EMA
IT & DATA MANAGEMENT RESEARCH, INDUSTRY ANALYSIS & CONSULTING

Prepared for:

BROADCOM

WAN Transformation with SD-WAN:

Establishing a Mature Foundation for SASE Success

April 2023 EMA Research Report Summary

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

Table of Contents

Introduction

Nearly one decade has passed since the phrase "software-defined wide-area networking" entered IT industry vernacular. Vendors and industry analysts coined the term to describe a class of technologies that enable an enterprise to build a wide-area network (WAN) where sites can connect via multiple redundant paths (including private and managed WAN services and public internet connections) securely and with centralized management and control.

The rise of software-defined WAN (SD-WAN) kicked off multiple waves of innovation as startups delivered solutions that made expensive routers and firewalls redundant in many remote sites. SD-WAN also triggered waves of mergers and acquisitions when router and firewall vendors bought SD-WAN providers to preserve and extend the value of their existing solutions.

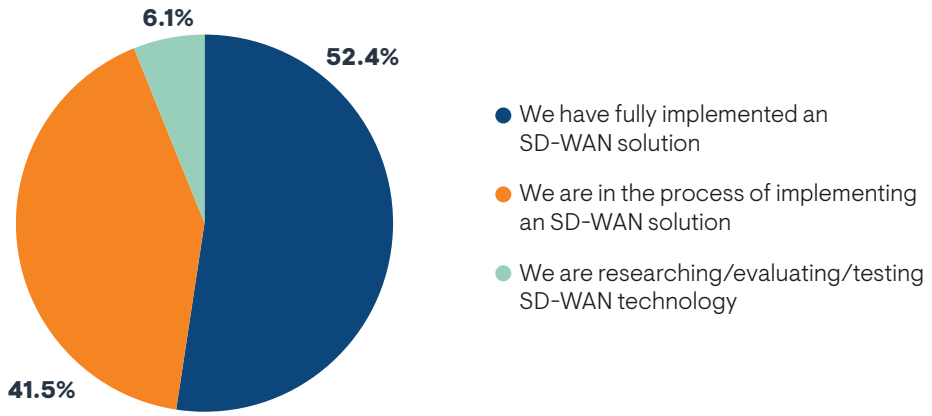
Now, a new wave of innovation has arrived with secure access service edge (SASE). Vendors and solution providers are integrating SD-WAN and multi-function cloud-based network security into unified platforms that provide connectivity and security for distributed, multi-cloud enterprises. While SASE holds promise, EMA heard anecdotally that many large enterprises struggle with their transition from pure SD-WAN to true SASE.

In fact, EMA believes that the industry's emphasis on SASE is trivializing the complexity of SD-WAN. Some enterprises make the mistake of designating SD-WAN as a just another SASE feature, a checklist item on an RFP that can be turned on with the click of a button. While some SASE vendors may succeed in delivering a turnkey solution that makes SD-WAN a relatively trivial component of the overall platform, many enterprises find that SD-WAN is a complex technology that requires careful planning and execution. When charting a path toward SASE, most IT organizations must establish an SD-WAN foundation that is scalable, stable, secure, and fully operationalized. This summary of new EMA research examines how enterprises are transforming their networks by building that foundation and taking the next step toward SASE.

Research Methodology

EMA surveyed 313 IT professionals across North America and Europe who have responsibility for and/or influence over their company's WAN strategy. To qualify for participation in the research, respondents' organizations had to be engaged with SD-WAN technology. **Figure 1** shows that more than 52% of enterprises in this survey have a fully deployed SD-WAN solution in production. Nearly 42% are in the process of implementing a solution, and only 6% are still at the research and evaluation stage.

FIGURE 1. CURRENT STATE OF SD-WAN ENGAGEMENT



In 2020, EMA research found that 99% of enterprises were engaged with SD-WAN in some way , so EMA believes that Figure 1 provides a snapshot of the current overall state of adoption of SD-WAN in the enterprise world. In other words, you won't find many IT organizations in which the network team hasn't at least started researching the technology for potential adoption.

Sample Size = 313

Figure 2 provides an overview of survey participants and their organizations. EMA captured a broad range of technical personnel, IT middle management, and IT executives from midmarkets to very large enterprises in more than one dozen industries.

For additional qualitative insights, EMA interviewed nine IT professionals one on one about their WAN strategies. These individuals are quoted anonymously throughout the report.

FIGURE 2. DEMOGRAPHICS OVERVIEW

Top Job Titles

23%	IT director
16%	IT manager/supervisor
15%	Network architect
11.8%	Network engineer/analyst
11.8%	CIO/CTO
9.3%	Project/Program manager

Company Size (Employees)

21.1%	500 to 999
41.5%	1,000 to 4,999
25.6%	5,000 to 9,999
11.9%	10,000 or more

Region

57.2%	USA and Canada
42.8%	France, Germany, and UK

IT Groups

23.3%	Network engineering/architecture
21.1%	CIO suite
15%	IT architecture
13.7%	IT project/program management
13.1%	IT asset/financial management and business analysis
8.9%	IT security/cybersecurity
4.8%	Network operations/IT operations

Top Industries

27.5%	Banking/Finance/Insurance
21.4%	Manufacturing
13.4%	Energy/Utilities
7.7%	Retail
5.8%	Professional/Technical services unrelated to IT
5.4%	Healthcare
3.8%	Logistics/Wholesale/Distribution
3.5%	Transportation
2.9%	Aerospace/Defense

Key Findings

- 66% of IT organizations prefer to consume SD-WAN as a managed service, but 58% prefer to share responsibility for Day 2 operations in a hybrid operating model.
- 43% of companies have multiple SD-WAN vendors now, primarily to address specific functionality requirements and to address the needs of different kinds of sites.
- 96% of IT decision-makers are interested in adopting integrated remote access capabilities from SD-WAN vendor to address hybrid workers.
- 71% of IT organizations apply WAN acceleration to their networks, and nearly all of them leverage their SD-WAN vendors for this acceleration.
- 86% of organizations are incorporating wireless services into their WANs, and most are using this connectivity as a primary connectivity option for at least some sites.
- 73% of organizations are monitoring SD-WAN with third-party network monitoring tools, but only 41% are fully satisfied with this third-party monitoring.
- Only 38% of organizations believe they have been fully successful with SD-WAN.
- More than 30% of IT professionals say it is difficult to advance from SD-WAN to SASE. Only 11% believe it is very easy.

The Nature of SD-WAN Engagement

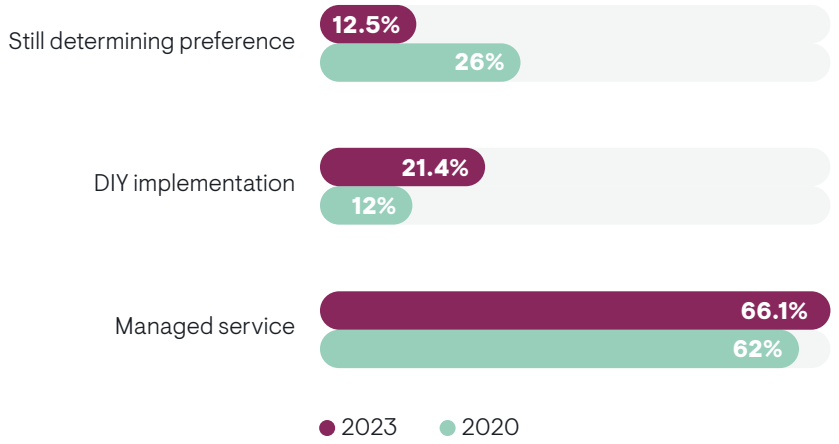
Managed versus DIY SD-WAN

When SD-WAN first emerged nearly ten years ago, many enterprises tried implementing the technology on their own, deploying an overlay on top of their existing WAN circuits. In recent years, most enterprises have embraced managed SD-WAN services over do-it-yourself (DIY) implementations. However, **Figure 3** reveals that DIY is holding steady as a niche strategy for many companies. It appears that most of the companies that were undecided about procurement strategy in 2020 have elected to follow a DIY path in 2023.

Company size had some influence over these preferences. The largest companies in our survey had an affinity for DIY SD-WAN while smaller companies were more likely to seek a managed service.

EMA observed some differences in preference based on where a research participant sat in an organization. For instance, technical personnel, such as network engineers and architects, were more likely to prefer a DIY approach, probably because it allows them to leverage their advanced skills. Meanwhile, IT middle management and IT executives had a clear preference for a managed service.

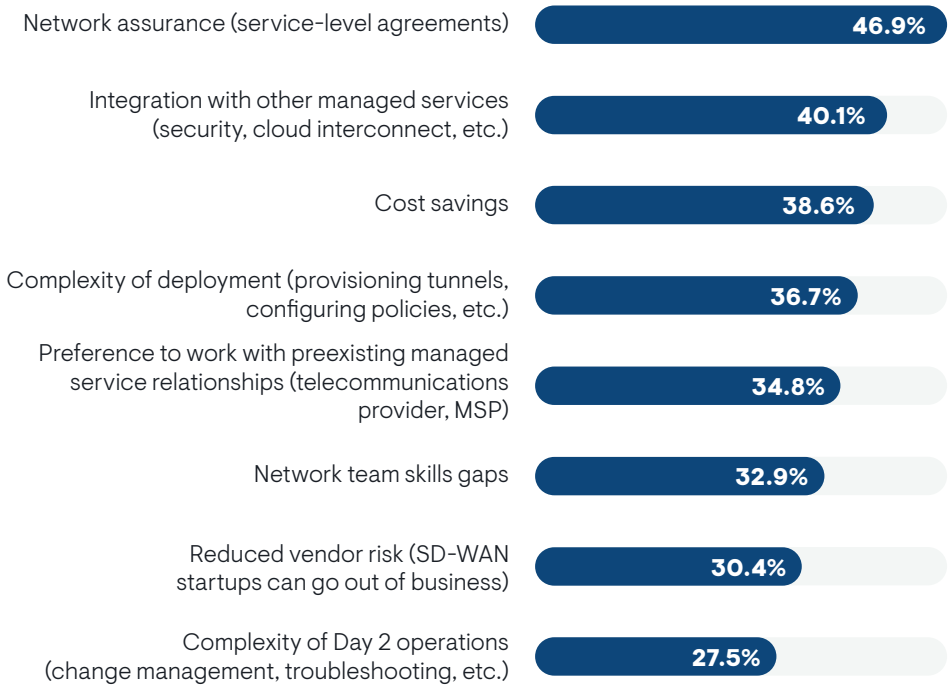
FIGURE 3. PREFERENCES FOR PROCURING, IMPLEMENTING, AND CONSUMING AN SD-WAN SOLUTIONS



Why a Managed SD-WAN Service?

Figure 4 reveals why many enterprises are choosing a managed SD-WAN service. The biggest factor is network assurance. Enterprises like the idea of getting an enforceable service-level agreement (SLA) on an SD-WAN service, which makes sense given how prominent internet connectivity is in SD-WAN underlays. Internet service providers (ISPs) typically don't offer an SLA, but a managed SD-WAN provider can add a lot of value if it offers an SLA on top of that internet-based underlay.

FIGURE 4. WHY DOES YOUR ORGANIZATION PREFER A MANAGED SERVICE FOR YOUR SD-WAN?



Sample Size = 207, Valid Cases = 207, Total Mentions = 596

"A lot of the pros [of managed SD-WAN] have to do with being able to guarantee 99.5% uptime, and if not, there is a penalty clause in the contract," said a vice president of architecture for a $5 billion energy company. He said his managed SD-WAN provider has overachieved so far, with just one outage over the last four years.

The same vice president also noted that he lacked the internal expertise or budget for a DIY approach to SD-WAN. "I said [to upper management], we don't have the right headcount, we don't have the resources, and we don't have enough CapEx to buy the hardware. Otherwise, I would have had to ask for 10 new employees and $3 million for hardware."

Many respondents also told EMA that they believe a managed SD-WAN service provides better integrations with other managed services that they consume. This integration was a higher priority to IT middle management and IT executive management. Technical personnel were less motivated by this.

Finally, many enterprises are also adopting managed SD-WAN to reduce costs and to mitigate the complexity of implementing the technology. Cost savings were more important to companies that have a larger number of sites connected to the WAN. Members of cybersecurity teams also considered integrations with other managed services to be a high priority, but members of network engineering teams did not.

Why a DIY SD-WAN?

Figure 5 reveals there are four primary reasons why an enterprise might prefer a DIY SD-WAN implementation. First, the network team has a fear of losing control over its network. Next, many believe that DIY SD-WAN can lead to cost savings, just as many believe that a managed service also can.

Many also cited that they have customization requirements that a managed SD-WAN service cannot address. Managed service providers necessarily limit the amount of customization they can offer because it can add complexity to customer environments that will drive up the provider's costs.

Finally, many enterprises have strong network engineering teams that have the skills needed to build and manage an SD-WAN solution. This removes the need for a managed service. Organizations that have been the most successful with their DIY SD-WAN solutions are much more likely to cite this as a driver of their decision. Later in this report, EMA will reveal that managed SD-WAN solutions tend to be more successful than DIY SD-WAN. However, when a strong network engineering team is driving the decision to go DIY with SD-WAN, enterprises tend to do well.

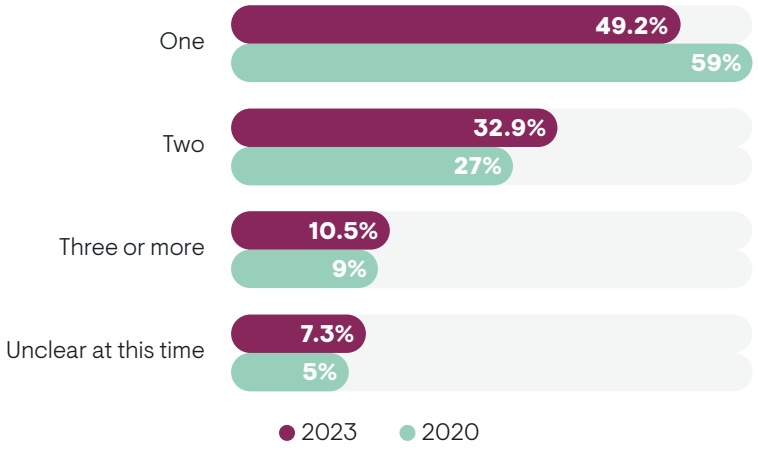
FIGURE 5. WHY DOES YOUR ORGANIZATION PREFER A DIY APPROACH?

Sample Size = 67, Valid Cases = 67, Total Mentions = 152

Multi-Vendor SD-WAN is Mainstream

Enterprises are increasingly adopting a multi-vendor approach to SD-WAN. **Figure 6** reveals that 59% of enterprises used or planned to use only one SD-WAN vendor in their networks. Today, that percentage has dropped to 49%, while the number of companies using two vendors has jumped from 27% to nearly 33%. The number who use three or more vendors has also ticked up slightly.

FIGURE 6. NUMBER OF SD-WAN VENDORS AN ENTERPRISE USES OR PLANS TO USE



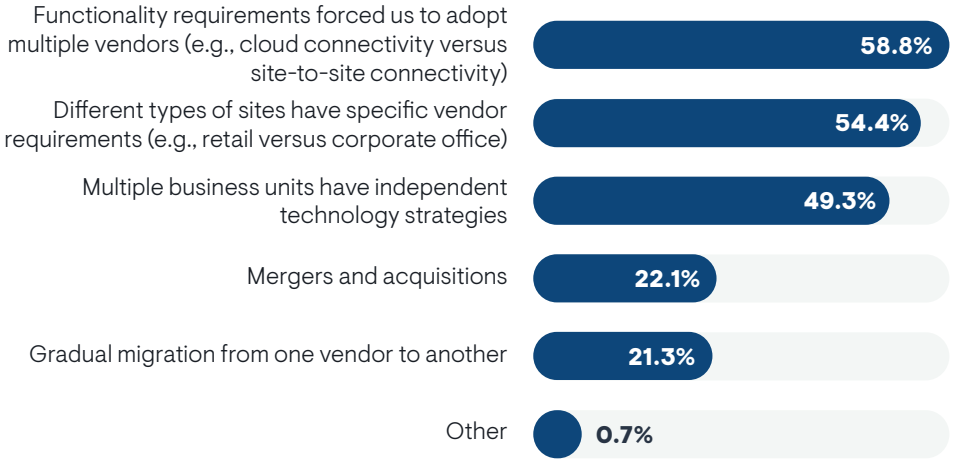
Larger companies were more likely to be multi-vendor. For instance, organizations with 10,000 or more employees were twice as likely as smaller companies to use three or more SD-WAN vendors.

Our research found that technical personnel tend to have greater awareness of multi-vendor SD-WAN strategies, while middle management and executives are more likely to believe they are using a single vendor. EMA often observes an awareness gap between management and technical personnel on technical networking technology. We also found that members of IT asset management or financial management groups were the most likely to perceive a single vendor strategy, which is surprising given that these groups tend to manage vendor relationships.

Drivers of Multi-Vendor SD-WAN

Figure 7 reveals why so many companies are adopting multi-vendor SD-WAN. Most multi-vendor organizations cited two drivers. First, they have functionality requirements that forced them to adopt two vendors. For instance, some vendors offer very strong functionality for establishing secure site-to-site connectivity, while others focus on site-to-cloud connectivity. This was more often a factor in smaller companies.

FIGURE 7. DRIVERS OF MULTI-VENDOR SD-WAN



Second, many organizations indicated that they have a diversity of sites that require different types of vendors. For instance, they might have large office campuses that require significant bandwidth and advanced security. The same company might also have many remote industrial sites that require ruggedized hardware and integrated wireless WAN connectivity.

Nearly half of organizations also told us that they have multiple business units with independent technology strategies. Larger companies were more likely to cite this issue.

Sample Size = 136, Valid Cases = 136, Total Mentions = 281

SD-WAN Requirements

This section explores the requirements that enterprises are setting for SD-WAN technology as they try to transform their networks and lay a foundation for SASE.

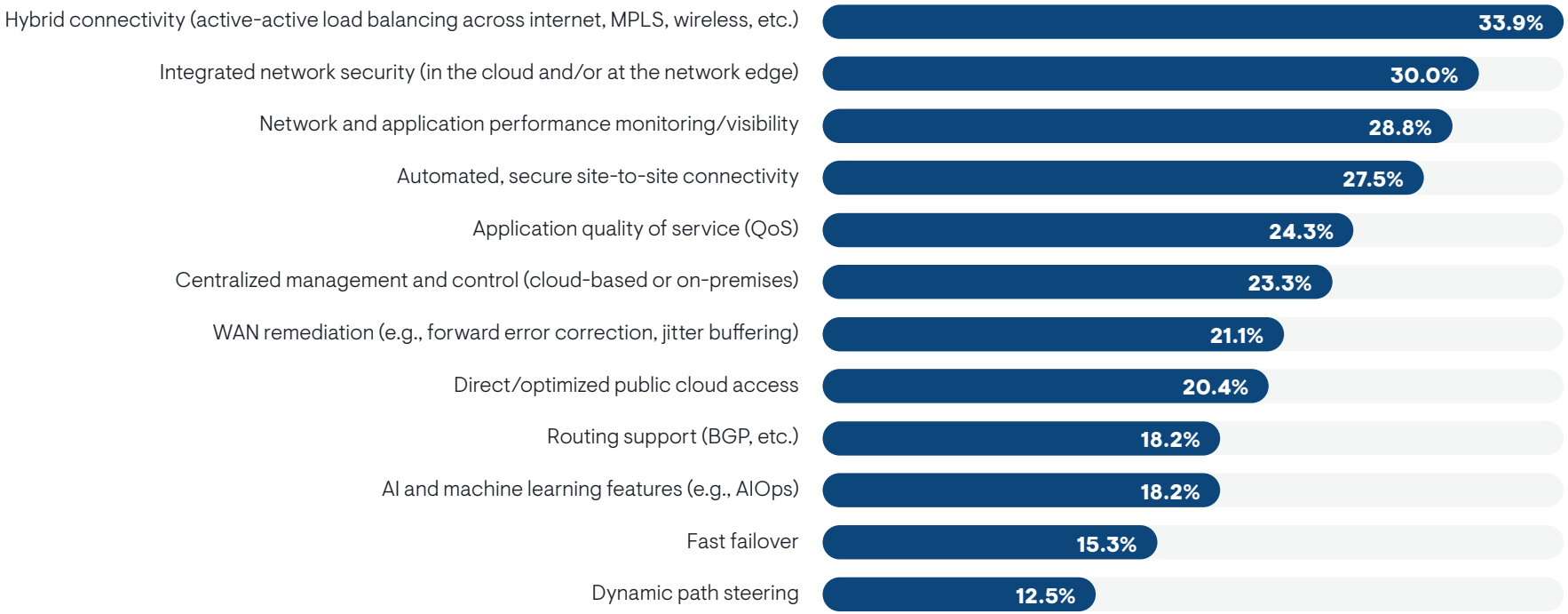
Critical Features

Figure 8 reveals the SD-WAN product features that organizations believe are most critical to their networks. The top feature is hybrid connectivity, the ability to forward traffic over multiple network connections simultaneously.

The secondarily critical features are integrated network security, native network and application performance monitoring, and automated, secure site-to-site connectivity. Native monitoring is most important to organizations that are still researching and evaluating SD-WAN solutions. It becomes less important as organizations deploy SD-WAN in production. On the other hand, it is more important to organizations that have a larger number of sites connected to a WAN. Integrated network security is also more important to organizations that have a large number of connected sites.

Automated site-to-site connectivity is all that matters for a senior network engineer for a $100 million manufacturer. “From most of the platforms I’ve seen, SD-WAN just means automatically building IPSec tunnels between all your nodes. That’s a completely valid thing to want and need if you have a larger organization with a lot of locations and a lot of sites.”

FIGURE 8. MOST CRITICAL SD-WAN FEATURES

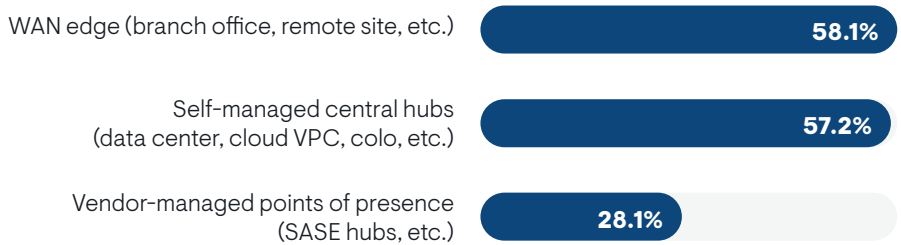


Sample Size = 313, Valid Cases = 313, Total Mentions = 856

Network Security

Integrated security is a core requirement of SD-WAN. The question many will ask is, where should that security reside? **Figure 9** reveals that IT organizations do not have a strict, one-size-fits-all approach to SD-WAN security. Most of them want to deploy network security at the SD-WAN edge and in self-managed hubs, such as data centers and cloud VPCs. It really depends on the type of network security service one is discussing. Some functions are best deployed at the edge and others in the cloud. Organizations that were less successful with their overall SD-WAN implementation were more likely to select the WAN edge, suggesting an edge-based SD-WAN security architecture is not a best practice.

FIGURE 9. PREFERRED LOCATION OF NETWORK SECURITY FUNCTIONS INTEGRATED INTO SD-WAN ARCHITECTURE



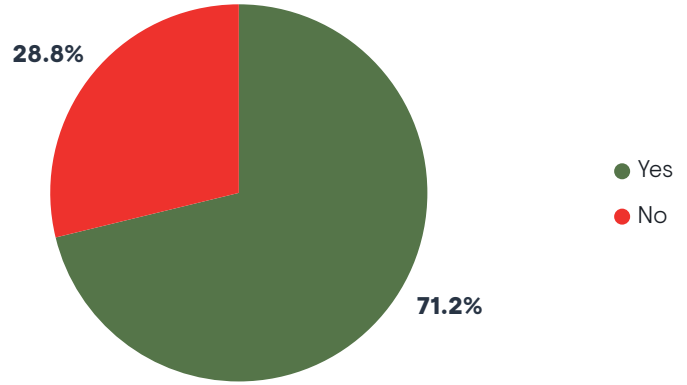
This chart also reveals that many enterprises aren't ready to embrace SASE solutions. Only 28% prefer to deploy an SD-WAN security capability in a vendor-managed PoP, like a SASE hub. Note, this question is framed as network security integrated into SD-WAN architecture. If EMA had posed this as a SASE question, the responses may have been significantly different. This points to the fact that many network teams are struggling to understand the nuanced differences between SD-WAN and SASE. In fact, members of the cybersecurity team were more likely to want a vendor-managed PoP than members of the network engineering team. Network engineering teams were more interested in WAN edge deployments. Meanwhile, the IT architecture group favored self-managed hubs.

Sample Size = 313, Valid Cases = 313, Total Mentions = 449

WAN Acceleration

SD-WAN enables enterprises to add more bandwidth to their WAN underlay via more affordable broadband internet connections, but more bandwidth does not guarantee application performance. An SD-WAN strategy must also include WAN acceleration. **Figure 10** reveals that more than 71% of these organizations are using WAN acceleration on their networks.

FIGURE 10. DO YOU USE WAN ACCELERATION TECHNOLOGY TO IMPROVE APPLICATION PERFORMANCE ON YOUR NETWORK?

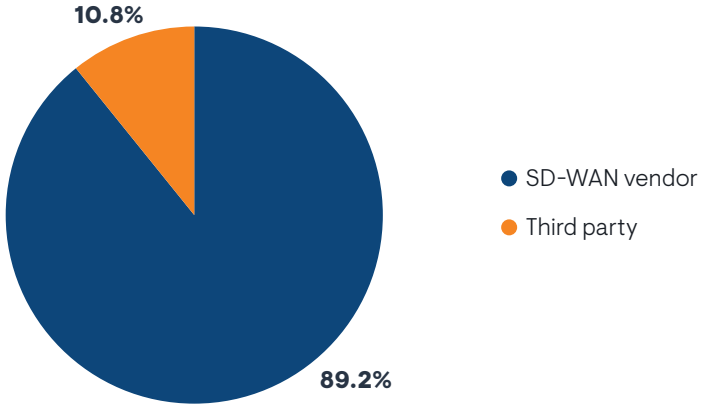


Adoption of WAN acceleration is highest among organizations that have fully implemented an SD-WAN product. It's also higher among enterprises that are the most successful with their SD-WAN implementation. Network engineering teams, cybersecurity, and IT governance groups are more likely to report use of WAN acceleration than the CIO's suite and network operations. This suggests that people who are only peripherally concerned about SD-WAN architecture and vendor relationships are less aware that WAN acceleration is a part of the SD-WAN strategy.

Sample Size = 313

Figure 11 reveals that nearly all companies rely on their SD-WAN vendor for WAN acceleration functionality. Only 11% have a third-party solution. Larger companies are more likely to use a third-party acceleration solution. This makes sense because larger companies – which have larger budgets – were more likely to use a standalone WAN optimization vendor in the pre-SD-WAN era when IT organizations invested in specialized technology to maximize their precious MPLS bandwidth.

FIGURE 11. IS YOUR WAN ACCELERATION PROVIDED BY YOUR SD-WAN VENDOR OR A THIRD PARTY?



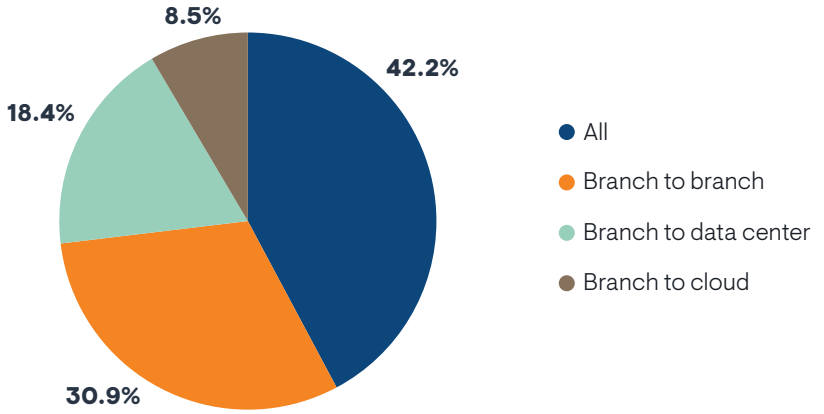
Sample Size = 223

Figure 12 reveals where enterprises are applying WAN acceleration. The most common approach is to accelerate all paths on the WAN, but 31% focus on branch-to-branch paths, 18% focus on branch-to-data center, and nearly 9% focus on branch-to-cloud.

EMA observed some variation based on SD-WAN topology. For instance, organizations with a full-mesh SD-WAN were much more likely to accelerate all network paths. Organizations with a partial mesh were more likely to focus on branch-to-branch paths. Organizations with a hub-and-spoke topology were more likely to focus on branch-to-branch or branch-to-data center.

Organizations with more successful SD-WAN implementations were the most likely to accelerate all network paths.

FIGURE 12. PATHS THAT ARE OPTIMIZED WITH WAN ACCELERATION



Sample Size = 223

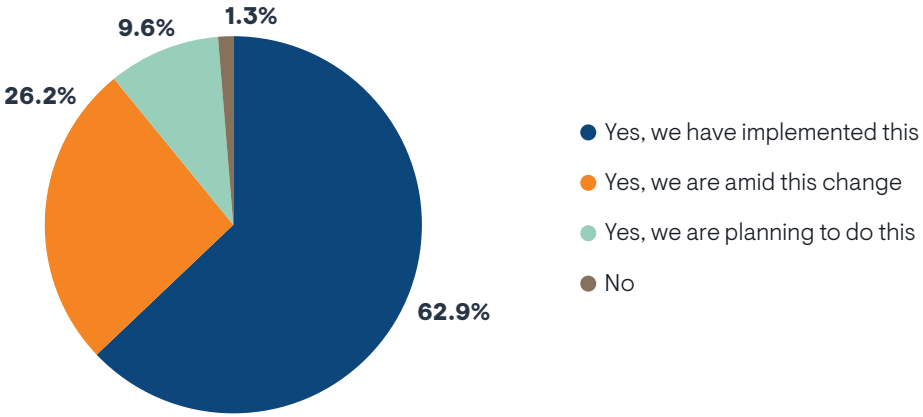
The SD-WAN Underlay

SD-WAN's ability to forward traffic over multiple redundant paths made the internet a viable option for primary WAN connectivity. Combined with site-to-site secure tunneling, acceleration and network path steering, the hybrid connectivity features of SD-WAN allow enterprises to reduce their reliance on expensive MPLS connectivity.

Internet Connectivity

Figure 13 reveals that 63% of organizations have increased their use of the internet as a primary means of WAN connectivity. Nearly all other organizations are moving forward with this. Companies that completed an SD-WAN implementation are the most likely to have done this already.

FIGURE 13. HAS YOUR ORGANIZATION INCREASED, OR DOES IT PLAN TO INCREASE, ITS USE OF THE INTERNET AS A PRIMARY OPTION FOR CONNECTING SITES TO YOUR WAN?

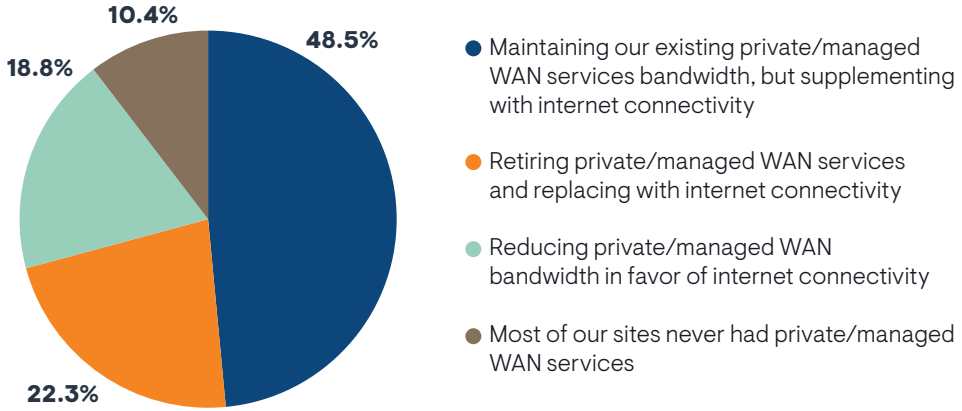


Sample Size = 313

MPLS Persists

Figure 14 reveals how the shift toward internet connectivity is affecting the use of managed WAN connections, like MPLS in enterprise networks. The most popular approach is to leave existing MPLS bandwidth unchanged. Organizations instead use the internet to boost overall bandwidth.

FIGURE 14. HOW INCREASED USE OF THE INTERNET FOR CONNECTING SITES TO THE WAN PRIMARILY AFFECTS USE OF PRIVATE/MANAGED WAN SERVICES, LIKE MPLS



The less common strategies are to reduce MPLS bandwidth in favor of the internet or to retire MPLS altogether.

Sample Size = 309

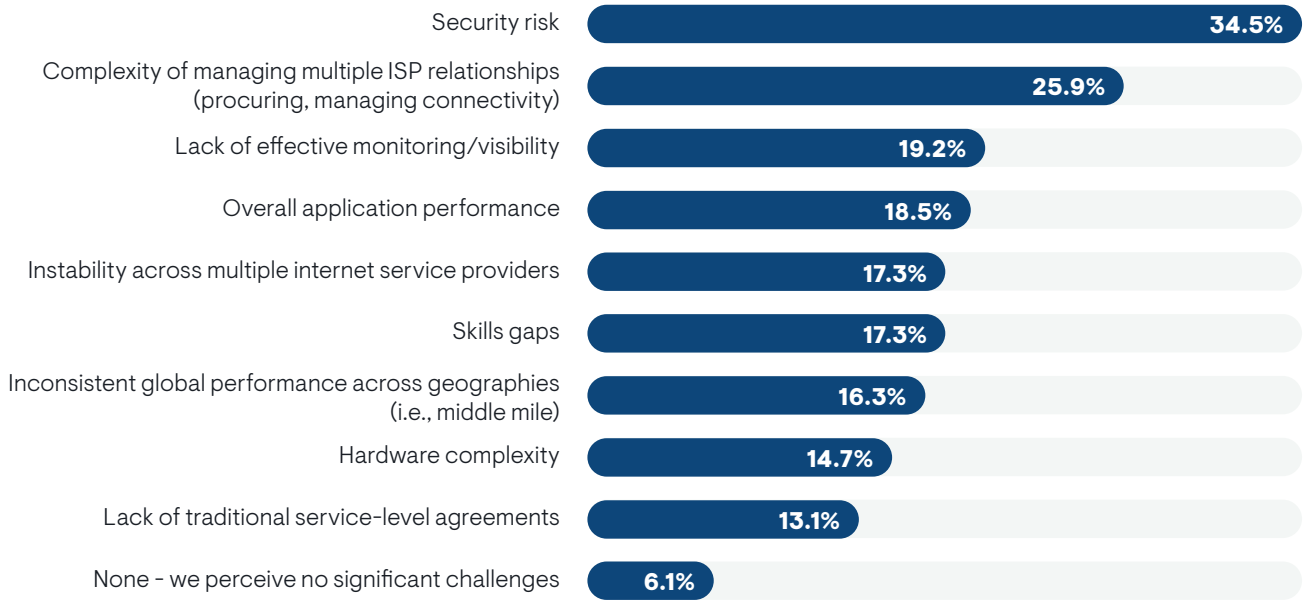
Internet Underlay Pitfalls

In general, the internet is not an enterprise-class WAN connectivity solution. Many ISPs offer business-class services, but these services are not comparable to the MPLS services offered by Tier 1 providers. **Figure 15** reveals the problems that organizations have encountered when they added the internet to their WAN underlays. The biggest issue is security risk. The internet is a public network that is inherently insecure. SD-WAN solutions can mitigate this issue, but security risk remains a top concern. The largest companies in our survey were the most concerned about security.

The second-biggest challenge is ISP complexity. Many enterprises find themselves working with multiple regional providers, and the management of these provider relationships becomes complex. The IT governance group (which owns vendor relationships) and the network operations team (which will often escalate tickets to an ISP's customer support organization) were the most likely to struggle with this issue.

Other leading challenges include poor monitoring, poor application performance, and poor quality or instability across different ISPs. The latter two challenges were more common in larger companies.

FIGURE 15. BIGGEST CHALLENGES TO USING THE INTERNET FOR PRIMARY WAN CONNECTIVITY

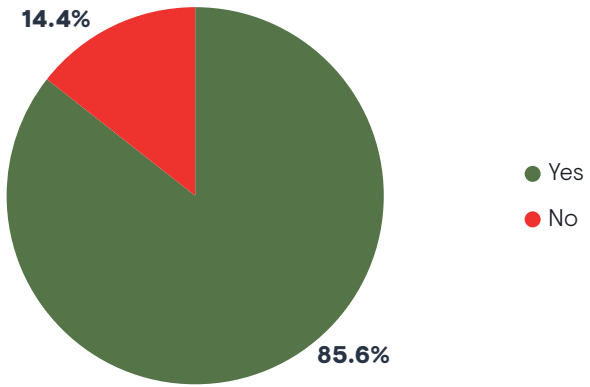


Sample Size = 313, Valid Cases = 313, Total Mentions = 572

Wireless WAN Connectivity

In this section, we explore the extent to which enterprises are adding wireless WAN services, like 5G, to their WAN underlays. **Figure 16** reveals that nearly 86% of enterprises are using wireless WAN services to connect sites to their networks. Smaller companies are more likely to be doing this.

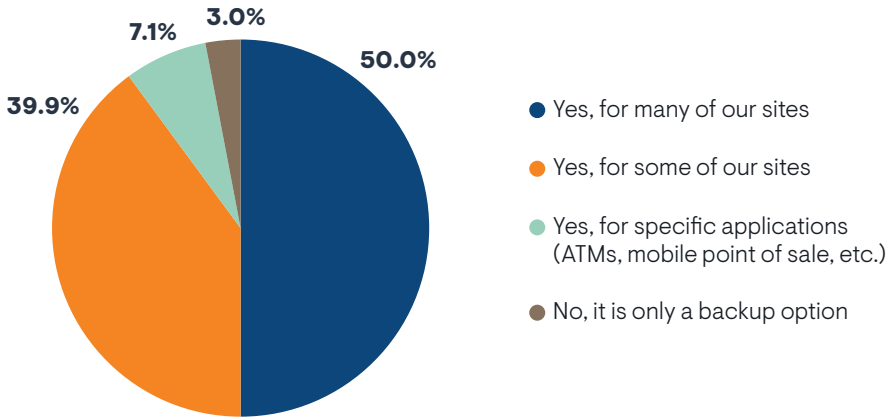
FIGURE 16. DOES YOUR ORGANIZATION USE OR PLAN TO USE WIRELESS CELLULAR SERVICES, LIKE 4G OR 5G, TO CONNECT ANY OF ITS SITES TO ITS WAN?



Until recently, wireless WAN services lacked the bandwidth and performance to serve as a primary WAN connection for most enterprise sites. Instead, companies used these services as a backup connection. With 4G and 5G services, wireless WAN offers enough bandwidth and performance to address the needs of many corporate sites. **Figure 17** reveals that only 3% of wireless WAN users use them solely as backup connectivity today. The rest are deploying it at least occasionally as a primary WAN connection.

Sample Size = 313

FIGURE 17. DOES YOUR ORGANIZATION USE THIS WIRELESS CONNECTIVITY AS A PRIMARY WAN CONNECTION FOR ANY OF ITS SITES?



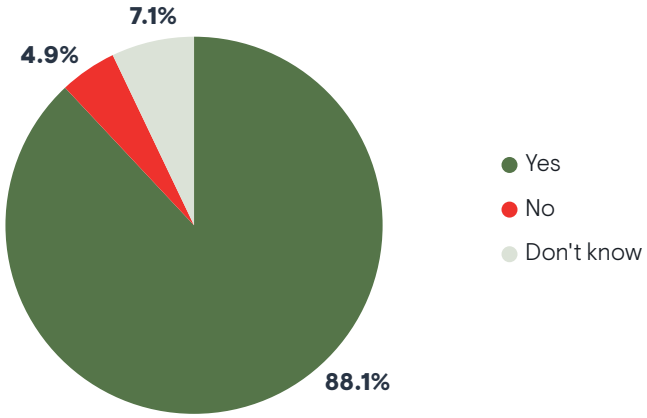
SD-WAN appears to drive the use of wireless WAN connectivity. Organizations that have fully implemented an SD-WAN solution are much more aggressive with their use of wireless as a primary WAN connection. Organizations that are more successful with SD-WAN are also more aggressive. Meanwhile, 20% of companies that are still in the planning stages with SD-WAN are using wireless solely as a backup connection.

Sample Size = 268

SD-WAN and Wireless WAN Integration

Figure 18 reveals that most of the enterprises in this research are integrating their wireless WAN services with their SD-WAN solution. This means that the SD-WAN gateways in their corporate sites have integrated wireless radios, and their SD-WAN solutions can apply features like path steering and application QoS to wireless WAN links.

FIGURE 18. IS THIS 4G/5G CONNECTIVITY INTEGRATED INTO YOUR SD-WAN SOLUTION, OR WILL IT BE IN THE FUTURE?

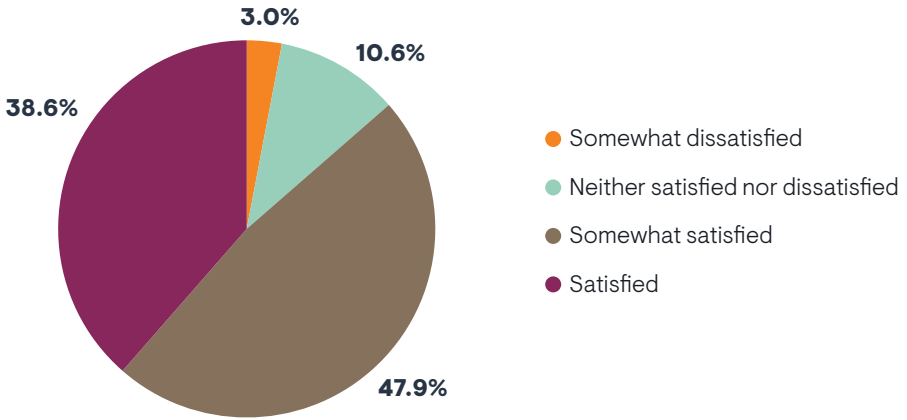


Smaller companies were more likely to have this integration. Members of the network engineering team were less likely (74%) than members of the CIO's suite (90%), the IT architecture group (98%), and the cybersecurity group (96%) to perceive this integration. Given that the network engineering team is most likely to own SD-WAN and wireless WAN connectivity, EMA believes the actual rate of integration is lower.

Sample Size = 268

Figure 19 reveals how satisfied organizations are with how their SD-WAN solution integrates wireless WAN connectivity. Nearly 39% reported being completely satisfied. Another 48% reported having some satisfaction, but they saw room for improvement. Satisfaction was highest among organizations that reported the highest level of success with their SD-WAN solutions, which is no surprise.

FIGURE 19. HOW SATISFIED ARE YOU WITH HOW YOUR SD-WAN SOLUTION INTEGRATES 4G AND 5G TECHNOLOGY INTO YOUR OVERALL NETWORK?



Engineers and admins were less satisfied than network architects, IT executives, and IT middle management. Overall, the IT architecture group and the IT governance group were happiest. Cybersecurity, network engineering, and the CIO's suite were less satisfied.

Sample Size = 236

SD-WAN Operations and Observability

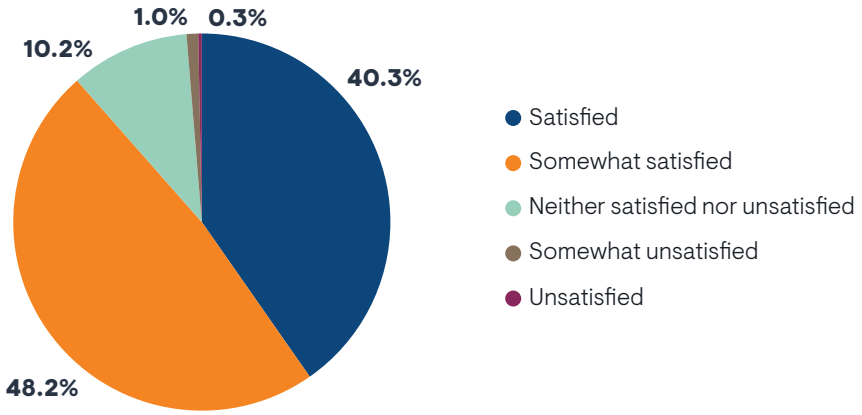
Native Monitoring Features of SD-WAN

SD-WAN solutions offer native monitoring of the SD-WAN overlay. Most of these capabilities consist of GUI consoles with global overviews of the overlay network and dashboard reporting on application performance, site performance, and other KPIs. Some also offer reporting on the WAN underlay.

Satisfaction with these native monitoring features is relatively high. **Figure 20** reveals that more than 40% are completely satisfied, while 48% see some room for improvement. Only 1.3% expressed genuine unhappiness. Satisfaction with this monitoring correlates with overall SD-WAN success. The most successful projects are the happiest, while IT teams that report SD-WAN project failure are giving the monitoring features a failing grade.

EMA observed some signs of trouble when we investigated the silos of an IT organization. The network engineering team and the cybersecurity team are the least happy with their SD-WAN solution's monitoring features. IT executives should be worried when their security teams are unhappy with network visibility. The network engineering team is typically responsible for troubleshooting complex network problems. If they're unhappy, Tier 2 and 3 trouble tickets will be hard to address.

FIGURE 20. SATISFACTION WITH THE NATIVE MONITORING CAPABILITIES OF SD-WAN SOLUTIONS



Sample Size = 313

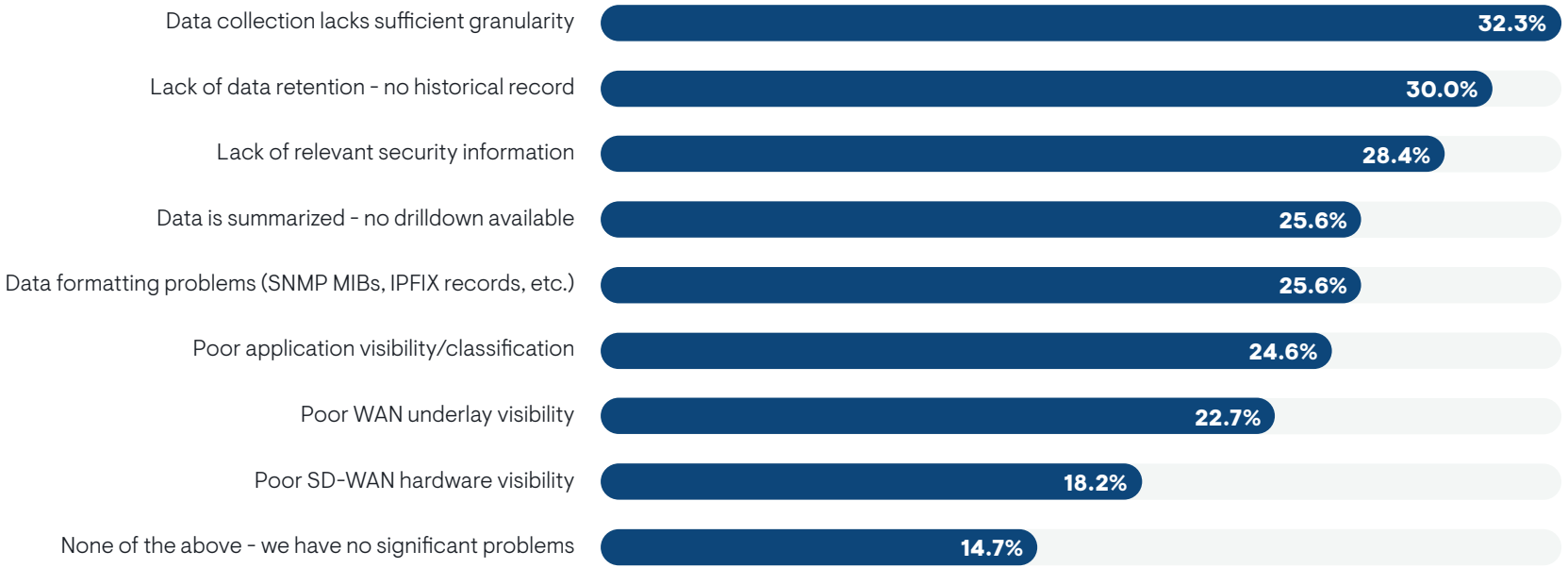
Figure 21 reveals the challenges that enterprises are encountering with native SD-WAN monitoring features. Note that nearly 15% claim to have no significant problems at all. In EMA's experience, it is quite rare to see more than 5% of survey respondents affirmatively indicate in a multiple choice question that they have no problems with a technology. This points to the fact that these features are generally getting the job done, but many see room for improvement.

The biggest issue is data collection granularity. The intervals at which SD-WAN solutions collect telemetry are too long, leaving potential gaps in visibility.

Next, many complained of a lack of data retention and a lack of security insights.

Poor SD-WAN hardware visibility is a minor issue overall, but less successful users of SD-WAN were more likely to struggle with it, suggesting an area of visibility that enterprises should focus on when implementing a solution.

FIGURE 21. THE MOST SIGNIFICANT ISSUES THAT ENTERPRISES EXPERIENCE WITH THE NATIVE MONITORING CAPABILITIES OF SD-WAN SOLUTIONS

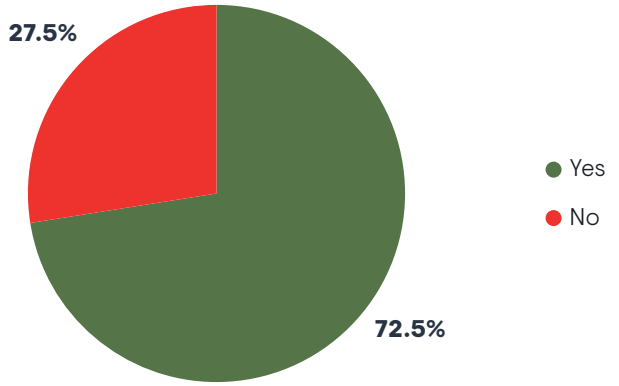


Sample Size = 313, Valid Cases = 313, Total Mentions = 695

Monitoring SD-WAN with NetOps Toolsets

While most enterprises are at least somewhat satisfied with the native monitoring capabilities of their SD-WAN products, most of them are turning to third-party tools anyway. **Figure 22** reveals that nearly 73% of organizations are monitoring their SD-WAN solution with a third-party operations tool. EMA has identified third-party monitoring of SD-WAN as a best practice. Successful users of SD-WAN are more likely (83%) to be doing this, while somewhat successful (67%) and unsuccessful (50%) are less likely.

FIGURE 22. DO YOU USE OR PLAN TO USE ANY THIRD-PARTY NETWORK MONITORING TOOLS TO MONITOR AND MANAGE YOUR SD-WAN SOLUTION?

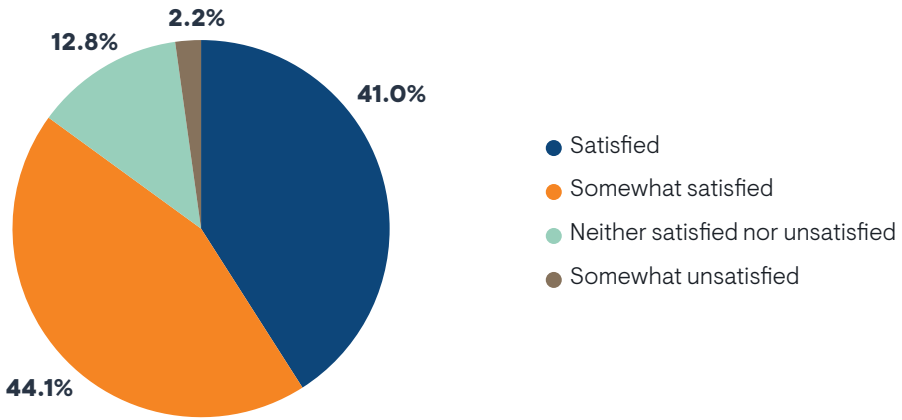


Sample Size = 313

The network engineering team was the least likely IT group to perceive third-party monitoring. The CIO's suite, IT governance, IT program management, and cybersecurity all reported higher rates of third-party monitoring. This suggests that security and asset management may be bigger drivers of third-party monitoring than network troubleshooting. In an earlier section, we noted that data retention (critical to forensic security analysis) and a lack of security insights were two of the three biggest weaknesses in the native monitoring capabilities of SD-WAN solutions.

Figure 23 reveals that 85% of organizations that do it are at least somewhat satisfied with their ability to monitor their SD-WAN environment with third-party tools. However, 44% do see some room for improvement and 2% are straight up dissatisfied. Satisfaction with this monitoring is extremely correlative with overall SD-WAN success, suggesting that effective third-party monitoring is essential. The method an organization uses to enable this monitoring (as covered in the previous chart) had no significant impact on satisfaction.

FIGURE 23. SATISFACTION WITH MONITORING SD-WAN WITH THIRD-PARTY NETWORK MONITORING TOOLS



The network engineering team was the least satisfied with this monitoring. The network operations and cybersecurity teams were somewhat more satisfied. The CIO's suite and the IT governance and IT architecture groups were most satisfied.

Survey data analysis revealed organizations that are unhappy with their third-party monitoring of SD-WAN were more likely to have concerns about the security risk posed by adding the internet to an SD-WAN underlay. This further reinforces that third-party monitoring is a security issue.

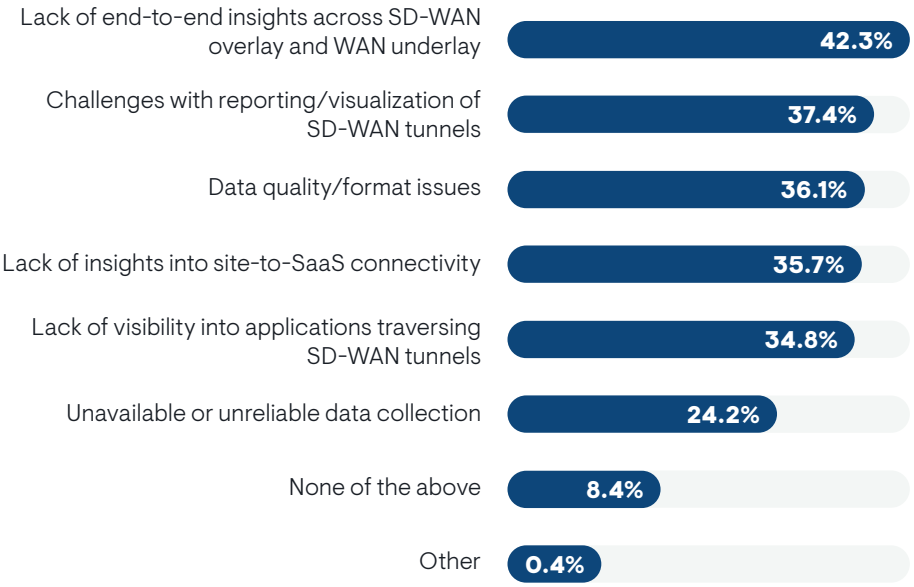
Sample Size = 227

EMA identified several other factors that influence this issue:

- Organizations with multi-vendor SD-WAN environments are less satisfied with third-party monitoring.
- Enterprises that adopt DIY SD-WAN are less satisfied with third-party monitoring than those that adopt a managed SD-WAN service.
- Organizations that rely on their MPLS provider to address their hybrid WAN backbone are less satisfied with third-party monitoring.

Figure 24 reveals the challenges that organizations encounter when they try to monitor SD-WAN with a third-party tool. The biggest issue is a lack of end-to-end insight across the SD-WAN overlay and underlay. Members of IT architecture and cybersecurity teams were especially likely to struggle with this issue.

FIGURE 24. ISSUES THAT CAUSE ORGANIZATIONS THE MOST PAIN WHEN TRYING TO MONITOR SD-WAN WITH A THIRD-PARTY NETWORK MONITORING TOOL



Sample Size = 227, Valid Cases = 227, Total Mentions = 498

There are four secondary sources of pain with third-party monitoring: reporting and visualization on SD-WAN tunnels, data quality, lack of insight into SaaS connectivity, and lack of visibility into applications traversing SD-WAN. Organizations that are less satisfied with their tool's ability to monitor SD-WAN were more likely to cite data quality as an issue. Members of network engineering teams were also unhappy with data quality.

Larger companies struggled more often with seeing the applications crossing their SD-WAN tunnels and smaller companies were more likely to struggle to get insights into site-to-SaaS connectivity.

Single-Pane-of-Glass View of SD-WAN Underlay

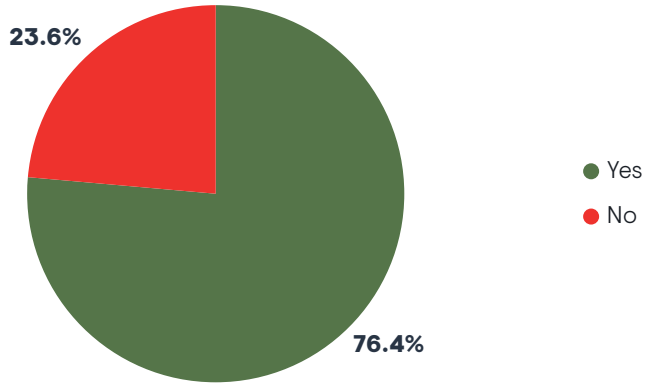
One key piece of effective third-party monitoring of SD-WAN is the ability to get an end-to-end view of the WAN underlay. With multiple links from multiple providers connecting each site, it's critical to have this high-level overview, especially when trying to correlate underlay insights with insights into the tunnels of the SD-WAN overlay.

Figure 25 reveals that 76% of organizations can monitor their SD-WAN underlay from a single console or dashboard. Organizations that can do this were much more likely to report satisfaction with the ability of their third-party tools to monitor SD-WAN.

Organizations with more sites connected to a WAN were less likely to have end-to-end underlay visibility. For instance, only 54% of organizations with 1,000 or more sites were able to achieve this.

Members of the network operations team were the least likely to report that they have this central monitoring capability with the underlay. Members of the network engineering team were more confident and members of the IT architecture and IT governance groups were the most convinced.

FIGURE 25. IS YOUR ORGANIZATION ABLE TO MONITOR ITS SD-WAN UNDERLAY FROM A "SINGLE PANE OF GLASS" (E.G., A CENTRAL CONSOLE OR DASHBOARD)?

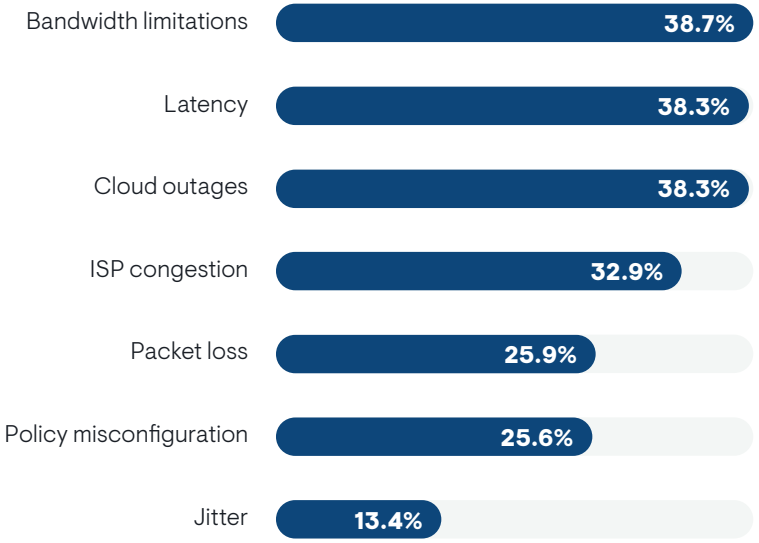


Sample Size = 313

WAN Application Performance Issues

Figure 26 reveals the application performance problems that organizations most struggle with on their WANs. There are three chief issues: bandwidth limitations, latency, and cloud outages. The cybersecurity team was more likely than the network engineering team to perceive bandwidth limits as an issue. Given their expertise, the network engineering team may be suggesting that bandwidth is not as big a problem as this survey suggests, especially with the internet offering an affordable route to supplementing overall WAN bandwidth. Network operations and IT governance teams were more likely to cite cloud outages as a source of trouble, while the IT architecture group, the CIO's suite, and cybersecurity were less concerned. The largest companies in this research were the most likely to report problems with latency.

FIGURE 26. APPLICATION PERFORMANCE PROBLEMS THAT NETWORK TEAMS ARE MOST STRUGGLING WITH ON THE WAN

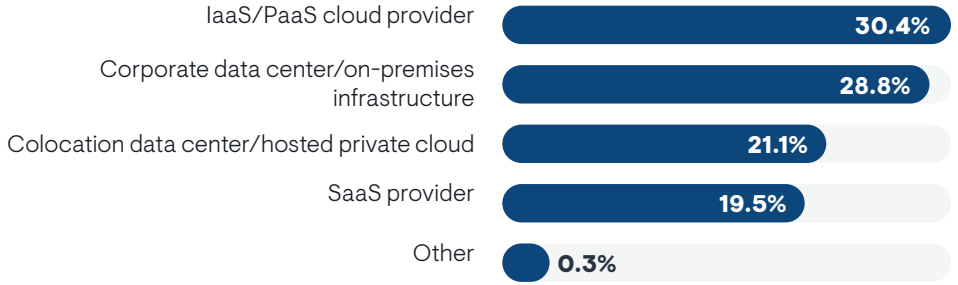


Sample Size = 313, Valid Cases = 313, Total Mentions = 667

ISP congestion was a secondary issue for organizations, and this was especially challenging for smaller companies in our survey. Jitter was the least problematic source of application trouble, but smaller companies identified it as a top issue. Policy misconfigurations, another minor issue, was more challenging for larger companies.

Figure 27 reveals the locations of applications that are having the most performance trouble on the WAN. Respondents singled out public cloud as the biggest source of application performance trouble, followed closely by corporate data centers and on-premises infrastructure. Members of the CIO's suite, the IT governance group, and cybersecurity were more likely to perceive the cloud as a source of trouble. Network engineering, IT architecture, and network operations teams were less likely to single out the cloud.

FIGURE 27. LOCATION OF APPLICATIONS (OF ANY TYPE) THAT STRUGGLE MOST ON THE WAN



Colocation data centers or hosted private cloud providers and SaaS providers were both less likely to cause application trouble. However, network engineering and network operations teams were both much more concerned than other groups about SaaS providers, suggesting that network teams have poor visibility into these providers. Larger companies were more likely to perceive colo data centers as a source of trouble, while smaller companies struggled more often with the public cloud.

Sample Size = 313

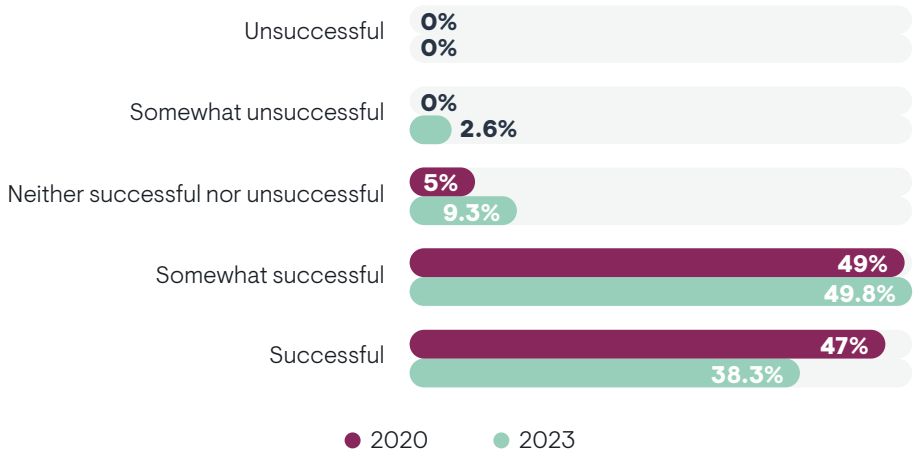
Overall SD-WAN Outcomes

Success and Failure

EMA often asks research participants to rate their overall success with a given technology. In our experience, IT professionals rarely give themselves a failing grade in this context, given that we are basically asking them to assess themselves as key decision-makers on technology strategy. Thus, we usually look at the difference between those who rate themselves as completely successful and those who see room for improvement (somewhat successful).

Figure 28 reveals that just 38% believe they've been completely successful with their SD-WAN solutions so far, while nearly 50% see room for improvement. A small number admitted to being somewhat unsuccessful. The chart also reveals how enterprises answered this question in December 2020. Overall, the number of enterprises that are doing very well with the technology has declined, but most of that decline is due to a larger number of organizations that are feeling neutral about overall success today. Most of these neutral organizations are still in the evaluation and vendor testing stage with SD-WAN. In other words, EMA captured a cross-section of the market that is more likely to be in the earlier stages of SD-WAN engagement than we did in 2020. Still, the slight rise in unsuccessful SD-WAN projects this year is concerning.

FIGURE 28. OVERALL SUCCESS WITH SD-WAN IMPLEMENTATIONS SO FAR



Smaller companies were the most optimistic. The IT governance and IT architecture groups and the CIO's suite were all more confident in SD-WAN success. Network engineering, network operations, and cybersecurity were all more pessimistic, suggesting that critical technical personnel are seeing cracks in the foundation that people further up the reporting chain are missing.

Some SD-WAN Best Practices

Throughout this research, we've pointed out where successful users of SD-WAN are doing things differently. Here are some additional best practices for readers to consider.

Procurement strategy: Enterprises that prefer managed SD-WAN services reported more success with the technology than enterprises that prefer DIY implementation.

Single-vendor network: Organizations that use or plan to use only one SD-WAN vendor are much more likely to report a highly successful SD-WAN implementation, while those that use two or more are likely to see room for improvement.

Full mesh topology: SD-WAN implementations with a full mesh topology were more successful than those with a partial mesh or hub-and-spoke networks.

Third-party monitoring: Organizations that had satisfactory visibility into SD-WAN with their third-party network operations tools were doing better with SD-WAN outcomes overall.

Benefits of SD-WAN

Figure 29 reveals the benefits that enterprises are getting from their SD-WAN investments. The biggest opportunity is improved network security. Network engineering, network operations, and cybersecurity personnel were the most likely to perceive this benefit.

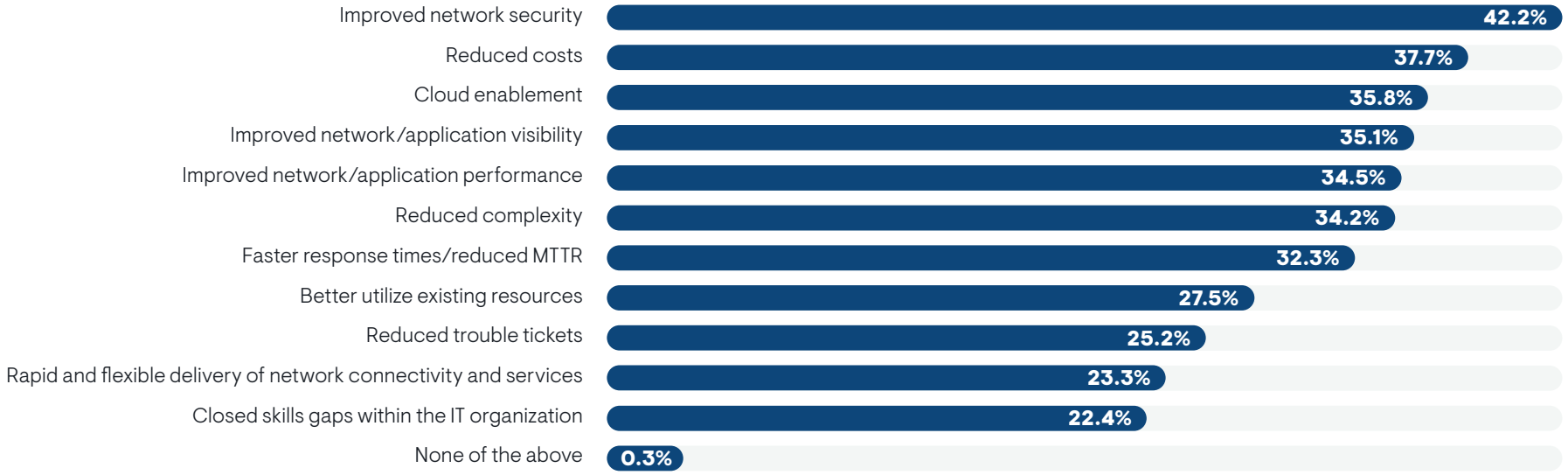
There are several secondary benefits, beginning with reduced costs, cloud enablement, and improved operational visibility. Organizations with a larger number of WAN-connected sites were more likely to benefit from cloud enablement and improved visibility, as well as reduced trouble tickets. Improved network and application performance was another secondary benefit, and it was especially recognized by the largest companies in this research.

Cybersecurity personnel were more likely to perceive the benefits of faster response times and better utilization of existing resources. Successful users of SD-WAN in general singled out faster response times as a big opportunity, too.

The vice president of architecture for a $5 billion energy company said SD-WAN has improved network performance and visibility and allowed him to improve overall utilization of resources. His legacy network was a major source of pain for the company that burned out his network team. "Everyone was affected across the board, including our headquarters and our refineries. Those sites were going down and up on a recurring basis. The network team was literally running around and putting out fires every day. It was chaotic."

Rapid and flexible deployment of services is a relatively minor driver, but a network engineer with a $24 billion manufacturer put it at the top of his list. "The number-one benefit of SD-WAN is flexibility, to be able to stand up an entire branch within minutes."

FIGURE 29. BENEFITS THAT ORGANIZATIONS HAVE EXPERIENCED OR EXPECT TO EXPERIENCE FROM THEIR USE OF SD-WAN TECHNOLOGY



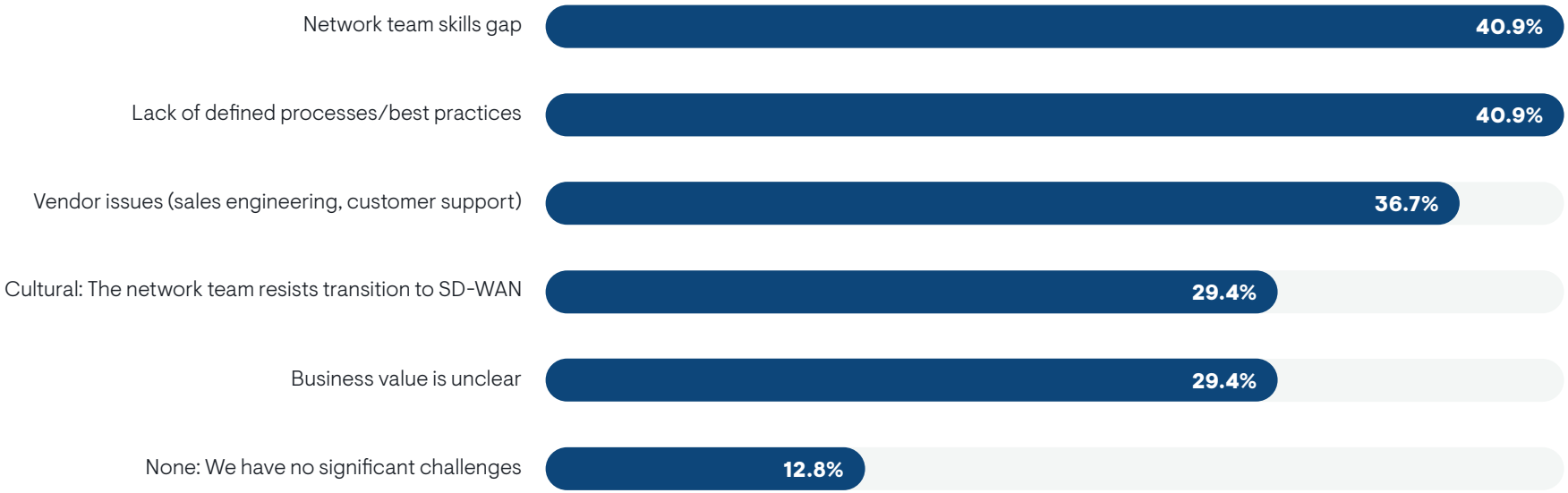
Sample Size = 313, Valid Cases = 313, Total Mentions = 1,097

Technical and Business Paint Points

This section explores the issues that might cause an organization to stumble with its SD-WAN investment. **Figure 30** identifies the business issues that are causing the most trouble. Overall, 87% are experiencing at least one significant problem. There are two major issues: network team skills gaps and a lack of defined processes and best practices for SD-WAN.

EMA perceives a gap between the CIO's suite and the rest of the IT organization on several key issues. This executive office is less likely to perceive problems with network team skills gaps, defined processes and best practices, and vendor relationship issues, such as sales engineering and customer support engagement. The latter two issues are of special concern to the cybersecurity team, so CIOs should take note.

FIGURE 30. BUSINESS CHALLENGES THAT CAUSE AN ORGANIZATION THE MOST PAIN WITH ITS SD-WAN IMPLEMENTATION

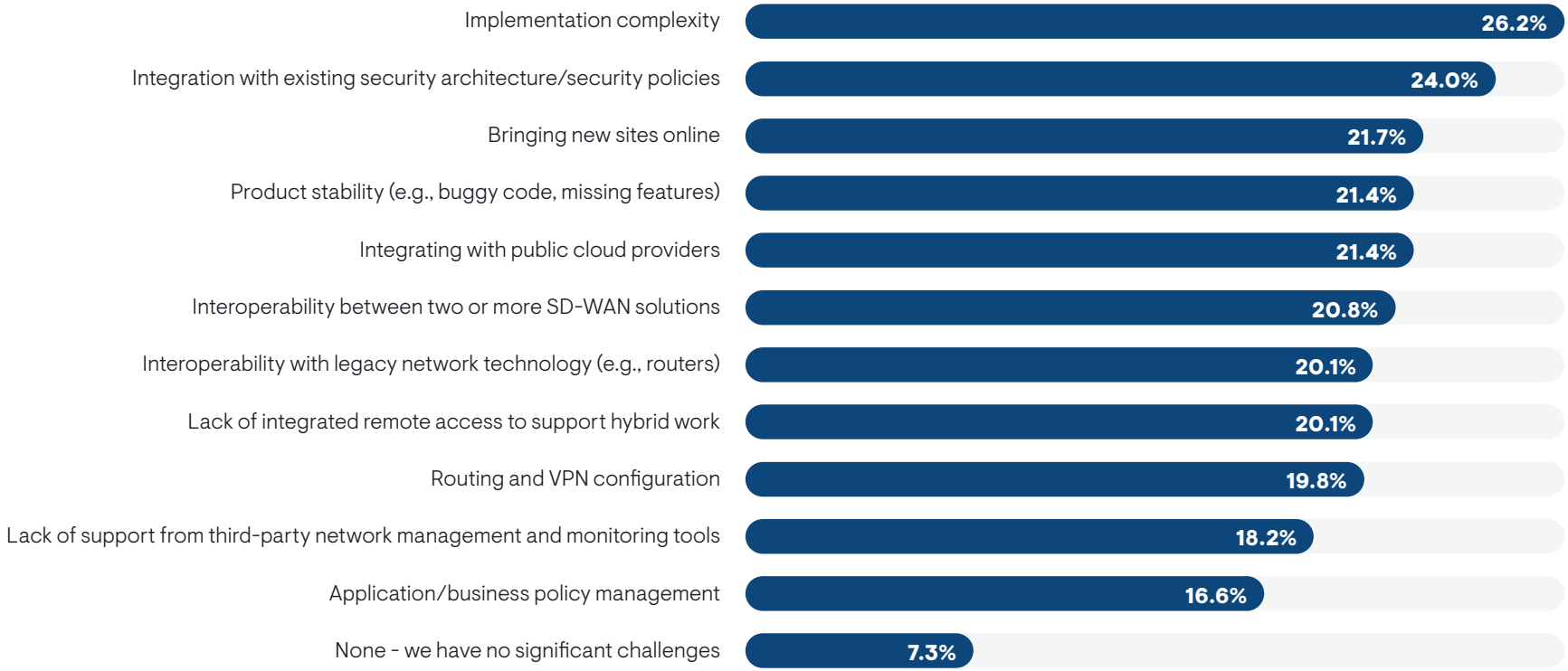


Sample Size = 313, Valid Cases = 313, Total Mentions = 595

Marketing hype is another issue that can obscure business value, according to a senior network engineer with a $100 million manufacturer. "The biggest frustration with SD-WAN has been cutting through all of the marketing BS and trying to figure out what it actually means," he said. "Every single vendor seems to have a different interpretation on what SD-WAN actually means."

Figure 31 reveals that nearly 93% of organizations are experiencing at least one major technical issue with SD-WAN. The two biggest problems are implementation complexity and integration with existing security architecture and policies. Implementation complexity was a more common problem for less successful users of SD-WAN technology, suggesting that this is an issue that can make or break a project. The network operations team was more likely than other groups to perceive both as major issues. The cybersecurity team was also more aware than other groups of implementation complexity.

FIGURE 31. TECHNICAL CHALLENGES THAT CAUSE AN ORGANIZATION THE MOST PAIN WITH ITS SD-WAN IMPLEMENTATION



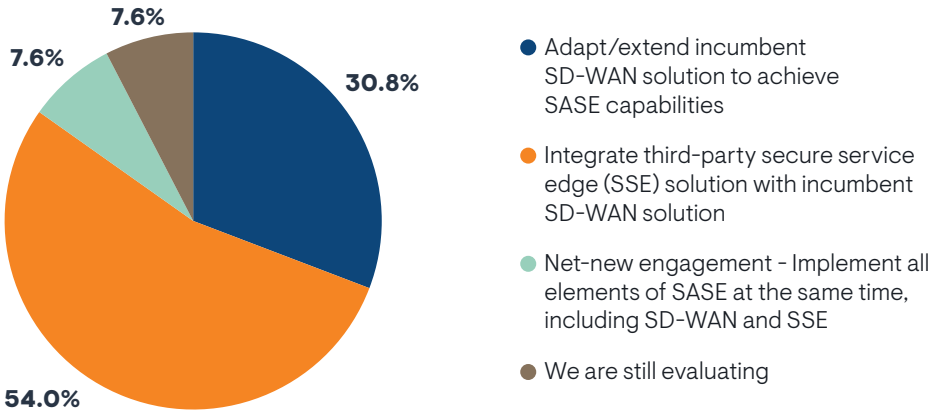
Sample Size = 313, Valid Cases = 313, Total Mentions = 744

The Transition to SASE

Vendor Strategy

Figure 32 reveals how organizations are navigating their journey from SD-WAN to SASE. Most companies plan to integrate a third-party secure service edge (SSE) solution with an incumbent SD-WAN solution. This approach is very popular in the CIO's suite, but members of network engineering and cybersecurity teams were unlikely to embrace it.

FIGURE 32. PREFERRED PATHS FROM SD-WAN TO SASE



Sample Size = 302

The largest minority is planning to adapt or extend its incumbent SD-WAN solution to achieve SASE, essentially adding SASE features from their strategic SD-WAN vendor. This approach is most popular among organizations that have already completed an SD-WAN implementation. Network engineering and cybersecurity personnel were more likely to favor this approach than other groups.

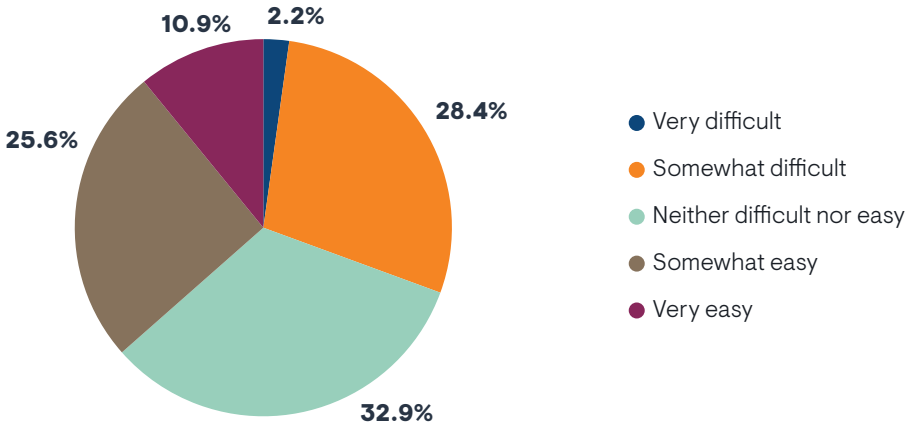
A small number of companies is pursuing a net-new engagement, implementing all elements of SASE at the same time, including SSE and SD-WAN. This approach is very popular among organizations that are unsuccessful with their SD-WAN solutions, suggesting that they plan to rip and replace a failed SD-WAN technology with a new SASE solution.

Nearly 26% of the largest companies in this research (10,000 or more employees) were still evaluating their course of action with SASE, suggesting that they are uncertain how to proceed.

Transitioning From SD-WAN to SASE

Figure 33 reveals that many organizations are having a bumpy ride along the path from SD-WAN to SASE. Less than 11% described this evolution as very easy. Instead, nearly 31% believe it's at least somewhat difficult. Another 25.6% describe it as somewhat easy, meaning they think it could be a smoother transition.

FIGURE 33. DO YOU THINK IT IS DIFFICULT OR EASY TO ADVANCE FROM AN SD-WAN PLATFORM TO ADOPTING A FULLY INTEGRATED SASE SOLUTION?



Research participants that told us they are extending their existing SD-WAN implementation to achieve a SASE solution were more likely to have an easy time with this transition.

As organizations decide between a single-vendor or multi-vendor SASE strategy, three considerations appear to help them on their journey. IT teams that focus on best-of-breed SSE and SD-WAN capabilities, strategic vendor relationships, and pace of innovation all reported an easier transition. Larger companies were more likely to struggle with the SASE transition.

Organizations that have had SD-WAN in place for at least four years were the most likely to report that their transition to SASE was easy, suggesting that a mature SD-WAN foundation makes the transition to SASE less rocky.

Sample Size = 313

An SD-WAN foundation will set you up for success if you follow a couple of other recommendations.

Single-vendor SD-WAN: Enterprises that use two or more SD-WAN vendors were more likely to struggle with SASE.

Managed solutions: Enterprises that prefer managed SD-WAN over a DIY SD-WAN implementation reported an easier transition to SASE. Undoubtedly, that SASE solution is also a managed service.

Hybrid Day 2 operations: Organizations that outsource or completely in-source SD-WAN operations struggle with SASE more than those that adopt a shared model with the IT organization and the managed services provider co-owning Day 2 operations.

Strong integration with 4G/5G: Organizations that have tight integration between SD-WAN and wireless WAN services do better with their SASE transition.

Full mesh topology: Organizations that adopt a full mesh network with their SD-WAN and SASE solutions experienced less difficulty than those that implement a partial mesh or hub-and-spoke network.

WAN acceleration: Organizations that apply WAN acceleration to their networks have an easier time, especially if that acceleration is applied to all network paths.

End-to-end WAN underlay visibility: Organizations that have a single dashboard view of their entire WAN underlay were more likely to have an easy path to SASE.

Don't chase lower prices: Respondents who told us they would switch SD-WAN vendors to save money had an extremely difficult time with their SASE journey.

Conclusion

IT organizations still have work to do with WAN transformation. Many SD-WAN implementations are solid, but most of them could be improved upon. EMA believes that enterprises need to embrace a managed services procurement model for SD-WAN, but they must hold fast to a hybrid approach to Day 2 operations, sharing change management and monitoring and troubleshooting responsibilities with their managed SD-WAN providers. Day 2 operations will require deep integration between SD-WAN solutions and incumbent network operations tools. It will also require the ability to have an end-to-end view of the WAN underlay, since many SD-WAN solutions lack the ability to provide this insight effectively.

Enterprises must also prepare for a future in which wireless WAN connectivity and secure remote access for hybrid work are integral parts of SD-WAN implementations.

SD-WAN is undeniably the foundation of SASE, which appears to be the future of networking and security. This research established that many enterprises, especially larger ones, are struggling with their transition from SD-WAN to SASE. Enterprises are split on what path they will take to SASE. Many intend to take a single-vendor approach with their existing SD-WAN solution provider, while many others believe that they should follow a best-of-breed approach that integrates SD-WAN with a third-party SSE provider. Regardless of the path they choose, enterprises must establish that firm SD-WAN foundation. The network is the bedrock of SASE. It is not simply something you can turn on with the click of a button in a SASE console. This research offered plenty of advice on how to build that foundation. EMA will continue to explore this topic in future research to help enterprises maximize their success.

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

4257.041123