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

Prepared for:

BROADCOM®

Modernizing Network Engineering and Operations in the Era of Hybrid and Remote Work

August 2023 EMA Research Report

By **Shamus McGillicuddy**, Vice President of Research
Network Infrastructure and Operations

Table of Contents

Introduction: The Rise of Remote and Hybrid Work

Since the advent of ubiquitous broadband internet service in the developed world, enterprises have offered employees the opportunity to work from home. With an internet connection, any information worker can be reasonably productive from home. However, until recently, the work-from-home option was primarily a perk rather than a strategic imperative. That paradigm shifted in 2020 with the COVID-19 pandemic. Suddenly, remote work was a business continuity strategy at a time when governments were urging everyone to limit their exposure to potential infection by staying home.

Initially, the world assumed that this global shift to remote work was temporary. However, the public health response was ultimately a great experiment that proved millions of people could be more productive and enjoy a better work/life balance when they worked from home. Many companies acknowledge this reality by allowing more of their workers to remain home, possibly because employers are seeing additional benefits, like reduced office real estate costs and the ability to hire from a global labor market rather than a local one.

Reasons for allowing remote and hybrid work

> To be more productive, reduce use of office space, and to hire the best talent anywhere in the world.

CIO, $1 billion civil engineering/construction company

> We want to encourage work/life balance.

Network administrator, $5 billion financial services company

> Employees demand the right to work remotely to better manage their lives, and we want to help them.

IT director, $500 million financial services company

> The first consideration is that we are hiring skilled people wherever they are.

IT project manager, $250 million professional services company

> The pandemic was the initial reason. Since, we have found that employees are more productive.

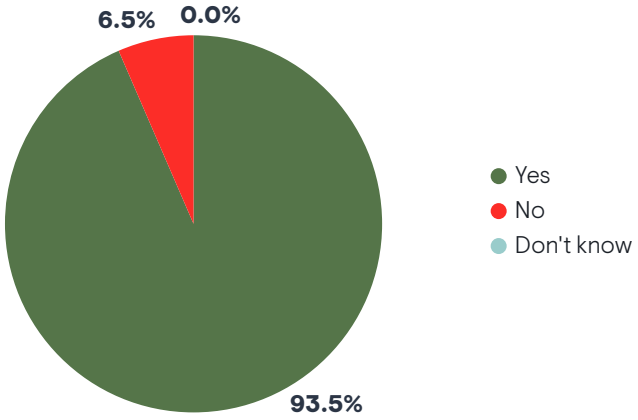
Network architect, $5 billion financial services company

> It keeps the workforce in the field and allows greater mobility versus being isolated at the office.

IT consultant, $5 billion professional services company

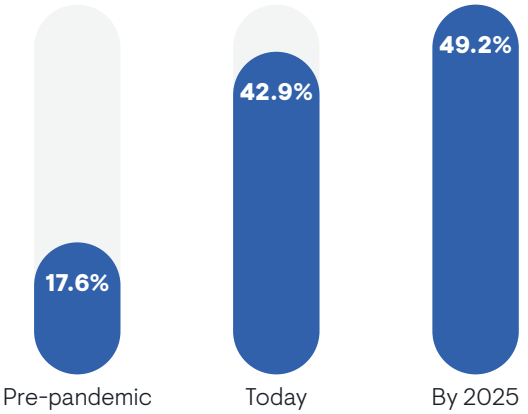
Figure 1 reveals that nearly 94% of enterprises have experienced a permanent increase in the percentage of their employees who work from home on at least a part-time basis since the start of the pandemic. **Figure 2** shows the extent of this paradigm shift and how permanent it is. The typical organization counted just 18% of its workforce as part-time or full-time remote employees prior to the pandemic. Today, that number is nearly 43%, and by 2025, it will climb beyond 49%.

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?



Sample Size = 354

FIGURE 2. PERCENTAGE OF EMPLOYEES WHO WORK(ED) FROM HOME AT LEAST PART-TIME IN THE PAST, PRESENT, AND FUTURE



While remote work is a permanent fixture in today's businesses, many are increasingly asking employees to come into an office a couple of days per week to encourage collaboration and cultural cohesion. More than 96% of enterprises now have hybrid workers, defined as employees who split their time working both at home and on the corporate premises. The typical enterprise reports that more than 39% of employees who work from home fit the description of a hybrid worker.

"We just started doing an organized approach to hybrid work," said an IT manager at a midsized software company. "If you live near one of the offices, you're expected to come in two days a week. Leadership wanted to see more people collaborating in the office."

IT Organizations Must Adjust Network Infrastructure and Operations for Hybrid Work

IT organizations are increasingly finding that they need to evolve their approach to supporting remote and hybrid workers. In particular, network connectivity for people working from home must be reliable, high-performing, and secure, especially for employees who interact directly with customers or work with highly sensitive data.

Moreover, IT organizations must be flexible enough to support hybrid workers no matter where they are. Many IT organizations will aim to provide hybrid workers with consistent access to corporate applications and data and a consistent user experience regardless of where they are. This continuity of access will ensure employee productivity.

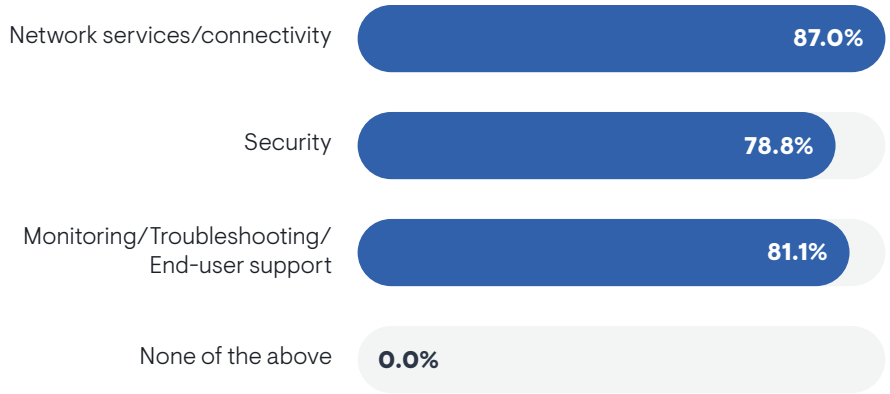
Given this major shift in the nature of work, network infrastructure and operations teams are facing significant pressure to adjust. Enterprise Management Associates (EMA) decided to conduct research into how IT organizations are evolving to support the remote and hybrid work boom.

This research report examines the strategies enterprises are developing to support the networking requirements of remote and hybrid workers, including network connectivity, security, and end-user experience. It explores the infrastructure changes enterprises are making and the tools they are adopting to monitor, troubleshoot, and secure these network services.

Research Methodology

EMA surveyed 354 IT professionals who are directly involved in supporting the networking requirements of employees who work from home. **Figure 3** details how respondents answered a qualifying question on the matter. It reveals that most of the survey respondents are responsible for these users' network connectivity and security and for monitoring and troubleshooting end-user experience. Anyone who selected "none of the above" was disqualified. EMA conducted the survey in May 2023.

FIGURE 3. ARE YOU INVOLVED IN ANY OF THE FOLLOWING ASPECTS OF SUPPORTING EMPLOYEES WHO WORK FROM HOME?



Sample Size = 354, Valid Cases = 354, Total Mentions = 874

Figure 4 reveals the demographics of EMA's research participants. We captured a mix of small, medium, and large enterprises across North America and Europe. Respondents ranged from administrators and engineers to C-level IT executives in a broad range of IT silos, including IT architecture, network engineering, and security. The chart also reveals the top industries in the survey led by manufacturing, professional services, retail, and financial services.

FIGURE 4. DEMOGRAPHICS

Job Titles

16%	Network/IT administrator
7%	Network/IT engineer
5%	Network/IT architect
11%	Project manager
14%	IT manager/supervisor
15%	IT director
14%	IT vice president
15%	CIO/CTO/CISO

IT Groups

18%	IT architecture
16%	Network engineering
15%	Project/Program management
15%	CIO's suite
10%	IT asset/financial management
9%	IT security/cybersecurity
9%	Network operations center
7%	IT service desk/service support/help desk

Industries

16%	Manufacturing
16%	Professional/Technical services - not related to IT
14%	Retail
14%	Banking/Finance/Insurance
8%	Healthcare/Hospitals
7%	Construction/Civil engineering
6%	Logistics/Wholesale/Distribution
5%	Energy/Utilities
4%	Media/Entertainment/Content provider
4%	Government

Region

69%	North America
31%	Europe

Revenue

35%	$100 million to <$500 million
26%	$500 million <$1 billion
24%	$1 billion to <$5 billion
11%	$5 billion+
5%	Unknown/Not applicable

Company Size (Employees)

23%	Small enterprise - 250 to 999
56%	Midsized enterprise - 1,000 to 4,999
21%	Large enterprise - 5,000 or more

Key Findings

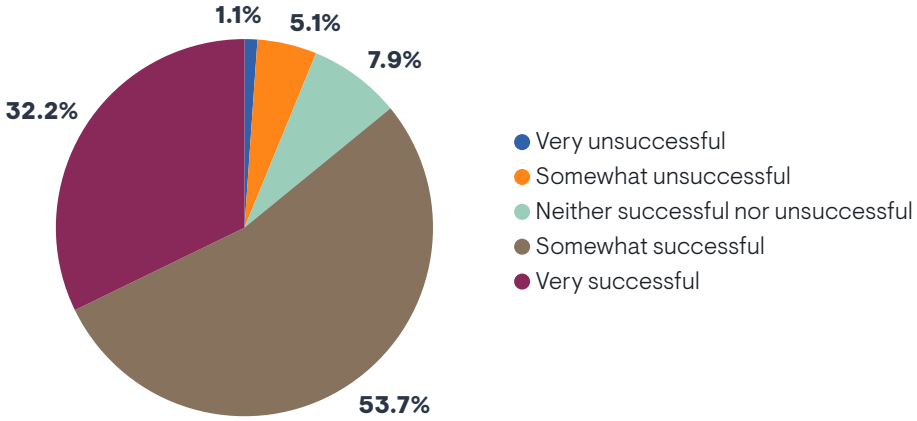
- Remote work increased employee productivity in 67% of organizations that track these impacts
- Supporting remote work increased the workload of 73% of network operations teams
- Only 32% of organizations have been completely successful in supporting the networking requirements of their remote workers
- The top challenges to remote network experience are poor home Wi-Fi setups, distance from applications, and poor ISP quality
- 83% of organizations have extended the cloud edge, moving applications closer to remote users to reduce latency and improve experience
- 72% of organizations are deploying network hardware to the homes of remote workers
- The average organziation is using 2.3 solutions for secure remote access, with VPNs (61%) remaining the most popular. Only 46% believe VPNs are the most effective solution. Many see value in secure direct access to the cloud, SASE, and ZTNA
- The most critical capabilities of a secure remote access solution are:
  1. Integrated network security
  2. Automated secure user-to-cloud or user-to-data-center connectivity
  3. Centralized management
  4. Network remediation (packet loss recovery, forward error correction)
- 87% of organizations have allocated budget to update network operations tools for remote and hybrid user support
- Nearly 49% of network operations teams started working with a new tool vendor to help them manage the network experience of remote workers
- Remote desktop access tools (81% of companies) remain the go-to solution for troubleshooting remote users' problems, but endpoint monitoring tools are increasingly popular, too (79%)
- 76% of organizations with hybrid workers have seen these digital nomads drive up bandwidth demand in their corporate offices
- 90% of organizations with hybrid workers had to upgrade Wi-Fi networks to address increased office mobility requirements
- 76% of organizations need to unify how they manage network access policies across on-premises networks and remote users

Overall Outcomes for Remote and Hybrid Work

Success with Supporting Home Workers

Figure 5 takes the temperature of network infrastructure and operations in this remote and hybrid work era. Just 32% of respondents believe their organizations have been completely successful with supporting the networking requirements and user experience of employees who work from home. Nearly 54% have seen some success but see room for improvement. A little more than 6% are reporting actual failure.

FIGURE 5. HOW SUCCESSFUL HAS YOUR IT ORGANIZATION BEEN AT SUPPORTING THE NETWORKING REQUIREMENTS AND USER EXPERIENCE OF EMPLOYEES WHO WORK FROM HOME?



"I think we've been really good," said an IT manager with a $6.5 billion oil and chemical company. "We already had a lot of support processes in place in the NOC and the SOC. We just needed to boost VPN bandwidth. We got it done well ahead of schedule."

Sample Size = 354

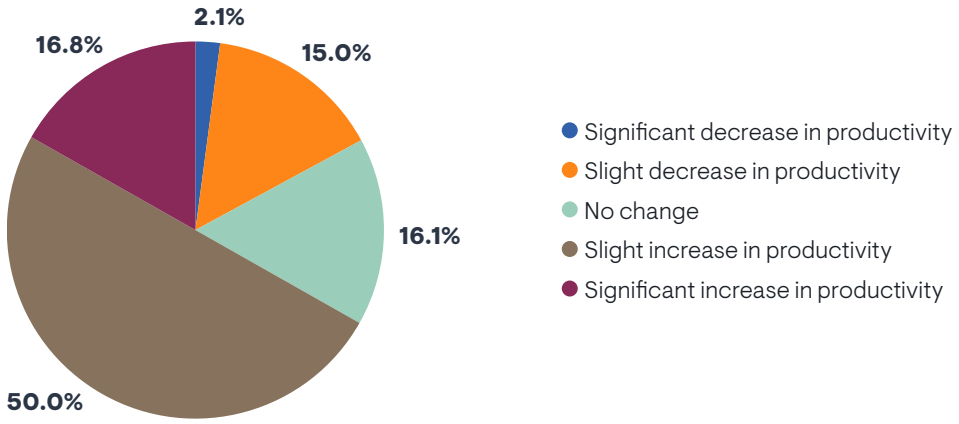
Members of the CIO's suite, the IT architecture group, and the network operations team are feeling the most optimistic about success. The network engineering team and the IT service management group are feeling more pessimistic. Larger enterprises are less successful than midsized enterprises.

Organizations that have been more successful are expecting a larger proportion of end users to work from home by 2025, suggesting that success leads to increased demand for remote connectivity and hybrid work.

Worker Productivity

More than 79% of EMA's research respondents reported that their organizations track whether employee productivity is impacted when they work from home. **Figure 6** reveals that only 17% have observed a drop in productivity. Nearly 67% saw a productivity boost. Critically, this boost of productivity was higher when the IT organization was successful with supporting the networking requirements of employees who work from home.

FIGURE 6. WHAT IS THE IMPACT OF REMOTE WORK ON EMPLOYEE PRODUCTIVITY?



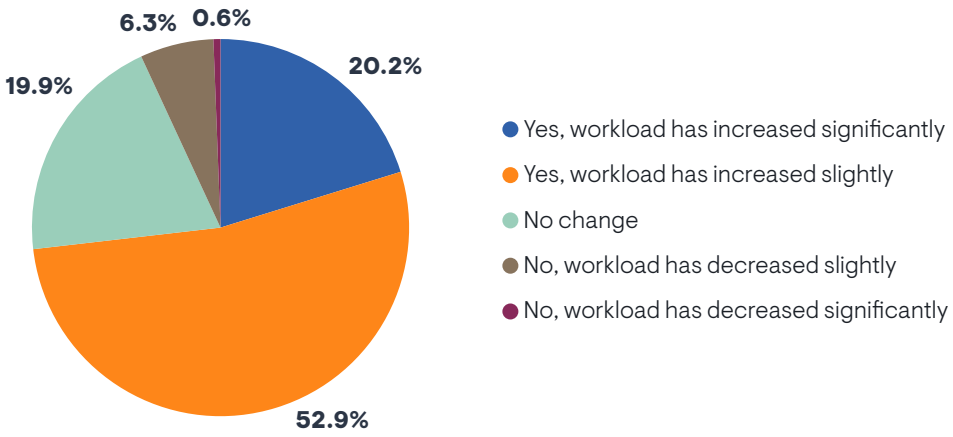
Sample Size = 280

Operational Overhead

EMA believes that supporting an expanded population of remote workers is putting a strain on the network operations team. IT organizations must adjust by making changes to network operations tools and process.

For example, EMA asked respondents who have seen a permanent increase in remote workers since the pandemic whether supporting these employees led to an increased workload for their network operations team. **Figure 7** reveals that 73% of network teams have seen an increase in work. Only 7% saw a decrease.

FIGURE 7. HAS THE OVERHEAD ASSOCIATED WITH SUPPORTING THESE REMOTE WORKERS LED TO AN INCREASED WORKLOAD FOR YOUR NETWORK OPERATIONS TEAM?



"The increased workload came when we started doing hybrid work," said an IT manager with a midsized software company. "Now we're supporting both, keeping the office running and everyone's home set up."

"It's added onto the anxiety and stress for IT operations," said an IT project manager for a $6.5 billion oil and chemical company.

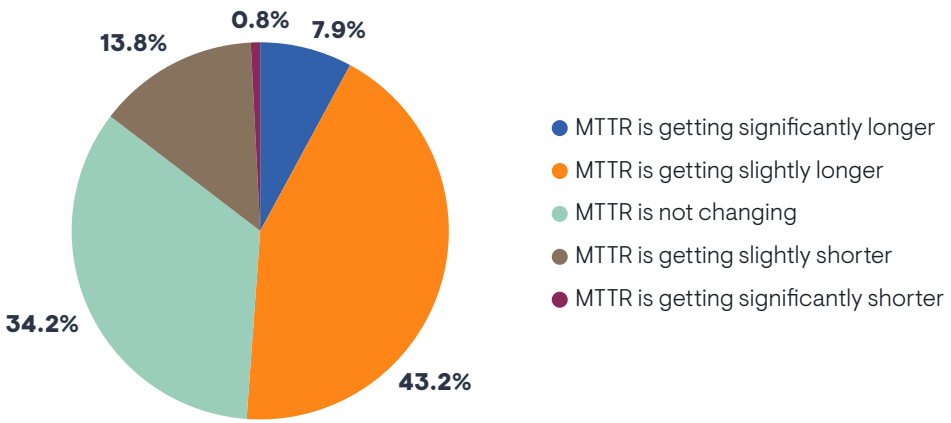
Sample Size = 331

Midmarket and large enterprises feel this increased workload more keenly. It's also heavier for organizations that told EMA that they aim to provide remote users with a network experience that is comparable to working on-premises.

Additionally, **Figure 8** reveals that remote work is making it harder for network operations teams to resolve network problems. The chart indicates that most network operations teams have seen the mean time to repair a network problem get longer since they started supporting people who work from home. This problem is more severe in larger enterprises.

Most network operations teams have seen the mean time to repair a network problem get longer since they started supporting people who work from home.

FIGURE 8. WOULD YOU SAY THAT SUPPORTING THE NEEDS OF PEOPLE WHO WORK FROM HOME HAS INCREASED OR DECREASED THE OVERALL MEAN TIME TO REPAIR (MTTR) NETWORK PROBLEMS IN YOUR ORGANIZATION?



Organizations that are seeing MTTR get longer were more likely to tell us they are making changes to their network operations toolsets, which we will explore later in this report.

Sample Size = 354

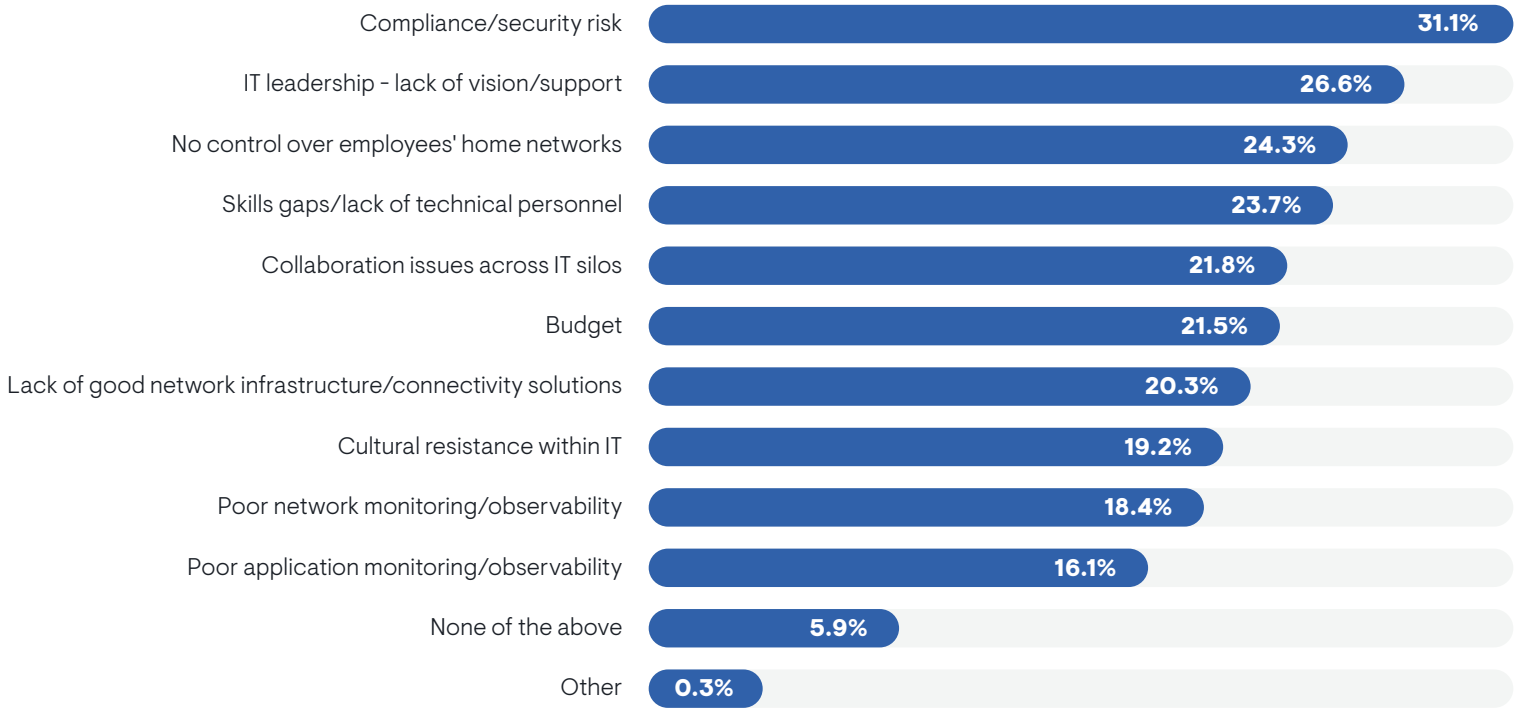
Challenges to Supporting Remote Workers

Figure 9 reveals the hurdles that IT organizations encounter when they try to support the networking requirements of their remote workers. Compliance and security risk are the biggest issues. Organizations that were less successful with supporting these requirements are the most likely to cite compliance and security risk as major challenges, suggesting it is the issue that separates best-in-class organizations from laggards.

Poor IT leadership, a lack of control over employees' home networks, and IT skills gaps or labor shortfalls are the chief secondary issues. Europeans were more likely than North Americans to complain about control over home networks. Technical staff were also more likely than IT middle managers to complain about this control issue. Also, larger enterprises struggled with it more than small and midsized enterprises.

Collaboration across IT silos was a tertiary challenge overall, but the network engineering team was particularly likely to call it out as a problem. Poor network monitoring and observability was another minor issue, but the cybersecurity team was more likely than others to struggle with it.

FIGURE 9. WHICH ISSUES PRESENT THE BIGGEST CHALLENGES TO YOUR IT ORGANIZATION'S ABILITY TO SUPPORT THE NETWORKING REQUIREMENTS OF USERS WHO WORK FROM HOME?



Sample Size = 354, Valid Cases = 354, Total Mentions = 811

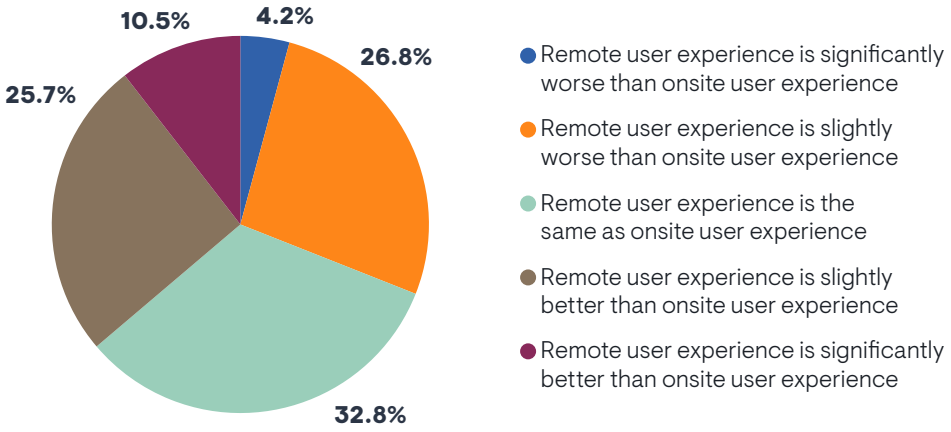
Remote User Experience

From frozen videos to file downloads that take forever, remote employee productivity can be extremely sensitive to network experience. This quality of experience will dictate whether IT organizations have been successful with supporting the networking requirements of remote and hybrid workers.

Comparing Remote User Experience to an On-Premises Experience

IT organizations can gain a good understanding of success based on whether user experience for remote employees is comparable to what they might get when working in the corporate office. **Figure 10** reveals that organizations are split on whether their remote workers are having such an experience. Overall, 31% say the work-from-home experience is worse and 36% say it's better. Nearly 33% perceive no difference. Organizations that have the most success in supporting the networking requirements of remote workers were more likely to say the remote user experience was better than an on-premises experience.

FIGURE 10. CURRENTLY, TO WHAT EXTENT IS THE USER EXPERIENCE OF PEOPLE WHO WORK FROM HOME COMPARABLE TO THE USER EXPERIENCE OF PEOPLE WHO WORK IN YOUR CORPORATE SITES/OFFICES?



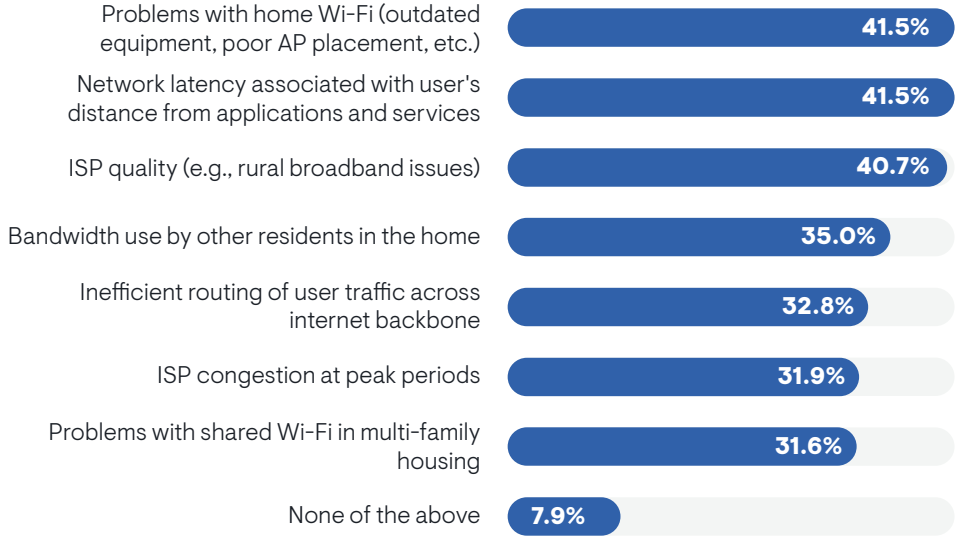
Sample Size = 354

Technical personnel tended to be more pessimistic than IT middle managers and executives about the remote user experience. The network engineering team was the most likely group to be pessimistic about the remote user experience. Larger enterprises tended to have the worst remote user experience.

Challenges to Network Experience

Figure 11 reveals the various issues that pose a challenge to network experience when users work from home. There are three major problems. First, the Wi-Fi infrastructure in employees' homes is outdated or poorly installed. Second, the physical distances between disparate users and the applications they access is adding network latency. Third, many enterprisers are dealing with substandard internet service providers. Europeans were more likely than North Americans to identify poor Wi-Fi as an issue. The latency issue was more common with large enterprises.

FIGURE 11. WHICH OF THE FOLLOWING ISSUES ARE PROVING TO BE SIGNIFICANT CHALLENGES TO THE NETWORK EXPERIENCE OF YOUR USERS WHO WORK FROM HOME?



Sample Size = 354, Valid Cases = 354, Total Mentions = 931

"The internet and Wi-Fi were definitely issues when we went remote," said an IT manager with a midsized software company. "Lots of people didn't have great setups and would raise issues with us about dropped Zoom calls, etc. We had to help them troubleshoot their networks. In some cases, we sent out ethernet adapters to hardwire laptops."

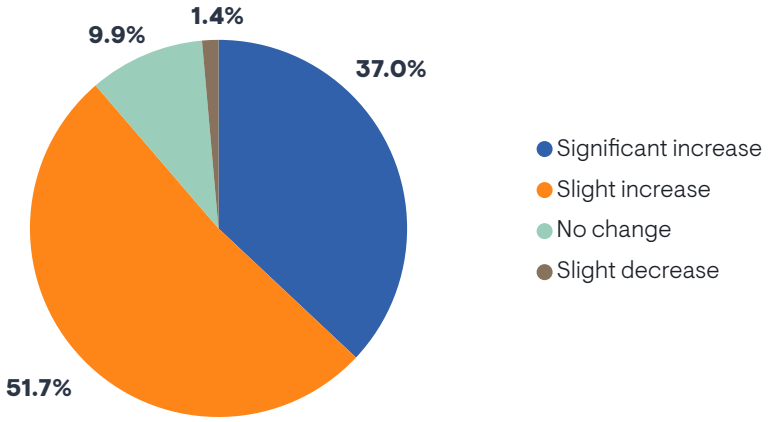
The other prominent source of trouble is bandwidth contention with other residents in a home. For instance, cohabitants of an end user might also work from home. Children might game or stream content while their parents are working. Organizations that aim to deliver a comparable user experience for all their remote workers reported that this bandwidth contention, as well as poor Wi-Fi quality, are more likely to cause them problems.

One other challenge to keep in mind is the heightened importance of real-time communications applications, such as voice and video, in the post-pandemic era. **Figure 12** reveals that nearly 89% of enterprises have observed increased usage of such applications since the beginning of the pandemic. These applications proved critical to collaboration and customer interaction during lockdowns. Since then, EMA observed that these applications have become more popular for both remote workers and on-premises workers. Such applications consume significant bandwidth and are highly sensitive to network performance.

"People were not as quick to use Microsoft Teams before the pandemic," said an IT project manager with a $6.5 billion oil and chemical company. "Utilization was at 50%. Now it's at 100%. Lots more video. And there are a lot of people who record videos, so we had to figure out storage."

The CIO's suite reported the largest surges in such application usage, followed by network engineering and network operations. IT architecture and end-user support reported the most modest growth in usage. Europeans reported a greater surge in real-time communication consumption than North Americans.

FIGURE 12. OBSERVED CHANGES IN THE USE OF REAL-TIME COMMUNICATIONS (VOICE, VIDEO, ONLINE MEETINGS) APPLICATIONS SINCE THE START OF THE PANDEMIC

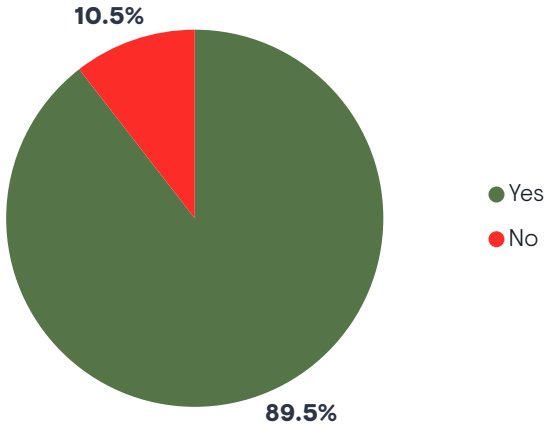


Sample Size = 354

Remote Work Drives Change in the IT Organization

Figure 13 reveals that nearly 90% of companies have reorganized IT operations to better support workers at home in recent years. Reorganizations are especially occurring in companies in which network operations had to make changes to their toolsets to better accommodate remote work. These findings all point to the fact that remote work at scale is highly disruptive to IT organizations.

FIGURE 13. HAVE THE REQUIREMENTS OF USERS WHO WORK FROM HOME CAUSED YOUR COMPANY TO REORGANIZE IT OPERATIONS IN RECENT YEARS TO BETTER SUPPORT THEM?



90% of companies have reorganized IT operations to better support workers at home in recent years.

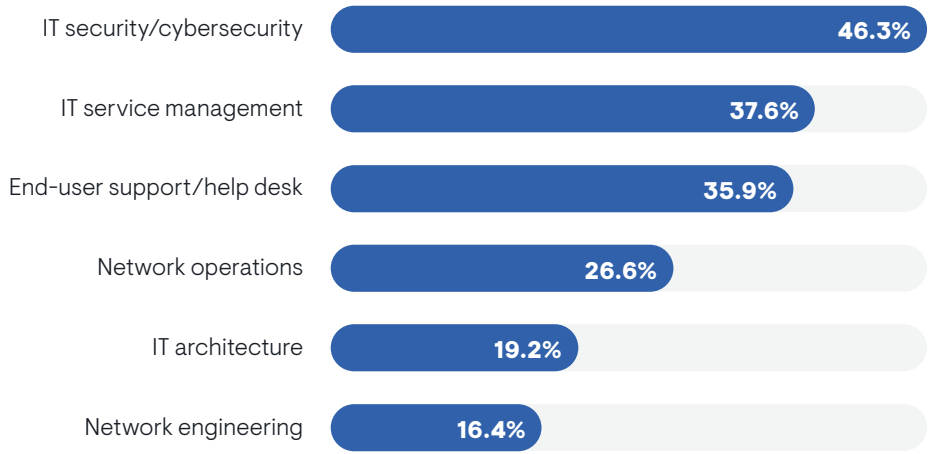
A goal to provide remote workers with an excellent user experience appears to drive reorganization. Nearly all the companies that conducted a reorganization indicated that they aim to provide a quality of network experience to remote workers that is comparable to the network experience of people who work at a corporate premises. Meanwhile, 100% of the organizations that have no intention of delivering a comparable network experience to remote workers reported no reorganization of IT operations.

Sample Size = 354

Setting the Agenda

Although network connectivity is essential to enabling remote work, network engineering and operations teams are rarely in the driver's seat when it comes to supporting end users who work from home. **Figure 14** reveals that security, IT service management (ITSM), and end-user support are the most likely to take lead roles. Security was more likely to lead in midmarket enterprises rather than larger companies. Network engineering and network operations appear to play a secondary role, as does the IT architecture group.

FIGURE 14. WHICH GROUPS WITHIN YOUR IT ORGANIZATION ARE MOST RESPONSIBLE FOR SUPPORTING END USERS WHEN THEY ARE WORKING FROM HOME?



Members of the CIO's suite were especially likely to identify security and ITSM as leaders of remote work strategy. The CIO's suite was also more likely to think network operations play a leading role.

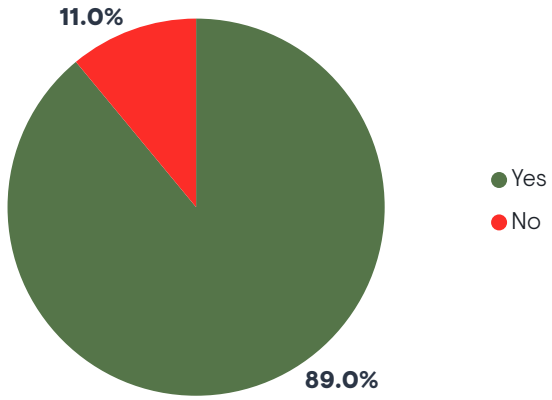
Sample Size = 354, Valid Cases = 354, Total Mentions = 644

End-user support was more likely to be front and center if organizations experienced a significant surge in traffic from real-time communications applications since the start of the pandemic. This suggests that these applications are creating a surge in help desk tickets from remote workers, and IT organizations are putting end-user support in the driver's seat to ensure that these applications are adequately supporting the business.

Network Team Influence

While network teams rarely lead the strategy for how an IT organization supports remote work, EMA believes that these teams need a seat at the table. Network infrastructure teams must be involved in architectural decisions that impact connectivity and security. Network operations will be called on to support user experience with tools and processes. **Figure 15** reveals that 89% of respondents believe their network teams have enough influence over these strategies today. Unfortunately, members of network engineering were less likely to respond affirmatively to this question (80%).

FIGURE 15. DO YOU BELIEVE YOUR NETWORK INFRASTRUCTURE AND OPERATIONS TEAM HAS SUFFICIENT INFLUENCE AND CONTROL OVER HOW YOUR IT ORGANIZATION ENABLES AND SUPPORTS PEOPLE WHO WORK FROM HOME?



Organizations that are the most successful with supporting the networking requirements of users who work from home were more likely to say the network team has enough influence. More critically, when the network team has enough influence, it is more likely to receive a budget allocation to update its network monitoring and troubleshooting tools to support remote workers.

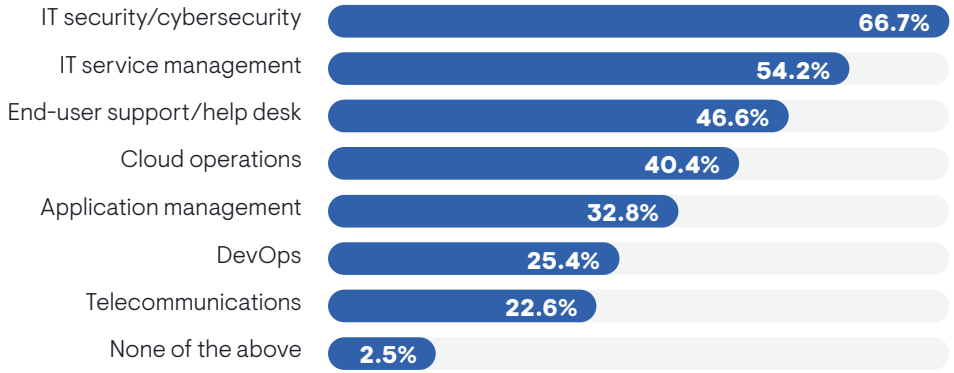
When the IT organziation has low expectations for the remote user experience, the network team is usually frozen out of decision-making. Respondents who reported that they do not aim to deliver a network experience to remote workers that is comparable to an on-premises experience were very likely (80%) to say the network team does not have enough influence.

Sample Size = 354

Key Partners for NetOps

Figure 16 reveals which groups network operations teams are partnering with as they support the needs of remote workers. Unsurprisingly, the top three groups are the same ones that lead overall efforts to support remote workers: security, ITSM, and end-user support. ITSM is an especially prominent NetOps partner in North America, while in Europe, application management is a more likely partner. Network operations is also more likely to partner with ITSM in companies that are more successful with their support of remote work. End-user support collaboration is especially more common in organizations that are more aggressive with delivering a comparable network experience to all remote workers.

FIGURE 16. HAVE THE REQUIREMENTS OF USERS WHO WORK FROM HOME CAUSED YOUR NETWORK OPERATIONS TEAM TO INCREASE ITS COLLABORATION WITH ANY OF THE FOLLOWING GROUPS IN RECENT YEARS?



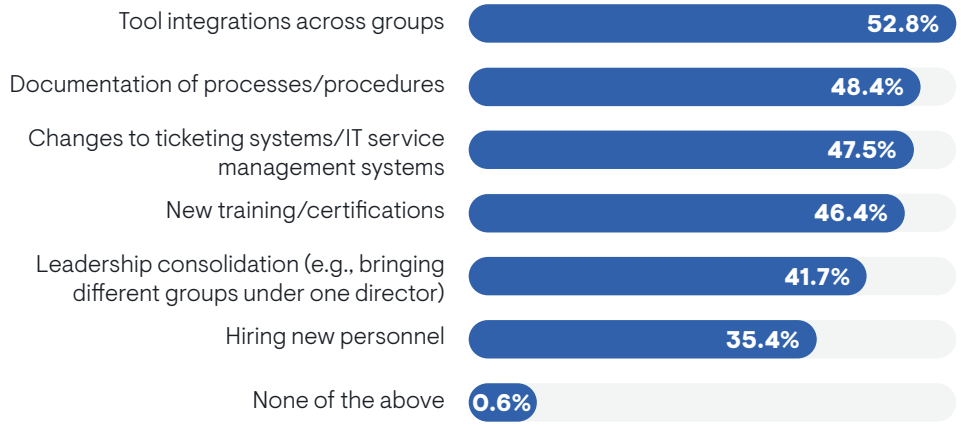
DevOps and telecommunications teams were tertiary priorities for NetOps partnership, but IT executives were more likely to see them as important collaboration targets.

Finally, EMA found that network operations teams are more likely to have budget to update their toolsets for remote work support if they are collaborating more often with end-user support, security, telecommunications, and cloud operations.

Sample Size = 354, Valid Cases = 354, Total Mentions = 1,031

Figure 17 reveals what organizations are doing to facilitate effective collaboration between network operations and other teams. The highest priority is tool integrations between groups. These integrations are especially common in companies that have experienced the biggest surges in traffic from real-time communications applications.

FIGURE 17. WHAT IS YOUR ORGANIZATION DOING TO FACILITATE THE NETWORK OPERATIONS TEAM'S COLLABORATION WITH OTHER GROUPS IN SUPPORT OF USERS WHO WORK FROM HOME?



Many organizations are also documenting processes and procedures, altering their ticketing and ITSM systems, and training personnel. Training and changing to ticketing systems also correlate with surges in real-time application traffic.

Leadership consolidation is less common, but North Americans reported it more often than Europeans. It's also more common in large enterprises, where leadership structure is typically more complex.

Hiring personnel is the least common step taken to facilitate NetOps collaboration, but is more popular among organizations that have been the most successful with supporting people who work from home. IT executives are also more likely to say it's a priority.

Sample Size = 345, Valid Cases = 345, Total Mentions = 941

Network Services for Remote Workers

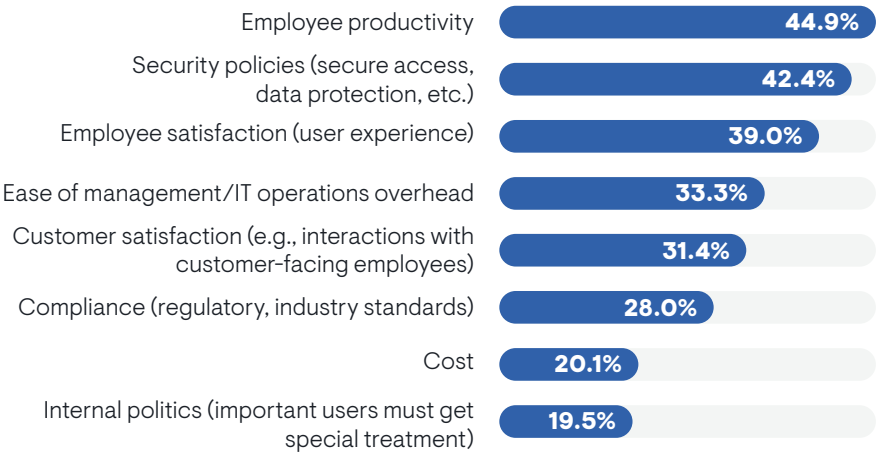
This section is the heart of this research. It explores how IT organizations securely connect employees who work from home and ensure a satisfactory network experience.

Setting Requirements and Goals

Determining Networking Requirements

Figure 18 reveals the factors that IT organizations consider when they are determining the networking requirements of users who work from home. First, organizations base their remote work strategies on the impacts of network experience on employee productivity. For instance, if users can't reach their applications due to poor network performance or faulty remote access technology, they can't get work done. IT organizations are thinking in terms of removing barriers that prevent employees from working efficiently and effectively. Members of network engineering, end-user support, and security teams all selected productivity as a top driver, while the IT architecture group was less likely to select it.

FIGURE 18. FACTORS THAT DETERMINE HOW AN ORGANIZATION ADDRESSES THE NETWORKING REQUIREMENTS OF EMPLOYEES WHO WORK FROM HOME



Sample Size = 354, Valid Cases = 354, Total Mentions = 915

Security policies drive networking requirements.

Second, security policies drive networking requirements. While productivity demands a well-performing network and access to applications and data, security policies pull decision-makers in the opposite direction. They need controls in place to ensure that authenticated users access only the resources they need and that their access of those resources from a remote location doesn't put the company at risk of a breach or data loss. Organizations that are more successful with how they support the networking requirements of remote users were more likely to identify security policy as a top driver of requirements. Members of network operations teams and the CIO's suite were more likely to select security than end-user support teams.

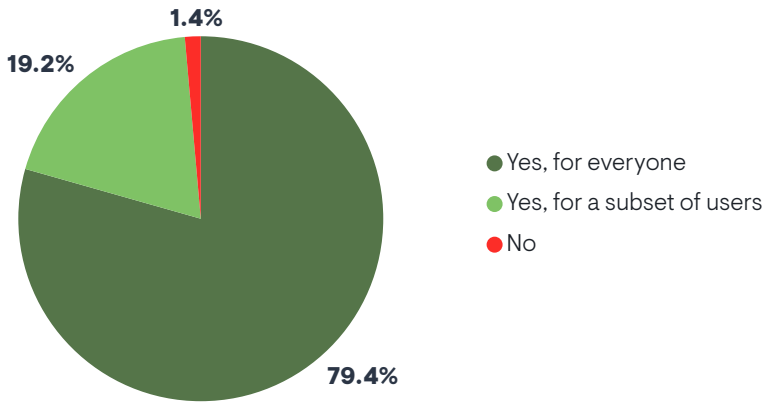
The secondary drivers of requirements were employee satisfaction (a key issue for retaining skilled workers), ease of management, and customer satisfaction (especially important for remote workers who interact with and support customers). Ease of management was more important to midmarket enterprises and less important to larger companies.

Cost and internal politics were the least likely drivers of remote networking requirements. However, IT executives were more likely than people further down the chain of command to believe internal politics play a role.

Network Experience Targets

Figure 19 reveals that 79% of IT organizations try to provide all remote workers with a level of network and application experience that is comparable to the experience they would have in a corporate office. Another 19% aim to provide this only to a selection of users. Only a little more than 1% have no intention of delivering on this level of experience. North American respondents were more ambitious than Europeans.

FIGURE 19. DOES YOUR IT ORGANIZATION AIM TO PROVIDE AN EQUIVALENT QUALITY OF NETWORK AND APPLICATION EXPERIENCE FOR PEOPLE WHO WORK FROM HOME AND PEOPLE WHO WORK IN YOUR CORPORATE SITES?



Real-time communication applications, such as voice and video, influence this issue. Few applications are more sensitive to network conditions than voice and video. Organizations that have seen increased use of such applications in recent years were more likely to aim for a commensurate user experience for remote workers.

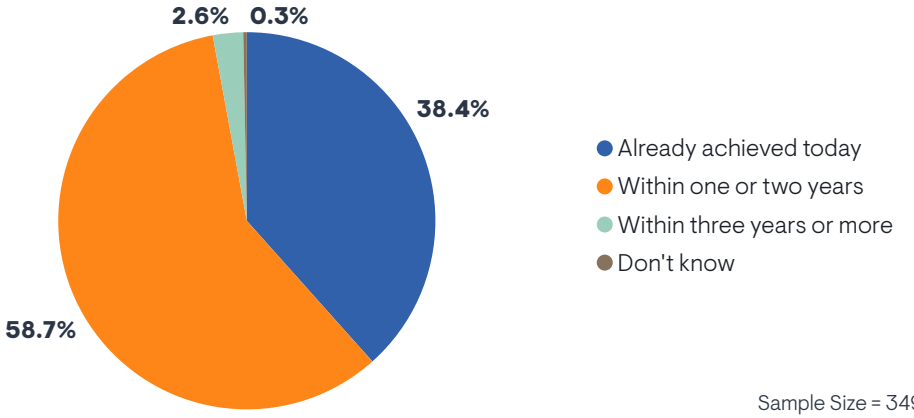
The intention to deliver a good quality of experience appears to be driven by a recognition that remote work is endemic. For instance, companies that do not try to deliver this experience reported to EMA that the pandemic did not lead to a permanent increase employees who work from home. Also, companies that have the most ambitious goals for user experience expect to have a larger remote employee population in the future. Organizations that aim for a comparable user experience for all remote workers are expecting that 51% of their end users will work remotely by 2025. Organizations that try to deliver this only for a subset of users expect 45% of their users to be remote in 2025. Organizations that have no intention of delivering a comparable user experience expect only 28% of their users to be remote in 2025.

Sample Size = 354

Notably, concerns about cost are at play here. Organizations that focus on delivering this quality of experience to only a subset of workers were more likely to tell EMA that cost is a determining factor in how they support the networking requirements of remote users. In other words, budget limits how expansive organizations will be with delivering effective solutions for remote users. On the other hand, organizations that aim to deliver a comparable experience for all users were more likely to cite security policies as a driver. This suggests that a poor networking experience at home is a potential security issue. For example, if home workers find their company's remote network access solution difficult to use or unreliable, they may look for ways to bypass it.

Among the majority of respondents who aim for a commensurate user experience for remote workers, **Figure 20** reveals the expected timeline for when these targets will be achieved. More than 38% have hit those targets today and nearly 59% expect to get there within two years.

FIGURE 20. EXPECTED TIMELINE FOR DELIVERING A COMMENSURATE USER EXPERIENCE FOR REMOTE WORKERS



Sample Size = 349

Organizations that are the most successful with their overall support of remote workers were more likely (55%) to have hit these targets already. Unsurprisingly, organizations that try to deliver an equivalent user experience for only a subset of their remote users are more likely to have already achieved this goal, while organizations that are trying to deliver this experience level for all remote workers are still working toward that goal.

Balancing Network Experience with Security

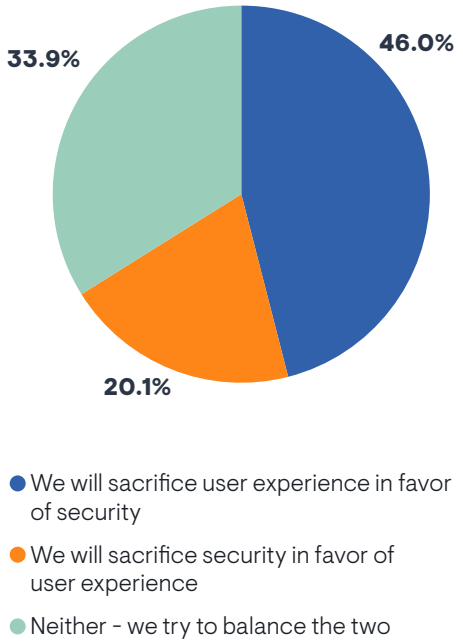
Depending on how an organization builds out its solutions for remote workers, it might have to sacrifice user experience for security, or vice versa. For instance, a security team might be so aggressive with security controls that users find it too difficult to access the applications and data they need for work. On the other hand, network teams might remove onerous security controls that add latency to applications or limit access to certain resources.

Figure 21 reveals that when faced with a binary choice, more organizations will prioritize security at the expense of user experience. Only 20% will place user experience above security. More than one-third refuse to choose, saying they will always try to find a balance between the two priorities.

North Americans were more willing to sacrifice user experience, while Europeans were more likely to insist on a balance. People who work within a CIO's suite were the most idealistic, typically believing that a balance of user experience and security is possible. On the other hand, people who work in network engineering, IT architecture, and security were all more likely to sacrifice user experience.

Organizations that were less successful with their strategies for supporting the networking requirements of remote users were more likely to sacrifice security for user experience.

FIGURE 21. REGARDING THE USER EXPERIENCE AND SECURITY OF PEOPLE WHO WORK FROM HOME, WHICH OF THE OPTIONS IS YOUR ORGANIZATION WILLING TO PRIORITIZE, EVEN IF IT NEGATIVELY IMPACTS THE OTHER?



Organizations that were less successful with their strategies for supporting the networking requirements of remote users were more likely to sacrifice security for user experience.

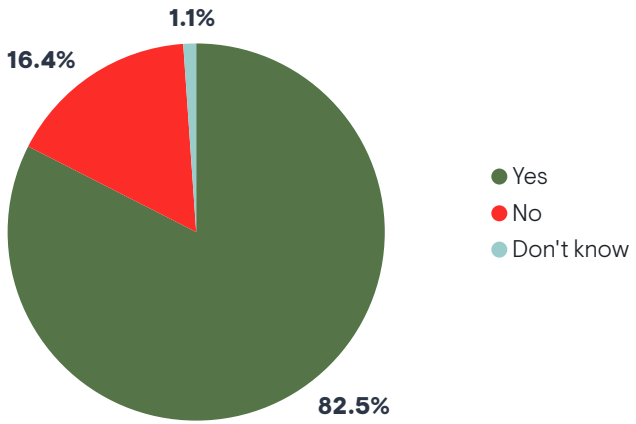
Sample Size = 354

Architectural Strategies for Remote Workers

Extending the Cloud Edge

Earlier, we noted that the latency associated with the physical distance of remote workers from the applications they use is a significant challenge to network experience in 42% of enterprises. Given the prominence of this issue, enterprises need to make changes to infrastructure. **Figure 22** reveals that nearly 83% of organizations have tried to optimize application experience by deploying resources closer to the homes of remote workers, including the use of new cloud regions or edge cloud deployments. IT executives were more aware of such changes than the middle manager or technical personnel in our survey.

FIGURE 22. HAS YOUR ORGANIZATION TRIED TO OPTIMIZE APPLICATION EXPERIENCE BY DEPLOYING APPLICATIONS CLOSER TO THE HOMES OF YOUR REMOTE WORKERS, SUCH AS IN NEW CLOUD REGIONS, EDGE CLOUD DEPLOYMENTS, OR EDGE COMPUTE DEPLOYMENTS?



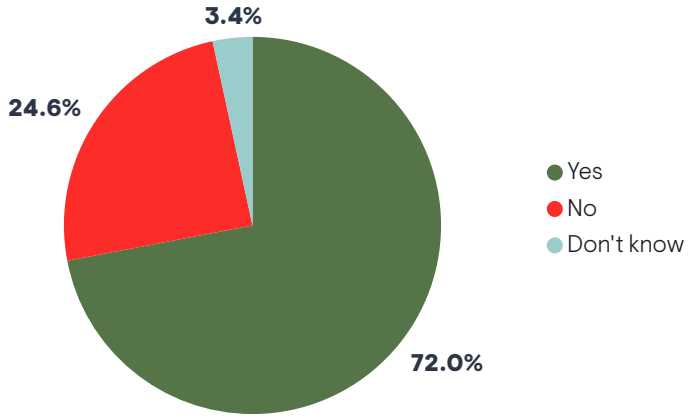
Sample Size = 354

This architectural change was more common in organizations that have seen significant growth in real-time application usage. Such changes are also more common in organizations that attempt to provide a network experience to remote workers that is comparable to the experience of on-premises workers. Conversely, 100% of organizations that have no intention of providing a comparable user experience told EMA that they are making no such changes to infrastructure.

Deploying Network Hardware to Homes

Most remote workers have an internet connection and a Wi-Fi access point for basic connectivity in their homes. IT organizations often rely on software to enable secure remote connectivity for these workers. However, sometimes software isn't enough. **Figure 23** reveals that 72% of organizations are deploying network hardware to the homes of at least some workers. This practice is more common in North America than Europe.

FIGURE 23. HAS YOUR IT ORGANIZATION INSTALLED, OR DOES IT PLAN TO INSTALL, NETWORK HARDWARE OF ANY KIND IN THE HOMES OF ANY REMOTE EMPLOYEES?



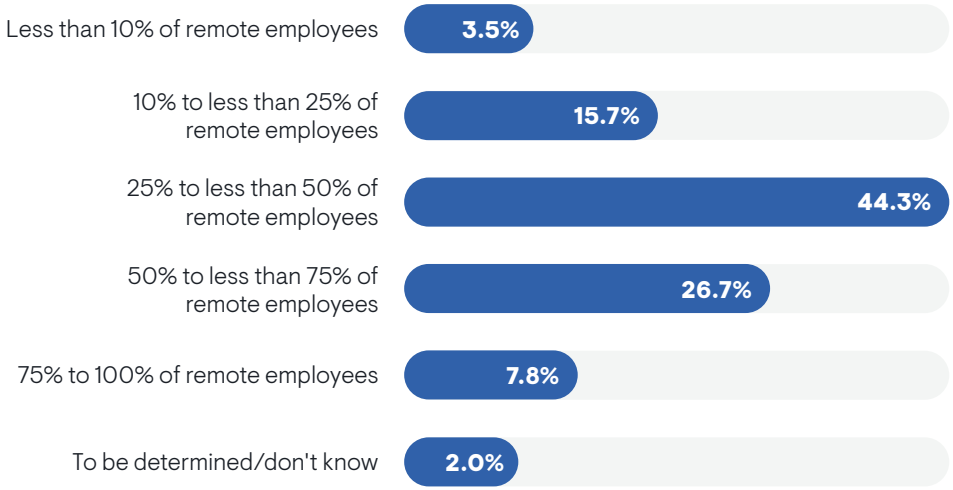
Sample Size = 354

Organizations that try to deliver a network experience to remote workers that is comparable to on-premises experiences are more likely to deploy hardware. It's also more common in organizations that are seeing increases in real-time application usage.

"We won't deploy hardware," said an IT manager with a midsized software company. "We will probably just firm up our policy to say if you don't have a stable network connection, you can't work from home."

Figure 24 reveals that most organizations are deploying network hardware to fewer than half of the homes of remote employees, with the most common expectation being from 25% to less than 50% of homes. Only 34% expect to deploy hardware to more than half of worker's homes. Hardware deployment is more expansive in organizations that try to deliver a network experience that is comparable to on-premises networks.

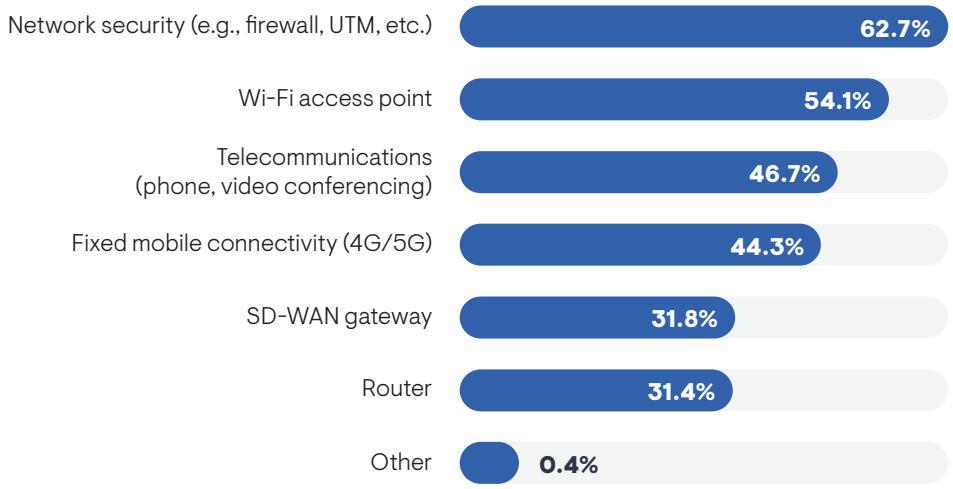
FIGURE 24. TO WHAT EXTENT WILL YOUR COMPANY DEPLOY NETWORK HARDWARE IN THE HOMES OF REMOTE EMPLOYEES?



Sample Size = 255

Figure 25 reveals the kinds of network hardware organizations are deploying to homes. Network security devices were selected most often. However, EMA suspects that deployment of security devices is relatively selective in an individual enterprise. The most likely scenario is for high-value end users, like a CEO, CFO, or other C-level executive. These types of users are attractive targets for malicious actors and most enterprises are going to deploy highly secure solutions for these executives' home offices.

FIGURE 25. WHICH OF THE FOLLOWING NETWORKING HARDWARE SOLUTIONS IS YOUR IT ORGANIZATION DEPLOYING OR PLANNING TO DEPLOY IN EMPLOYEES' HOMES?



Most organizations are also deploying Wi-Fi access points to homes. This finding is unsurprising given that Wi-Fi issues are a leading cause of networking problems for remote workers.

Sample Size = 255, Valid Cases = 255, Total Mentions = 692

Many organizations are also deploying telecommunications gear (phones, video conferencing endpoints) and fixed mobile routers (4G/5G). The former can improve the experience of real-time communications applications, while the latter can overcome issues associated with low-quality wireline ISPs, another common cause of poor remote user experience. Deployment of telecommunications equipment was more likely in organizations that have seen a significant increase in use of real-time communications applications.

Deployments of SD-WAN gateways and enterprise routers are relatively rare. Most router deployments occur in organizations that are trying to deliver network experience to home users that is comparable to an on-premises network experience.

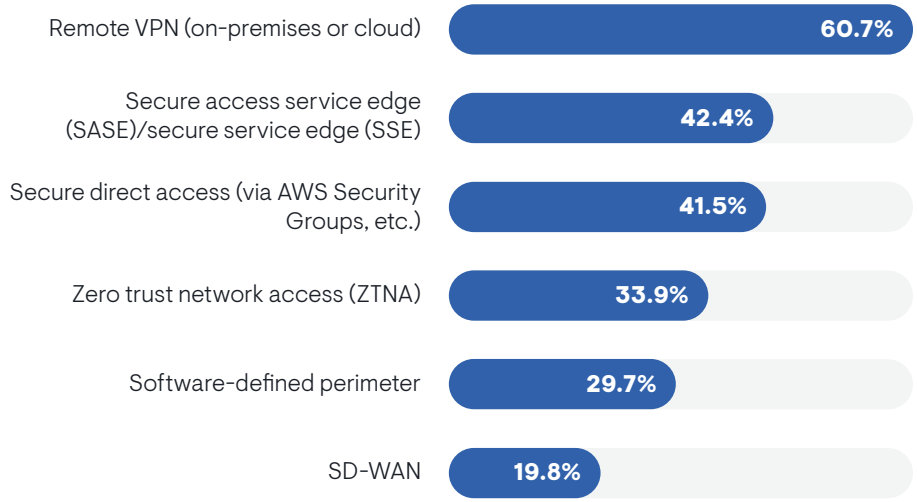
Secure Remote Connectivity Solutions

When working remotely, employees need access to internal resources on the corporate network. To enable this, IT organizations deploy secure remote connectivity technology. Remote VPN technologies have been the de facto standard for decades, but newer technologies are offering alternatives that provide more granular policy controls, improved scalability and flexibility, and better performance.

Figure 26 reveals what organizations are using for secure remote connectivity today. The average respondent selected 2.3 solutions, pointing to a multi-product strategy for remote access. VPNs remain the standard for remote access, but secure access service edge (SASE) and secure direct access to public clouds are quite popular, too. SASE products offer cloud-delivered security technology that can control access to corporate resources. Many SASE solutions offer other remote access technologies, such as VPNs and zero trust network access (ZTNA), from within their overall security solutions. Secure direct access via the security controls of a cloud provider allows IT organizations to regulate which kinds of traffic can access cloud-based resources.

An IT project manager at a $6.5 billion oil and chemical company said his company coincidentally started expanding its VPN infrastructure just before the pandemic, increasing capacity from 1,000 to 6,000 simultaneous remote connections. “When the pandemic hit, we had to reprioritize projects and had to move resources off other projects to get it down quicker.”

FIGURE 26. TECHNOLOGIES USED TO PROVIDE SECURE REMOTE CONNECTIVITY TO APPLICATIONS AND DATA



More than one-third are ZTNA, which governs access to specific resources rather than blanket access to a network via a VPN. ZTNA also enables granular policy controls that define the specific circumstances under which an authenticated user can access those resources.

Less popular is a software-defined perimeter (SDP), which is very similar to ZTNA. ZTNA and SDP are often used interchangeably, but there are nuanced differences. While a ZTNA solution focuses on authenticating least privilege access on an individual basis to specific resources, SDP solutions create individualized perimeters around specific resources and then establish secure connections into those perimeters. ZTNA tends to impose tighter controls on what can be accessed by whom.

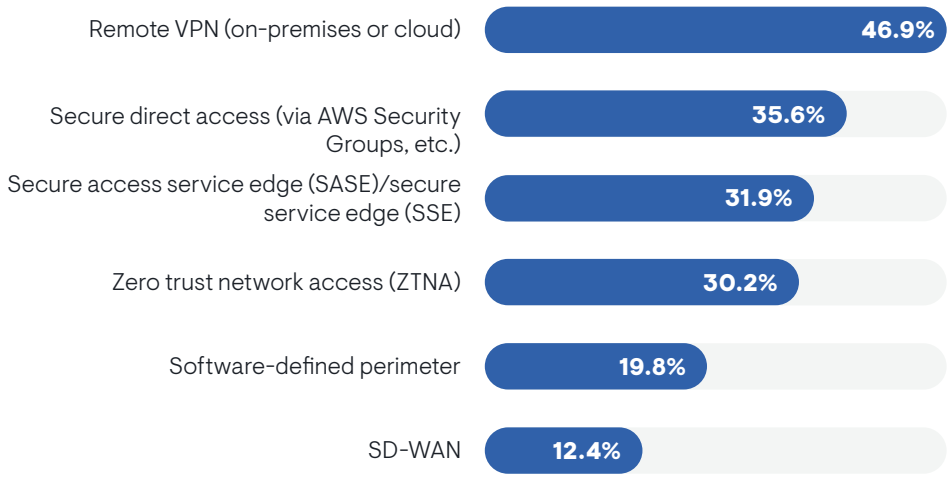
Finally, less than 20% are using SD-WAN, a solution that typically relies on hardware at the user edge to establish a secure point-to-point connection.

Sample Size = 354, Valid Cases = 354, Total Mentions = 807

Organizations that aim to deliver a network experience that is comparable to an on-premises experience to as many remote users as possible are more likely to use SASE. Organizations that are experiencing large surges of real-time communications application usage are more likely to use a VPN or secure direct access to a cloud.

Figure 27 reveals how IT professionals feel about these solutions. In addition to asking them what they use for remote access, we asked them to identify which solutions are most effective at supporting secure connectivity for people who work from home. Here, we see the relative value of VPN technology drops, along with SDPs and SD-WAN. SASE and secure direct access are perceived as relatively more effective and ZTNA is roughly flat, with more than 30% of respondents identifying it as effective. The big takeaway here is that many people who have specific experience with VPN technology are admitting it is not an effective solution for secure remote access. Organizations need to look at the alternatives on this chart.

FIGURE 27. REGARDLESS OF WHETHER YOU CURRENTLY USE THEM FOR THIS PURPOSE, WHICH OF THE FOLLOWING TECHNOLOGIES DO YOU THINK ARE MOST EFFECTIVE AT SUPPORTING SECURE REMOTE CONNECTIVITY FOR USERS WHO WORK FROM HOME?

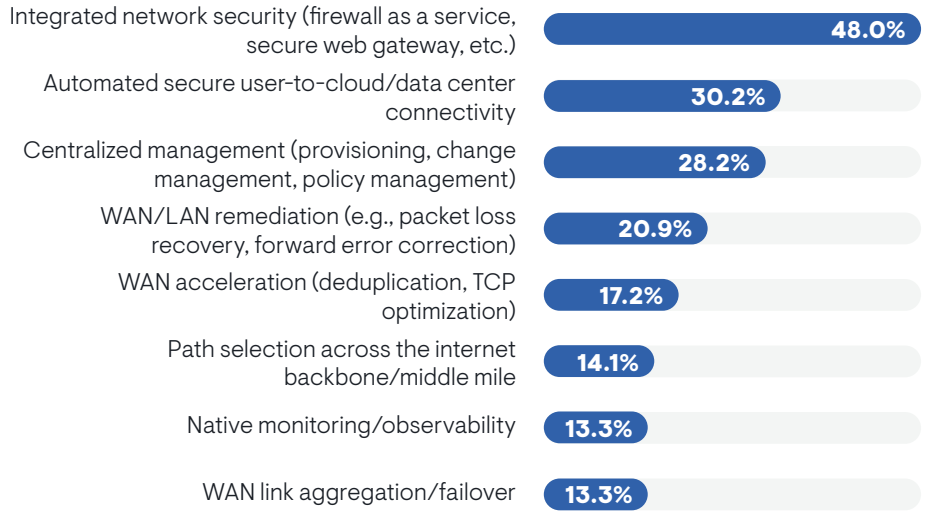


Sample Size = 354, Valid Cases = 354, Total Mentions = 626

Members of network engineering, network operations, and cybersecurity teams were more likely than others to select ZTNA as an effective solution. Positive impressions of ZTNA were also more common among the largest enterprises in this survey. Organizations that try to deliver a network experience that is commensurate with on-premises networks to a maximum number of remote workers also showed more enthusiasm for ZTNA.

Figure 28 identifies the capabilities that organizations require from the remote access solutions that are used to support working from home. First, they want a solution that has integrated network security functionality, such as firewall as a service and secure web gateways. This explains the popularity of SASE in this survey. SASE vendors often combine their secure remote access solutions with a full stack of cloud-delivered network security services, allowing security services to scan all traffic from remote workers in a single pass before it reaches its destination. Integrated network security is a higher priority for IT executives than technical personnel. In particular, the network engineering team is less enthused by it.

FIGURE 28. FOR SECURE REMOTE CONNECTIVITY SOLUTIONS USED TO CONNECT YOUR END USERS WHO WORK FROM HOME, WHICH OF THE FOLLOWING CAPABILITIES ARE MOST IMPORTANT TO HAVE?



Sample Size = 354, Valid Cases = 354, Total Mentions = 656

Secondarily, organizations want solutions that can automatically establish secure connections to whatever resources are available on-premises or in the cloud, and they want a centralized management environment that allows admins to provision connectivity, manage access policies, manage changes, and do other tasks.

Finally, organizations are looking for remote access solutions that enhance and protect network experience through network remediation (e.g., packet loss recovery and forward error correction), WAN acceleration (e.g., deduplication, TCP optimization), or path selection across the internet backbone (latency reduction). The largest enterprises in this research were twice as likely as small and midsized enterprises to want a path selection feature.

WAN link aggregation and native observability features are relative afterthoughts. However, organizations that are the least successful with supporting the networking requirements of remote employees are more likely to prioritize WAN link aggregation.

EMA observed some differences in requirements based on the kinds of remote access solutions enterprises use. For instance, a native observability capability and path selection across the internet were higher priorities for ZTNA users than VPN users. WAN/LAN remediation features were more important to SASE users than VPN users. Integrated network security was more important to SASE users than SDP users.

End users are not fully aware of and properly trained on how to engage with remote access technology.

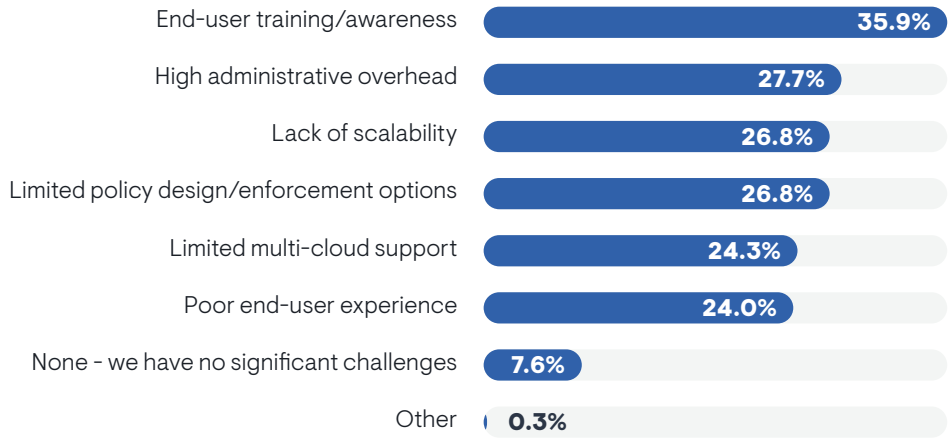
Figure 29 reveals the challenges that enterprises are encountering with their secure remote access solutions. The biggest issue is a people problem. End users are not fully aware of and properly trained on how to engage with remote access technology. They may undermine the technology by bypassing access controls or sharing credentials. Members of cybersecurity teams were especially concerned by this issue, while members of network operations and end user support groups were less troubled. Awareness and training concerns were also more prominent in larger enterprises.

High administrative overhead, lack of scalability, and limited options for policy design and enforcement were the chief secondary challenges. Scalability was a bigger issue for organizations that are less successful with supporting remote workers. High administrative overhead was a bigger issue for end-user support teams.

Organizations that use secure direct access from cloud providers and SASE were more likely to complain about limited access policy design and enforcement, while users of VPN and ZTNA solutions were less concerned. Anyone that continues to rely on VPNs has probably not developed a need for robust policy design, so they don't see their VPN's weakness in that area as an issue. On the other hand, ZTNA solutions are excellent in this regard, so it's not a challenge.

Limited multi-cloud support is a tertiary challenge, but users of SDP solutions were especially likely to complain about it.

FIGURE 29. WHAT DO YOU FIND MOST CHALLENGING ABOUT THE SOLUTIONS YOU USE TO PROVIDE SECURE REMOTE ACCESS TO WORKERS WHO WORK FROM HOME?



Sample Size = 354, Valid Cases = 354, Total Mentions = 614

Operationalizing the Remote Network Experience

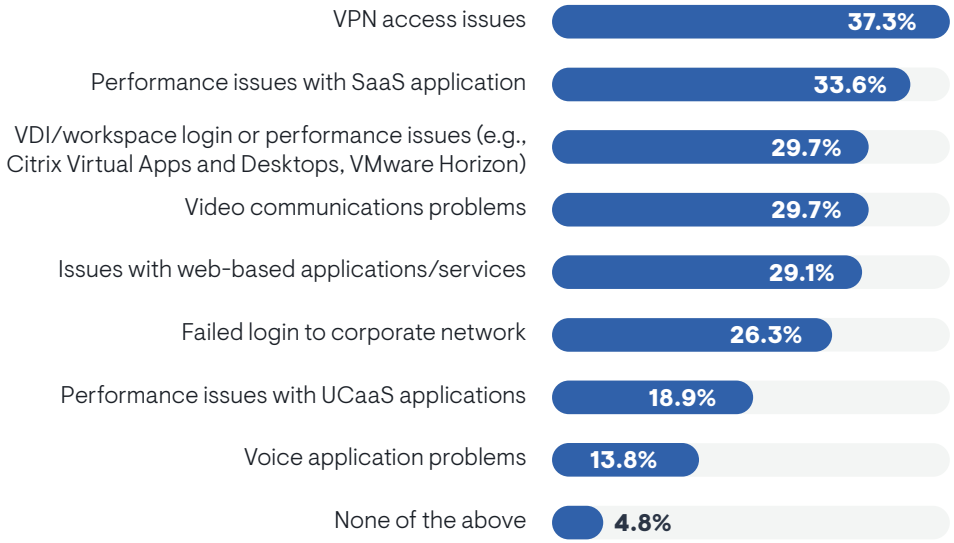
This section focuses on how IT operations, especially the network operations team, are evolving to support remote and hybrid workers, first by looking at typical user complaints and then by exploring changes to network operations tools.

The Network Experience at Home

Typical End-User Complaints

Figure 30 reveals that the most common complaint from remote users is a problem with VPN access. They try to log into a VPN and the connection fails for some reason. Technical personnel selected this issue more often than IT executives. Members of IT architecture and end-user support groups were more likely to select VPN access issues than network engineering and network operations teams.

FIGURE 30. WHICH OF THE FOLLOWING PROBLEMS DO EMPLOYEES MOST OFTEN REPORT WHEN THEY ARE WORKING FROM HOME?



Sample Size = 354, Valid Cases = 354, Total Mentions = 790

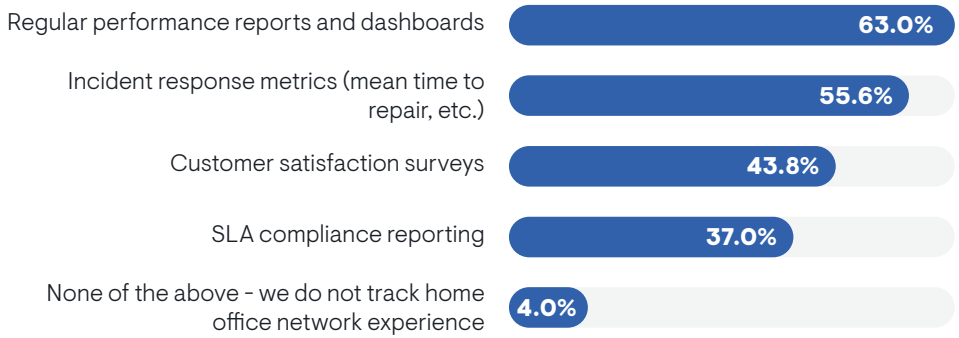
The second leading complaint was SaaS application performance, followed by problems with virtual desktops, video communications, and web-based applications. North Americans were more likely than Europeans to hear complaints about SaaS performance. Video performance complaints correlated strongly with an overall lack of success with supporting remote workers, suggesting that it is a critical issue that must be addressed.

Complaints about voice applications and UCaaS applications were the least common. Voice issues came up more frequently for larger companies.

Tracking Experience

Figure 31 reveals how IT organizations try to track end-user sentiment about network experience for employees who work from home. At least 96% of the surveyed organizations are trying to do something here. Updates to network operations tools will be essential, given that the top priorities are performance reports and dashboards. These reports and dashboards are especially popular with organizations that aim to provide a network experience to remote workers that is comparable to an on-premises experience.

FIGURE 31. HOW DOES YOUR ORGANIZATION TRACK AND REPORT ON NETWORK EXPERIENCE FOR PEOPLE WORKING FROM HOME?

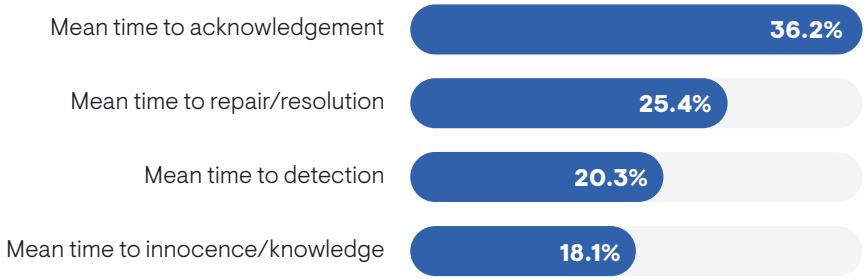


Sample Size = 354, Valid Cases = 354, Total Mentions = 720

Most companies also use incident response metrics. Customer satisfaction surveys and SLA compliance reporting are least popular. The CIO's suite is especially enamored with satisfaction surveys. The network engineering team is extremely likely to use SLA compliance reports.

Figure 32 reveals the response metrics that network operations teams consider most important when dealing with issues that impact users who work from home. Overall, mean time to acknowledgement is more important than mean time to repair and other metrics. In other words, IT leaders want to optimize the time it takes for IT support to acknowledge user complaints. Fixing the problem is a lower priority from an operational metrics perspective.

FIGURE 32. WHEN TRACKING INCIDENT RESPONSE METRICS FOR ISSUES THAT IMPACT USERS WHO WORK FROM HOME, WHICH STATISTIC IS MOST IMPORTANT TO YOUR NETWORK OPERATIONS TEAM?



Europeans were more likely than North Americans to emphasize mean time to repair. Mean time to knowledge (or innocence) was a higher priority in North America than Europe.

Organizations that are more successful with supporting remote users were more likely to emphasize mean time to detection, while less successful organizations often focused on knowledge or innocence. IT executives also tended to focus on knowledge and innocence more often than technical personnel and middle managers. Finally, organizations that have observed a surge in real-time communications application usage are more likely to focus on detection or repair, less likely on acknowledgement or innocence.

Sample Size = 354

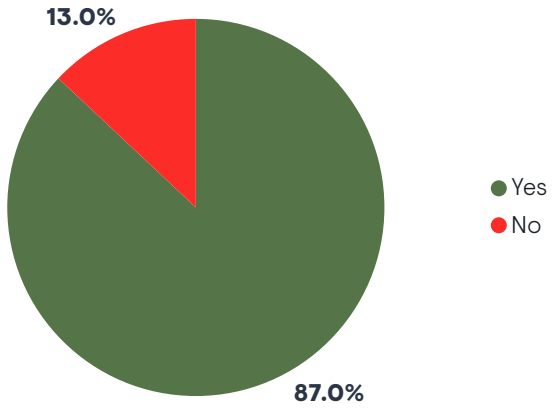
Network Observability for Remote User Experience

This section explores how network operations teams and their partners need to adjust their toolsets to address the rise of remote and hybrid workers.

Allocating Budget for Tool Transformation

Figure 33 reveals that 87% of organizations have allocated budget to improve how network monitoring and troubleshooting tools support the experience of remote workers. Unsurprisingly, this allocation of budget is more frequent when the network operations team is taking the lead with supporting remote workers.

FIGURE 33. 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?



Sample Size = 354

Budget allocation is also more frequent with the following conditions:

- The pandemic permanently increased the number of employees who work from home
- Surges in remote and hybrid work increased IT operations overhead
- Use of real-time communications applications increased
- IT tries to deliver a network experience to remote workers that is comparable to working on-premises
- Remote users frequently complain of issues with virtual desktops and SaaS applications
- IT organizations are trying to accelerate mean time to detection of issues that affect the network experience of people working from home
- Home Wi-Fi visibility needs improvement

Working with New Tools and New Vendors

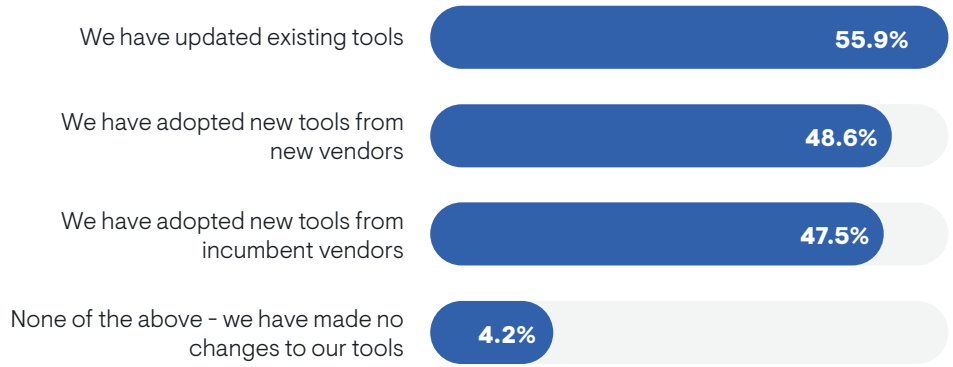
Figure 34 reveals at a high level how this budget allocation is spent. Nearly 56% are modifying their existing tools to improve how network operations teams support the needs of employees who work from home. Many are also adopting new solutions. Nearly 49% adopted tools from new vendors and 48% adopted new tools from incumbent vendors. Organizations that reported having a budget allocation were more likely to add new tools, both from existing and new vendors. North Americans were more likely to adopt new tools from new vendors. Members of the CIO's suite, network engineering, and IT architecture were more likely to work with new tool vendors, but network operations and end-user support were less likely.

An IT manager for a midsized software company offered an example of how his team updated their toolsets. "We wrote up a script that does some basic metrics and says, 'It looks like your ISP is dropping packets.' We will provide end users with the script and have them run it. Then, it emails the results to our [alerting system]. If they're not tech savvy, we will remote into their desktop and run the script for them."

Other factors that correlate with the adoption of new NetOps tools rather than just updates of existing tools:

- Increased use of real-time communications applications
- Installation of network hardware in home offices
- Need to track daily location of hybrid workers
- Challenges with secure remote access user experience

FIGURE 34. HOW HAS YOUR NETWORK OPERATIONS TEAM UPDATED ITS TOOLSET TO ADDRESS SUPPORT OF USERS/EMPLOYEES WHO WORK FROM HOME?

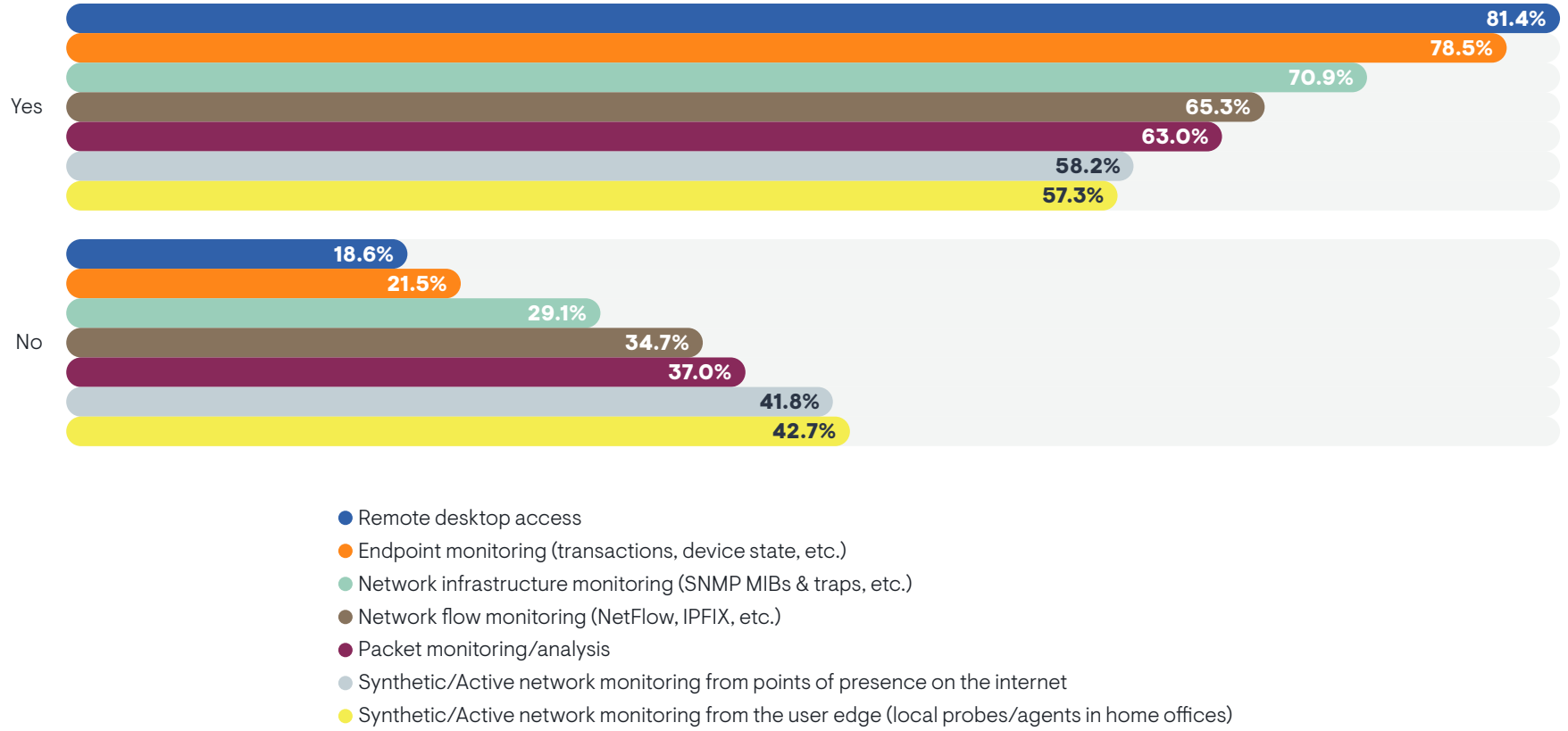


Sample Size = 354, Valid Cases = 354, Total Mentions = 553

Tools NetOps Uses

Figure 35 reveals the types of tools that network operations teams use to monitor and troubleshoot the network experience of remote users. Remote desktop access is the most popular tool. Obviously, the ability to take control of a user's computer remotely is a helpful and effective troubleshooting tool, but it doesn't scale when thousands of workers are remote. However, organizations that were more successful with supporting remote users were more likely to use these tools.

FIGURE 35. IS YOUR NETWORK OPERATIONS TEAM USING ANY OF THE FOLLOWING TOOLS TO MONITOR AND TROUBLESHOOT THE NETWORK EXPERIENCE OF USERS IN HOME OFFICES?



Sample Size = 354

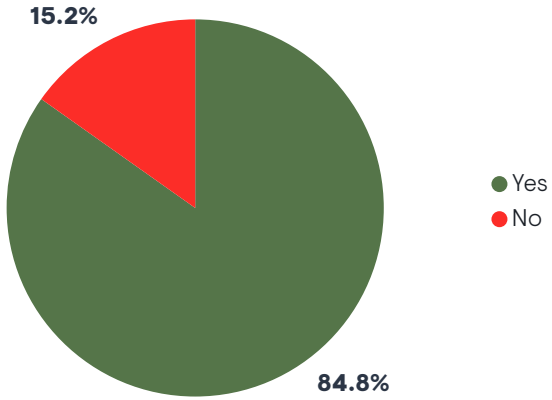
Endpoint monitoring tools are also very popular. Unlike remote desktop access they scale more readily, allowing IT operations personnel to monitor and troubleshoot from the endpoint perspective across regions rather than on an individual basis. Endpoint monitoring was more popular among enterprises that have allocated budget for network toolset updates. Organizations that are the most successful with supporting the networking requirements of remote workers were more likely to use these tools.

Traditional network performance management solutions, including network infrastructure monitoring, flow monitoring, and packet monitoring, were secondarily popular.

Active/synthetic monitoring (both from probes at the network edge and from points of presence across the internet) were the least popular tools, but still in use by the majority of companies. Synthetic tools were more likely in use among organizations that have allocated budget to update network toolsets. The latter type of synthetic monitoring tool was more popular among organizations that try to deliver a network experience to remote workers that is comparable to the experience of working on-premises.

Figure 36 zooms in on how active and synthetic monitoring tools are used. In the past, EMA observed that enterprises were selective in how they used such tools given that some vendors license their products by the number of tests running or the number of test agents active. Rather than continuously monitor key applications to identify trends and anomalies, these organizations only monitored certain applications during times of high usage or in response to end-user complaints. Figure 36 reveals that nearly 85% of organizations that use active and synthetic tools are now continuously monitoring applications with them. This allows them to identify trends in application performance, set baselines, and identify anomalies more quickly.

FIGURE 36. DOES YOUR ORGANIZATION PROACTIVELY MONITOR KEY APPLICATIONS WITH ACTIVE/SYNTHETIC MONITORING TOOLS EVEN WHEN USERS ARE NOT ACTIVE FOR TRENDING/ANOMALY DETECTION PURPOSES?



Continuous monitoring with active and synthetic tools is more common under the following conditions:

- Use of real-time communications application is increasing significantly
- The IT organziation has allocated budget to improve how the NetOps toolset supports remote work
- The IT organziation aims to provide a network experience to remote workers that is comparable to the experience of working on-premises

Sample Size = 264

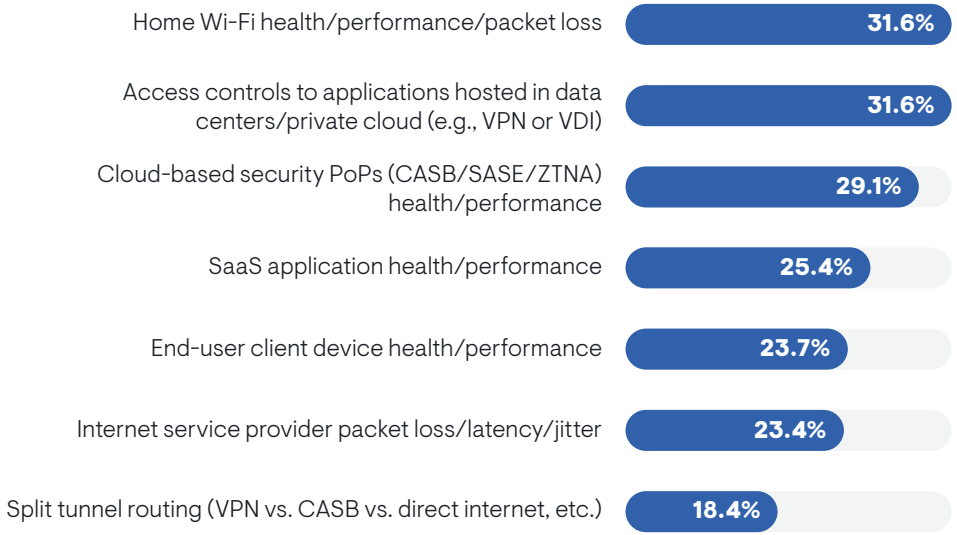
New NetOps Tool Requirements

Figure 37 reveals what visibility network operations teams need from the tools they use to manage the experience of remote workers. The two top priorities are insights into home Wi-Fi health and performance and the controls that govern access to applications hosted in data centers or private cloud environments. An example of the latter is a VPN concentrator.

Observability of cloud-based security health and performance is also a high priority. The CIO's suite, network engineering, and network operations teams are all more likely to think cloud-based security observability is important.

Observability of SaaS applications, end-user client devices, and internet service providers are secondary priorities. SaaS observability is a higher priority for organizations that have seen a surge in real-time communications application usage.

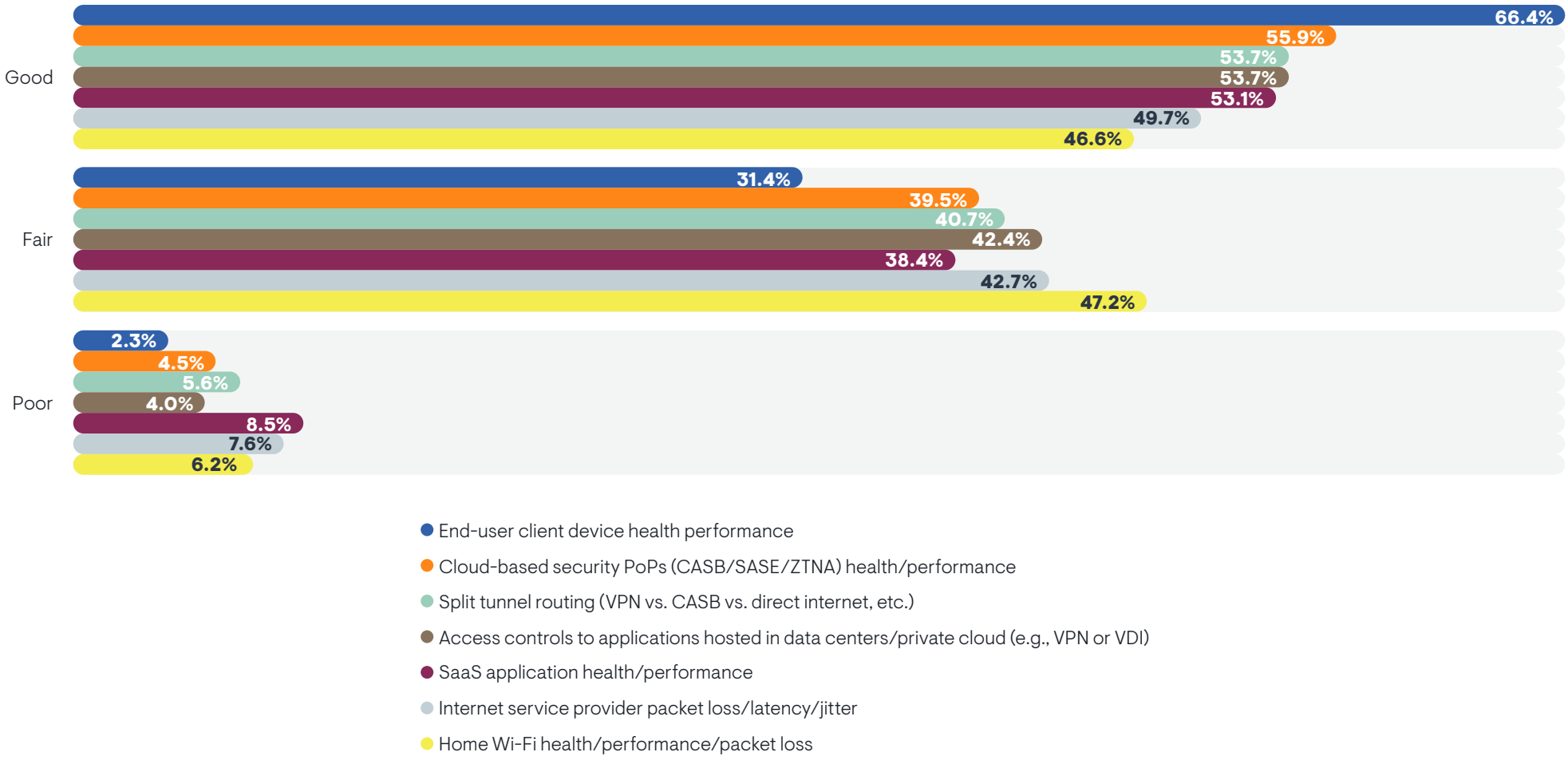
FIGURE 37. ERROR DOMAINS THAT IT OPERATIONS MOST NEED TO SEE WHEN MONITORING AND TROUBLESHOOTING THE NETWORK EXPERIENCE OF END USERS WHO ARE WORKING FROM HOME



Sample Size = 354, Valid Cases = 354, Total Mentions = 649

While home Wi-Fi is the highest priority for observability, **Figure 38** reveals that this visibility is the most difficult to achieve. EMA asked respondents to rate their current ability to understand each error domain that can potentially impact remote user experience. Home Wi-Fi observability was the most difficult domain to monitor and troubleshoot.

FIGURE 38. RESPONDENTS RATE THEIR VISIBILITY INTO POTENTIAL ERROR DOMAINS FOR THE NETWORK EXPERIENCE OF END USERS WHEN THEY ARE WORKING FROM HOME



Sample Size = 354

Many respondents were also feeling less confident in their ability to understand internet service provider performance and SaaS application performance. They were most confident in their visibility into end-user devices and cloud-based security. Respondents who indicated that their organizations had allocated budget to improve the ability of their network operations toolset to manage the experience of remote workers reported better visibility into end-client devices, home Wi-Fi, access controls in the data center, and cloud-based security.

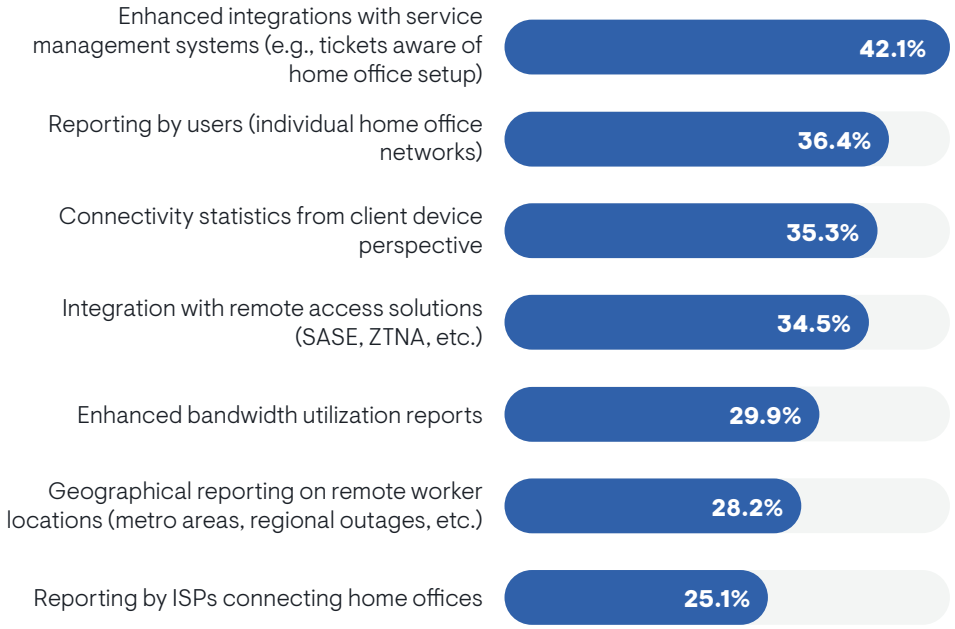
Large enterprises reported poorer visibility into home Wi-Fi and internet service providers than small and midsized enterprises.

Figure 39 reveals what kinds of enhancements to network monitoring tools are helpful to supporting remote work. The biggest need is enhanced integration with service management systems. Such enhancements could, for example, enrich trouble tickets with information about an end user's home office setup and whatever network telemetry that can be extracted from that setup. Organizations that are the most successful with supporting remote networking requirements are the most likely to seek this enhanced integration. The CIO's suite and the network engineering team have a stronger affinity for it than the IT architecture group.

Reporting organized by individual users, connectivity statistics from the client device perspective, and integration with secure remote access solutions are also popular tool enhancements. Like enhanced integration with service management, more successful organizations also favored integration with remote access solutions . The network operations and security teams were also more likely to seek this integration, while network engineering was less interested. The cybersecurity team and the CIO's suite showed a stronger interest in client-side connectivity statistics than the network operations team.

Reporting organized by the ISPs that connect home offices was the least sought tool enhancement. However, large enterprises were more interested in this capability, probably because their workers are more distributed and use a wider variety of ISPs.

FIGURE 39. NETWORK MONITORING TOOL FEATURES AND ENHANCEMENTS MOST VALUABLE FOR MANAGING THE USER EXPERIENCE OF PEOPLE WORKING FROM HOME



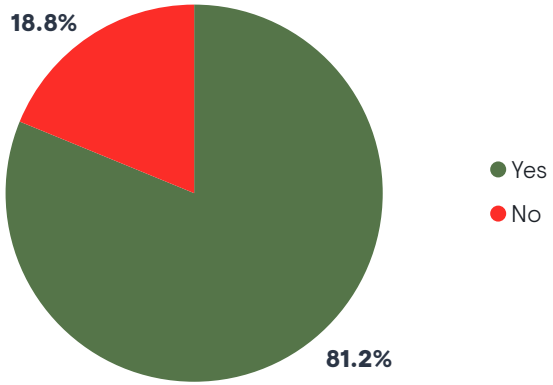
Sample Size = 354, Valid Cases = 354, Total Mentions = 820

Hybrid Workers in Focus

Where Are You Today?

One essential question that IT operations will have when taking a support call from a hybrid worker is, "Where are you?" This will set the context for how IT will proceed with solving a given problem. Location will be an essential piece of information. **Figure 40** reveals that most IT organizations are aware of this issue. More than 81% of organizations that have hybrid workers try to track where those people are on a given workday. Small and midmarket enterprises were more likely to track location than large enterprises.

FIGURE 40. DOES YOUR IT ORGANIZATION TRY TO TRACK WHERE HYBRID WORKERS ARE WORKING ON A GIVEN DAY?

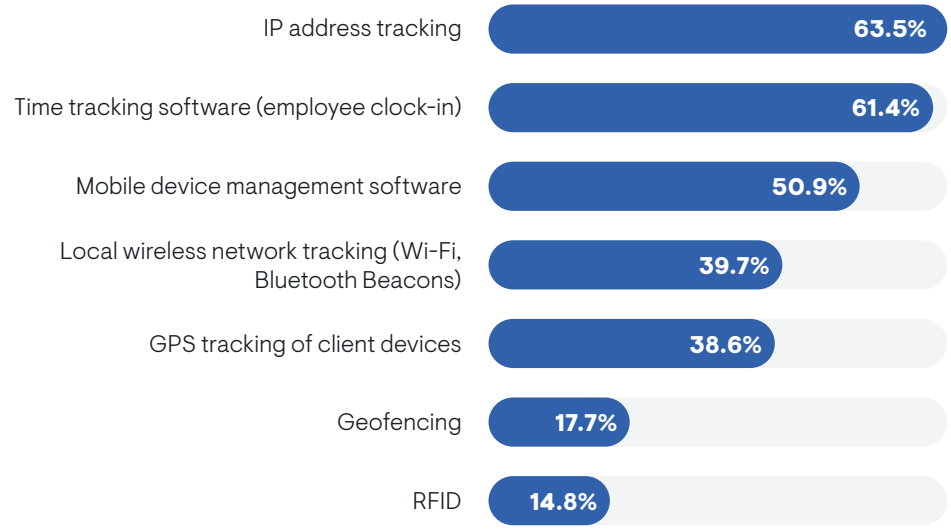


This tracking is important for effective end-user experience. Respondents who told EMA that their organizations attempt to provide a consistent user experience regardless of location were more likely to track the location of hybrid workers.

Sample Size = 341

Figure 41 reveals the methods that organizations are using to track the location of these hybrid workers. Most rely on IP address tracking tools and time tracking software (typically used by human resources organizations). Time tracking software was more popular in organizations that are the most successful in supporting the networking requirements of remote and hybrid workers.

FIGURE 41. HOW DOES YOUR IT ORGANIZATION GET VISIBILITY INTO WHERE HYBRID WORKERS ARE LOCATED ON A GIVEN DAY?

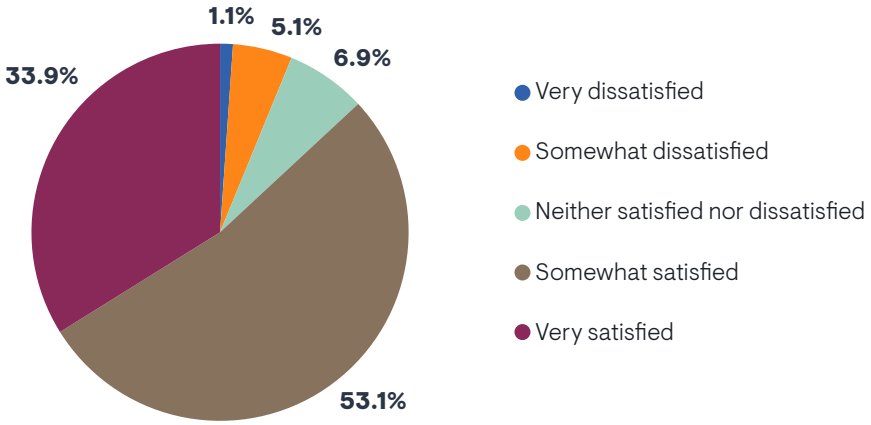


Slightly more than half also rely on mobile device management software. Using the location tracking capabilities of local wireless networks is less popular, but larger enterprises had a strong affinity for it.

Sample Size = 277, Valid Cases = 277, Total Mentions = 794

Figure 42 shows that only 34% of organizations are fully satisfied with their ability to track the location of hybrid workers. Respondents who use RFID technology for this purpose reported the least satisfaction with hybrid worker tracking.

FIGURE 42. HOW SATISFIED ARE YOU WITH YOUR IT ORGANIZATION'S VISIBILITY INTO WHERE HYBRID WORKERS ARE WORKING ON ANY GIVEN DAY?



Midmarket enterprises expressed more optimism about this visibility than small and large enterprises. Smaller companies probably lack the resources to do it, and larger companies are likely struggling with the scale and complexity of the problem. Satisfaction with this visibility correlates strongly with whether an organziation is successful with its overall support of the networking requirements of remote workers.

Sample Size = 277

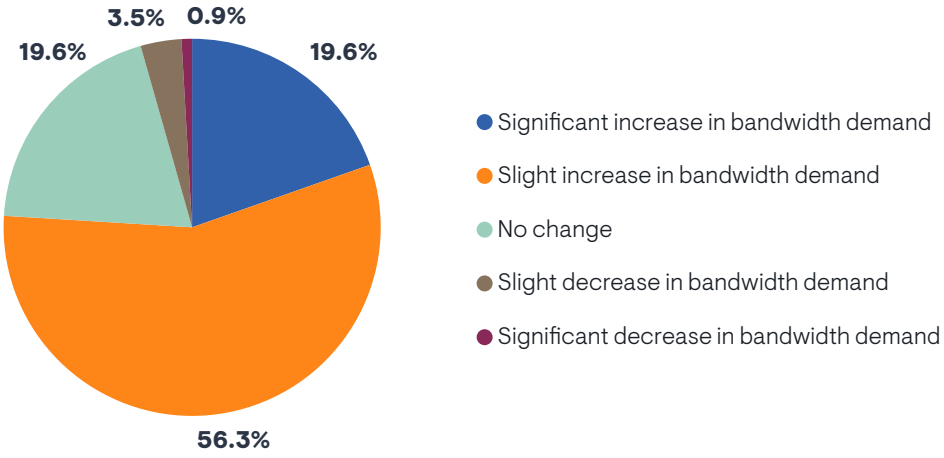
Impacts of Hybrid Work

The massive expansion of remote work during the pandemic changed the nature of work. This research already established that usage of real-time applications, like voice and video, increased during the pandemic. With the rise of hybrid work, these changes will inevitably have impacts on on-premises networks as workers return to the office.

Bandwidth Demand

Figure 43 reveals that 76% of organizations with hybrid workers have seen increased bandwidth demand. The CIO's suite, network engineering, and IT service management reported the most significant increases to bandwidth demand.

FIGURE 43. HAS THE PRESENCE OF HYBRID WORKERS IN YOUR ORGANIZATION HAD ANY IMPACT ON BANDWIDTH DEMAND FOR YOUR ON-PREMISES NETWORKS (E.G., OFFICE NETWORKS, BRANCHES, ETC.)?



Sample Size = 341

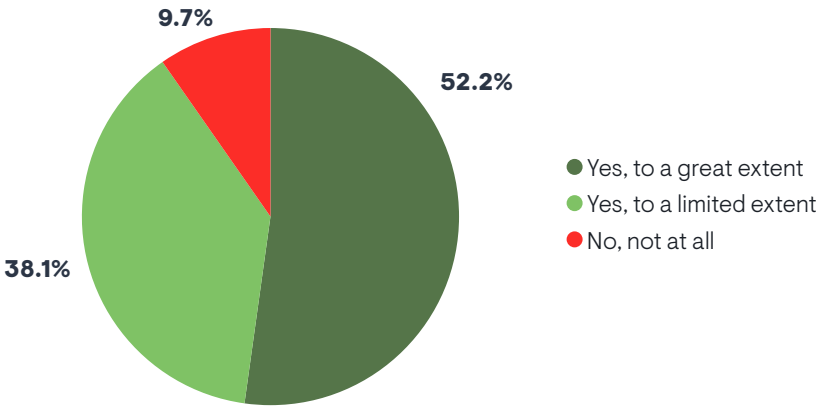
"With Teams usage at 100%, bandwidth demand is going up," said an IT project manager with a $6.5 billion oil and chemical company. "We had to upgrade MPLS virtually everywhere."

Bandwidth demand was also higher in organizations that were seeing the biggest increase in real-time application usage. Organizations that are the most successful with supporting the networking requirements of remote workers are more likely to see more on-premises bandwidth demand, suggesting that a successful user experience at home leads to more intense network usage in the office.

Increased Office Mobility

Figure 44 reveals that more than 92% of organizations with hybrid workers are seeing more demand for office mobility, forcing them to expand or upgrade their existing Wi-Fi networks. Hybrid workers are less tied down by a physical desk. When they come into the office, they may spend most of their time meeting with coworkers in various conference rooms. They need to be able to work anywhere in the office, which places more demand on wireless networks in terms of coverage and user density. These Wi-Fi updates are more extensive in midsized and large enterprises.

FIGURE 44. HAS THE PRESENCE OF HYBRID WORKERS IN YOUR ORGANIZATION CREATED NEW MOBILITY REQUIREMENTS THAT PROMPTED YOUR ORGANIZATION TO EXPAND AND/OR UPGRADE ITS WI-FI NETWORKS?



Sample Size = 341

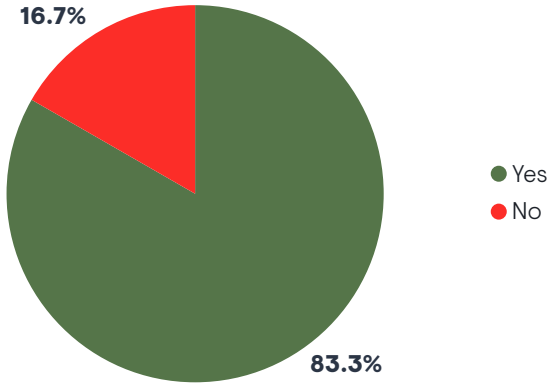
"Campus wireless is an ongoing battle," said an IT project manager with a $6.5 billion oil and chemical company. "Most tickets we have seen with hybrid work have been on the wireless side. People are doing hoteling. They're moving around, and the access points don't match up with the people now. The coverage they have isn't great."

Real-time communications applications are a potential driver of these Wi-Fi upgrades. Organizations that saw the highest increases in such application usage were the most likely to make extensive updates to their Wi-Fi networks.

Location-Based Services

According to **Figure 45**, more than 83% of organizations with hybrid workers need to implement location-based technologies to enable a hybrid workplace, such as reservation and usage tracking of shared resources like hot desks and conference rooms. Technical personnel were more likely than IT middle management to think this is needed. Demand was also highest in midsized and large enterprises.

FIGURE 45. HAS THE PRESENCE OF HYBRID WORKERS IN YOUR ORGANIZATION CREATED ANY INTEREST IN USING LOCATION-BASED SERVICES TO FACILITATE THINGS LIKE RESERVING AND TRACKING THE AVAILABILITY OF HOT DESKS, CONFERENCE ROOMS, AND OTHER RESOURCES IN OFFICE ENVIRONMENTS?

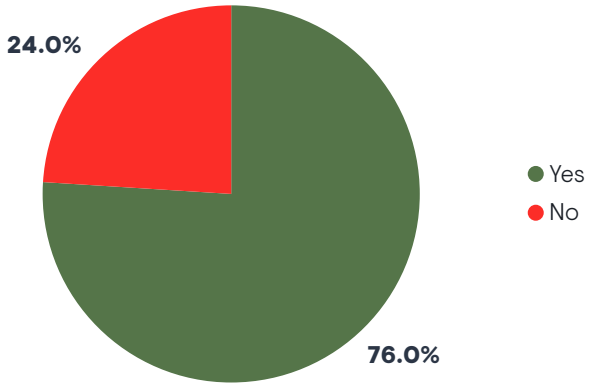


Sample Size = 341

Unified Network Access Policies

With users distributed across corporate offices and homes, IT organizations will increasingly need a unified approach to how they manage network access. **Figure 46** reveals that 76% of organizations need to unify access policies and controls across on-premises networks and the home offices of employees. This requirement was least prominent in organizations that rely on VPNs for secure remote access. Larger companies were more likely to need policy unification.

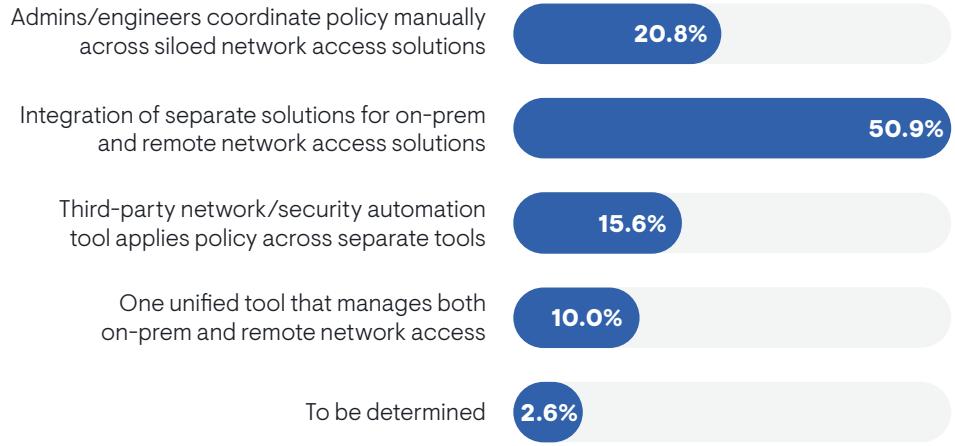
FIGURE 46. DOES YOUR ORGANIZATION NEED TO UNIFY NETWORK ACCESS POLICIES ACROSS ON-PREMISES NETWORKS AND THE HOME OFFICES OF EMPLOYEES?



Sample Size = 354

Figure 47 reveals how organizations intend to unify these access policies. The majority try to integrate siloed solutions for on-premises and remote access solutions. These organizations tended to be less successful with their overall support of remote workers.

FIGURE 47. YOU INDICATED THAT YOUR ORGANIZATION NEEDS TO UNIFY NETWORK ACCESS POLICIES ACROSS ON-PREMISES NETWORKS AND HOME OFFICES. HOW WILL YOUR ORGANIZATION ACHIEVE THIS UNIFICATION?

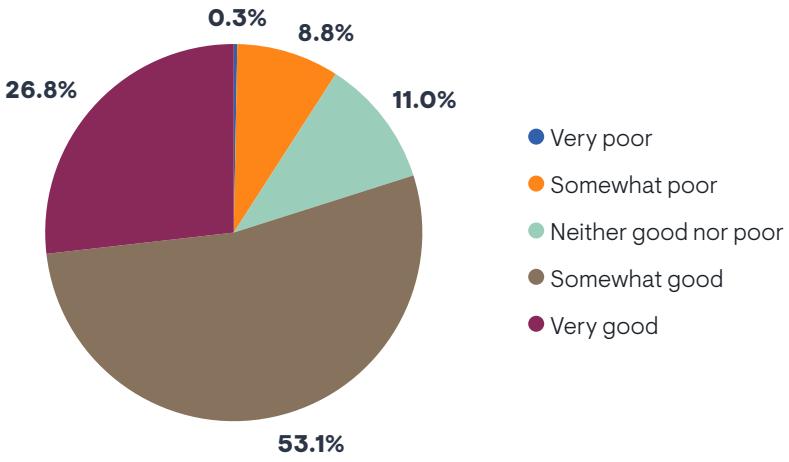


Nearly 37% keep their solutions siloed, with most of this second group manually coordinating policies across siloed solutions (21%) and the rest (16%) using a third-party automation solution to coordinate. Technical personnel were more likely than executives to perceive manual coordination of policy, suggesting that executives are not aware of how much work is being done manually. Only 10% claim to have a single unified solution for access control.

Sample Size = 269

Figure 48 reveals how effective organizations are with unifying policy management across on-premises networks and home offices. Only 27% are completely confident in their abilities to execute. The majority (53%) feel okay, but see room for improvement. EMA found that organizations that use SD-WAN for secure remote access were the most confident in their ability to unify policy management. Users of SASE and VPNs were less confident. Midmarket enterprises were more confident than larger companies. Members of network engineering and IT service management teams were the most pessimistic, while the CIO's suite, IT architecture, and network operations were more optimistic.

FIGURE 48. HOW DO YOU FEEL ABOUT YOUR ORGANIZATION'S ABILITY TO CONSISTENTLY MANAGE NETWORK ACCESS POLICIES ACROSS YOUR ON-PREMISES NETWORKS AND THE HOME OFFICES OF YOUR REMOTE USERS?



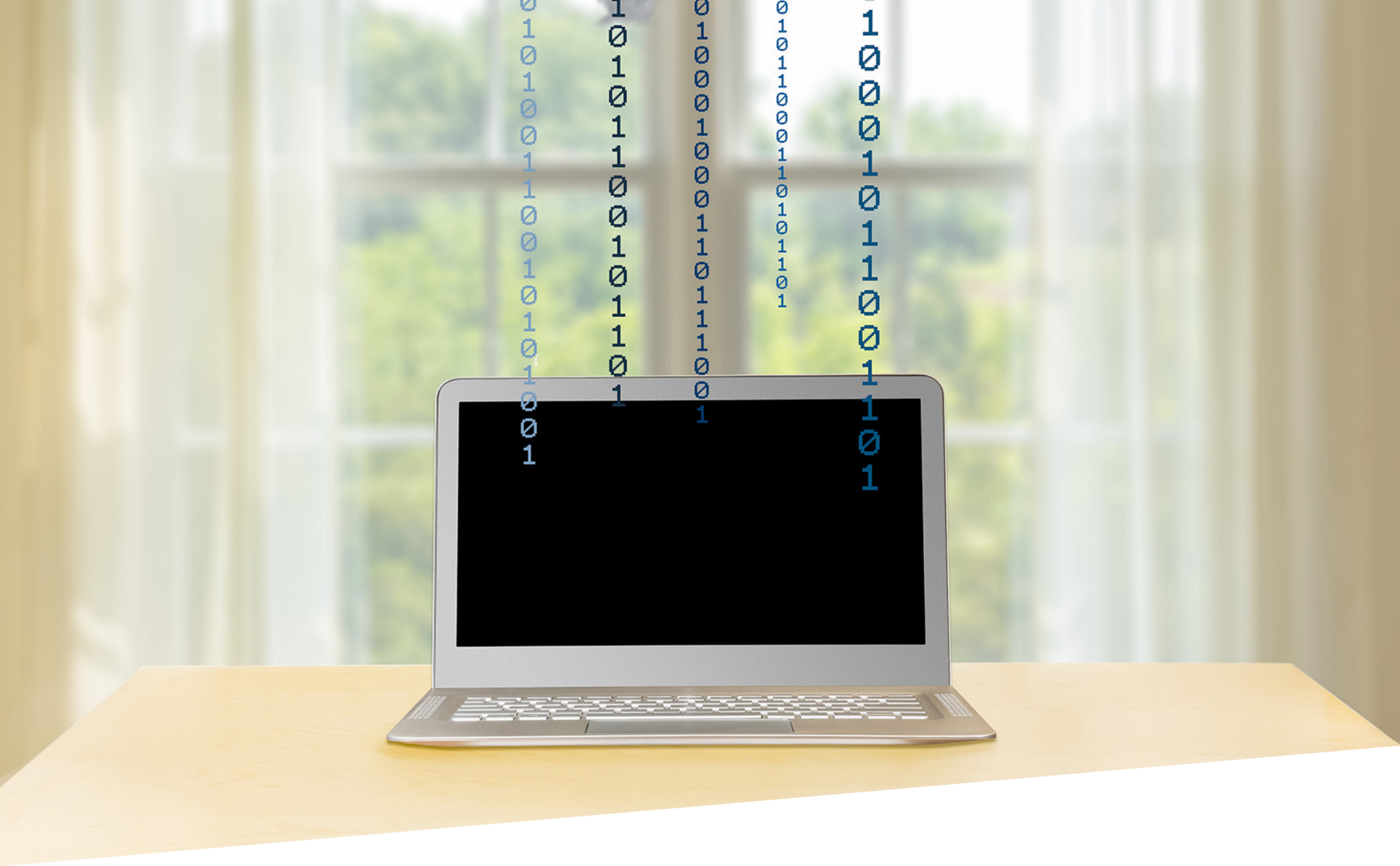
Sample Size = 354

Critically, EMA discovered that organizations that are more effective with unifying access policies across on-premises networks and remote users reported higher productivity gains with remote work. EMA suggests that an effective approach to unified policies removes friction from the home office user experience. We also found that effective unification of access policies correlates with reduced concerns about the security compliance risks associated with remote and hybrid work.

Organizations that rely on manual coordination of policy management were split, with many feeling effective and others feeling ineffective with their unified approach to policy management. Organizations that integrate their access control systems tended to be less effective with unified policy management. Organizations that used third-party automation tools were feeling neutral about their overall effectiveness.

Other factors that correlated with effective unification of access polices:

- The network team has sufficient influence over how remote workers are supported
- Security policies and customer satisfaction drive remote user networking strategies
- Organizations try to balance security and user experience rather than sacrifice experience for security
- Organizations look for secure remote access solutions that have integrated network security solutions
- Expectations for a higher population of remote workers in 2025
- Satisfaction with tools used to track locations of hybrid workers



Conclusion

Given that enterprises have empowered a growing number of their employees to work from wherever they want, whether as full-time remote users or hybrid workers, secure and reliable connectivity will be essential to productivity and collaboration. Although the network team rarely leads organizations' strategy for supporting remote work, it has a critical role to play.

This research found that it better supports remote work when the network infrastructure and operations group has sufficient influence. These network teams are increasing their use of alternative approaches to VPNs for secure remote access, like SASE, ZTNA, and emerging high-performance services specifically designed for hybrid work. They are deploying network hardware from employees' homes to where appropriate. They are adopting new network monitoring and observability tools to improve how they manage the network experience of remote workers.

Moreover, the rise of hybrid work is having an impact on the on-premises network. Hybrid workers rely on rich, real-time communications applications for collaboration, and these applications are putting pressure on network teams to increase available bandwidth. Hybrid workers are also more mobile within an office requiring expansions and updates to Wi-Fi networks. As these hybrid workers float between on-premises and home networks, there is also a need to unify network access policy.

Given all these factors, networking professionals have a job to do. They must seize leadership roles as much as possible to ensure that remote and hybrid workers have secure access to high-performing network connectivity no matter where they are located on a given day. Despite attempts by some employers (and commercial real estate interests) to push people back to the office, the proliferation and expansion of remote and hybrid work is a permanent reality both in North America and Europe.

Appendix: Demographics

FIGURE 49. WHICH OF THE FOLLOWING BEST DESCRIBES YOUR ROLE IN THE IT ORGANIZATION?

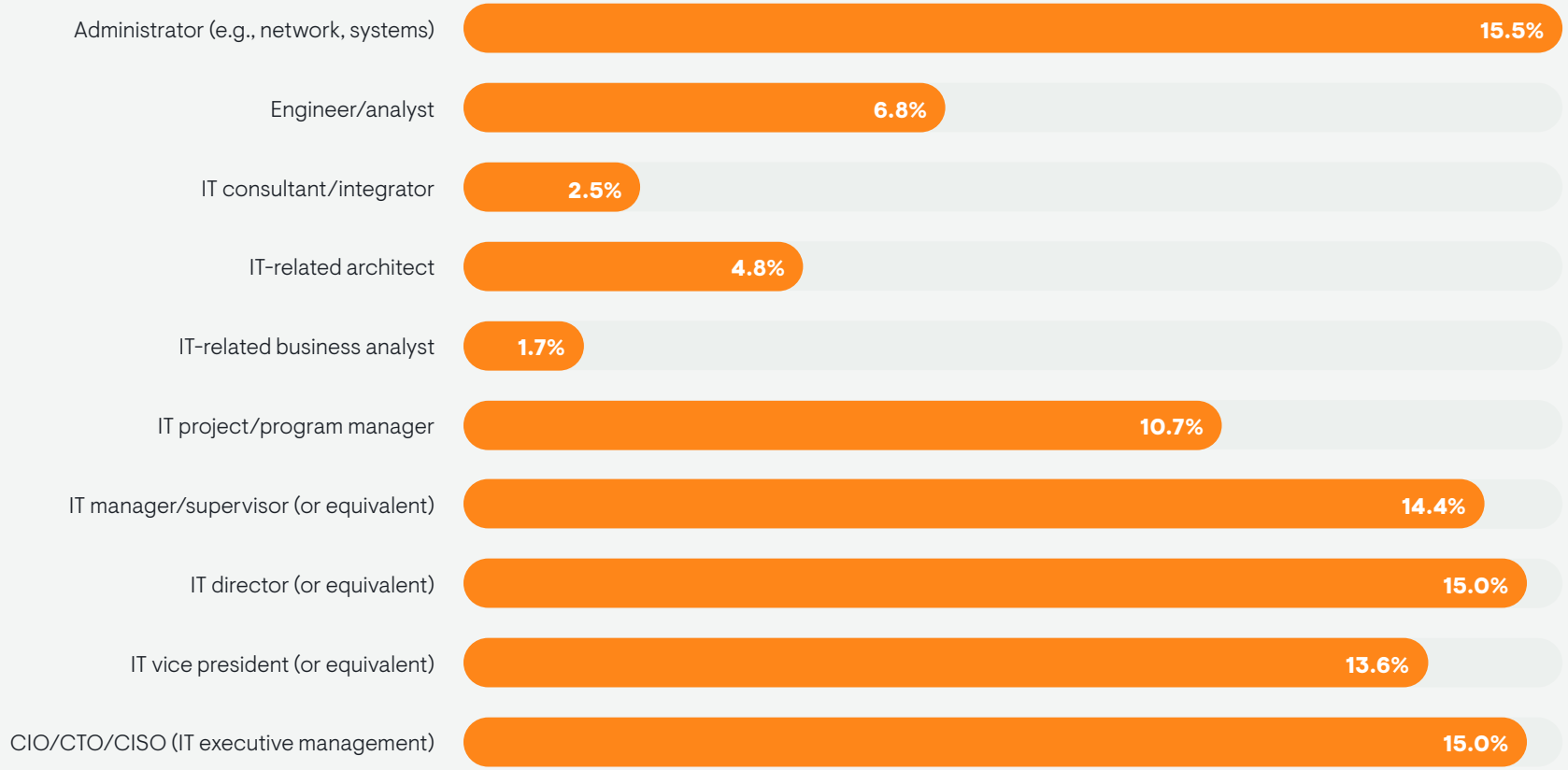


FIGURE 50. WHICH OF THE FOLLOWING BEST DESCRIBES YOUR GROUP WITHIN IT?

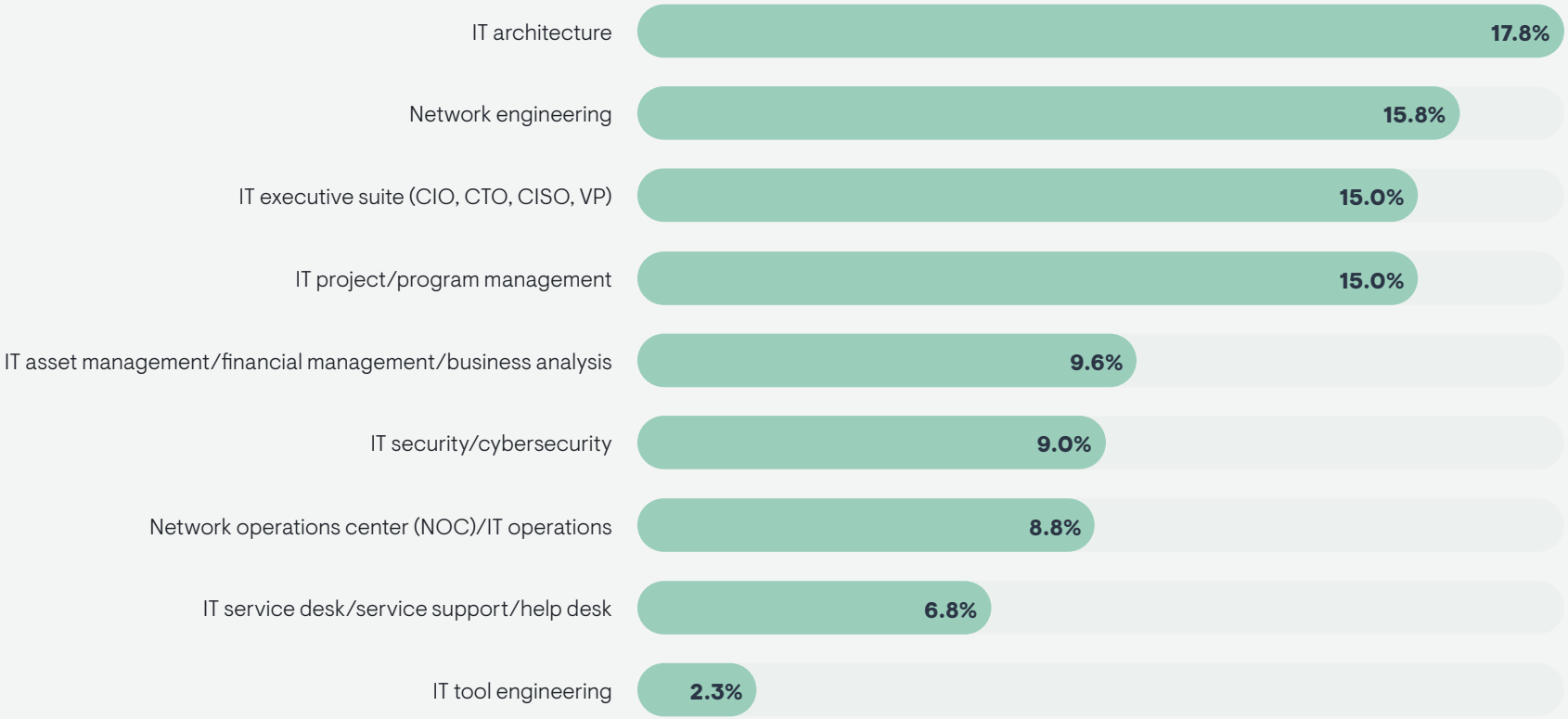
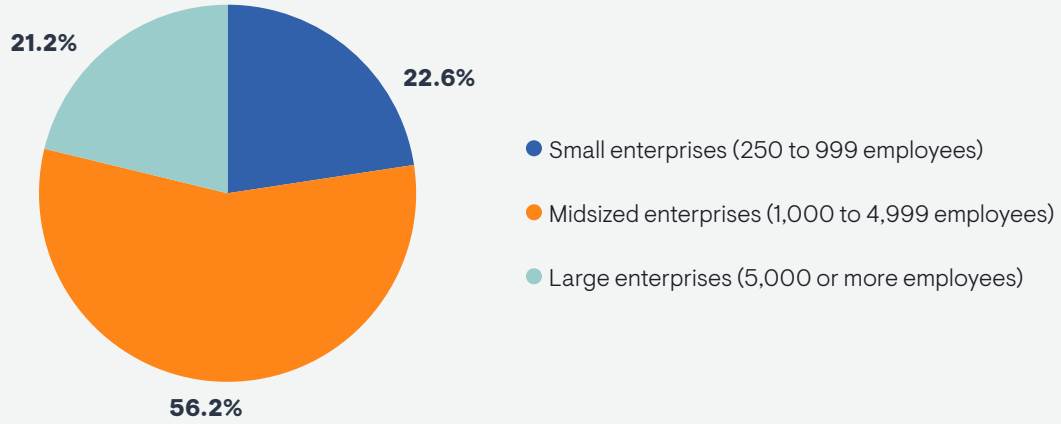
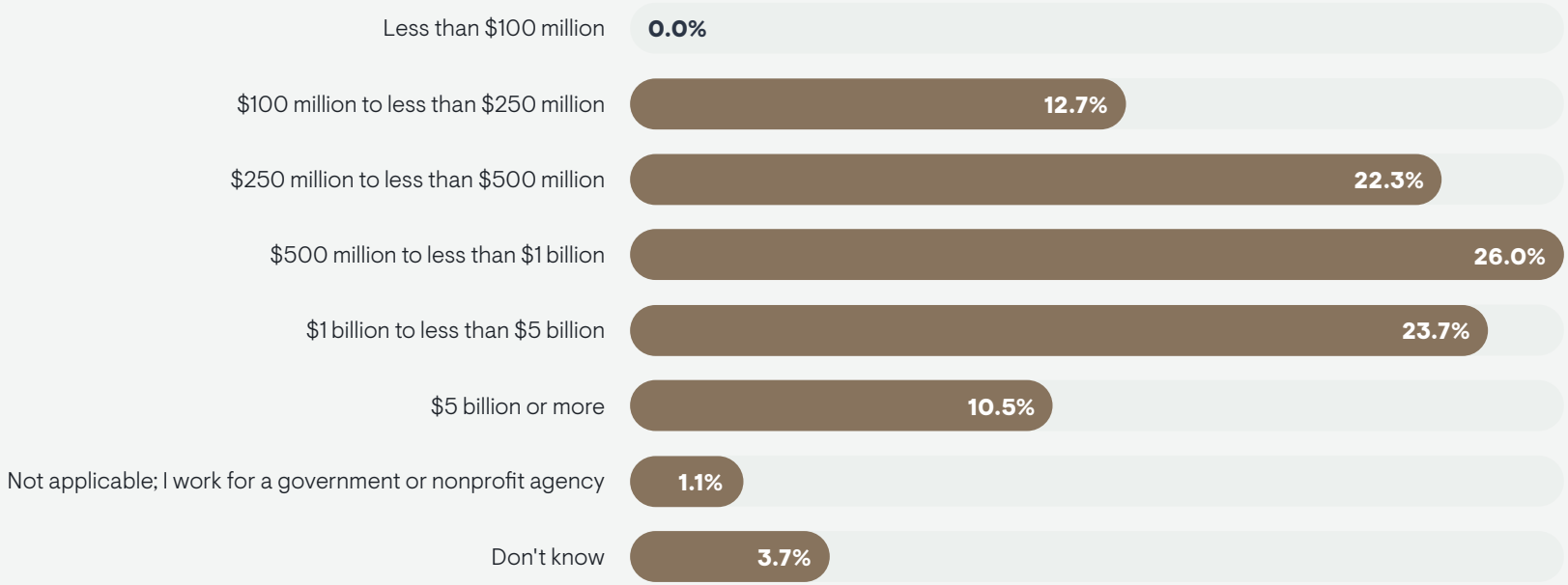


FIGURE 51. HOW MANY EMPLOYEES ARE IN YOUR COMPANY WORLDWIDE?



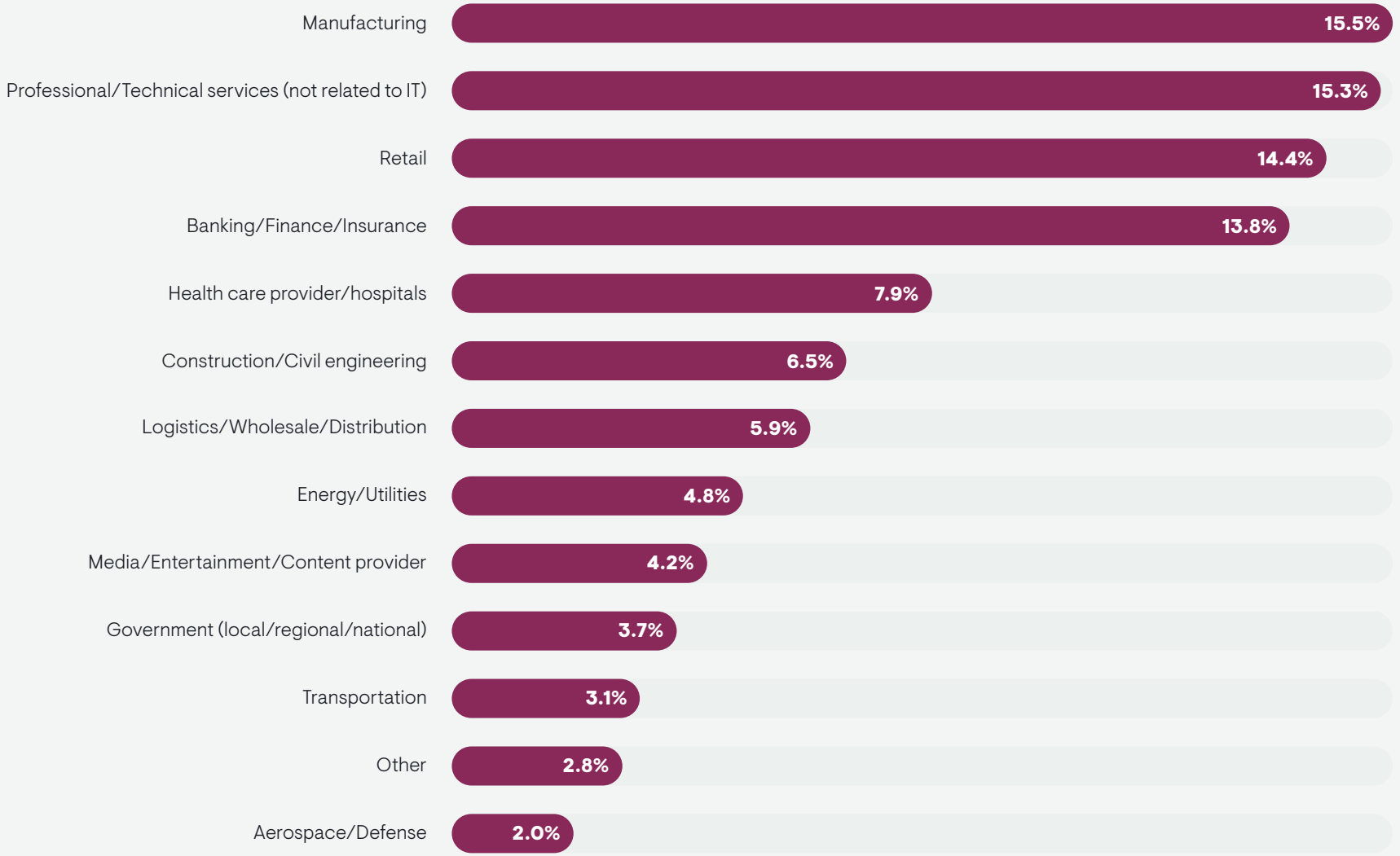
Sample Size = 354

FIGURE 52. WHAT IS YOUR ORGANIZATION'S ANNUAL SALES REVENUE?



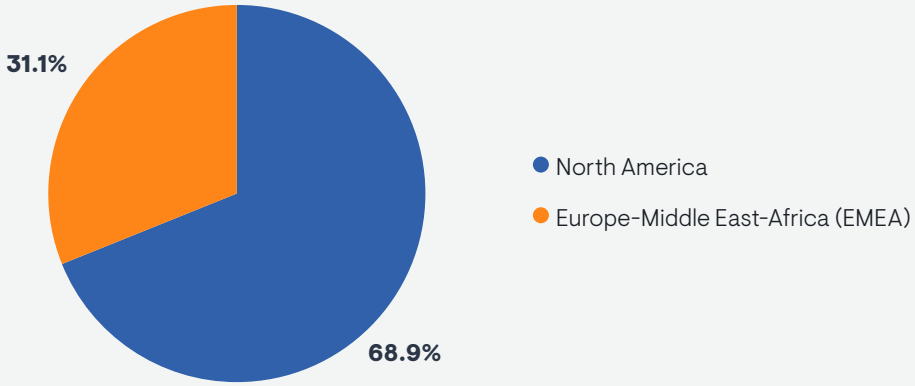
Sample Size = 354

FIGURE 53. WHICH OF THE FOLLOWING BEST DESCRIBES YOUR COMPANY'S PRIMARY INDUSTRY?



Sample Size = 354

FIGURE 54. IN WHICH REGION ARE YOU LOCATED?



Sample Size = 354

Case Study: Global 500 Media Company Sees 8x Boost to Remote Worker Experience with Cloudbrink

With nearly all its 15,000 employees permanently working from home on at least a part-time basis post-pandemic, a major division of a multi-billion-dollar global media company transformed its approach to secure remote access with Cloudbrink, a provider of hybrid access as a service (HAaaS).

Searching for a Solution

At the beginning of the COVID-19 pandemic, the IT organization scaled up its legacy VPN technology to support its remote workers. "We pushed [the VPN] out to everybody not knowing how it was going to affect certain groups," said the company's director of IT infrastructure. "We realized it was not something we could sustain long-term."

The IT organziation recognized that end-user experience for employees working on video games, films, and television was a major issue. Many of those workers were using applications sensitive to network performance, and they frequently had to transfer very large files from their home offices. The legacy VPN solution could not support this bandwidth demand, and it did nothing to mitigate performance issues associated with the Wi-Fi access points and internet service providers that connected employees from home.

The IT organization tested around 20 alternative VPN, zero trust network access (ZTNA), and software-defined perimeter (SDP) solutions, but none of them were able to deliver the combination of security and performance that was needed.

The IT organization next tried using an SD-WAN solution, deploying SD-WAN devices in the homes of the 3,500 employees who were most impacted by performance issues. The SD-WAN solution offered some performance improvement, but not enough. Also, the cost of managing and deploying the hardware and maintaining the software licenses for those edge deployments was much too high. The IT organization wanted to boost performance higher but minimize costs.

Solving Remote Access Problems with Cloudbrink

That's when the IT organization discovered Cloudbrink. Cloudbrink enables secure remote connectivity with the same lightweight agent that one expects from a VPN or ZTNA solution, but it goes a step further by offering an SD-WAN-like quality of experience capabilities with its hybrid access as a service offering. It maintains a network of edge points of presence (PoPs) globally that guarantees a short path from the user to a Cloudbrink gateway. The Cloudbrink service is available to customers in an as-a-service consumption model, which means no software management and maintenance overhead. The solution also uses a proprietary stateless protocol that remediates jitter, delay, and packet loss and steers traffic around bad network paths.

The media company saw immediate results with Cloudbrink. "On average, we're seeing performance improve by a factor of four to eight times," said the director of IT infrastructure. "It makes a big difference, especially when users are reaching out to applications that reside in different offices around the world. Cloudbrink's intelligence for low-latency, quickest-hop routing has been a game-changer."

The director also said, "The performance boost has been so stark that many users have returned their SD-WAN gateways, preferring to rely on Cloudbrink. Of the 3,500 SD-WAN appliances the IT organization shipped to homes, only 500 remain in the field."

In terms of increased productivity, "The studios really need the speed. A game build consists of hundreds of thousands of files. Before Cloudbrink, they would start a file transfer at the end of the day and hope it would be done in the morning. Now, we watch them do those same transfers in one or two hours. They're able to do multiple transfers per day."

All this was achieved without any sacrifice around security, the main driver of any remote access solution. “Our info security group put Cloudbrink through the wringer. We wanted to make sure they could provide a secure connection from end to end. We also like their role-based access control in the administrative environment, and Cloudbrink has been able to tie into our logging infrastructure.”

The IT organization now considers Cloudbrink a true business partner. Twenty-five percent of its employees are experiencing excellent secure productivity using the solution today, and they see a future in which 100% are onboarded. The company is also considering using the technology in its own products. For instance, it sees an opportunity to run Cloudbrink agents on its gaming consoles to boost customer experience.

“I haven’t seen anything like it on the market,” the director of IT infrastructure said.

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**.

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

4319.091223