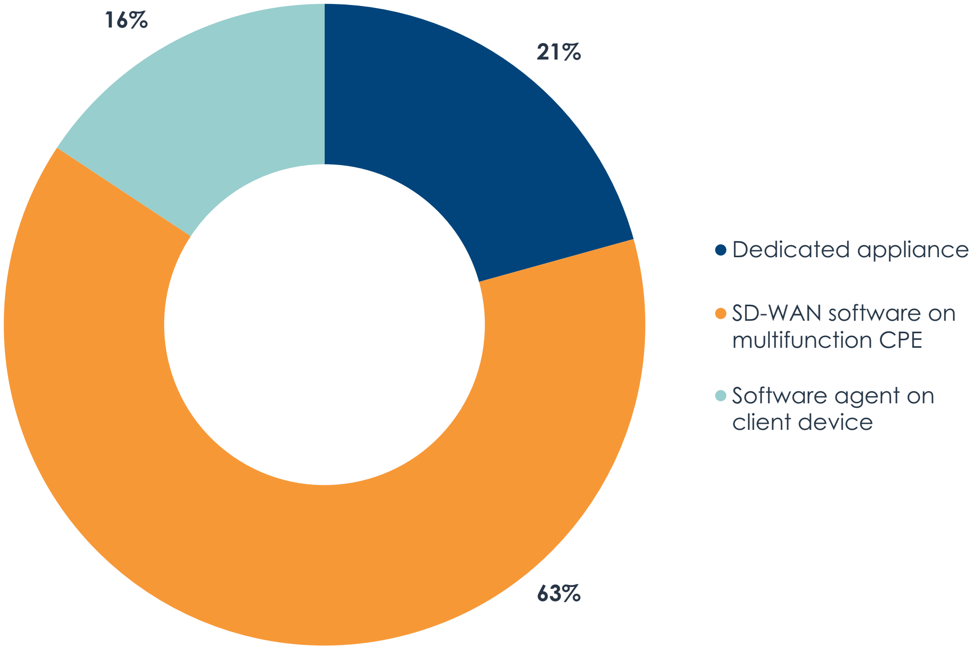

Figure 7. Preferred deployment model for SD-WAN capabilities installed in home offices

IT organizations believe SD-WAN offers four key capabilities in home offices, as **Figure 8** reveals. Integrated security is the most valuable functionality. Information security (53.8%) and IT governance/project management (55.6%) were the most likely to prioritize it. Network/IT operations professionals were the least likely (29.9%) to value it.

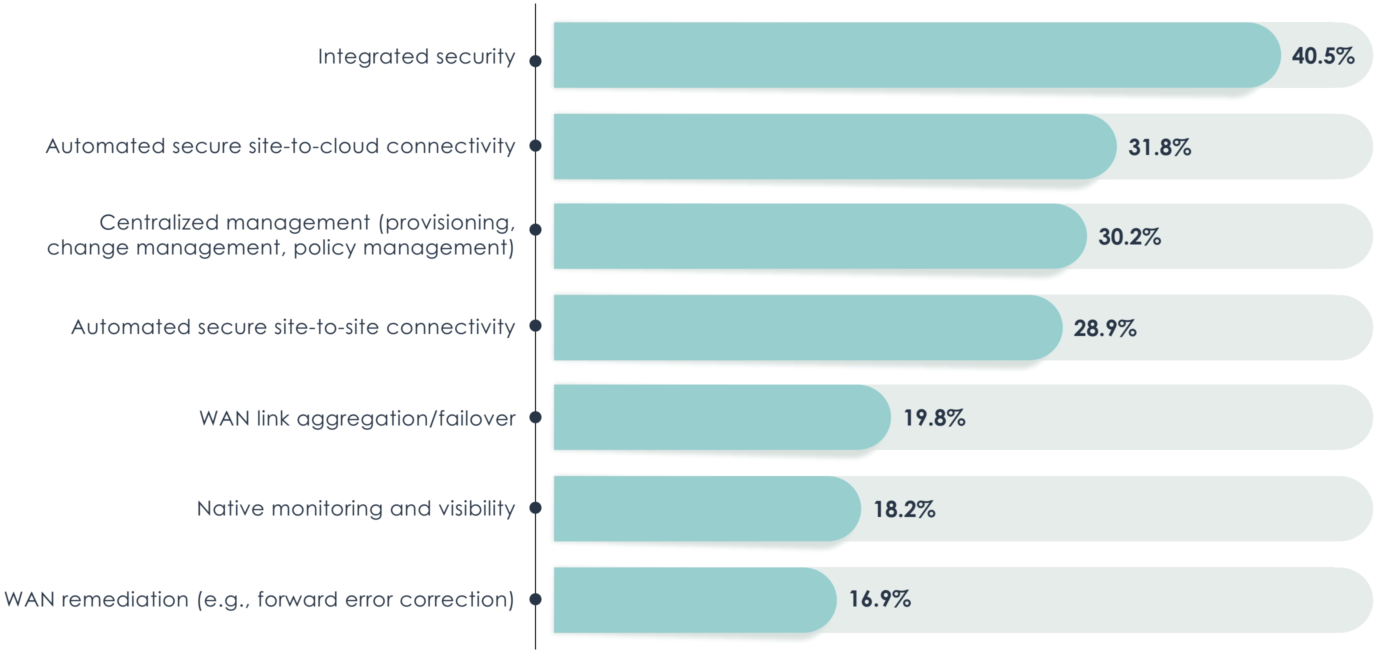

Figure 8. SD-WAN capabilities that offer the most value in home offices

Sample Size = 246

Automated, secure, site-to-cloud connectivity and central management, and automated, secure site-to-site connectivity are the other priorities. WAN link aggregation isn't a big opportunity, given that homes rarely have multiple connections. Native monitoring functionality is also not a significant opportunity, but members of network and IT operations teams were more likely (31.3%) to select it. The data shows that best-in-class enterprises are less likely (11%) to believe that the native monitoring and visibility capabilities of SD-WAN are valuable in home offices. This suggests that IT organizations are better off using third-party tools to get insight into the end-user experience.

Secure access service edge (SASE) is a new class of technology that unifies SD-WAN, secure remote access, and cloud-based security services into a single solution or, in the case of a small but growing number of vendors, a unified platform. Given the novelty of the technology, EMA verifies that survey respondents are familiar with it before asking any questions about the technology. In this research, 83.3% of respondents knew about SASE. Awareness was higher in North America (88.9%) than in Europe (76.6%).

The three solutions that form the core of a SASE platform are ideally suited to enabling secure connectivity to home offices. EMA asked research respondents if the disruptions brought on by the pandemic had prompted more engagement with SASE solutions. **Figure 9** reveals that 81% of IT organizations either engaged with or accelerated engagement with SASE due to the pandemic.

97% plan to use SASE to support network access for employees who are working from home.

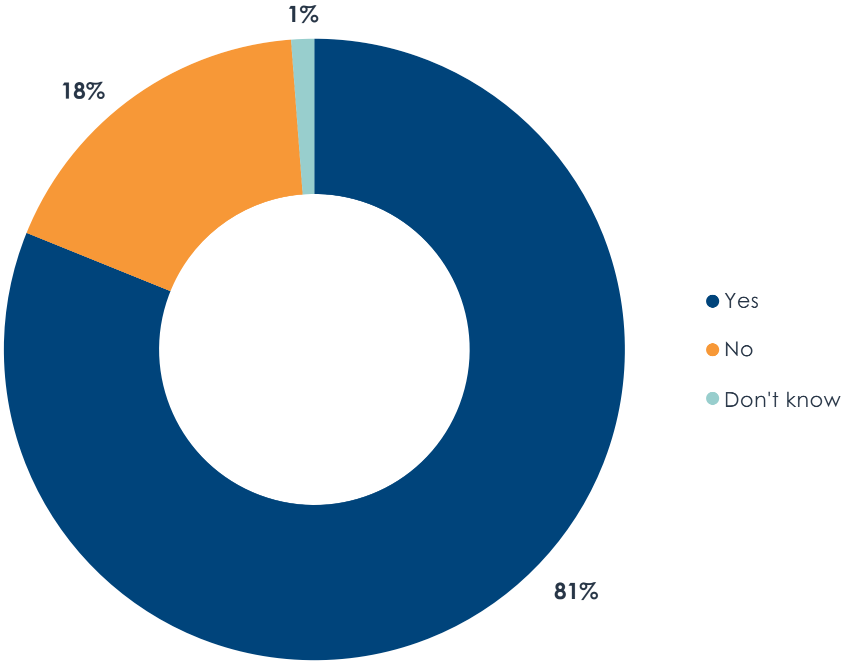

Figure 9. Did the pandemic trigger or accelerate your IT organization's engagement with SASE technology?

Retooling NetOps

Success and Failure with WFH Operations

Only 31% of IT organizations are completely successful with supporting the networking requirements of users who work from home. Fifty-seven percent are only somewhat successful, meaning they see room for improvement.

Figure 10 reveals the challenges that network teams struggle against as they try to support their WFH users. No one issue is emerging as a leading pitfall to avoid. Instead, network teams are encountering a wide variety of issues, with budget and infrastructure complexity edging out others as the top worries.

Infrastructure complexity is more common in large enterprises (32.5%) and least common in small enterprises (14%).

IT leadership problems are also common, but research respondents who are the most successful with supporting WFH users were the least likely to cite this issue (17.9%). On the other hand, respondents who were unable to assess whether they've been successful or not were the most likely to complain about poor IT leadership (38.5%). Perhaps these people don't understand what success means because their executives have failed to set goals and expectations.

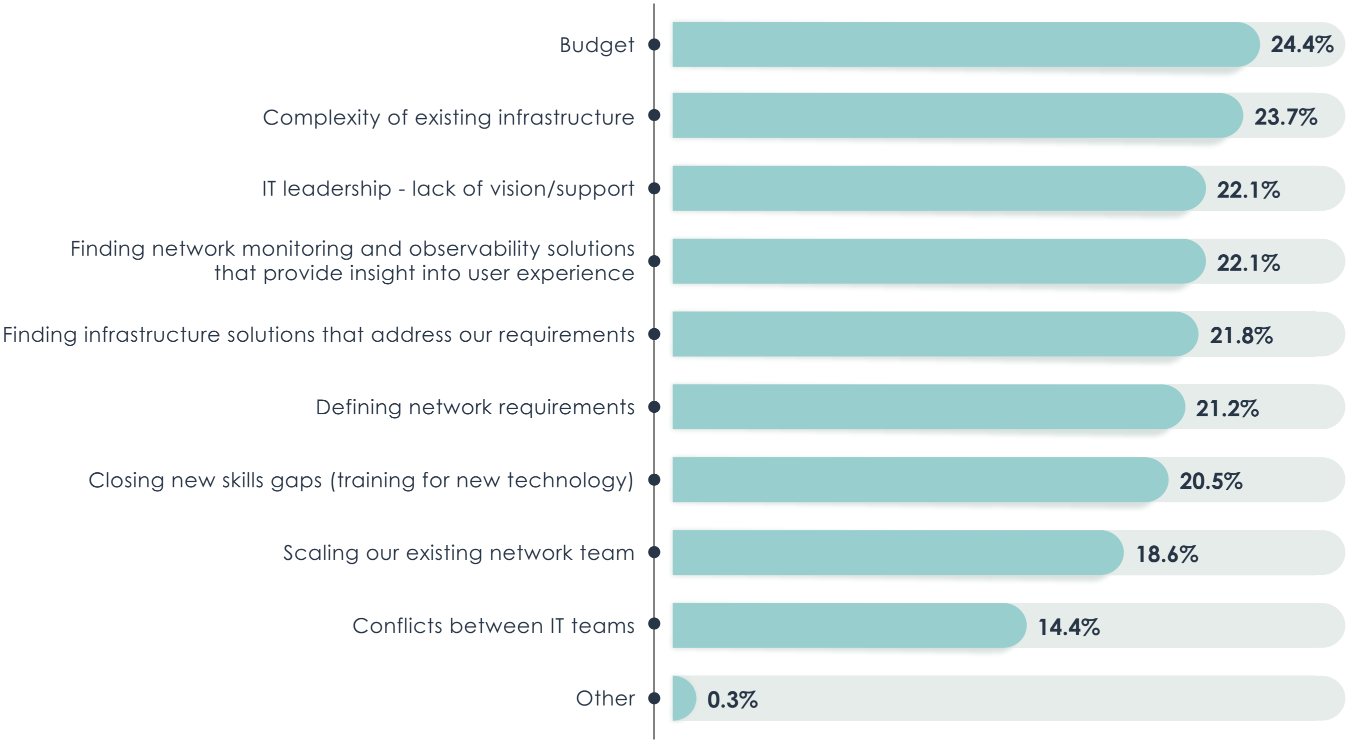

Figure 10. Most significant challenges to supporting the network requirements of users who work from home

Sources of Work-From-Home Trouble

In interviews with EMA analysts, network infrastructure and operations professionals say they start any WFH troubleshooting process by trying to isolate the problem to the user's ISP or local Wi-Fi. However, they are often starting in the wrong place.

Network infrastructure and operations professionals say they start any WFH troubleshooting process by trying to isolate the problem to the user's ISP or local Wi-Fi. They are often starting in the wrong place.

"When people say they have a problem at home, the first thing we need to know is, is it the ISP or is it the home office? We need to know if there are too many devices on Wi-Fi or whether it's the internet provider," said a network engineer with a large insurance company.

"Determining whether it is the ISP or local Wi-Fi is one of the tougher questions to answer. We might have an ISP that goes down or has peering issues with my ISP, and that's hard to troubleshoot because ISPs are not talking to each other," said an IT project manager with a nonprofit biotechnology company.

Figure 11 suggests that home offices' Wi-Fi networks are indeed the top source of home-office user experience complaints—but VPN concentrators, WAN edge devices, and application performance in a data center or cloud are all nearly as likely to be the cause. One-quarter of research respondents also said that core network services like DHCP, DNS, and IP address space are a common source of trouble, too.

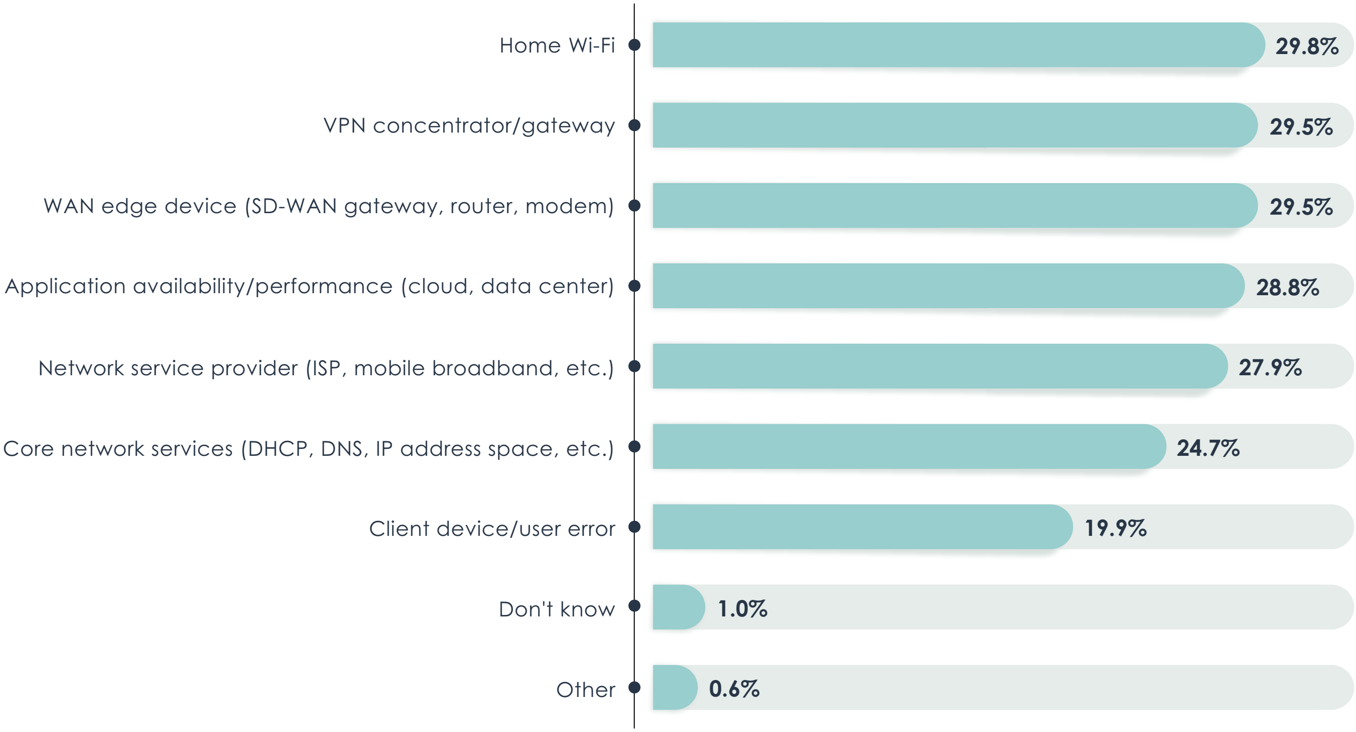

Figure 11. Most frequent sources of issues that generate complaints and help desk tickets from users working from home

Adjusting Network Operations Toolsets

Network infrastructure and operations teams must take a strategic approach to optimizing their toolsets for WFH operations. This may require time and money to accomplish. Not every IT organization is ready to recognize this.

> *"I don't think we have enough visibility to support working from home," said a network engineer with a large regional bank.*

"I don't think we have enough visibility to support working from home," said a network engineer with a large regional bank. "A lot of it comes down to fighting fires as they come up and not being able to get ahead. We need to fix monitoring for all remote users, but instead we're focused on fixing monitoring for just one person at a time."

Ninety-six percent of IT organizations are allocating budget to improve the ability of their network operations toolsets to support the user experience of their WFH users, as **Figure 12** reveals. Seventy-three percent will have that budget ready this year. Best-in-class enterprises are even more likely (83.5%) to allocate budget this year.

"If you don't pay for [WFH] monitoring, you'll hurt yourself," said a network engineer with a large regional bank. "I don't think a lot of companies understand that visibility is important until it's a problem. 'Did we get an alarm for this problem? No? Then we need a new tool.'"

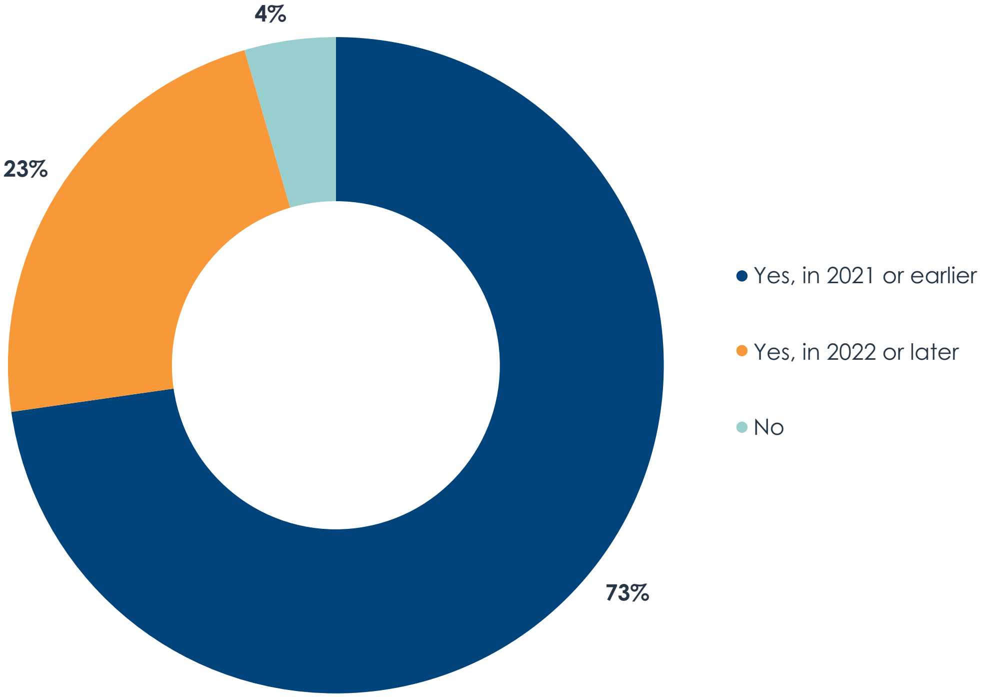

Figure 12. Has your IT organization allocated budget to improve the ability of its network monitoring and troubleshooting tools to support the user experience of users who work from home?

Figure 13 reveals how IT organizations are modifying their incumbent network monitoring and troubleshooting tools to improve how they support remote users who work from home. New security-related insights and new dashboards and reporting capabilities focused on home offices and remote users are both priorities for a majority of IT organizations. Also, nearly half are increasing the scalability of their tools in response to WFH requirements. IT executives are especially convinced that they need to add security-related insights (66.7%), improve scalability (61.7%), and add new WFH dashboards and reports (58.3%).

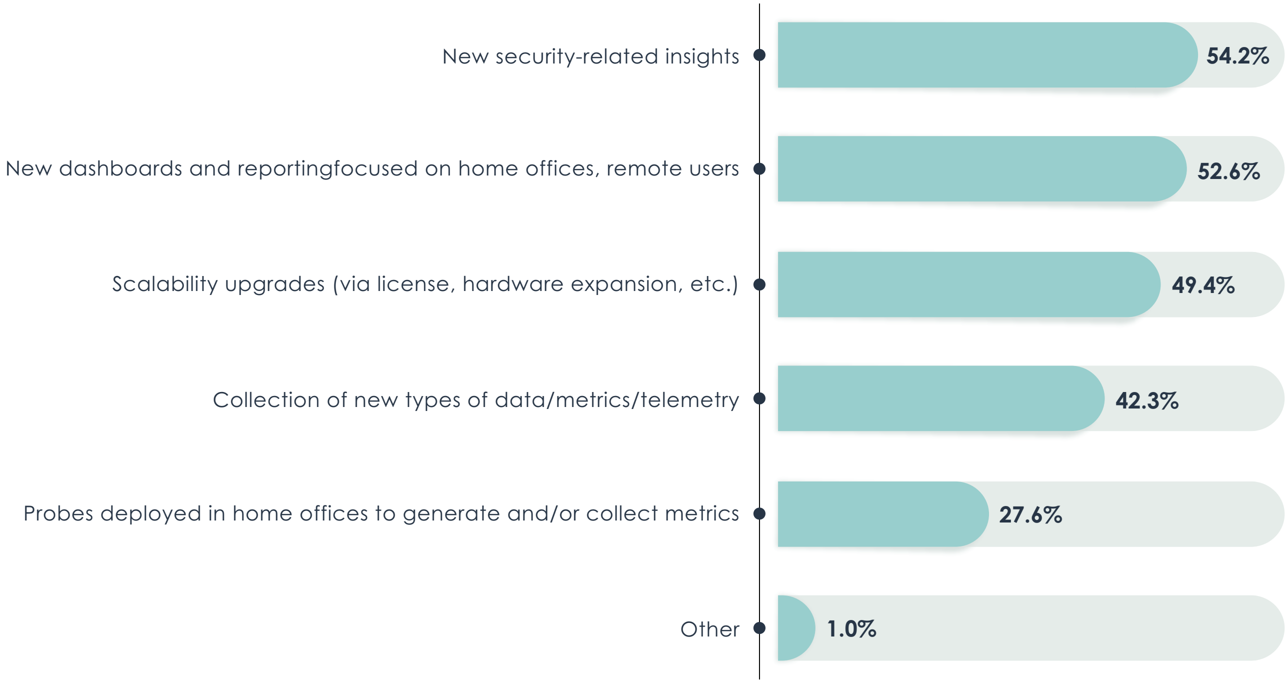

Figure 13. Modifications and enhancements to network operations tools for WFH management

Figure 14 reveals what kinds of tools and telemetry network operations teams are using to monitor and troubleshoot the user experience of WFH users. Remote desktop access is the most popular. Many support technicians use these tools to log onto an end user's computer to troubleshoot directly. It's useful, but it's not efficient or scalable, especially when there are hundreds or thousands of users who need help. Respondents from IT governance and project management teams were more likely (52.8%) to value remote desktop access. People in IT architecture (30.2%) and network operations groups (30.7%) were less likely to value such tools. They're also less popular with large enterprises, which naturally have more users.

Endpoint monitoring tools and network infrastructure monitoring tools are also quite popular for managing WFH experience. Endpoint monitoring tools may pose an end-user privacy conflict for some companies. This type of tool is most popular among IT organizations in which user privacy concerns have no influence on WFH operations strategies (58.3%).

Network flow monitoring tools are also useful for many companies. Flow monitoring and infrastructure monitoring tools both typically require onsite network hardware deployments as a source of local telemetry. If that hardware isn't installed, some companies may take an alternative approach to collecting telemetry for these tools.

"We can install a module on our VPN clients that allows us to get NetFlow from the end user's PC. We haven't done it yet. It's a time and resources issue to set it up, test it, and add it to a general image distribution for our PCs. It's not a priority, but we should do it," said a network engineer with a large regional bank.

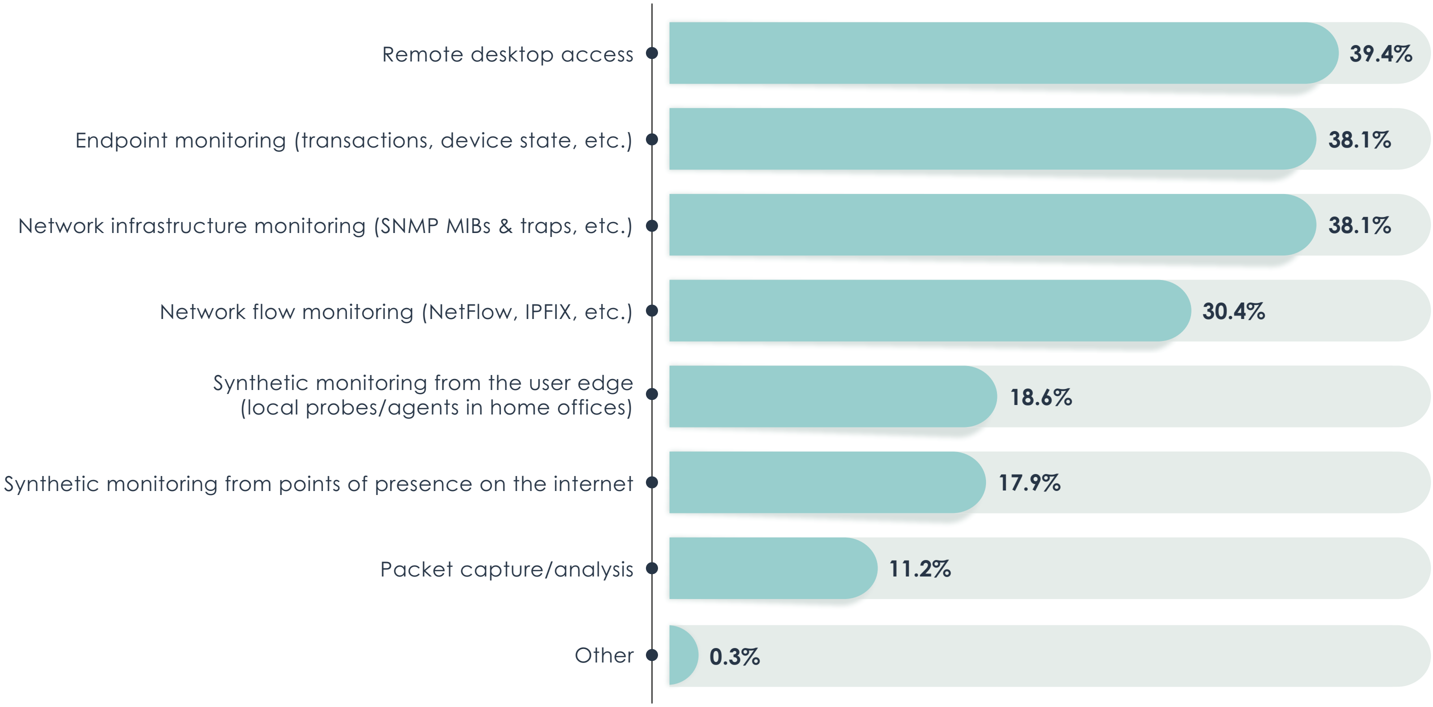

Figure 14. Types of tools that are most valuable for monitoring and troubleshooting the user experience of users in home offices

Figure 15 identifies network monitoring tool features and integrations that IT organizations need to support WFH operations. The clear priority is integration with SD-WAN and SASE solutions, which will allow monitoring tools to pull telemetry from these infrastructure solutions. SD-WAN and SASE solutions have native monitoring capabilities, but past EMA research has determined that the majority of IT organizations supplement this native visibility with third-party monitoring tools. Integration is required because SD-WAN and SASE solutions are inconsistent in their ability to export data via standard protocols like SNMP and IPFIX.

One-third of IT organizations prioritize integrations with help desk and service management systems, which will offer network operations opportunities to correlate tickets with network information, such as which ISPs are generating the most end-user complaints.

Other priorities include improved correlations of insights across data silos, reporting on home office LAN availability and performance, reporting on ISP performance, enhanced bandwidth utilization reports, and enhanced alert and alarm management features.

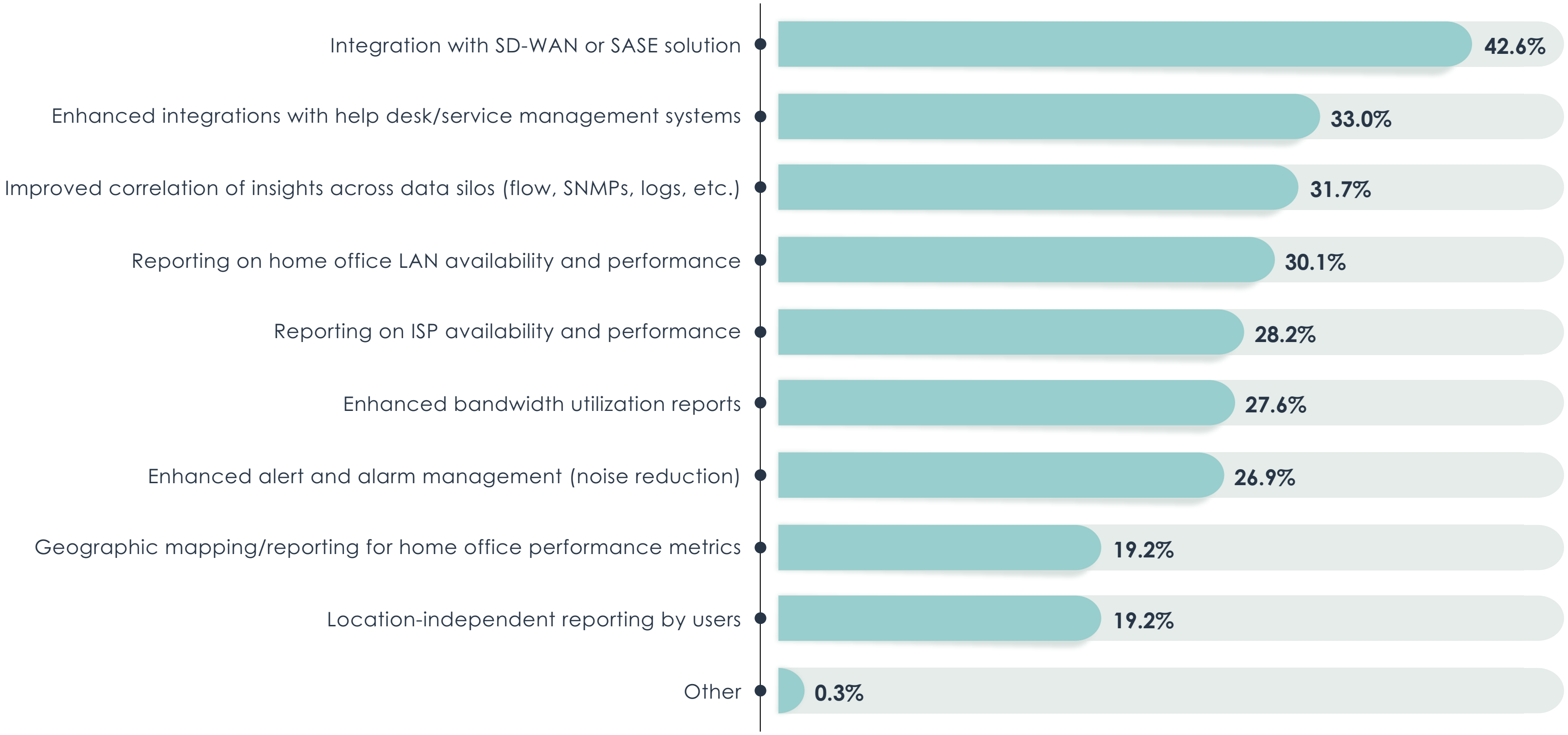

Figure 15. Network monitoring tool features and enhancements that would be most valuable for managing the user experience of people working from home

Pandemic Impacts on On-Premises Infrastructure

Accelerated Cloud Migration

Figure 16 reveals that 70% of enterprises have increased their use of cloud services during the pandemic, confirming multiple reports that the global emergency accelerated cloud adoption. Nearly 40% described this growth in cloud adoption as only slight. North Americans were more likely (77.7%) to report more cloud adoption than Europeans (61%).

Cloud applications appear to be essential to supporting the work-from-anywhere future. Research respondents who have been the most successful with supporting WFH networking requirements are the most likely (47.4%) to report a significant increase in cloud services use.

70% of enterprises have increased their use of cloud services during the pandemic.

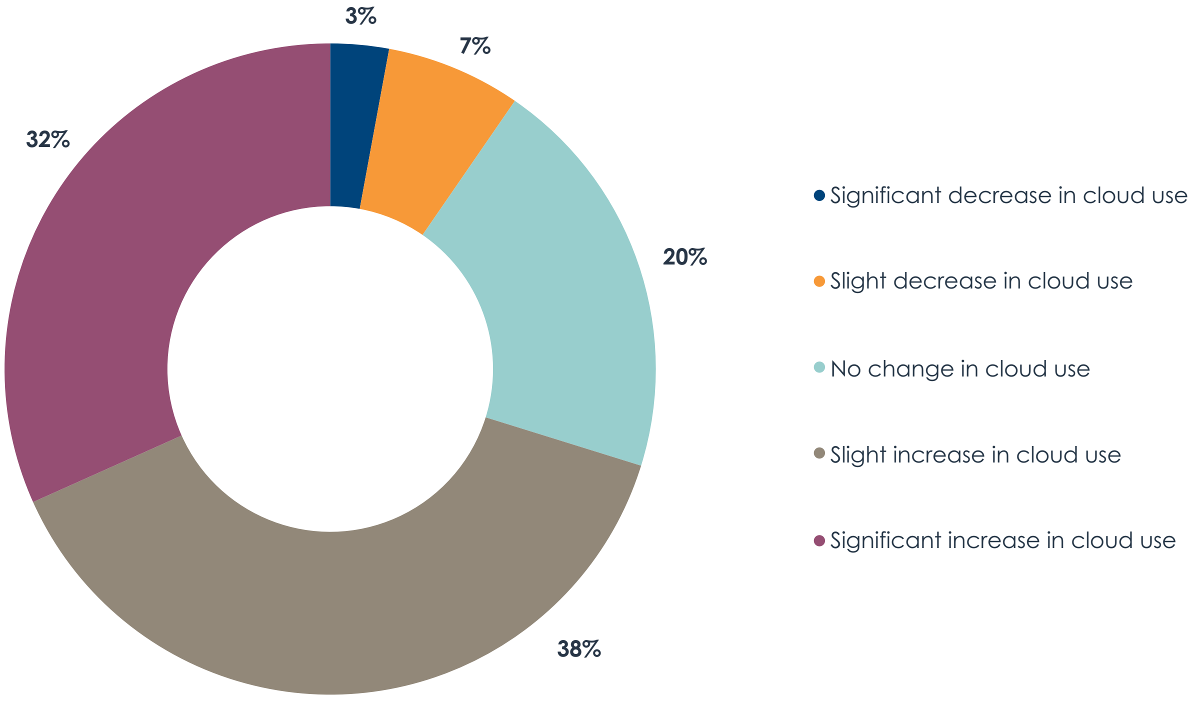

Figure 16. The pandemic's impact on the amount of cloud services used by enterprises, including IaaS and SaaS

Local Area Network Investment

Although most enterprises are experiencing a surge in employees who are working from home, on-premises local-area network (LAN) infrastructure investments are on waning. This research found that 60.9% of IT organizations said the pandemic has triggered an increase in LAN infrastructure investments over the next two years.

Figure 17 reveals that new security and compliance requirements are the primary reason why a majority of IT organizations are increasing their LAN infrastructure investments post-pandemic. Information security professionals were especially likely (76.9%) to cite this driver, but IT architects were less likely (44.8%). Post-pandemic business conditions are dictating this implementation of a more secure network.

Many enterprises are also dealing with increased bandwidth demand and mobility requirements in their LANs.

"Lots of our doctors' offices and satellite offices were having bandwidth issues because telemedicine was pumping so much video onto the network. Our [Wi-Fi] site surveys weren't set up for that," said a network engineer with a small healthcare enterprise. "Doctors were also bringing in their own devices to do telemedicine, so our BYOD program really exploded. How can we safely, from a compliance perspective, support and bring on all these devices? We have some pending upgrades for our wireless LAN controllers and for network segmentation and high-availability. Access point density needs to be increased, too."

"I think we're going to have smaller cubicles in smaller offices, so we'll need more switching capacity and port density," said a network engineer with a large insurance company.

Many companies are also dealing with new connectivity requirements for IoT solutions. This is especially common among manufacturers (62.9%) and IT services and consulting firms (54.2%). The IT executive suite is also more likely to perceive IoT as a driver (53.6%).

Location-based services is a relatively uncommon driver of LAN investment, but it is another high priority for the IT executive suite (53.6%). Network operations (20.7%) and information security (19.2%), on the other hand, are unaware of this emerging requirement.

"Our doctors' offices and satellite offices were having bandwidth issues because telemedicine was pumping so much video onto the network," said a network engineer with a healthcare enterprise.

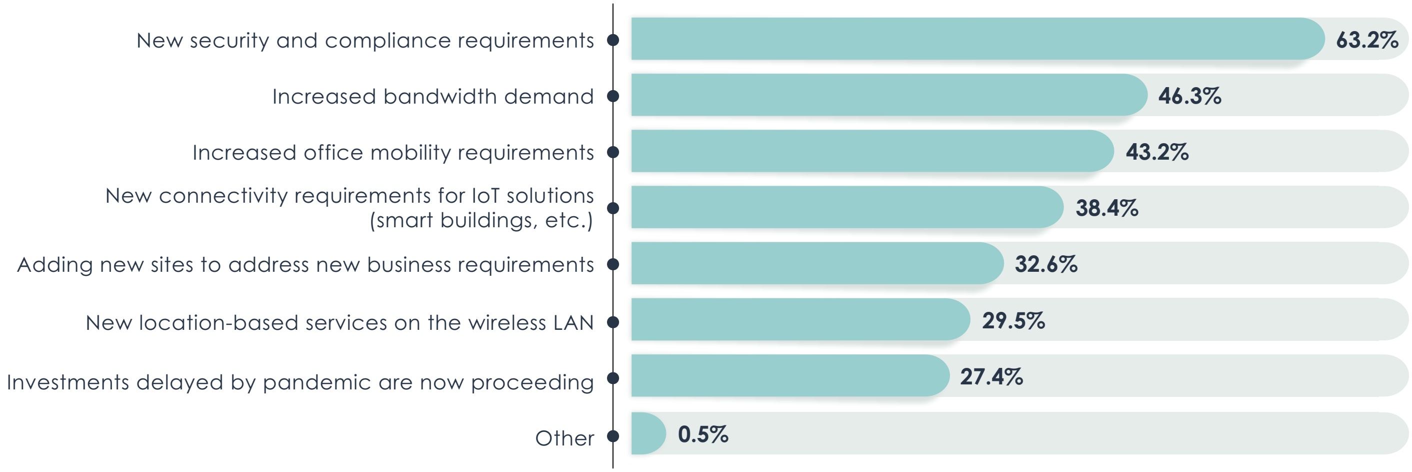

Figure 17. Reasons for increased investment in LAN infrastructure

SD-WAN Investment

This research has established that many IT organizations are using SD-WAN to support the network requirements of their remote employs in home offices. What about the traditional SD-WAN installation in corporate sites? With work-from-anywhere becoming more universal, one might assume IT organizations are reducing their investment in WAN solutions in branch offices and other sites.

This research found that the opposite has happened. Fifty-nine percent of companies are increasing their SD-WAN investments for on-premises installations over the next two years. Another 33% report no change in investment plans at all.

Figure 18 reveals the ways a majority of IT organizations are expanding their investments in SD-WAN. First, the pandemic has set new security requirements that dictate SD-WAN investment. Next, it the expansion in cloud adoption that occurred during the pandemic has driven new cloud access requirements at corporate sites. Members of the IT executive suite (65.5%), the IT governance group (65.2%), and the information security team (63.0%) are all more likely to cite new cloud access requirements.

Many enterprises are also significantly impacted by increased network complexity and bandwidth demand. IT executives are more likely to recognize both of these drivers.

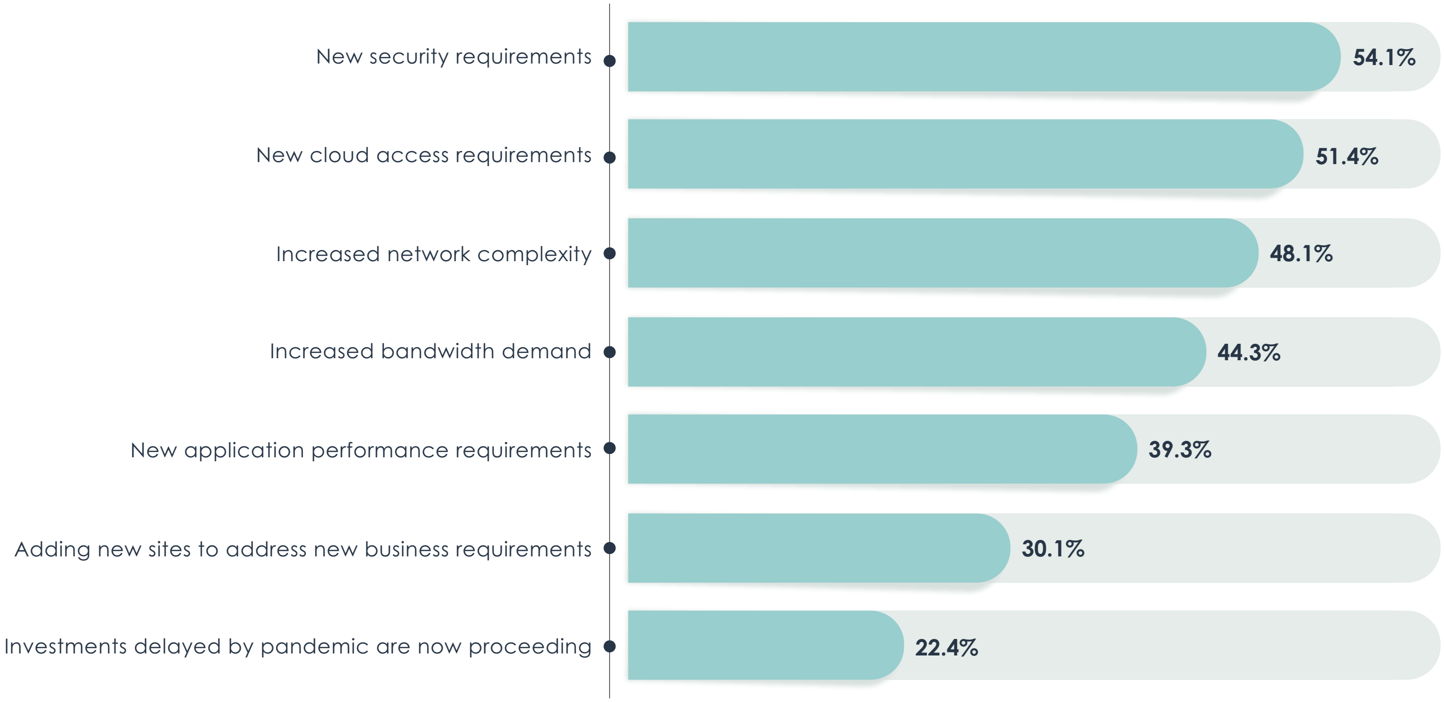

Figure 18. Drivers of increased investments in SD-WAN

Changing How the Network Infrastructure and Operations Team Works

Breaking Down Siloes with Information Security and the Help Desk

Next, 65.7% of network teams are increasing their overall collaboration with security teams, as **Figure 19** reveals. Stretching the edge of the network to the homes of employees has increased risk and created a bigger demand for collaboration between these groups. Additionally, many of the solutions enterprises are adopting, such as SD-WAN and SASE, converge network and security infrastructure, which requires collaboration during design, implementation, and operations. This increased collaboration is more common in North America (74.8%) than Europe (54.6%).

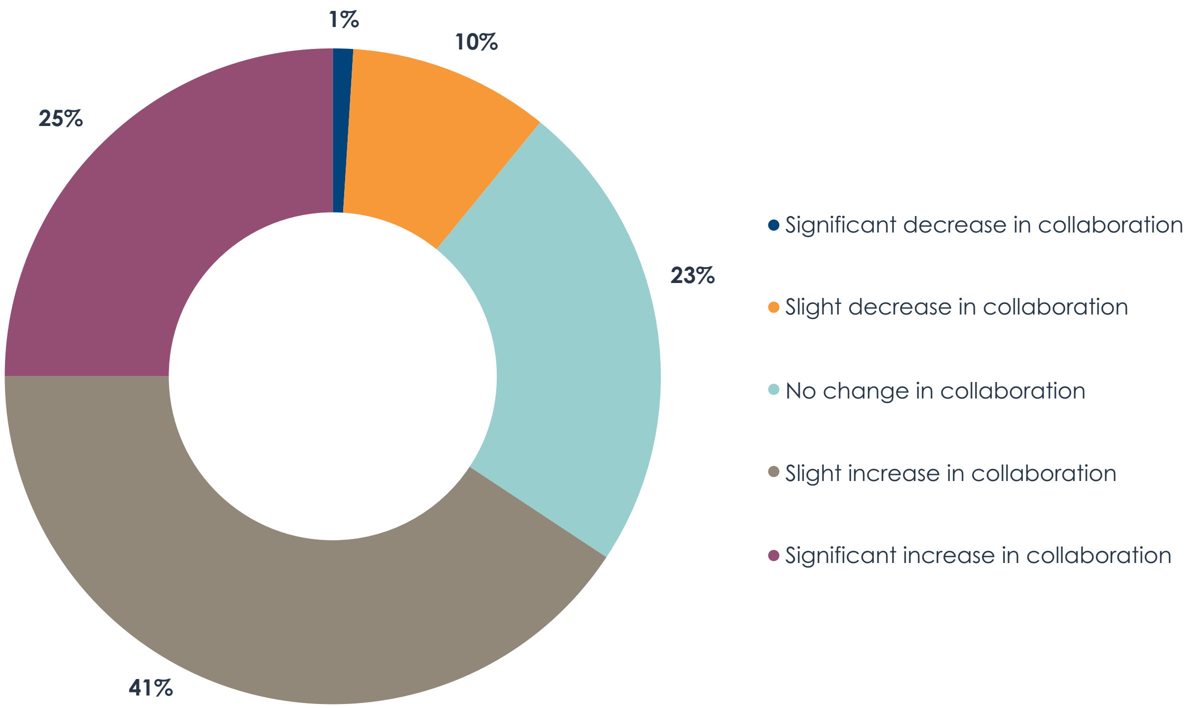

Figure 19. How the requirements of post-pandemic networks are affecting the level of collaboration between the network team and the security team

Figure 20 reveals where that collaboration is happening. Infrastructure design and implementation are the first priorities for these groups when they work together to address post-pandemic requirements. Members of IT architecture teams were especially likely to identify this as a focus (50.9%). North Americans (47.4%) are also more likely to identify infrastructure design and implementation as a collaboration priority, versus only 34.8% of Europeans.

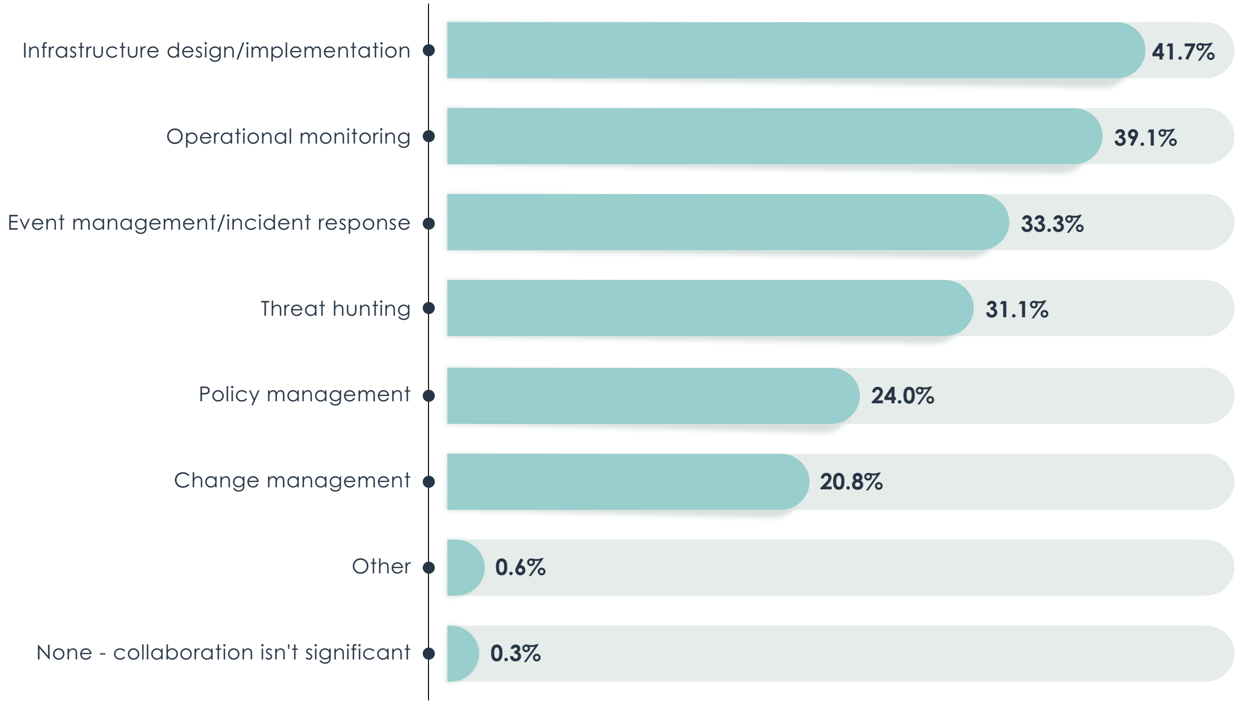

Figure 20. Where network and security teams are focusing most of their collaboration

Committing to Network Automation

IT organizations had to accelerate transformation during the pandemic, setting up new services for the rapid changes that companies had to embrace during the crisis. IT organizations also had to be agile and responsive to change. In the network infrastructure and operations world, this led to a renewed commitment to network automation. **Figure 21** reveals that 91% of IT organizations permanently expanded their use of network automation tools, with nearly 45% describing this expansion as significant.

"[Network automation] has actually been a big topic for two or three years," said a network engineer with a large insurance company. "It's driven by the cloud. They want us to be less hands-on and automate things, spending less time on configurations. I'm not a big fan of automating things in the LAN and the WAN. I don't see the value. But, you have to do what upper management asks you to do."

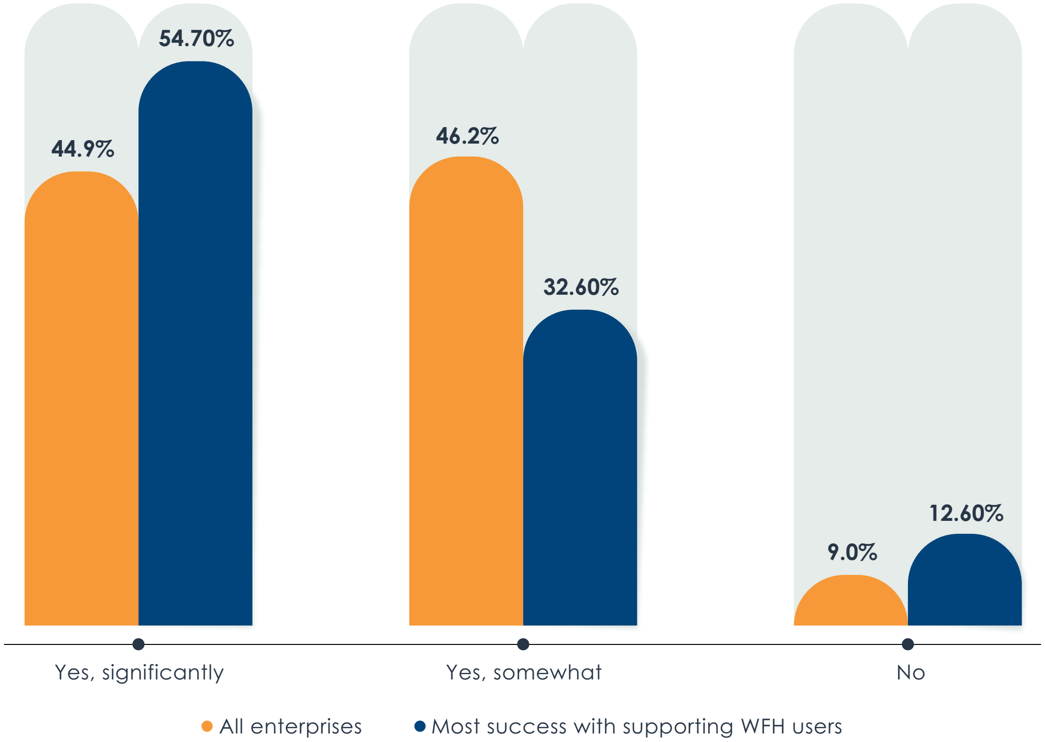

Figure 21. Has the pandemic permanently expanded your IT organization's use of network automation tools?

Figure 22 reveals what aspects of network management IT organizations want to automate the most. The biggest target is monitoring and troubleshooting. This suggests an increased focus on analytics and AIOps capabilities that automate anomaly detection, fault isolation, and root-cause analysis. The IT executive suite is especially focused on automating these tasks (60%).

The secondary priorities for automation are configuration and change management, infrastructure provisioning, and device lifecycle management. Network design and policy design and management are the lowest priorities. EMA observed some different perspectives from silos within the IT organization.

- Infrastructure provision: Prioritized by network engineering and network operations
- Configuration and change management: Prioritized by IT service management, IT governance and project management, IT architecture, and network operations.
- Device lifecycle management: Prioritized by network engineering and IT architecture

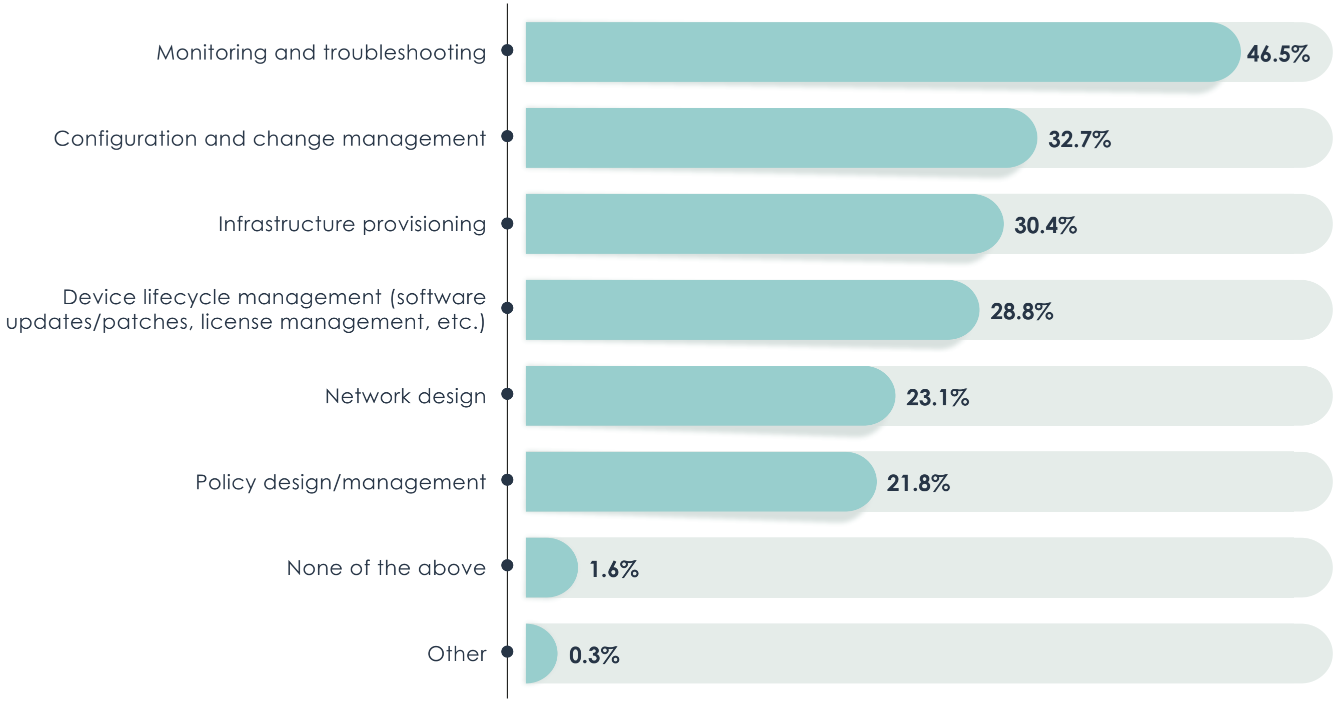

Figure 22. Aspects of network management that IT organizations most need to automate

Figure 23 identifies the features and capabilities that IT organizations most need from network automation tools coming out of the pandemic. The priority is anything that can help network infrastructure and operations teams break out of their silos. They are seeking cross-IT orchestration integrations. For example, they need northbound integration with IT orchestration and DevOps tools. This is especially important to IT governance and project management (50%) network operations (46.6%) and information security teams (51.4%).

Second, IT organizations need multi-domain network automation, such as an automation pipeline that works across the LAN, WAN, cloud, and beyond. The third big priority is operational analytics, which echoes the popularity of monitoring and troubleshooting automation revealed in Figure 37. The IT executive suite is especially interested in this capability (51.1%). North Americans (41.5%) are much more interested in this than Europeans (24.1%).

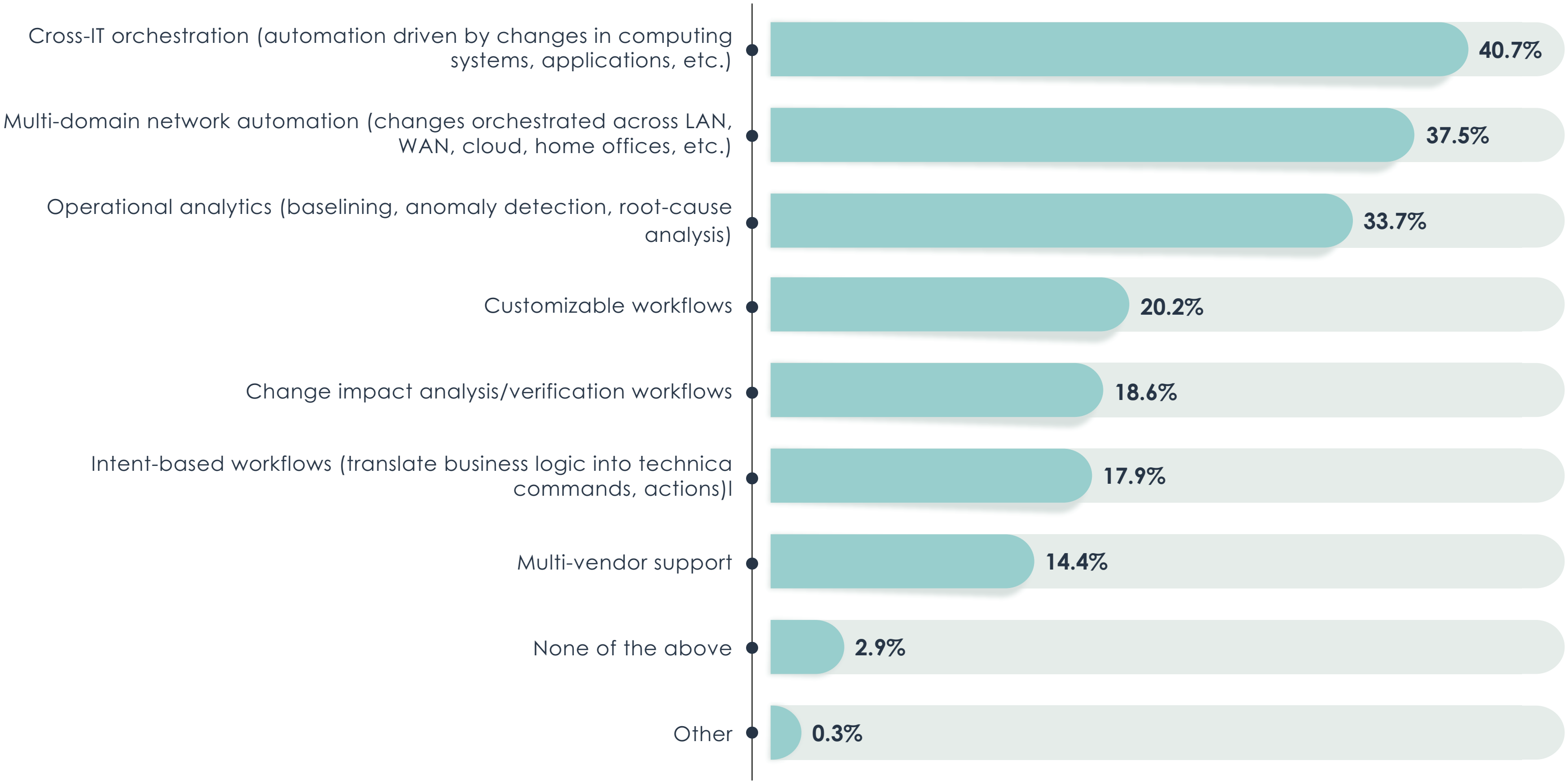

Figure 23. Network automation features and capabilities that IT organizations are prioritizing post-pandemic

The Roadblocks

Finally, EMA asked respondents to reveal the roadblocks that are preventing network teams from adapting the entire network to post-pandemic requirements. **Figure 24** reveals that compliance or security risk is the most prominent issue, followed closely by technical issues with network operations tools and technical issues with network infrastructure or services. These latter two findings suggest that network vendors and service providers need to step up their game to support the changes IT organizations are making to their networks.

The chief secondary challenges are budget issues and skills gaps, which IT executives should make note of, especially since people who work within an IT executive suite were much less likely to identify skills gaps as an issue (15.6%). The network operations team (35.1%) is more likely to perceive this gap.

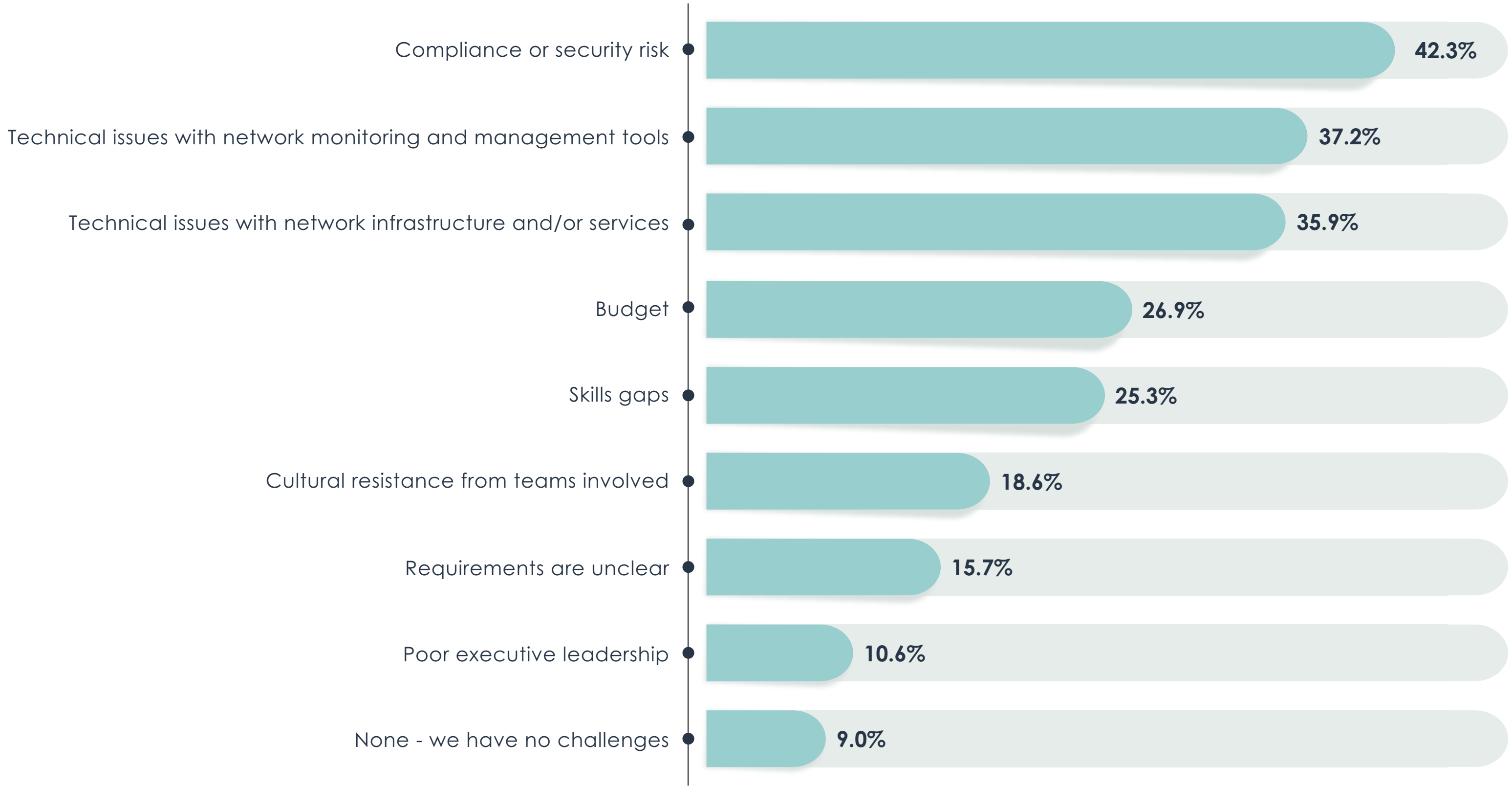

Figure 24. Most significant challenges to a network team's ability to adapt the network to post-pandemic requirements

Conclusion

This research makes it clear that network infrastructure and operations teams are transforming their approach to supporting the business in response to new permanent requirements introduced by the pandemic.

Work-from-anywhere is no longer a luxury. IT organizations must take an architectural approach to delivering a secure, quality experience to end users who work from home. This may require installing a variety of network hardware in homes and it may lead some companies to pay for their employees' internet connections, too.

Not only must network teams revise WFH infrastructure strategies in a post-pandemic world, they must also transform operations. Quite often, the tools they use to manage, monitor, and troubleshoot on-premises networks offer limited or no value in a WFH environment. Network teams must define their new tool requirements carefully and, more importantly, convince management to allocate budget for new tool investments.

This research also found that network teams are not pulling back investments in the on-premises network. Most IT organizations are increasing their investments in LAN and SD-WAN infrastructures post-pandemic. They are also looking at leveraging location-based services on their wireless LAN infrastructure to make their enterprises more resilient during future public health emergencies.

EMA will continue to monitor how the network infrastructure and operations industry is evolving as the world emerges from the COVID-19 pandemic. In the meantime, this report has offered some guidance and some potential best practices for network professionals to follow.

Demographics of Survey Participants

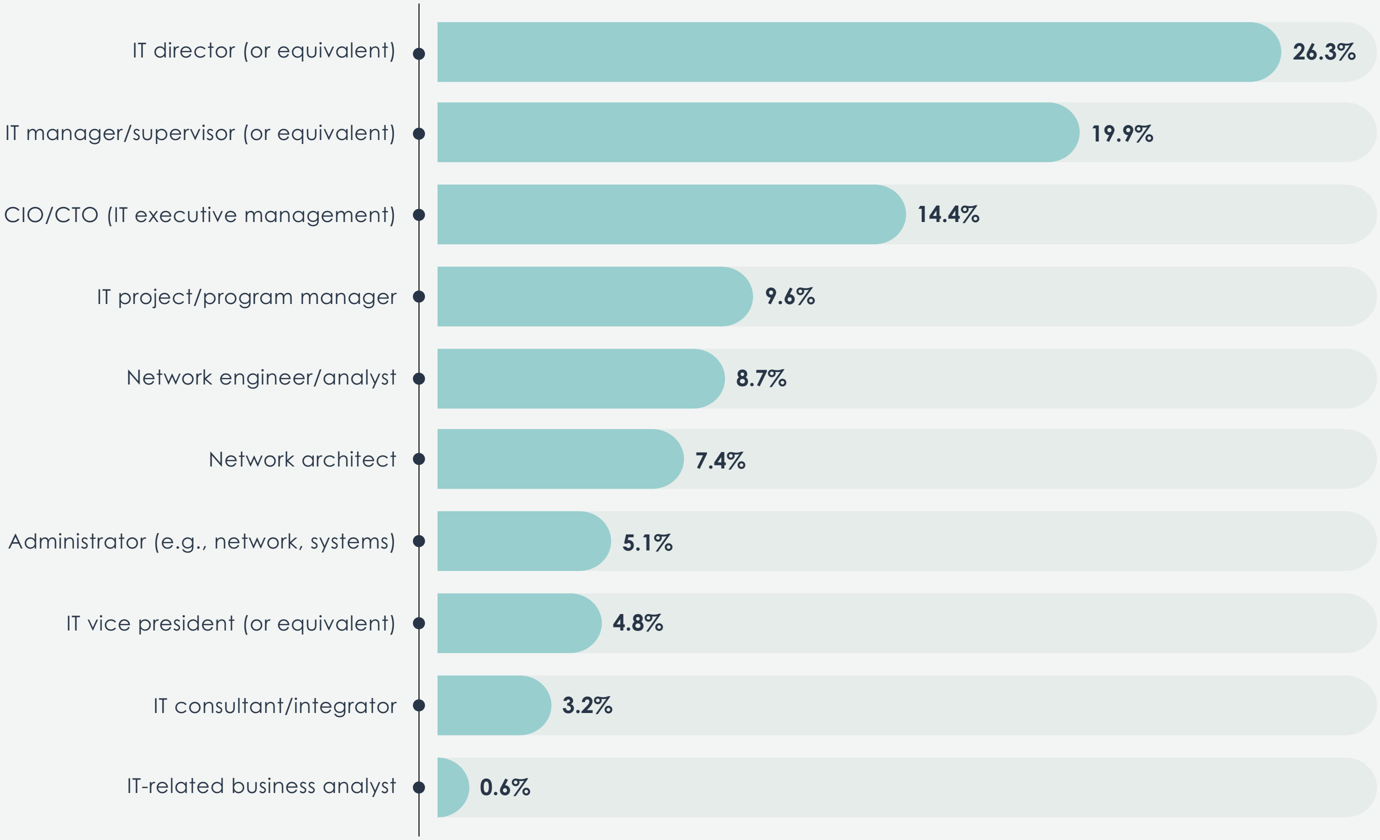

Figure 25. Job titles

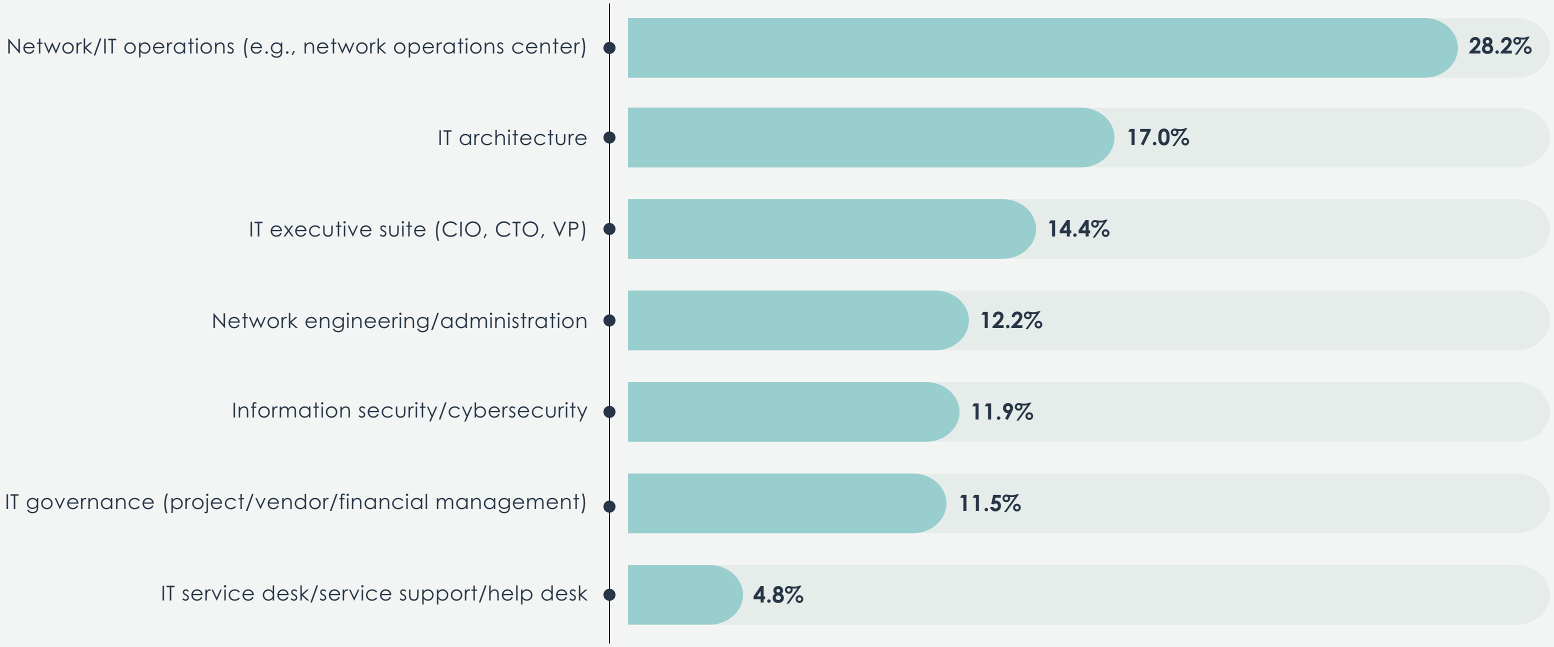

Figure 26. Groups within the IT organization

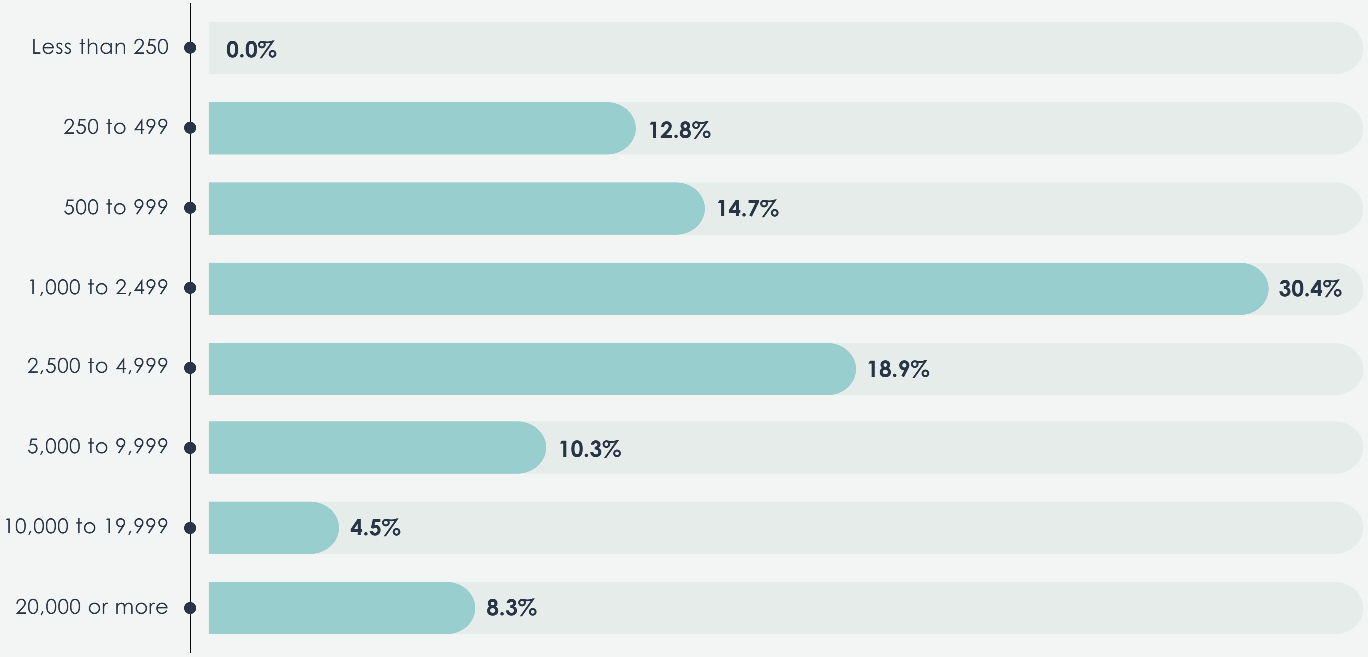

Figure 27. Company size by number of employees

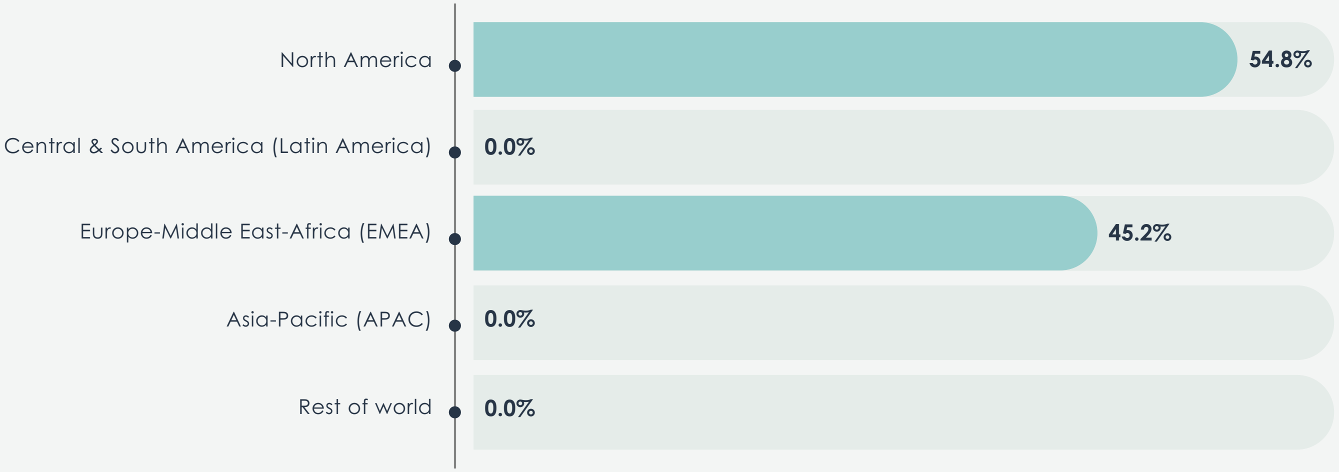

Figure 28. Geographic location of research participants

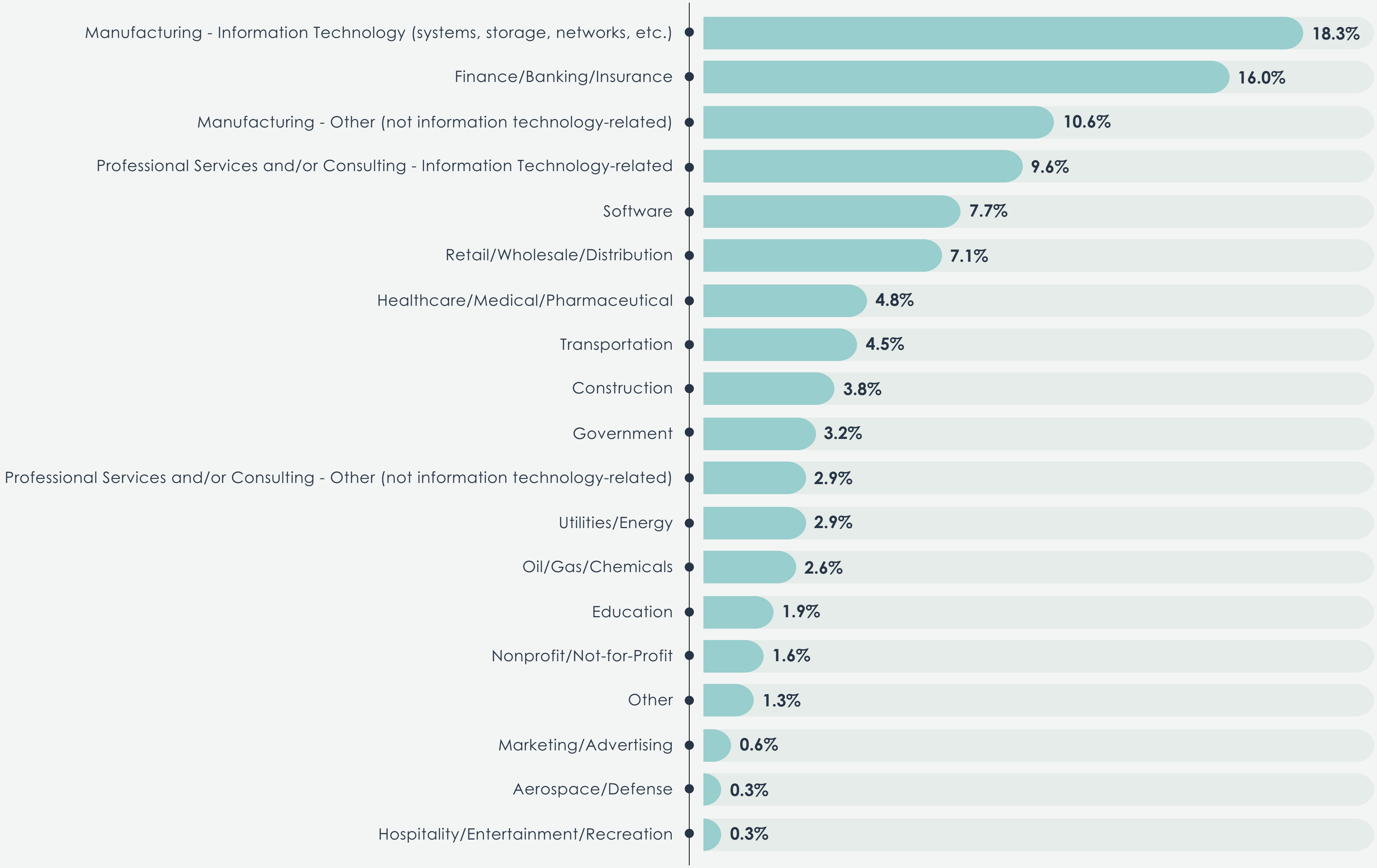

Figure 29. Primary industry of represented companies

Case Study: Offshore Drilling Enterprise

A leading global provider of offshore drilling services needed a reliable WAN for emergency communications, cloud services, suppliers, and crewmembers. The company chose a managed Riverbed SD-WAN service with integrated WAN optimization and application acceleration delivered by RigNet, a managed services provider for the oil and gas industry.

Challenge: Make the Most of WAN Bandwidth on the Seas

For drilling contractors, every aspect of the business requires fast access to up-to-date data. “Communications standards for rigs are extremely high—especially in ultra-deep water and harsh environments,” says Brendan Sullivan, Global CIO and CTO for RigNet. “If data stops flowing or IP phones stop working, the rig has to shut down.” That’s costly: oil and as operators pay upward of $1 million per day to rent a rig.

Unlike businesses operating on land, rigs generally keep the same equipment for 10 years or more. When an operator refreshes above-deck and below-deck networks on rigs and offices, it needs a solution that can adapt to changing business demands.

One RigNet customer, a leading global provider of offshore drilling services, required a reliable WAN for emergency communications and cloud services like SAP and Microsoft Office 365. Suppliers aboard the provider’s rigs needed to connect to their own applications. Crewmembers working 28 days at a time needed access to the network for personal use.

“To meet the needs of our customers, their suppliers, and crews, we aim to double each rig’s bandwidth without doubling costs,” Sullivan says. “We think of it as ‘stuffing more stuff’ on the network with the same performance.”

Solution: Riverbed SD-WAN

RigNet meets these needs with a managed SD-WAN service based on Riverbed® technology. In customer data centers, RigNet deploys Riverbed SteelConnect EX, which combines routing, SD-WAN, WAN optimization, next-gen firewall, and unified threat management all in one device. “Consolidating all the network services in one SteelConnect EX reduces the footprint in our customers’ data centers by 90%,” says Daryn Richard, Head of Engineering for RigNet. A converged device also simplifies management and reduces the opportunity to make mistakes.

For the offshore driller mentioned, RigNet and Riverbed engineers worked together to define policies for the SD-WAN. Policies control which transport to use (satellite, LTE, or microwave) under what conditions, which traffic gets priority, and where traffic can and cannot flow to meet specific country regulations.

On the customer’s rigs, RigNet deployed three SteelConnect CX580s appliances for WAN optimization, SD-WAN, and a warm spare that can take over any other function. When oil drillers acquire new sites, RigNet can simply ship the plug-and-play appliances to rigs, where staff only need to connect them.

Results: Double the Bandwidth for Less Than Double the Cost

Rapid deployment—just four months

Despite the complexity of ocean deployment—including two weeks of COVID-19 quarantine before engineers boarded helicopters—the solution was ready to use in just four months. "Riverbed Professional Services worked side by side with our team so we could learn and document best practices," Sullivan says. "It's been one of the most pleasant experiences I've ever had with a vendor. We gained expertise and confidence to bring a critical solution to the front line."

Consistent performance with policy-based decisions

Managing service quality in a worldwide network is complicated, even more so in harsh ocean conditions with ships in motion. When rigs cross network boundaries or performance starts to decline, the Riverbed SD-WAN automatically switches to the best transport based on performance SLAs and real-time circuit conditions.

Improved quality of life for crews

Offshore drilling companies look for ways to relieve crewmembers' stress and improve quality of life. By optimizing WAN bandwidth, the Riverbed solution helps crewmembers stay connected. They appreciate being able to video chat with friends and family, watch movies, and play games. It's a morale-builder and a competitive advantage for recruitment and retention.

Visibility for simpler IT operations

Crewmember satisfaction is so crucial on rigs, in fact, that some RigNet customers give personnel a direct line to the CEO for complaints. "Riverbed helps us manage service quality because we have visibility into all network activity from a single portal," Richard says. "We can even see detailed stats like the number of people on FaceTime or YouTube at a given time, and service quality for each application."

Business agility

The oil and gas industry is marked by frequent mergers and acquisitions. RigNet's managed service reduces the time to onboard a new location to the network from weeks to hours. Sullivan sums it up: "In terms of challenging network conditions, oil rigs are right up there with the International Space Station. Riverbed SD-WAN helps us make the best use of our customers' bandwidth by combining all the techniques—SD-WAN, WAN optimization, SaaS acceleration, and advanced security—in one device."

EMA™

25 YEARS

About Enterprise Management Associates, Inc.

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

1995 North 57th Court, Suite 120, Boulder, CO 80301 +1 303.543.9500 www.enterprisemanagement.com 4102.071621