# Enterprise WAN Transformation: SD-WAN, SASE, and the Pandemic

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

Sponsored by:

LiveAction

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

# Enterprise WAN Transformation: SD-WAN, SASE, and the Pandemic

## Table of Contents


Executive Summary ..... 1
Introduction ..... 1
Demographics Overview ..... 2
The Hybrid WAN ..... 3
- Internet Connectivity ..... 3
- Wither MPLS? ..... 4
- Drivers of Internet-Based WAN Architecture ..... 5
- Hybrid WAN Outcomes ..... 6

Software-Defined WAN in the Enterprise ..... 7
- Solution Requirements ..... 9
- Integrated Secure Remote Access ..... 10
- SD-WAN Security ..... 12
- Operationalizing SD-WAN ..... 14
- SD-WAN Outcomes: Success and Challenges ..... 18

Secure Access Service Edge Insights ..... 19
- Ranking SASE Platform Attributes ..... 20
- SASE Engagement ..... 21

WAN Operations ..... 22
- WANOps Success ..... 22
- The Internet's Impact on WANOps ..... 23

The COVID-19 Pandemic and the WAN ..... 25
- The Work-From-Home Impact ..... 25
- Supporting the Remote Worker ..... 28
- SD-WAN and the Pandemic ..... 29
- SASE and the Pandemic ..... 30

Conclusion ..... 31
Case Study: LiveAction ..... 32




EMA

# Enterprise WAN Transformation: SD-WAN, SASE, and the Pandemic

## Executive Summary

This summary report of new Enterprise Management Associates research explores the state of WAN transformation amidst an unprecedented business environment introduced by the COVID-19 pandemic. It takes a comprehensive approach at reviewing how enterprises evaluate, implement, and operationalize SD-WAN. It looks at early engagement with SASE and it examines how the pandemic has affected WAN transformation.

## Introduction

Wide-area networks (WAN) have gone through profound transformation over the last six years. Cloud services have been a major driver of this change, as has the emergence of the internet as a source of affordable, high-bandwidth WAN connectivity. In the middle of the last decade, a set of technologies emerged to enable these transformational drivers. The industry referred to this technology as software-defined WAN (SD-WAN).

Enterprise Management Associates (EMA) began publishing biennial research on WAN transformation in 2016. The primary motivation for launching this ongoing research project was recognition of the expanding acceptance of SD-WAN technology as an enabler of network transformation. EMA has been continuously surveying enterprise IT decision-makers about how they use SD-WAN to build hybrid networks, establish connectivity for cloud-based applications and services, streamline network operations, improve network security, and reduce costs.

This report summarizes the findings of new research, based on a survey of 303 IT professionals, that explores the state of WAN transformation in 2020. It looks at the adoption of the internet for frontline WAN connectivity and identifies best practices for SD-WAN implementation and operationalization.

## Demographics Overview

This research surveyed 303 IT professionals with direct and current experience with their organizations' WANs. They all had some combination of responsibility for evaluating, purchasing, implementing, and/or operationalizing WAN technologies.

**Top Job Titles**

- 22% IT director
- 19% CIO/CTO/CISO
- 17% IT manager/supervisor
- 15% Network architect
- 10% Project manager
- 6% Network operations staff/analyst

**Top IT Groups**

- 28% IT executive suite
- 21% IT architecture
- 21% Project/program management
- 12% Network operations center/ IT operations
- 9% IT security/cybersecurity
- 9% Network engineering

**Company Size (Employees)**

- 22% Midsized (250 to 999)
- 63% Large (1,000 to 9,999)
- 15% Very Large (10,000+)

**Geography**

- 14% Australia
- 35% Europe
- 50% North America

**Top Industries**

- 19% Manufacturing
- 11% Finance/Banking/Insurance
- 9% Retail/Wholesale/ Distribution
- 9% Construction
- 9% Software
- 8% IT-related consulting or professional services
- 7% Aerospace/Defense
- 7% Healthcare/Medical/ Pharmaceutical

**Figure 3** reveals the size and scope of the networks represented by this research. EMA excluded smaller networks (fewer than 10 sites) from its survey.

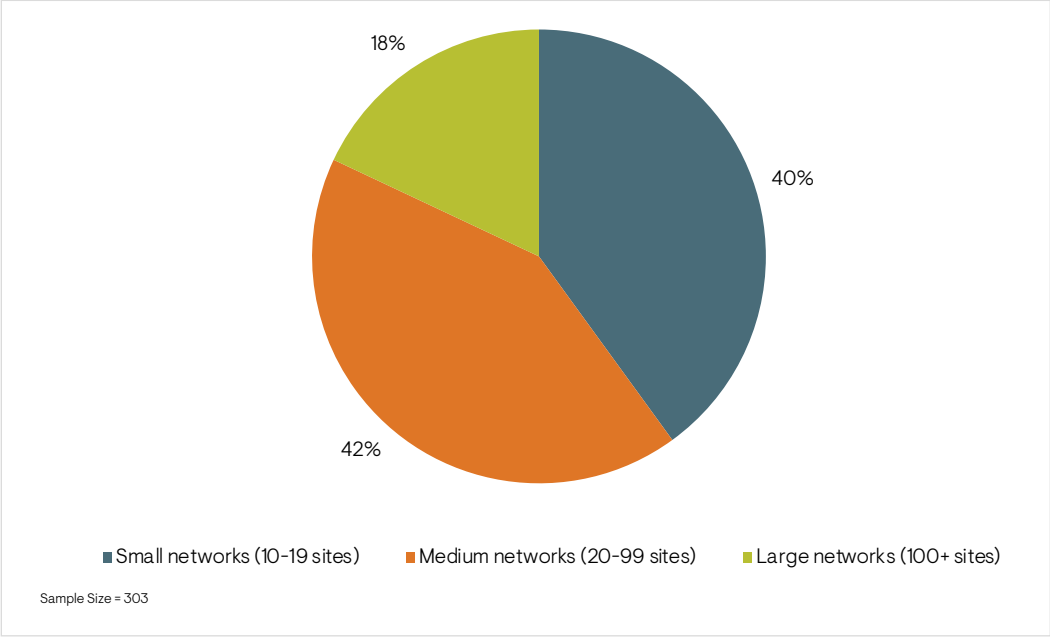


*Figure 3. Number of WAN-connected corporate sites*

## The Hybrid WAN

Before examining SD-WAN engagement, EMA first explored a major driver of SD-WAN adoption: the hybrid WAN. Managed WAN services, such as MPLS, continue to play a significant role in enterprise networks, but the internet has proven itself a viable option for WAN connectivity, even essential in the case of direct cloud connectivity. Many enterprises are adopting hybrid networks, a combination of managed WAN services and internet, to address a variety of WAN requirements.

### Internet Connectivity

**Figure 4** reveals that 98% of enterprises plan to increase their use of the internet in their WAN architecture. Sixty-five percent have done this already, while 28% are making the change today. EMA found that enterprises with larger networks (more sites) tend to be more advanced with this changeover. EMA also found that North American respondents (73%) and Europeans (60%) were more likely to already have incorporated the internet into their networks, versus only 49% of Australians. Aerospace, construction, manufacturing, IT consulting and professional services, and retail companies are all more likely to be using hybrid networks today, while education, government, and general professional services organizations are less likely.

***98% of enterprises plan to increase their use of the internet in their WAN architecture.***

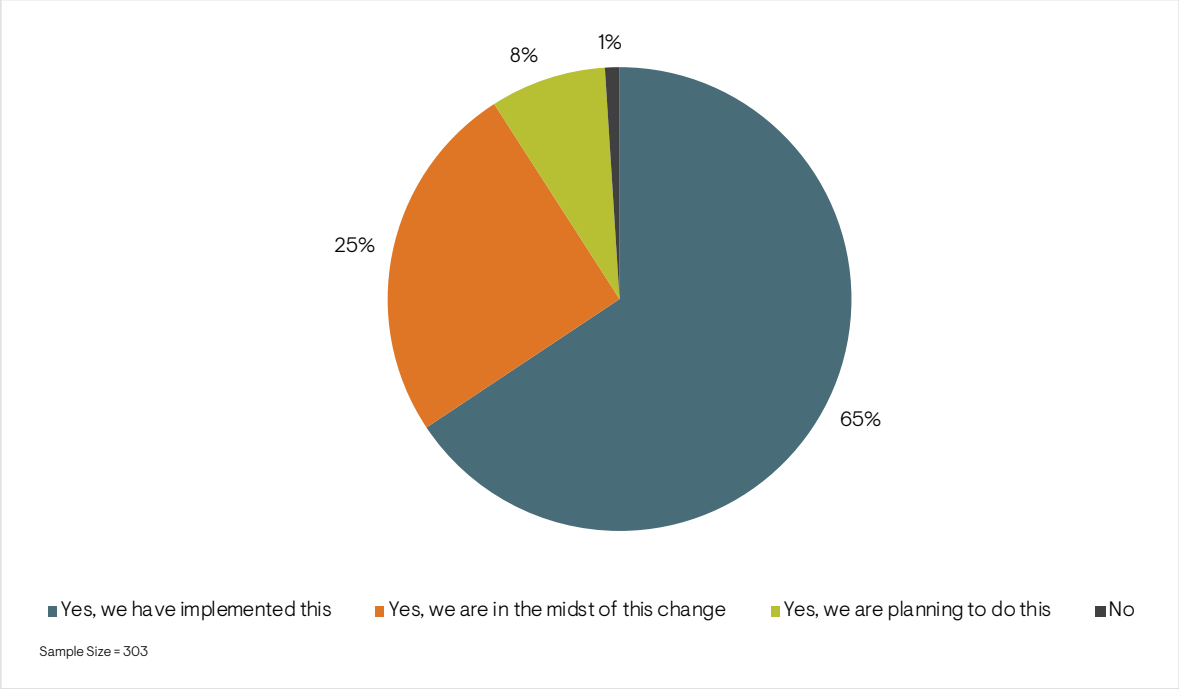


*Figure 4. Is your organization planning to increase its use of the internet as a primary option for connecting sites to your WAN?*

## Wither MPLS?

The implication of internet-based WANs is that managed WAN services like MPLS will fade away. **Figure 5** reveals that this is not the case. Of enterprises that are expanding the role of the internet in their network architecture, more than half are making no change to their MPLS footprint. For them, the internet is supplementing the managed WAN services they already have. Only 17% of companies are actually retiring most of their MPLS connectivity. Another 23% are reducing their overall MPLS bandwidth in favor of the internet, but not entirely replacing it.

***Only 17% of companies are actually retiring most of their MPLS connectivity.***

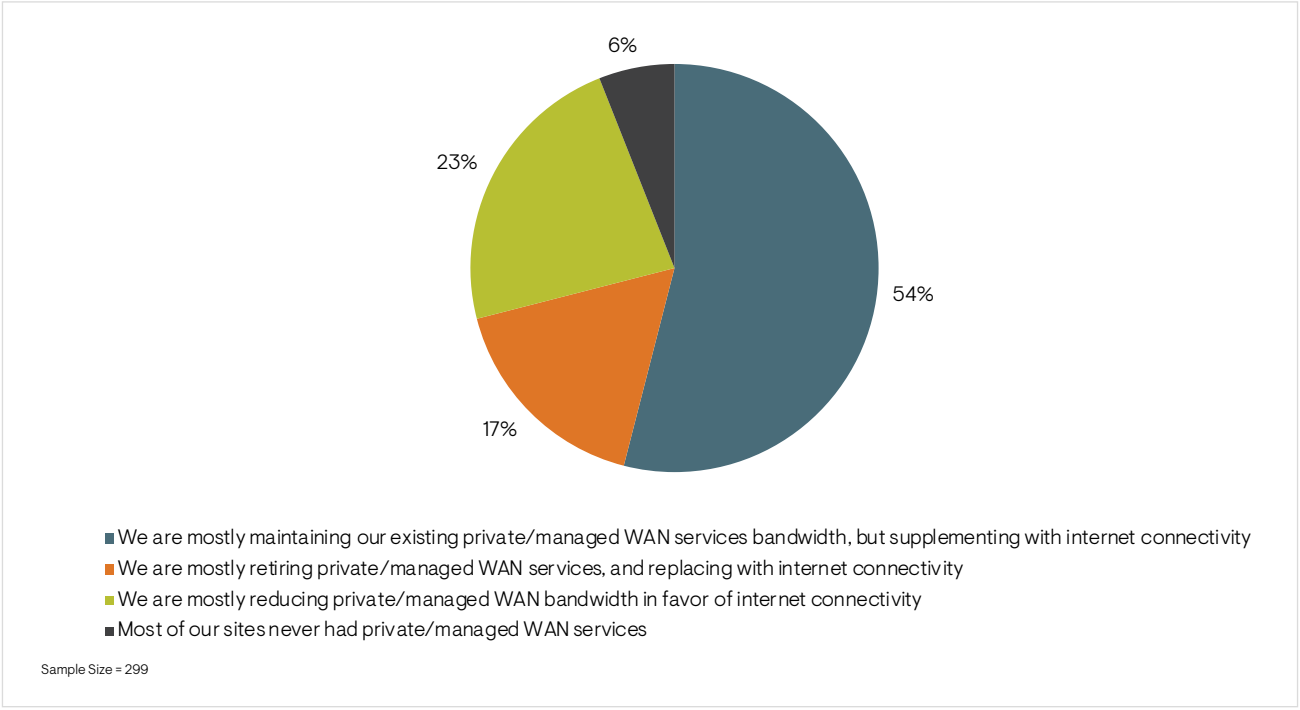


*Figure 5. How increased use of the internet affects existing investments in managed WAN services, like MPLS*

## Drivers of Internet-Based WAN Architecture

It is indisputable that the internet has become essential to enterprise WAN architecture. **Figure 6** reveals the primary drivers of this transition. IT organizations are trying to enable connectivity to cloud services and increase network flexibility. Secondarily, they see the internet as a means to addressing high bandwidth requirements, since MPLS services are often bandwidth constrained. They recognize that ISPs are able to provision and activate internet services much more quickly than network providers can deliver managed WAN services. These four top drivers of internet-based WAN are identical to EMA's findings from 2018.

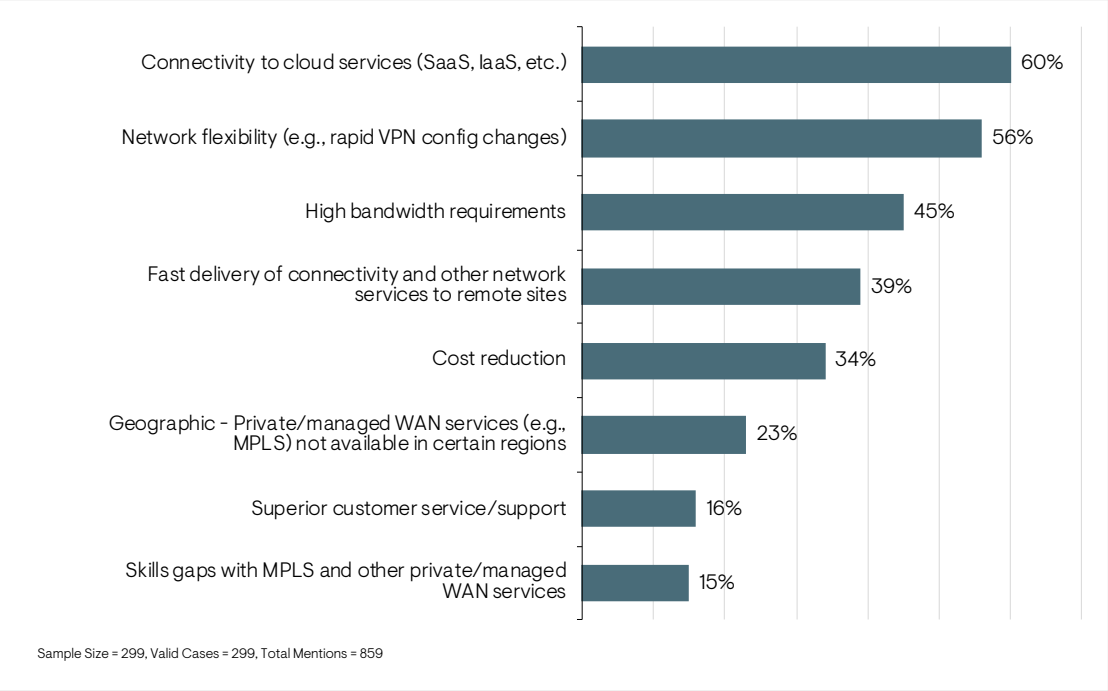


*Figure 6. Drivers of using the internet for primary WAN connectivity*

## Hybrid WAN Outcomes

Although the internet is less reliable than managed WAN services, it is a ready source of affordable, high-bandwidth connectivity. Most enterprises have seen an improvement in overall performance and user experience since they started relying on the internet for frontline WAN connectivity. **Figure 7** reveals that 92% of the enterprises that have started using internet-based WAN connectivity have observed improvements. Only 39% claim that this improvement is significant.

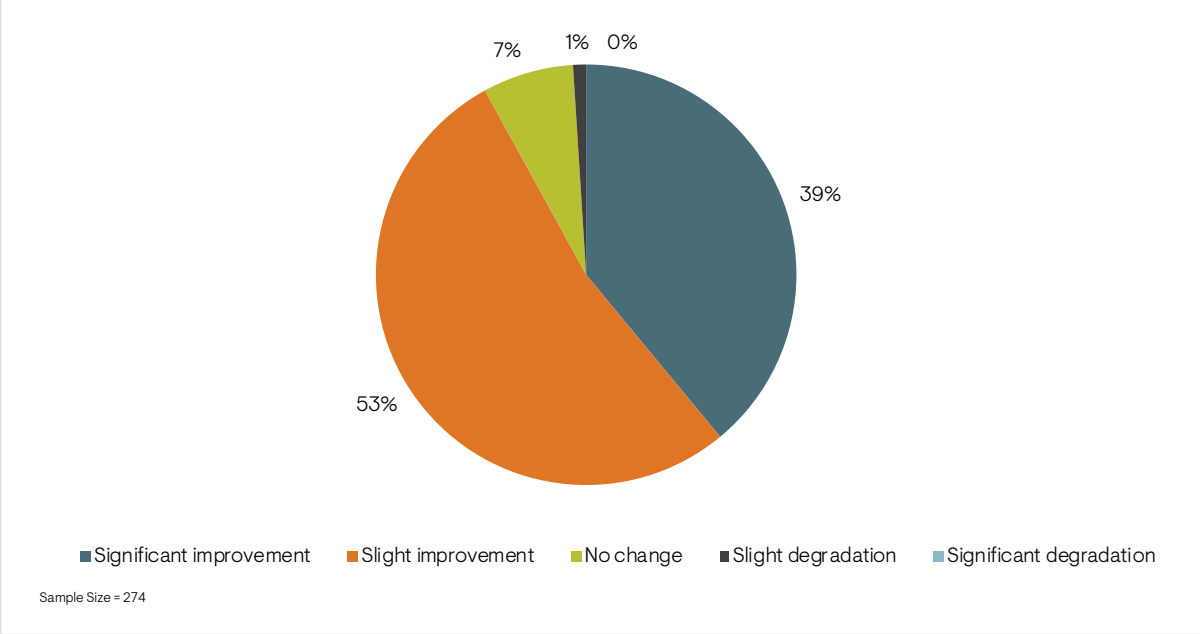


*Figure 7. Observed changes in overall network performance and user experience since implementing internet-based WAN architecture*

The more notable finding here may be that only 1% of enterprises observed any degradation of services. Reducing one's reliance on managed WAN services does not negatively impact end-user experience. This research will reveal that nearly all of these enterprises are engaged with SD-WAN.

***Reducing one's reliance on managed WAN services does not negatively impact end-user experience.***

## Software-Defined WAN in the Enterprise

**Figure 8** reveals that 98% of enterprises are engaged with SD-WAN. The technology is fully implemented in 37% of them. Two years ago, EMA found only 28% of enterprises had completed an SD-WAN implementation.

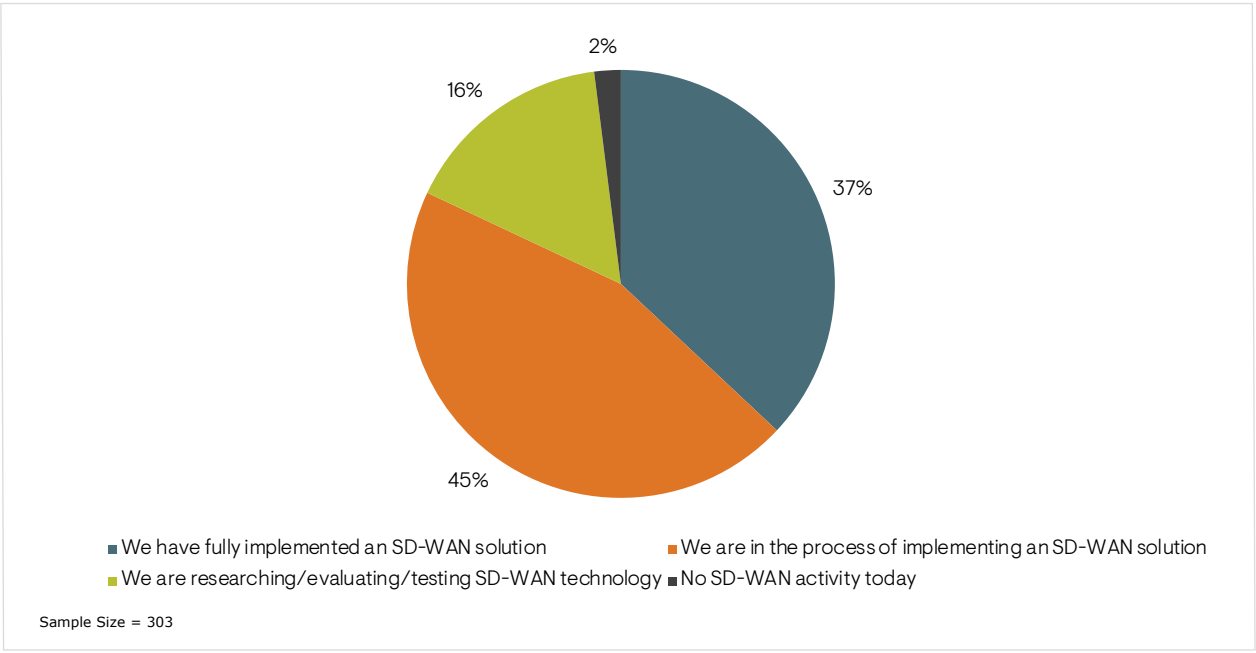


*Figure 8. SD-WAN engagement*

## Managed Versus DIY SD-WAN

**Figure 9** reveals enterprise preferences for procuring and implementing an SD-WAN solution. Only 12% of enterprises take a do-it-yourself (DIY) approach, in which the design, installation, and configuration of SD-WAN is handled in-house. A large majority prefer a managed service, whether from a vendor, its channel partners, or a network service provider. More than one quarter are still undecided on their preference. Managed SD-WAN is an apparent best practice. Enterprises that are successful with SD-WAN technology are more likely (74%) than somewhat successful enterprises (53%) to prefer a managed SD-WAN service offering.

***Enterprises that are successful with SD-WAN technology are more likely to prefer a managed SD-WAN service offering.***

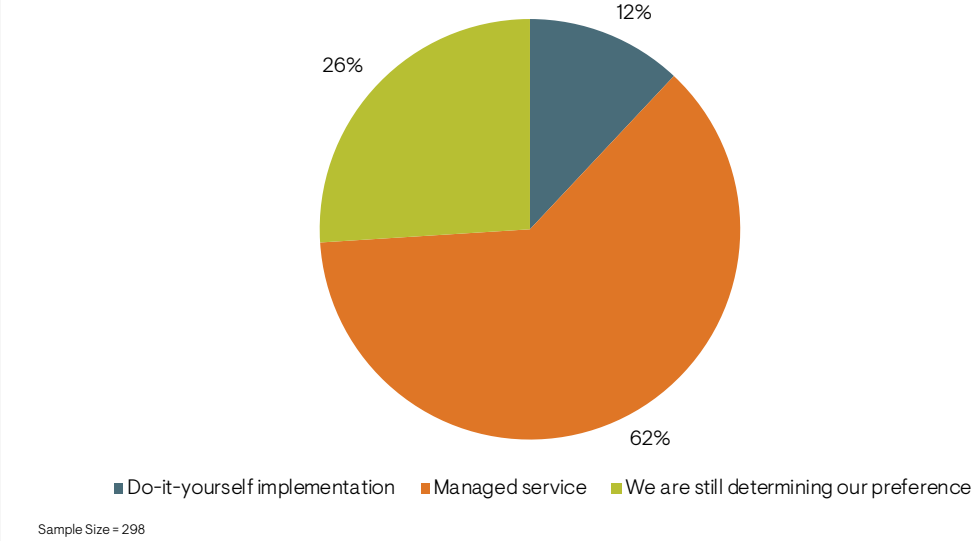


*Figure 9. Procuring and implementing SD-WAN: Do-it-yourself versus managed services*

## Solution Requirements

EMA asked respondents to identify the most important capabilities of their SD-WAN solutions. Hybrid connectivity and integrated security are the most essential, as **Figure 10** details. Hybrid connectivity refers to the ability to aggregate bandwidth across multiple links, including internet and managed WAN services. This improves overall network availability through link diversity. Enterprises that reported success with SD-WAN were more likely (51%) to select hybrid connectivity as a critical feature, versus only 37% of somewhat successful organizations.

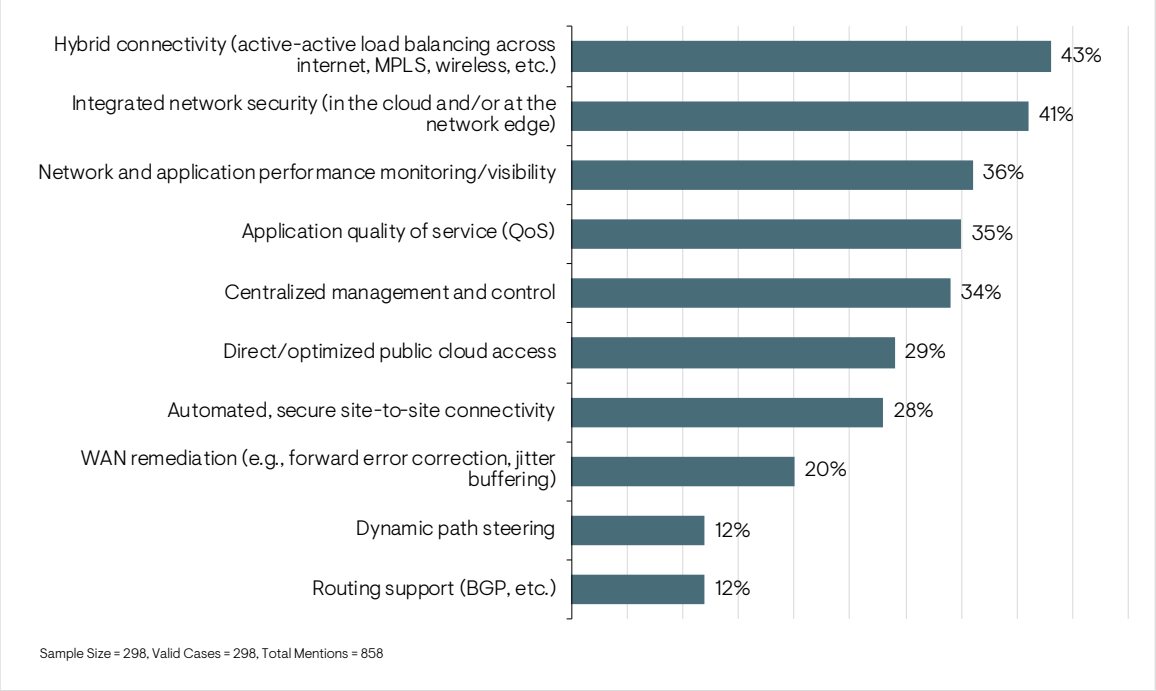


*Figure 10. Most critical SD-WAN product capabilities*

There are other capabilities that can enhance the quality of this hybrid connectivity, such as WAN remediation and dynamic path steering, but research participants consider them less important capabilities overall. SD-WAN vendors tout WAN remediation and traffic steering as differentiators, which will appeal to organizations with stringent performance requirements. However, basic hybrid connectivity remains the foundational requirement of SD-WAN.

Integrated security is the other major requirement of SD-WAN. Later in this research, EMA will find that many SD-WAN investments are driven by a need to improve network security. EMA will also explore some of the requirements they have for this capability. Integrated monitoring, application quality of service tiering, and centralized management and control are the top secondary requirements. Centralized management is a higher priority for organizations that are successful with SD-WAN (41%).

## Integrated Secure Remote Access

Past EMA research found that IT organizations see the potential value of integrating SD-WAN solutions with secure remote access solutions. For instance, this would provide a unified policy management opportunity.

SD-WAN vendors have moved in this direction with the emergence of secure access service edge, which combines cloud security, SD-WAN, and remote access into a single platform. The subsequent rise in work-from-home populations during the COVID-19 pandemic increased interest in this convergence of platforms. EMA asked respondents if they are interested in integrated secure remote access solutions from their SD-WAN vendors. **Figure 11** reveals that 96% of enterprises have interest, and 44% say it would be extremely valuable.

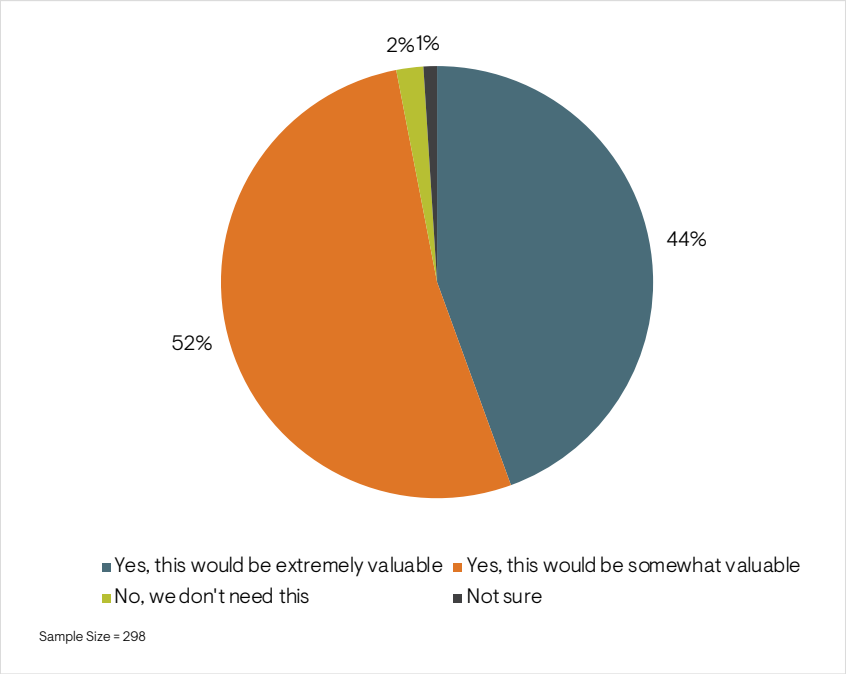


*Figure 11. If your SD-WAN vendor offered an integrated security remote access capability, would you adopt it?*

If enterprises do move forward with supporting remote users with SD-WAN, the technology offers several functions that could be useful, beyond a simple VPN replacement. **Figure 12** reveals what enterprises think SD-WAN can do for them. Obviously, secure remote access is the most important one. The site-to-site tunneling capabilities of SD-WAN vendors can be used to create a secure remote connection for home workers. Managers of smaller networks (10 to 19 sites) are the most likely to see the value of this capability.

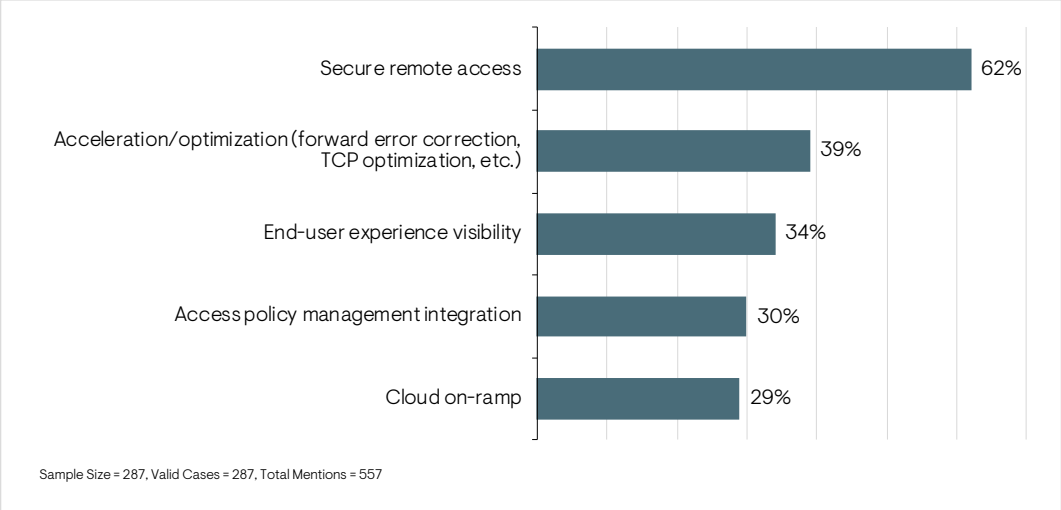


*Figure 12. Which of the following SD-WAN capabilities would be most valuable for supporting remote users?*

Some enterprises see other potential benefits for supporting remote users with SD-WAN. The top secondary opportunity is WAN remediation. Many SD-WAN vendors use features like forward error correction and TCP optimization to improve performance. Nearly two in five enterprises believe this capability can help in home offices. Middle managers (45%) see more potential for remediation than technical specialists (29%). Operators of large networks (100 more sites) are the most interested in this capability (47%).

More than one-third of enterprises believe that the native network and application monitoring capabilities of SD-WAN will translate well to the home office. Slightly fewer are interested in the opportunity to integrate network access policies across SD-WAN and secure remote access. and. Technology specialists are the most likely to see value in policy management integration and cloud access, versus middle management and executive management.

## SD-WAN Security

Earlier, this research found that integrated security is a critically important SD-WAN capability. However, the list of security functions that are integrated into SD-WAN can be rather long. It starts with firewalls and intrusion detection and prevention, but it can also include malware protection, data loss prevention, and cloud access security brokers (CASB). Some vendors offer a broad portfolio of native security technologies that they can layer into an SD-WAN architecture. Others are startups that build out their security offering through partnerships and third-party integrations.

### Native Versus Third-Party Security

Enterprises have a couple of directions to go with SD-WAN security. They can rely on the native security capabilities of their chosen SD-WAN vendor or pursue a best-of-breed, third-party approach. **Figure 13** reveals that only 28% of enterprises expect their SD-WAN vendors to provide a full suite of native security functions. More than one-third prefer integrated third-party solutions. Slightly more say their preference varies depending on the security capability. For instance, this latter group might be perfectly happy with a branch firewall developed by their SD-WAN vendors, but they will prefer a third-party CASB provider to integrate with the SD-WAN solution rather than rely on a native CASB offering.

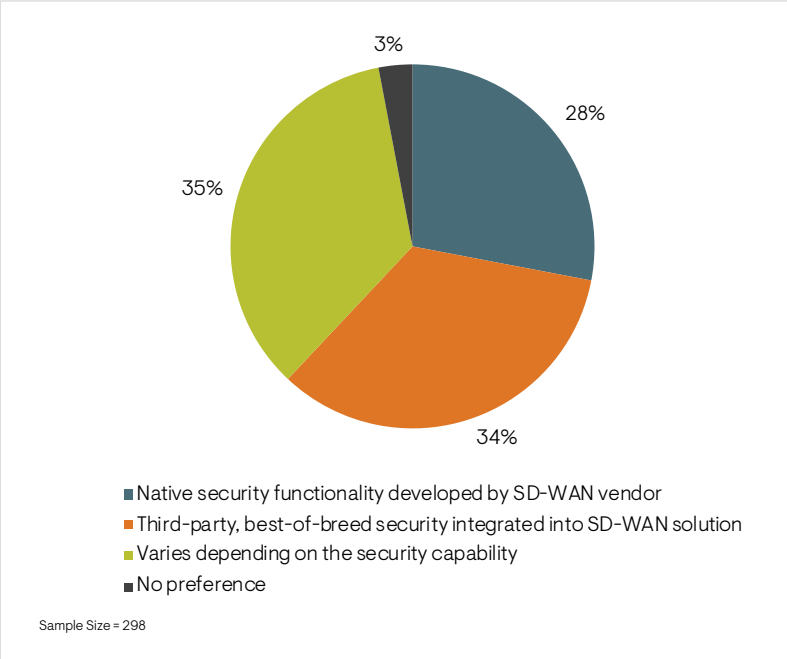


*Figure 13. Native or third-party security technology integrated into SD-WAN architecture*

## Edge Versus Cloud

**Figure 14** reveals deployment preferences for SD-WAN security. Only 16% of enterprises prefer that integrated SD-WAN security capabilities be deployed at the WAN edge. Instead, 44% prefer cloud-based security. A slightly smaller number say the nature of the security capability determines where they want it deployed. Some belong at the edge, and others can be delivered via the cloud. Europeans and Australians are both more likely to take a cloud-only approach, while North Americans are more likely to say their decision is based on the individual security function.

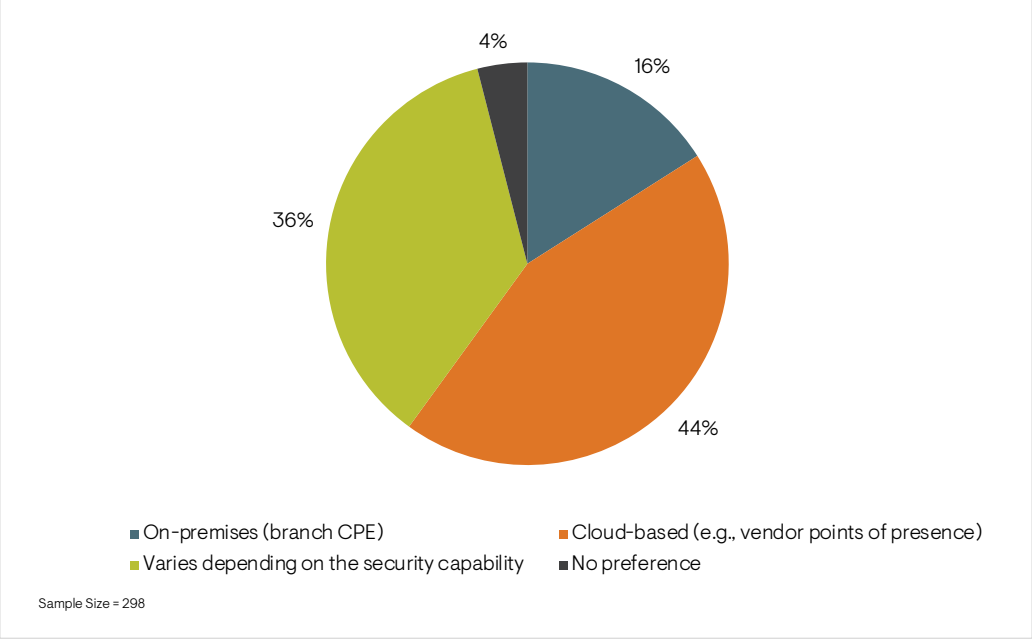


*Figure 14. Preferred deployment model for security technology integrated with SD-WAN architecture*

## Operationalizing SD-WAN

### Who Owns SD-WAN Operations?

While most enterprises consume SD-WAN as a managed service, they do not take a backseat with SD-WAN operations. **Figure 15** reveals the operational models that enterprises adopt with SD-WAN. Sixty-three percent of organizations prefer a hybrid strategy in which the internal network team and the SD-WAN provider share responsibility for tasks, such as change management, monitoring, and troubleshooting. This gives the IT organization direct control over the network without necessarily relying on internal staff for every task.

***Sixty-three percent of organizations prefer a hybrid strategy in which the internal network team and the SD-WAN provider share responsibility for tasks, such as change management, monitoring, and troubleshooting.***

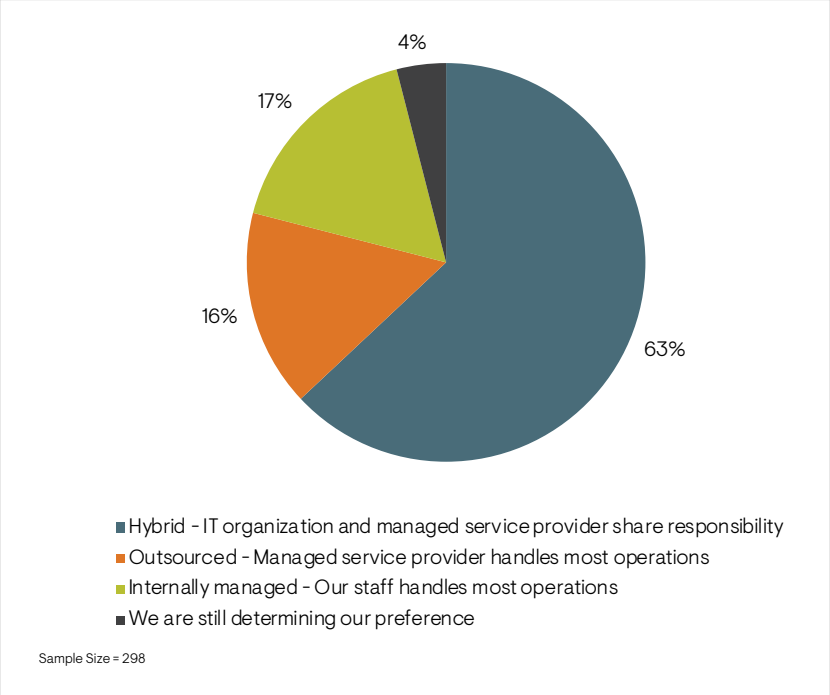


*Figure 15. Preferred approach to SD-WAN operations (change management, monitoring, troubleshooting, etc.)*

## Challenges with Native SD-WAN Monitoring

One distinguishing characteristic of SD-WAN technology is native monitoring. These solutions usually have integrated network and application monitoring features that centralize and streamline monitoring and management of the SD-WAN overlay. EMA asked research participants whether they have encountered any significant problems with these native monitoring features. **Figure 16** reveals that an extraordinary number of enterprises (35%) claim to have no significant challenges with native SD-WAN monitoring capabilities. A "none of the above" option for a question of this type usually receives a no more than 3% or 6%. The results here suggest that most enterprises have generally good results with native SD-WAN monitoring. Unsurprisingly, 44% of enterprises that are successful with SD-WAN claimed to have no significant challenges, versus 26% of enterprises that are only somewhat successful.

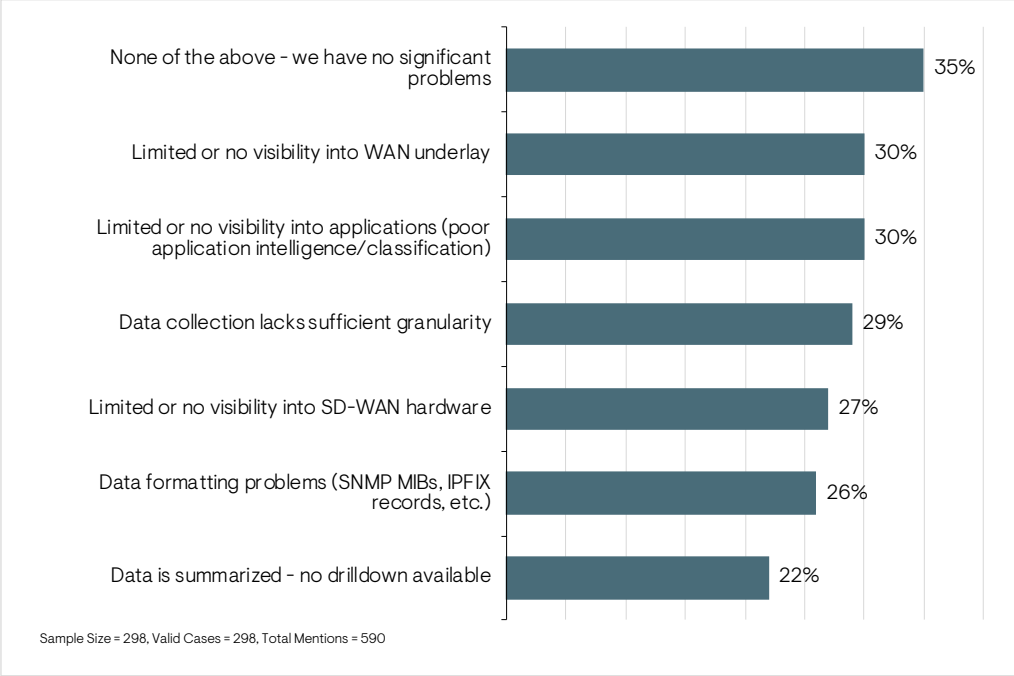


*Figure 16. Significant challenges or shortcomings of native monitoring capabilities of SD-WAN solutions*

Among enterprises that have encountered challenges, the three leading issues are poor visibility into the WAN underlay (e.g., ISP networks), poor visibility into applications (e.g., inferior application classification), and poor granularity in data collection (e.g., long polling intervals). WAN underlay visibility and data granularity are more common challenges for enterprises that are less successful with SD-WAN, suggesting that these are visibility issues that can truly undermine an SD-WAN implementation. Enterprises should carefully evaluate whether a solution will meet their necessities for underlay visibility requirements and data collection granularity.

## Monitoring SD-WAN with Third-Party Tools

Regardless of whether they are happy with the native monitoring capabilities of SD-WAN, 91% of enterprises use or plan to use third-party tools to monitor and manage their SD-WAN technology. Forty-one percent say these third-party monitoring tools are critical to SD-WAN operations. Enterprises that are successful with SD-WAN are more likely to say it is critical (51%).

***91% of enterprises use or plan to use third-party tools to monitor and manage their SD-WAN technology.***

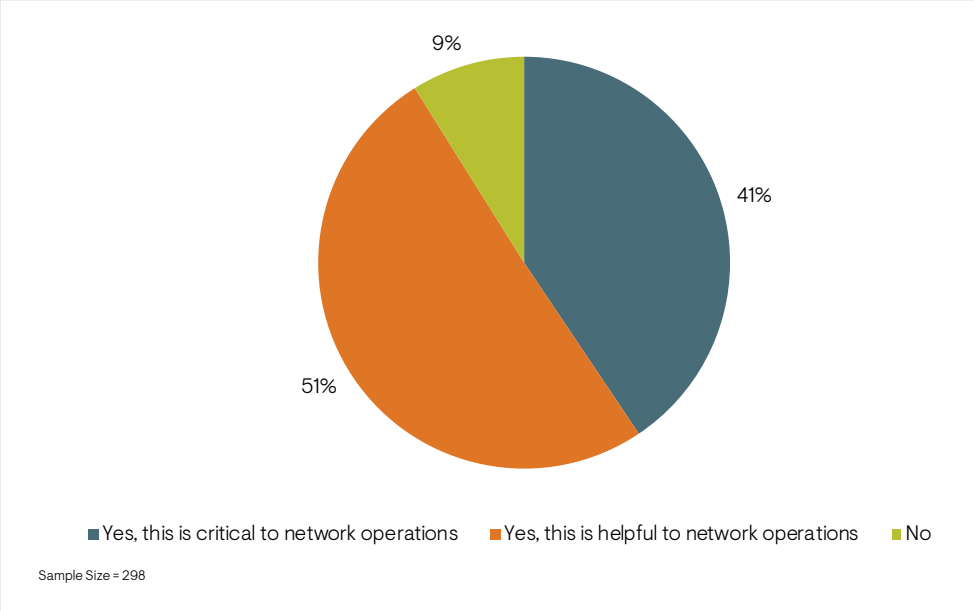


*Figure 17. Ninety-one percent of enterprises use or plan to use third-party network monitoring tools with SD-WAN*

Network engineers, whose visibility requirements are higher than most, are also more likely (63%) to say third-party monitoring is critical. IT consultants (58%) also fall into this camp. Network architects (33%), NOC analysts (6%), and project managers (14%) are the least likely to feel this way.

**Figure 18** reveals that only 48% of enterprises are fully satisfied with their ability to monitor SD-WAN with their third-party tools.

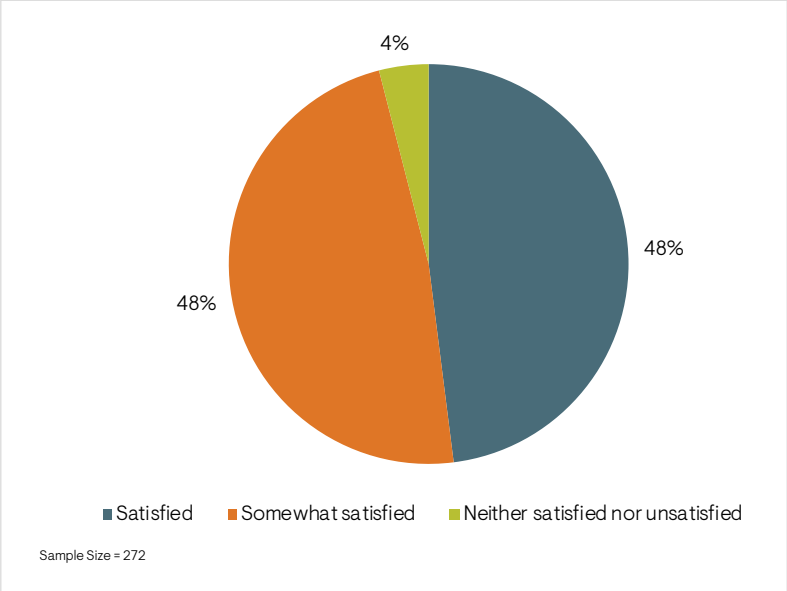


*Figure 18. Satisfaction with third-party monitoring of SD-WAN*

EMA found several correlations between this satisfaction and other aspects of an SD-WAN strategy. Overall, satisfactory third-party monitoring correlates with:

- Managed SD-WAN, rather than DIY
- Adoption or planned adoption of a solution that addresses the internet middle mile
- Preference for native SD-WAN security, rather than third-party
- Satisfaction with native SD-WAN monitoring
- Willingness to acquire new tools to monitor internet-based WAN

## SD-WAN Outcomes: Success and Challenges

### The Benefits of SD-WAN

EMA asked enterprises to identify the most important benefits they have experienced or expect to experience via their adoption of SD-WAN. **Figure 19** reveals that improved network security is the biggest opportunity. Owners of large networks (100 or more sites) and medium networks (20 to 99 sites) are more likely to experience improved security. The aerospace, finance, and software industries were also more likely to improve security with SD-WAN, while healthcare was less likely.

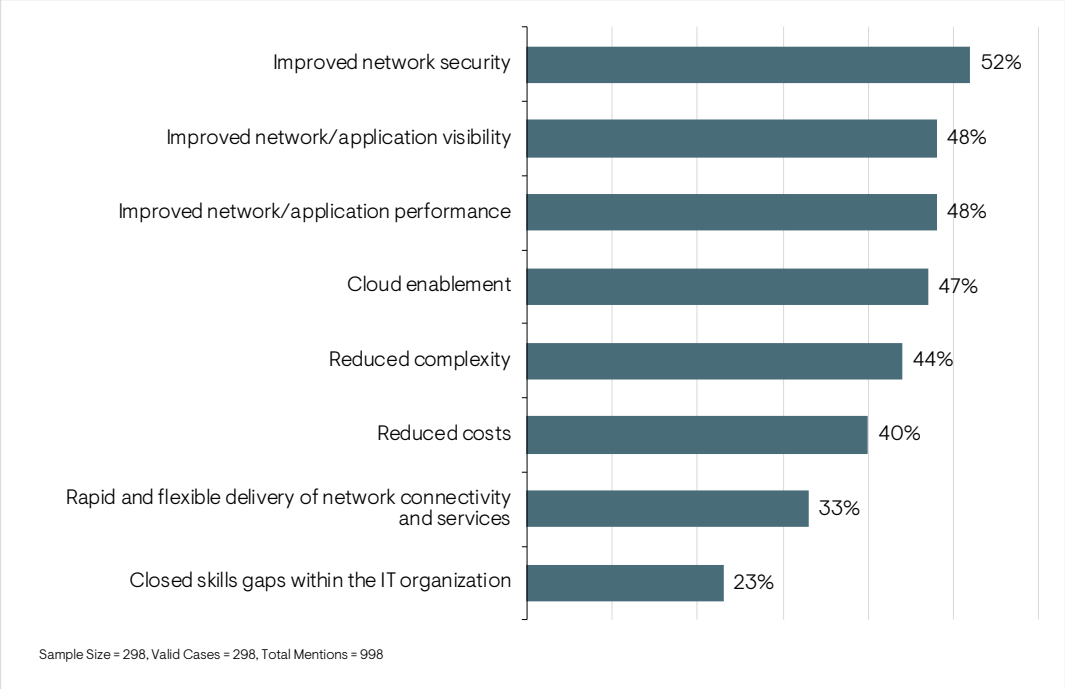


*Figure 19. Achieved or expected benefits of SD-WAN adoption*

Nearly half of enterprises also reported improvements to network and application visibility, improvements to network and application performance, and cloud enablement. Australians were more likely to experience better performance and North Americans and Europeans were more likely to experience cloud enablement.

The other big opportunities with SD-WAN appear to be reductions to complexity and costs. On the other hand, enterprises are unlikely to see much value from rapid and flexible delivery of network services or the closing of skills gaps within the network team.

### Success with SD-WAN

Throughout the SD-WAN section of this research, EMA called out correlations between SD-WAN strategies and SD-WAN success. EMA's source for these correlations is the data in **Figure 20**, which shows that only 47% of research respondents feel that their SD-WAN implementations have been an unqualified success. A slightly larger number of them see room for improvement.

***Only 47% of research respondents feel that their SD-WAN implementations have been an unqualified success.***

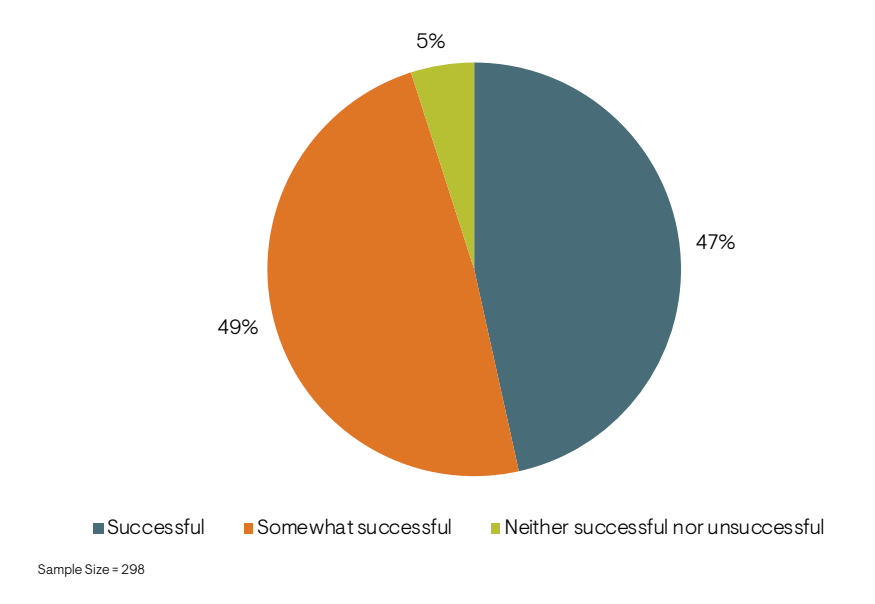


*Figure 20. Success with SD-WAN thus far*

## Secure Access Service Edge Insights

Secure access service edge (SASE) is an emerging product category that involves the integration of SD-WAN, secure remote access (e.g., remote VPNs), and cloud-based security into a single solution. Many SD-WAN and security vendors have started pivoting in that direction, but few have delivered a complete solution yet. Adoption is expected to ramp up over the next few years, but it is low at the moment. EMA has observed aggressive marketing that might lead some enterprises to believe that their existing investments in SD-WAN and/or cloud-based security constitute a SASE implementation.

Since the research respondents in this study are experts on WAN strategy, with representation from networking and security teams, EMA asked whether they were familiar with the SASE concept. Seventy-five percent of these WAN professionals are familiar with SASE. Individuals from the security group (96%) were the most familiar with it, while individuals who work in project management (65%) or network operations (63%) were less likely to have heard of it.

## Ranking SASE Platform Attributes

EMA asked research participants who were familiar with SASE to rank the importance of the attributes of a SASE solution, with 1 being most important and 5 being least important. **Figure 21** reveals that cloud-based, multi-function network security and site-to-site SD-WAN connectivity are the most critical SASE capabilities. Secure remote access ranks a close third. North Americans favor site-to-site SD-WAN connectivity highly, while Europeans are especially partial to cloud-based security.

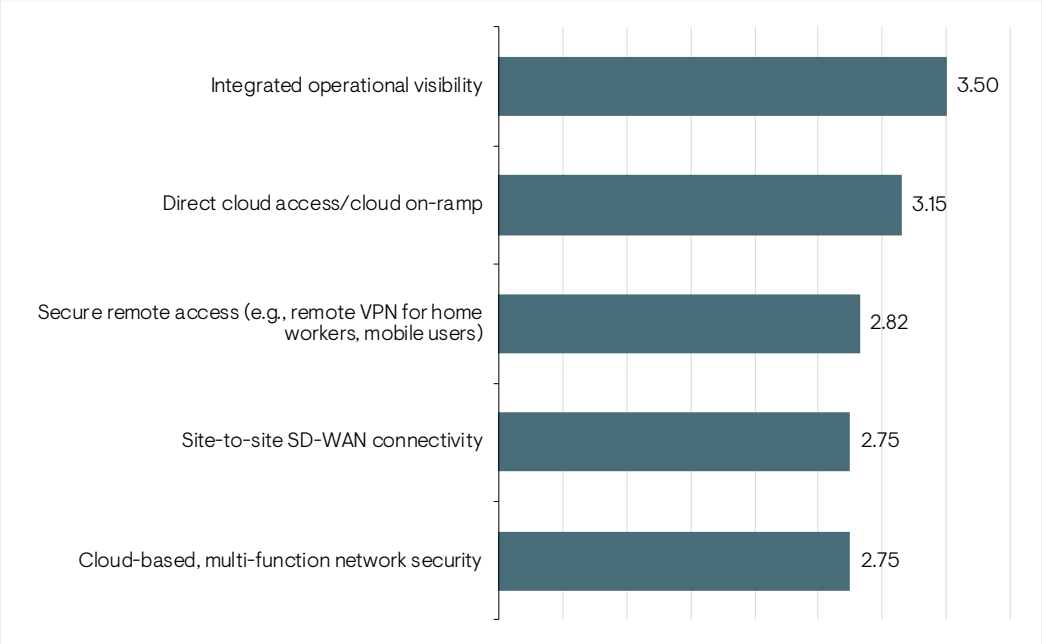


*Figure 21. Mean responses: Ranking SASE platform attributes 1 to 5*

## SASE Engagement

**Figure 22** shows the extent of SASE activity within enterprises today. The 25% of participants who told EMA that they were unfamiliar with the term SASE were not invited to answer the question represented by this chart; however, this chart assumes that their response to the question would have been "no engagement right now." This allowed EMA to offer an approximate adoption rate across all 303 enterprises the survey. Overall, 10% claim that they have fully implemented a SASE solution. EMA believes this number is inflated by overmarketing of SASE by SD-WAN and cloud security vendors.

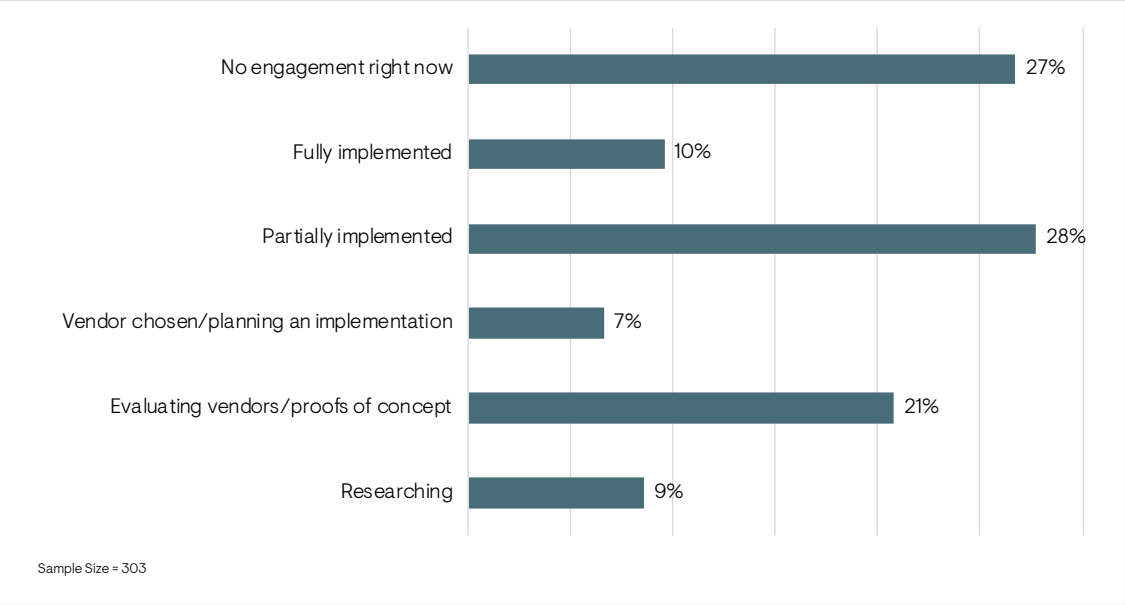


*Figure 22. Enterprise engagement with SASE*

## WAN Operations

### WANOps Success

First, **Figure 23** reveals that a slight majority of enterprises rated themselves successful with overall WAN operations. Only 42% saw room for improvement. North Americans (57%) are more likely to be successful, versus only 40% of Australians. Technology specialists (65%) were more likely to claim success, but only 48% of middle managers and 43% of IT executives agreed. This latter finding points to a worrisome disconnect between rank-and-file engineers and management over the quality of WAN services.

*A slight majority of enterprises rated themselves successful with overall WAN operations.*

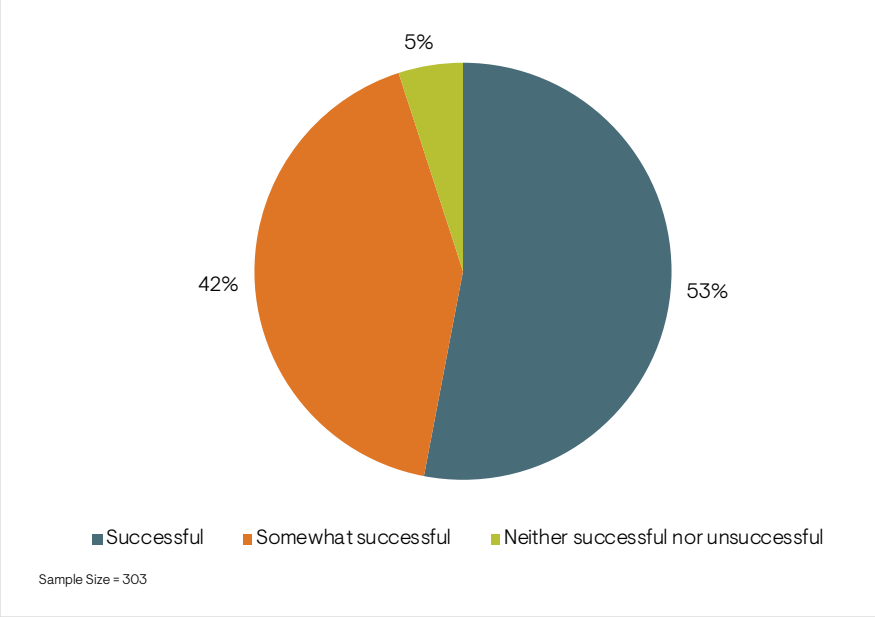


*Figure 23. Overall success with managing and monitoring the WAN*

## The Internet's Impact on WANOps

As enterprises transform their networks with internet connectivity, network operations tools will necessarily have to change. Without the service-level agreements (SLAs) associated with MPLS services, enterprises need to take a more aggressive approach to WAN monitoring if they want to protect performance and user experience. SD-WAN solutions offer some native visibility, but as an earlier section revealed, almost all enterprises require third-party monitoring.

**Figure 24** reveals that 94% of enterprises had to make changes to their network management toolset to accommodate internet visibility. Forty-seven percent acquired new tools and 46% had to upgrade or adapt their existing tools. Enterprises that are successful with WAN operations were more likely to acquire new tools (57%). Somewhat successful organizations tended to upgrade or adapt existing tools (56%).

***94% of enterprises had to make changes to their network management toolset to accommodate internet visibility.***

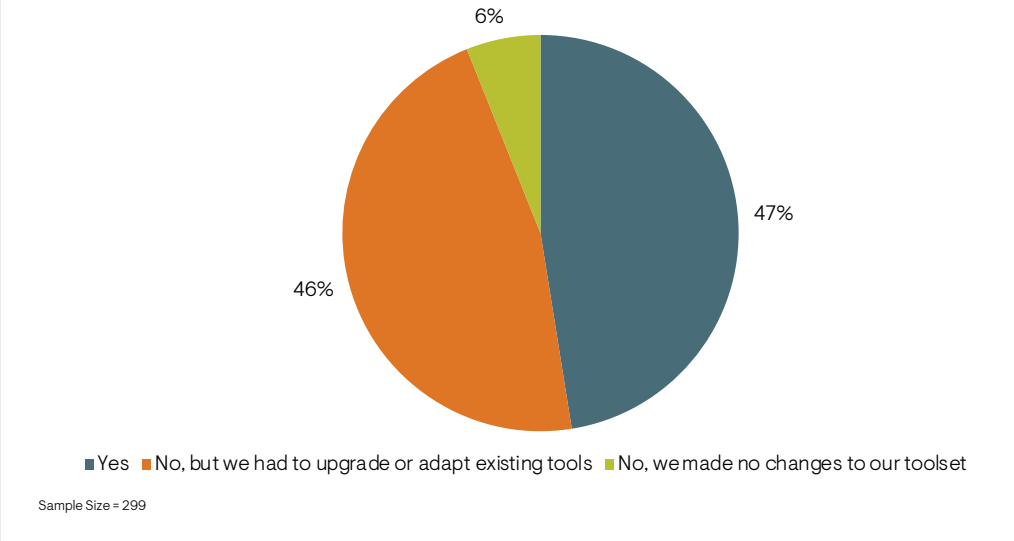


*Figure 24. Has increased use of the internet for WAN connectivity prompted your organization to acquire new monitoring and management tools?*

**Figure 25** reveals how the internet is affecting the value of different types of performance metrics for WAN operations. It shows that synthetic traffic, endpoint transactions, routing data, cloud provider flow logs, and packets have all increased in value for a majority of enterprises.

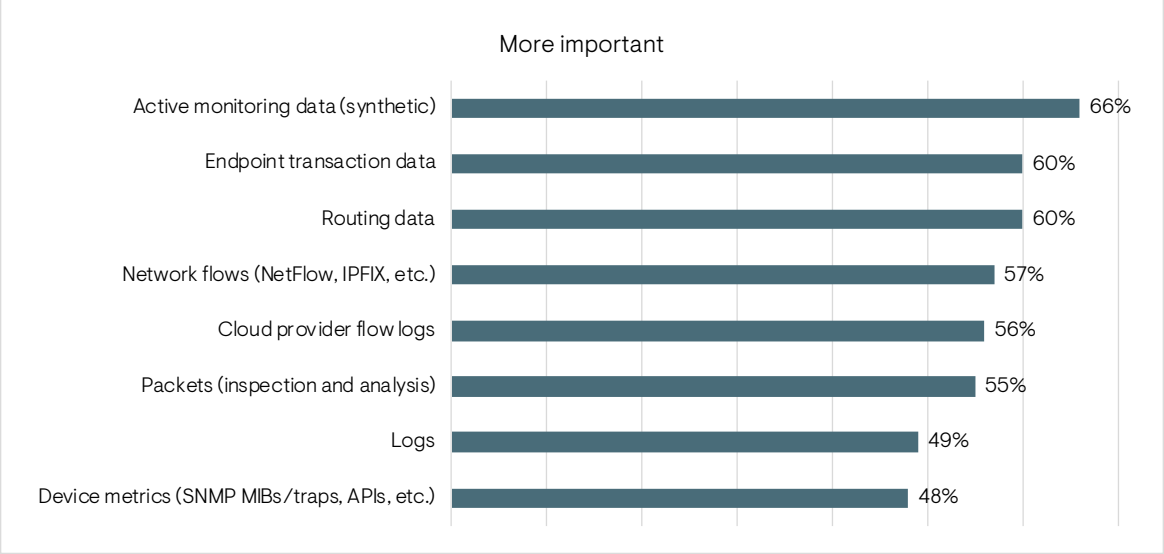


*Figure 25. Operational data that has become more important since adopting the internet for WAN connectivity*

**Figure 26** looks at specific internet metrics that enterprises find most useful for monitoring and troubleshooting the internet-based components of their WANs. End-to-end loss, latency, and jitter across internet paths and internet and ISP outage reports are the most valuable. DNS availability and resolution time are also quite valuable. Hop-by-hop loss, latency, and jitter are less valuable than end-to-end measurements. CDN metrics and BGP routing changes are of least importance.

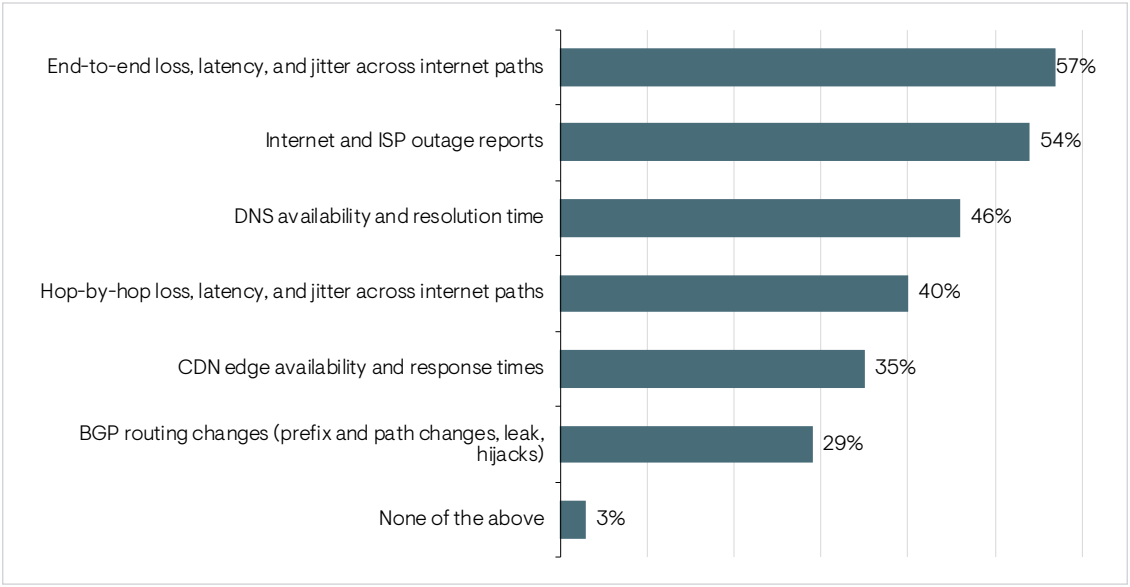


*Figure 26. Internet metrics most useful for monitoring and troubleshooting internet-based WAN connectivity*

## The COVID-19 Pandemic and the WAN

### The Work-From-Home Impact

EMA took the opportunity with its research to review how the COVID-19 pandemic is affecting enterprise WAN strategies. First, 93% of enterprises have seen an increase in the number of their employees who are working from home regularly. Next, EMA asked those respondents to characterize that increase by estimating the percentage of workers who regularly worked from home before the pandemic and the percentage who are doing so now during the crisis. **Figure 27** shows that remote workers have more than quadrupled during the pandemic.

***Remote workers have more than quadrupled during the pandemic.***

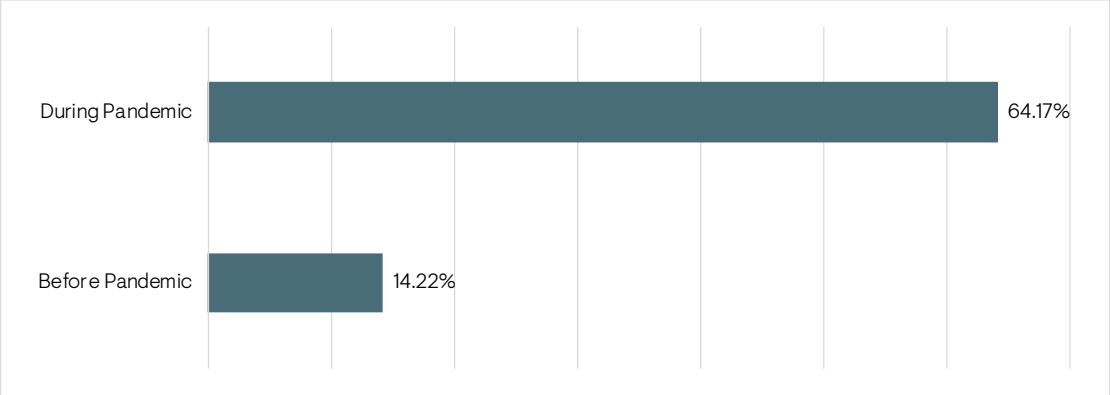


*Figure 27. Percentage of people regularly working from home, prior to and during the pandemic*

## Elevated Work-From-Home Populations are Permanent for Many

**Figure 28** shows that half of enterprises believe that the elevated remote workforce is permanent, with 23% expecting the number of users working from home to remain significantly higher than it was pre-pandemic. Midmarket enterprises (32%) are more likely to anticipate a significantly increased permanent remote workforce. Education, finance, government, healthcare, and nonprofit organizations all expect significantly larger permanent remote user populations.

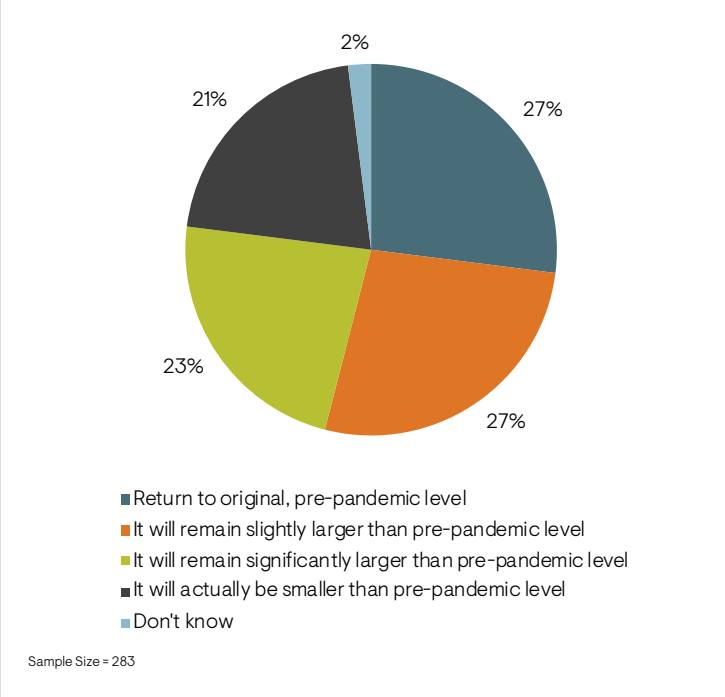


*Figure 28. How the end of pandemic restrictions will impact the elevated remote workforce*

Twenty-one percent of respondents said the remote workforce will actually shrink after the pandemic. This is a much higher number than expected, and EMA believes that some of these responses reflect the millions of layoffs that enterprises have experienced during the long months of this crisis. Very large enterprises are the most likely to expect this reduction (30%), which makes sense. Larger enterprises are more likely to experience layoffs, while smaller companies are more likely to close their door permanently.

## Remote Workers are Flooding the Network with Voice and Video

With so many people working from home, face-to-face interaction is rare. During the pandemic, many workers have compensated with real-time applications, including voice, video, and online meetings. **Figure 29** reveals that nearly 95% of enterprises have observed increased real-time application traffic on their WANs since the pandemic started. Most of them characterize this increase as significant.

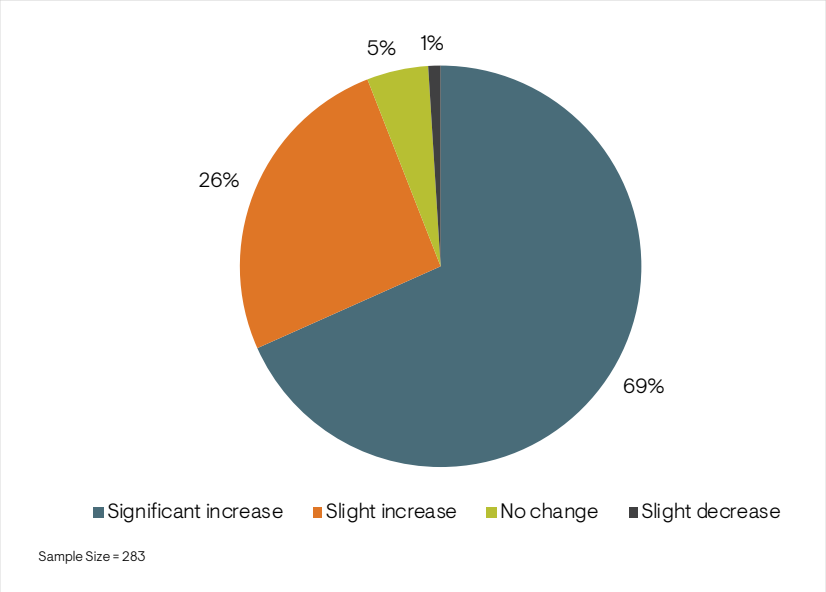


*Figure 29. Observed change in volume of real-time application traffic during pandemic*

This growth in real-time applications will present network managers with several challenges, not the least of which is network congestion. If these applications are traversing corporate networks in any way, they will compete with other business-critical applications for bandwidth. If this traffic is traveling over VPN tunnels, for instance, VPN concentrators will be overwhelmed.

## Supporting the Remote Worker

EMA suspects that IT organizations will have to adjust network architecture and network operations tools and practices to support users who work from home. These users will need more than a secure connection to the corporate network. They will want a good connection. The future WAN will be about working from anywhere, not working in a connected office. In the short term, this means that IT organizations need to figure out how to support users when they experience network and networked application trouble.

***The future WAN will be about working from anywhere, not working in a connected office.***

### Monitoring Tool Preferences

**Figure 30** reveals that enterprises primarily value three classes of tools for managing the user experience of remote workers. First, they prize remote desktop access tools, which can be essential for troubleshooting. Second, they are turning to internet monitoring tools and endpoint monitoring tools. Large and very large enterprises are more likely to see value in endpoint monitoring than midmarket companies, which suggests they are a luxury that only bigger IT budgets can afford. NOC analysts are most likely to perceive the value of remote desktop access tools, while security professionals are the least likely, perhaps because they see them as a security risk.

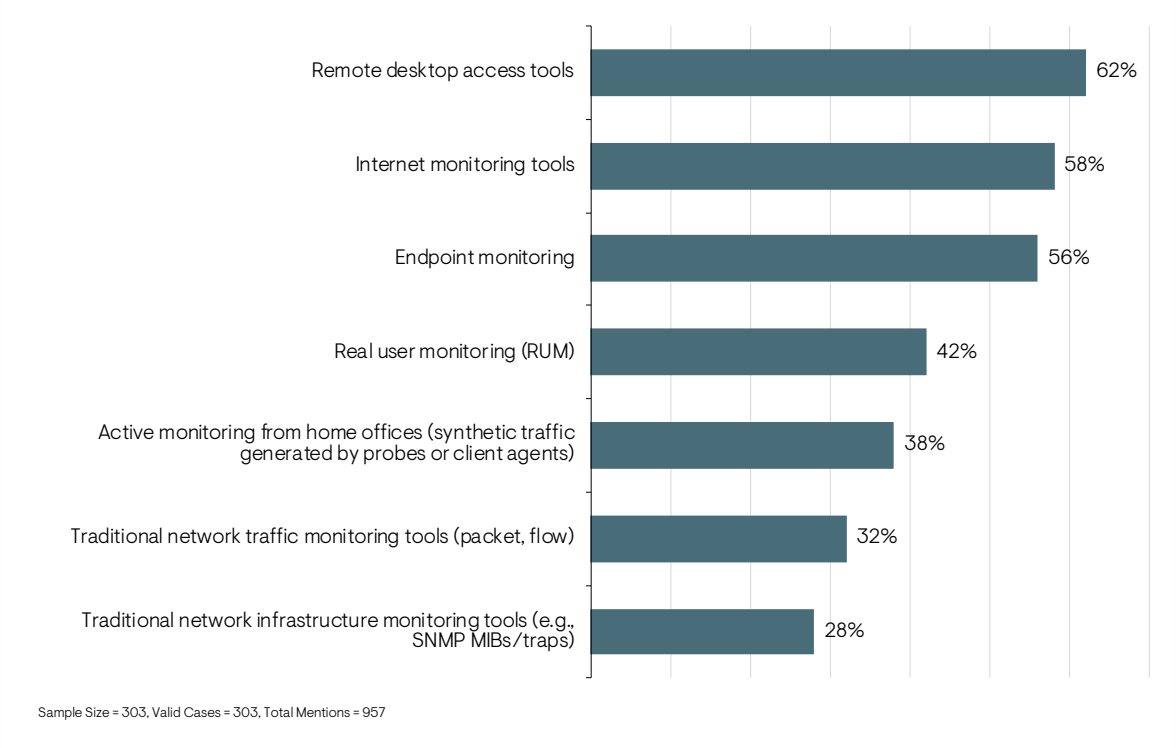


*Figure 30. Most useful tools for monitoring and troubleshooting user experience for remote workers*

Real user monitoring (RUM) tools, which rely on web browser instrumentation, are of secondary value. North Americans (50%) are more likely to rely on RUM tools, as are very large enterprises in general (61%).

Quite a few also see the value of active monitoring tools that generate synthetic traffic from a home office. Midmarket enterprises (40%) showed more of an affinity for these tools.

## SD-WAN and the Pandemic

**Figure 31** reveals that 60% of enterprises have actually accelerated their SD-WAN plans during the pandemic. Only 3% canceled an SD-WAN project and 14% paused a project. The rest reported no effect on the timing of SD-WAN. Enterprises that are successful with SD-WAN are the most likely to report that the pandemic accelerated their SD-WAN plans (69%).

***60% of enterprises have actually accelerated their SD-WAN plans during the pandemic. Only 3% canceled an SD-WAN project .***

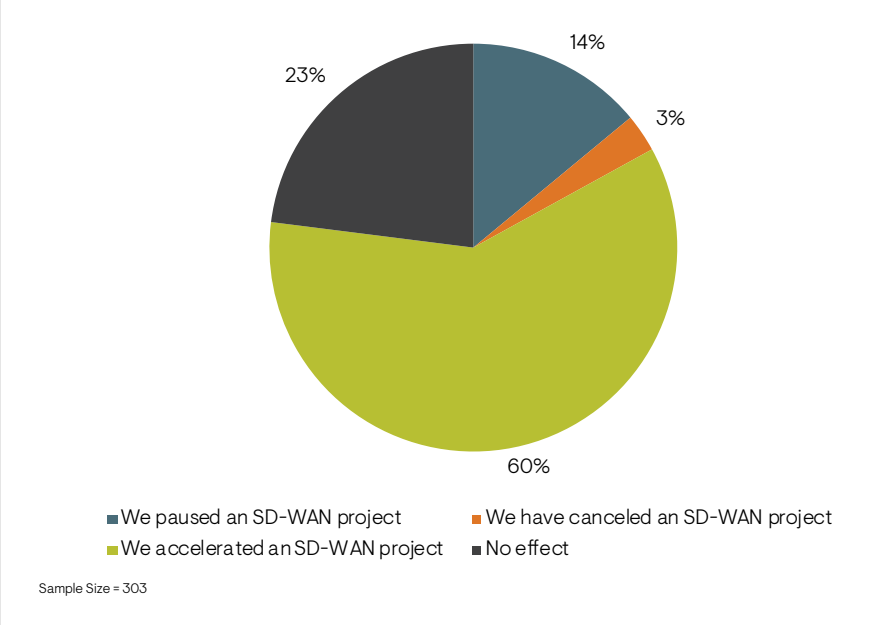


*Figure 31. The pandemic's effect on the timing of SD-WAN plans*

These findings are interesting. On the one hand, one might expect that SD-WAN is less valuable to an enterprise when most end users are working from home instead of the SD-WAN-connected branch office. On the other hand, SD-WAN solutions provide on-ramps to cloud services, which many enterprises are using more during the pandemic. Also, SD-WAN's centralized management capability reduces the need for network engineers to visit a remote site, which is ideal under pandemic conditions. Plus, certain industries have continued to have plenty of workers coming to corporate sites. For instance, construction companies, manufacturers, and oil and gas companies were all more likely to accelerate an SD-WAN project.

## SASE and the Pandemic

As with SD-WAN, **Figure 32** reveals that the pandemic disrupted only a small number of SASE engagements. Only 12% paused a project and 4% canceled one. SASE projects were a little less likely to be accelerated than SD-WAN projects were. Success with SD-WAN appears to leave enterprises primed for SASE, because 61% of enterprises successful with SD-WAN have accelerated SASE plans. Only 47% of somewhat successful enterprises did so.

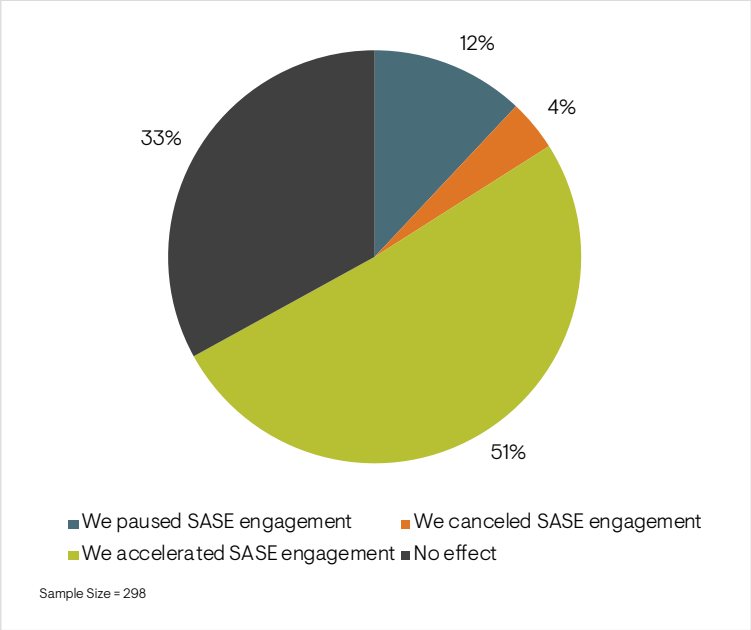


*Figure 32. The pandemic's effect on the timing of SASE plans*

## Conclusion

Despite the disruption of the COVID-19 pandemic, enterprises are moving forward with WAN transformation. At this point, the use of the internet for frontline WAN connectivity is nearly universal. Despite the proliferation of hybridized networks, the majority of enterprises have no plans to reduce their investments in managed WAN services like MPLS. Transformation isn't about cost cutting with cheaper services. It's about supplementing MPLS bandwidth, adding agility, and connecting to the cloud.

That's where SD-WAN comes in. This research found that nearly all enterprises are engaged with SD-WAN today, with almost 40% having fully implemented it. SD-WAN-based network transformation is about more than the internet, of course. Enterprises are counting on the technology to improve security, enhance operational visibility, optimize performance, enable cloud connectivity, and reduce overall complexity.

Enterprises are also establishing a preference for how they proceed with SD-WAN. Managed SD-WAN services are the future, but IT organizations want hybrid operations so they can share control with a vendor or MSP. Moreover, the native visibility capabilities of SD-WAN solutions are effective, but IT organizations want to go further. Most use third-party network operations solutions to monitor and manage SD-WAN.

IT organizations clearly see SD-WAN as extensible to the remote worker environment, which brings us to the emerging SASE market. Enterprises are clearly aware of this new solution category, and many are trying to adopt first-generation products now.

The pandemic has accelerated both SASE and SD-WAN engagement. Enterprises that are most successful with SD-WAN are the most engaged with using these technologies to protect operations during the pandemic.

EMA will continue to track the progress of SD-WAN and SASE and related technologies as they evolve to serve enterprises moving toward a digital future. EMA believes the pandemic has revealed that WAN architecture has to change even more than it has during these years of hybridization with SD-WAN. As business models evolve in this new reality, the network must follow. SD-WAN and SASE have much more to offer this future than people realize.

# Large Bank Deploys and Optimizes New WAN Architecture with LiveNX from LiveAction

## Introduction

When a large online bank initiated a new WAN infrastructure project with Cisco, it turned to LiveNX, a network performance management solution to help with planning, implementing, and optimizing the network implementation.

The bank chose LiveAction over Cisco Prime, which offered sufficient planning and implementation support, but not enough support for the bank's network optimization requirements.

## Day 0: Baselining and Planning

The bank required a baseline understanding of what was running in its network. It used the real-time network topology mapping capabilities of LiveNX to baseline network devices, interfaces, applications, VPNs, and users. Additionally, LiveNX also provided other useful visual analytics for baselining policy and behaviors, such as:

- Site-to-site visual analytics to discover traffic types and paths and to understand behaviors between sites
- Application behavior charts and graphs to baseline SLAs and application consumption patterns—bandwidth and class
- Service provider analysis answering questions like:
  - Which service provider path should applications take?
  - What applications should be added to application route policies?
  - What impacts do service providers have on QoS policies?

## Day 1: Build and Deploy

The bank's IT team especially appreciated LiveNX's ability to scale management and visibility to over 10,000 network devices, its policy verification functionality, and its ability to optimize tunnels, traffic, and application performance. For instance, while building and deploying a new Cisco WAN, the bank used LiveNX for:

- Validating application routing through intuitive visual analytics
- Isolating and identifying the root cause of problems with historic replays of network activity
- Capacity planning with reports that reveal whether the network can support critical traffic

During deployment, the online bank used LiveNX to identify intermittent asymmetric VoIP routing issues. It revealed a Cisco IOS defect that was causing traffic-class churn at a hub site. It also was able to optimize traffic flows from branches to the data center to address routing loop issues and verify WAN application traffic steering.

## Day 2+: Optimizing Network Operations

Once deployed, the online bank used LiveNX's patented visual analytics and dashboards to monitor WAN utilization and detect faults and traffic drops. The network operations team leveraged LiveNX's application dashboards to monitor performance of the bank's most popular applications and used QoS dashboards to identify performance trends. It optimizd WAN capacity planning with easy-to-use reports.

Ultimately, the bank found that LiveNX provided the scale and breadth of functionality needed for enterprise visibility, path analysis, and ongoing WAN capacity planning.

## About Enterprise Management Associates, Inc.

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

---



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

4049.120220