RESEARCH SUMMARY: WIDE-AREA NETWORK TRANSFORMATION

How Enterprises Succeed with Software-Defined WAN

ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) Research
Written by Shamus McGillicuddy
December 2018

SPONSORED BY:

infovista

EMA™

IT & DATA MANAGEMENT RESEARCH • INDUSTRY ANALYSIS • CONSULTING

TABLE OF CONTENTS

Executive Summary

This research summary highlights the results of new research from Enterprise Management Associates (EMA), "Wide-Area Network Transformation: How Enterprises Succeed with Software-Defined WAN." Based on a survey of 305 enterprise WAN decision-makers and subject matter experts, this research examines all aspects of WAN transformation, from cloud enablement to internet migration, and then looks at how SD-WAN fits into the picture.

Introduction: A WAN Revolution

Enterprise Management Associates (EMA) recently published "Wide-Area Network Transformation: How Enterprises Succeed with Software-Defined WAN," a survey-based research report that examines how enterprises are modernizing their wide-area networks (WANs). This research summary highlights the findings of that research, including an examination of how SD-WAN is enabling enterprises to support new technology and business initiatives

Research Methodology

This research is based upon an online survey of 305 IT professionals at distributed enterprises. To qualify for this survey, respondents had to meet several key criteria.

Direct Involvement in the WAN

Each research participant had to be directly involved in planning, implementing, or managing their organization's WAN. The average respondent was involved in at least five aspects of the WAN lifecycle. **Figure 1** reveals their responses when asked to identify the one stage of the WAN lifecycle in which they were primarily involved. The majority of them typically manage and monitor the network, either for performance, security, or capacity optimization. A minority are involved in evaluating WAN technology, procuring it, or implementing it on their network. Thus, most of these respondents are network operators and a minority are network planners.

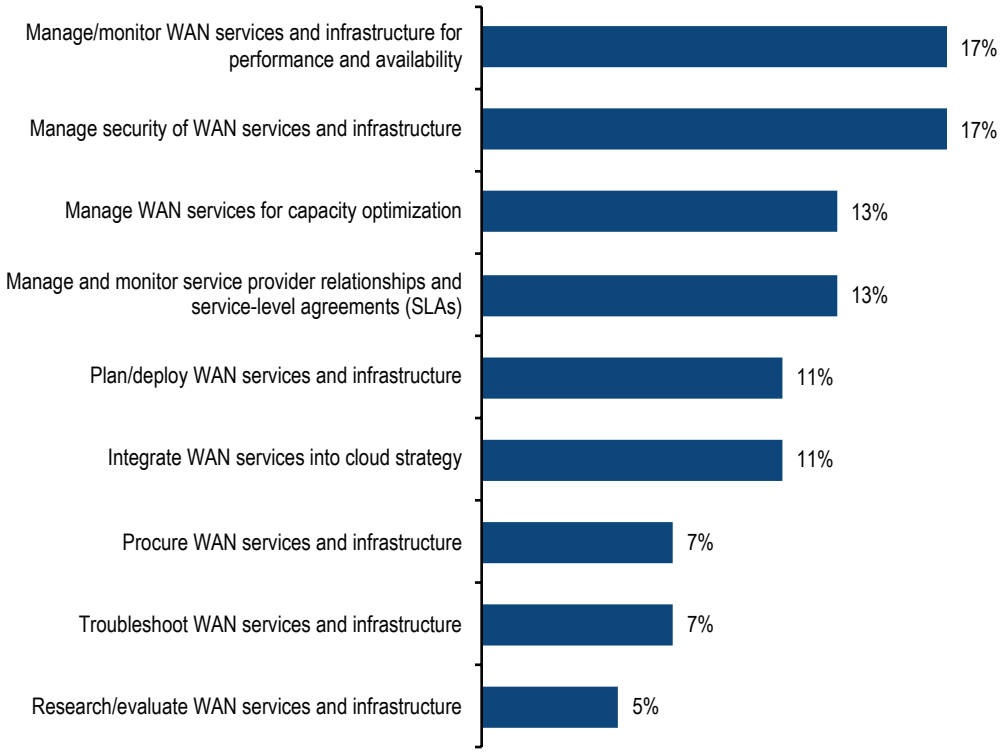

Figure 1. On which aspect of your organization's WAN planning/management/operations are you primarily focused?

Minimum Number of Sites on the WAN

Each participant's organization had to have a minimum of 30 remote sites or branch offices connected to the WAN. **Figure 2** reveals a wide range of responses. Fifteen percent had 30 to 50 sites on the network, and seven percent had more than 1,000 sites.

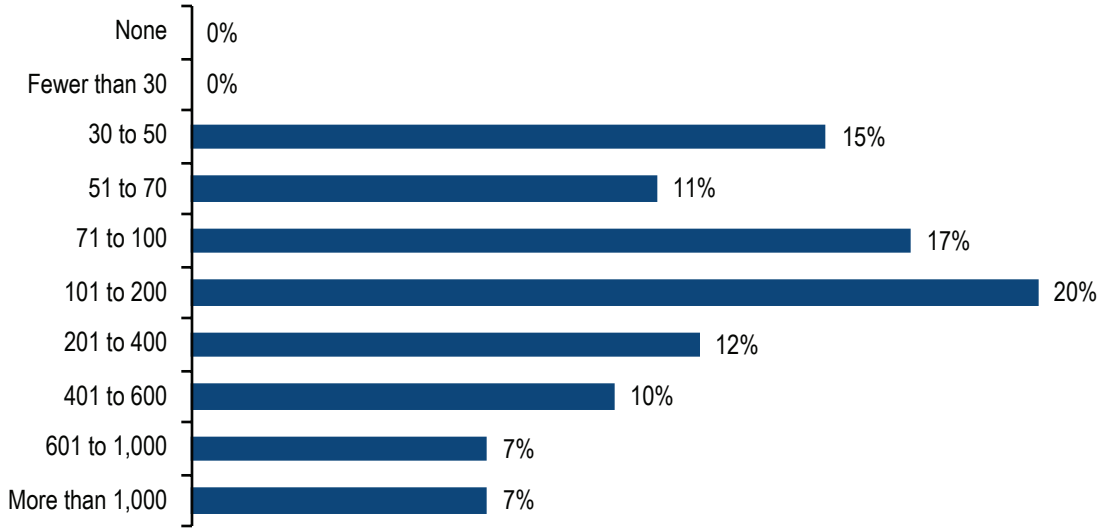

Figure 2. How many remote sites does your company have connected to its WAN?

To understand how networks of different sizes are built and managed, EMA grouped these responses into three categories:

Other Qualifiers for Research Participation

Subject matter expertise: EMA required all respondents to work within an IT organization and to possess a minimum level of subject matter expertise. Anyone who worked in a low-level position (e.g., IT administrator) was dropped from the survey.

Size of company: EMA targeted enterprises with this survey. Thus, EMA set minimums for global employee totals and annual revenue. At the time of this survey, each respondent worked for an organization with at least 500 employees and $20 million in revenue.

Drivers of Change: Technical Initiatives and Business Trends

EMA asked enterprises to identify the business issues and the technical initiatives that are most impacting their overall WAN strategies. Responses to these questions reveal why so many enterprises are transforming their WANs today.

Technical Initiatives Influencing WAN Strategy

Figure 3 reviews the technical initiatives that guide enterprise WAN strategy. Security is by far the biggest technical driver, which is both surprising and unsurprising. It's unsurprising given the fact that EMA research found security to be a major driver of network strategy in general for well over a decade. However, this security focus is somewhat surprising in the context of this research, given that security is not a major technical challenge to the WAN. Enterprises that spend a minimal amount of their IT budgets on the WAN (less than 15 percent) are the most focused on security (46 percent).

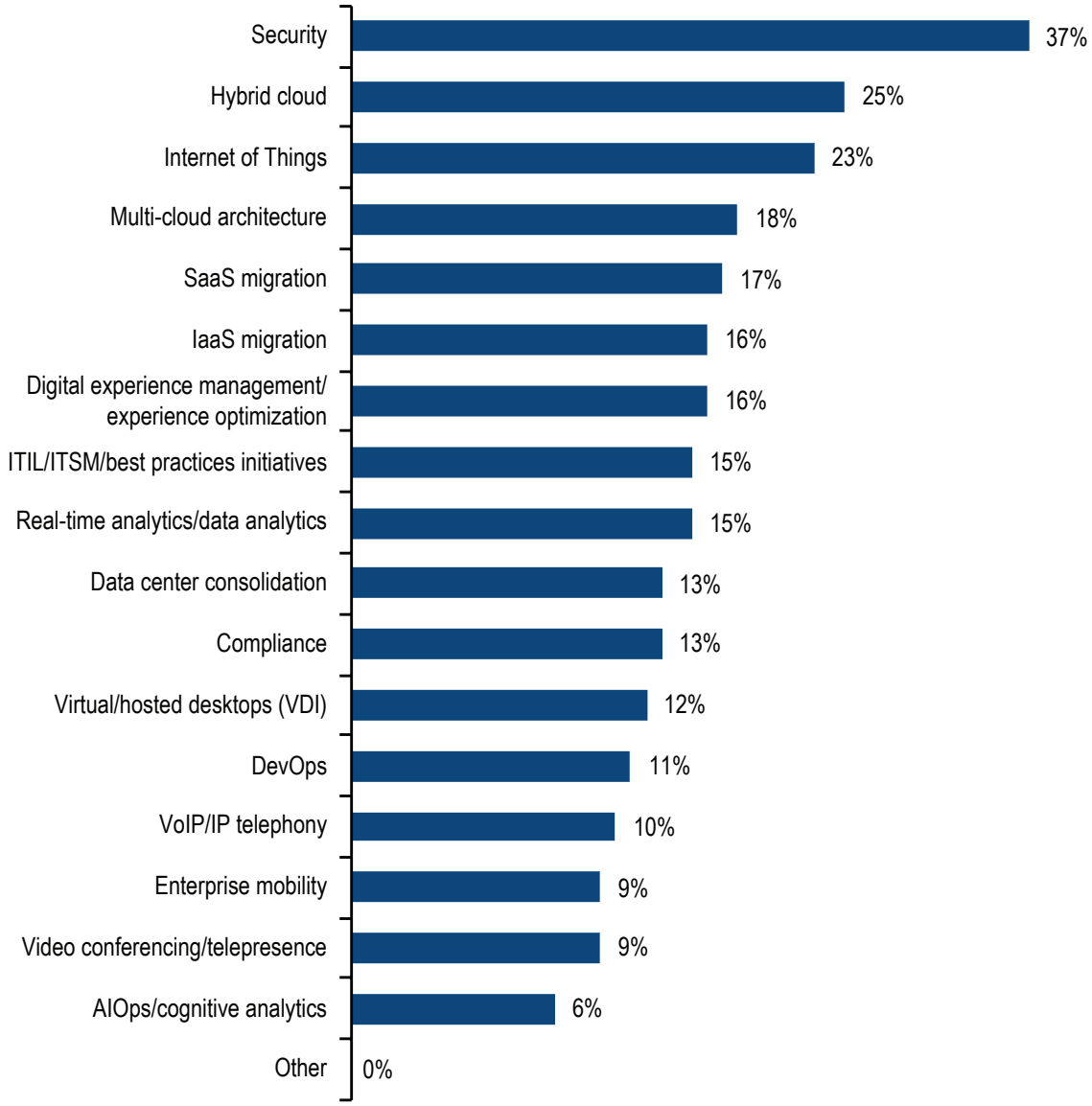

Figure 3. Technology initiatives that are most influential on your wide-area network strategy

Hybrid cloud and the Internet of things (IoT) are the next two most common technical drivers. Hybrid clouds, which span both private infrastructure and public cloud infrastructure, impact technology in a number of ways. First, the network interconnects between private and public infrastructure will require attention. Second, with applications spanning both of these environments, enterprises will need to re-architect how remote sites connect to corporate applications.

IoT creates even a broader set of variables. IoT devices at corporate branches can impact both WAN and LAN infrastructure. Then, there is the complication of IoT devices connecting from remote locations, like farms, vehicles, weather monitoring probes, and so on. These devices will need connectivity from unusual and challenging locations.

The next three leading drivers are multi-cloud architecture, SaaS migration, and IaaS migration. Together with hybrid cloud, these three drivers make it quite clear that cloud technology in general is a major influence on WAN strategy. IT executives tend to be more cloud-focused than staff, citing hybrid cloud (31 percent), IaaS (22 percent), and SaaS (27 percent) as influences on WAN strategy more often. This latter finding suggests that IT executives are more focused on long-term cloud strategy and preparing the network for a shift toward the cloud.

Organizations with larger WANs tend to prioritize some of the initiatives toward the bottom of the list in Figure 6. For instance, organizations with more than 400 remote sites list compliance (22 percent), digital experience management (22 percent), and DevOps (19 percent) more often. Mobility is a major driver for organizations with 101 to 400 sites (46 percent).

Business Strategies and Initiatives Influencing WAN Strategy

Business growth and digital business transformation are the two most influential business drivers of WAN strategy, according to **Figure 4.** IT executives (47 percent) cite digital business transformation as a driver at a much higher rate than IT staff (24 percent). IT executives are also more focused on corporate restructuring (23 percent). North Americans (41 percent) are more focused on business growth and digital transformation (40 percent) than Europeans (25 percent for both).

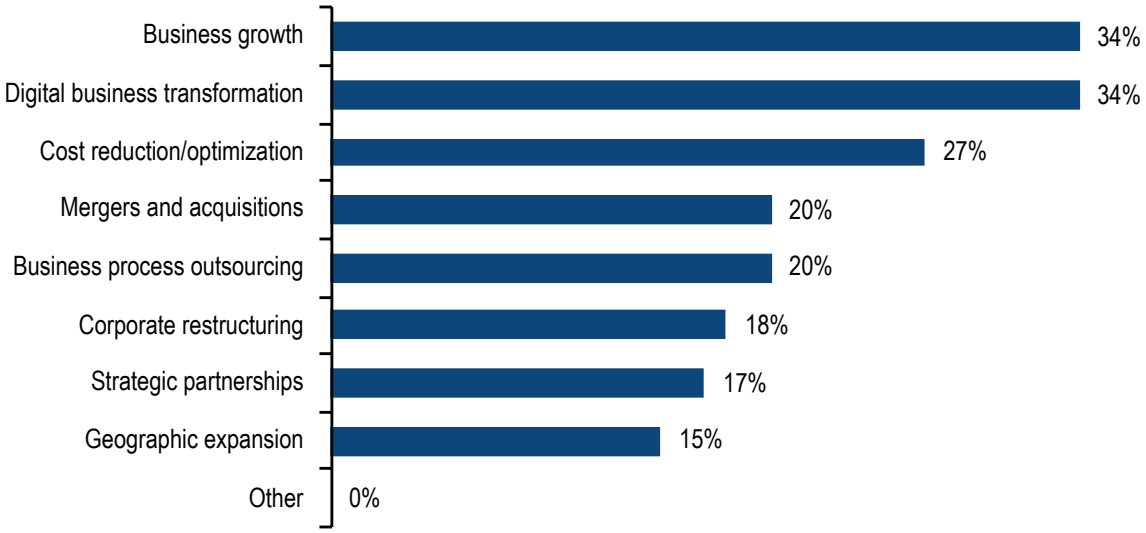

Figure 4. Business initiatives/strategies that are most influential on wide-area network strategy

Cost reduction and optimization is also a significant influence. IT staff (33 percent) are more focused on cost than IT executives (20 percent). Other business initiatives were less impactful in general, especially strategic partnerships and geographic expansion. Europeans (21 percent) prioritize geographic expansion more than North Americans (12 percent).

The Cloud: Forecasting Tremendous Traffic Growth

Clearly, the cloud is both a major strategic driver and a significant challenge for the enterprise WAN. Furthermore, this isn't about the future. Cloud migration is already in full swing, and it will only continue. The average enterprise in this survey can already trace 48 percent of the network traffic at branch offices and remote sites to public cloud applications, such as SaaS and IaaS environments. This finding has major implications for WAN architecture, network service assurance, and security, since remote sites clearly need optimized and secure connections to cloud services. Enterprises that rate themselves as very successful with the WAN have a higher percentage of cloud traffic at these remote sites (60 percent), versus just 39 percent of less successful networking organizations. Cloud enablement is also clearly a barometer for success.

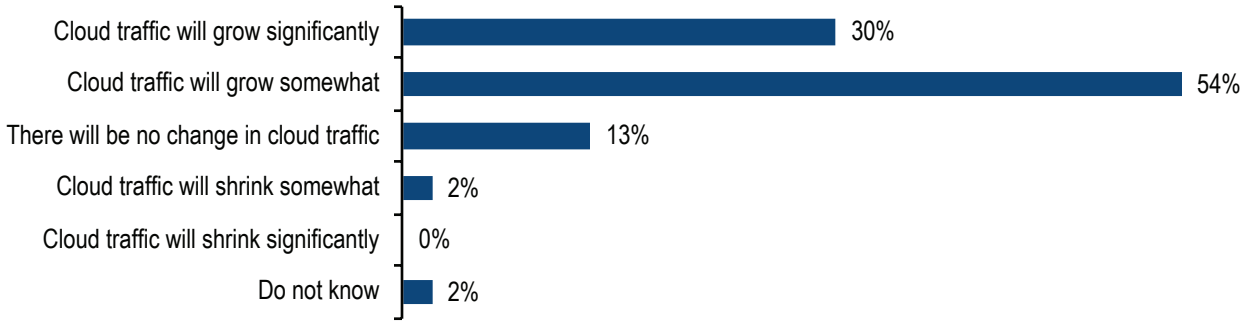

Figure 5. Enterprises projecting the percentage of traffic attributable to external public cloud services at remote sites over next three years.

Again, more successful organizations see the cloud as a bigger factor down the road. Respondents who claim to be very successful with their WAN are more likely (64 percent) to anticipate significant cloud traffic growth, versus only ten percent of less successful respondents. IT executives, who are usually more focused on long-term planning, are also more likely (36 percent) to project significant cloud traffic growth than staff (25 percent).

From a geographic perspective, North Americans see cloud as a bigger traffic factor in the years ahead. Thirty-six percent of North Americans expect significant cloud traffic growth, versus 20 percent of Europeans. Instead, 20 percent of Europeans expect no change in cloud traffic growth, versus eight percent of North Americans.

Enterprises Connecting Remote Sites Directly to Cloud Services

Growth in cloud traffic will force enterprises to re-architect their networks. The easiest and cheapest way to connect to cloud services is via the Internet, but traditional WANs usually have centralized Internet access. Internet-bound traffic is routed from remote sites, across the MPLS network, and into a data center, where access policies and security services are applied. Latency-sensitive cloud applications do not tolerate this approach, so many enterprises are now allowing their remote sites to connect directly to the cloud, as **Figure 6** illustrates. Already, 56 percent of enterprises allow direct cloud connections from remote sites, and most of those require secured cloud connections. Nearly a quarter of companies take an alternative approach, routing cloud traffic through a third-party hub, where cloud connectivity and security services are applied.

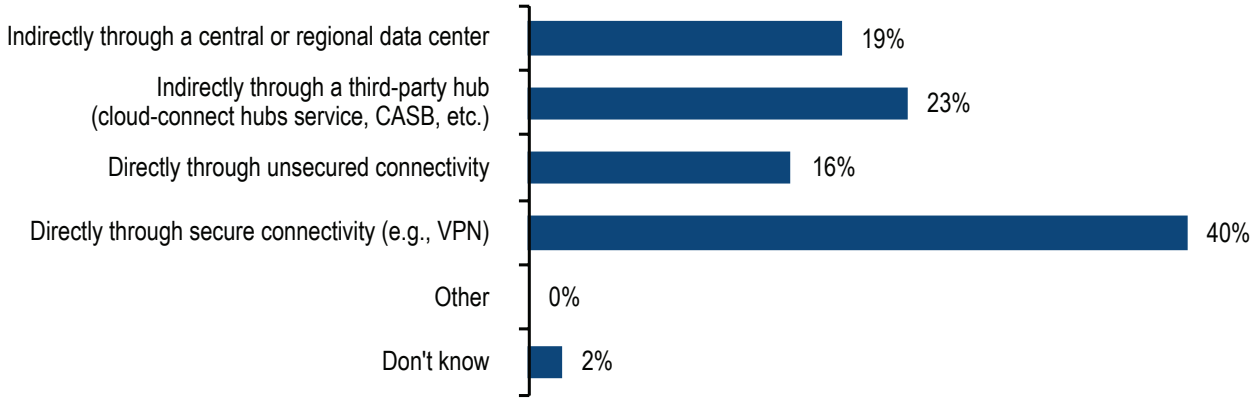

Figure 6. Preferred approach to connecting remote sites to public cloud

Some enterprises might configure routers and firewalls to allow local Internet breakouts from remote sites, but it's difficult to scale this approach securely across large numbers of branch offices. Given that many enterprises are using the cloud for critical applications, this direct connectivity must be well-managed and secured. In fact, in a later section, EMA will explore how enterprises are increasingly using the Internet as a primary connectivity option. This trend, combined with the need for cloud connectivity, is a significant driver of SD-WAN adoption.

WAN Connectivity Trends: Strategic Importance of the Internet

The Rise of Internet-Based WANs

The shift from MPLS-based to Internet-based networking has been widely recognized for quite a few years. Conventional wisdom holds that a hunger for affordable bandwidth and the expanded use of public cloud services drove this shift, and SD-WAN solutions facilitated it. In 2016, EMA found that 74 percent of enterprises were increasing their use of the Internet for primary WAN connectivity.[1] In 2018, EMA found that 87 percent of enterprises are increasing or planning to increase their use of the Internet for primary WAN connectivity. Small (92 percent) and medium enterprises (89 percent) are more aggressive than large enterprises (75 percent).

[1] EMA, "Next-Generation Wide-Area Networking," July 2016.

This rise of the Internet doesn't necessarily mean the death of MPLS and other private WAN services. **Figure 7** shows that only 15 percent of users of Internet-based WANs are actually retiring MPLS connectivity. Twenty-one percent are reducing MPLS bandwidth in favor of the Internet, but not retiring it. A majority (52 percent) simply supplement their MPLS connectivity with the Internet. They are enhancing the WAN—not eliminating MPLS. Healthcare (64 percent) and transportation companies (67 percent) were more likely to supplement MPLS with Internet.

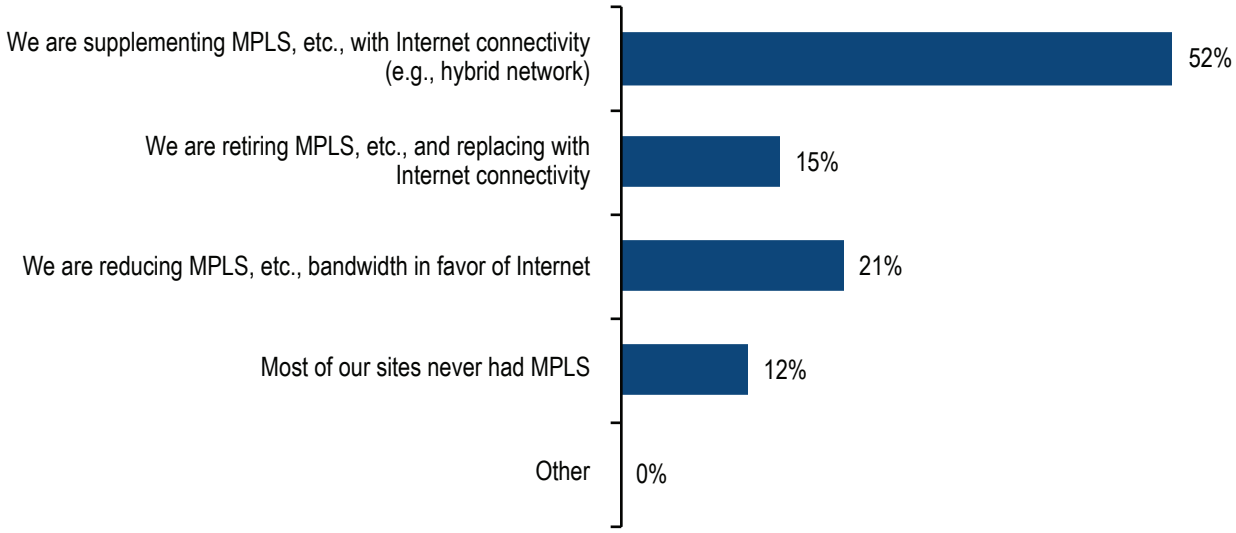

Figure 7. How the increased use of Internet connectivity for enterprise traffic affects the use of private WAN services like MPLS

The internet service provider (ISP) market is much more fragmented and variable than the private WAN services market. These ISPs vary wildly in terms of quality and geographic reach. A global enterprise expanding into an overseas market might find itself choosing between a dozen ISPs that it has never encountered before. This situation can present significant risk to companies that want to shift from MPLS to the Internet.

Figure 8 reveals Internet service procurement strategies for enterprises that are engaged in expanding their use of the Internet for primary WAN connectivity. Enterprises are most likely (41 percent) to work primarily with their private WAN providers, who deliver Internet services as a supplement to MPLS connectivity. These WAN providers might operate their own Internet service and/or partner with local ISPs to deliver a globally integrated service. The popularity of this approach emphasizes how important MPLS providers remain, even as many enterprises decrease their overall reliance on MPLS networks.

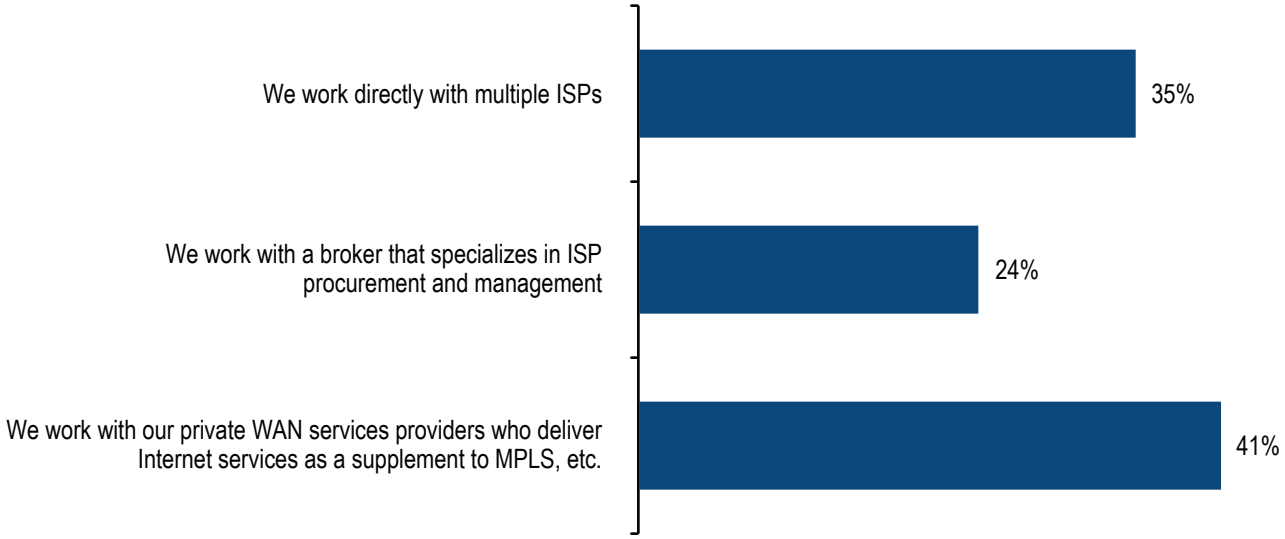

Figure 8. Preferred connectivity procurement strategies for enterprises that expand use of the Internet as a primary WAN connection

Many enterprises (35 percent) take more of a do-it-yourself approach, working directly with multiple ISPs to source Internet connectivity. Depending on geography and other factors, this approach could add complexity. Government organizations, no strangers to complexity, are especially likely (63 percent) to take this approach.

Finally, 24 percent are working with brokers who specialize in ISP procurement and management. Software companies, many of which are probably offering SaaS services, prefer this approach (38 percent).

Drivers of Internet-Based WAN Strategies

Network flexibility and cloud connectivity are the top drivers of the shift toward Internet connectivity, as **Figure 9** reveals. With the Internet, enterprises are able to make quick changes to the network, such as VPN configuration changes or cloud connectivity changes. The Internet is inherently easier to configure than most private WAN services, and is also very cloud-friendly, since this is the most common and affordable connectivity option for accessing public cloud services. For instance, connecting to Amazon Web Services or Microsoft Azure via the Internet is much more affordable and less complex than buying and provisioning private WAN connectivity services offered by those providers. Cloud connectivity requirements drive IT executives (50 percent) more than IT staff (35 percent).

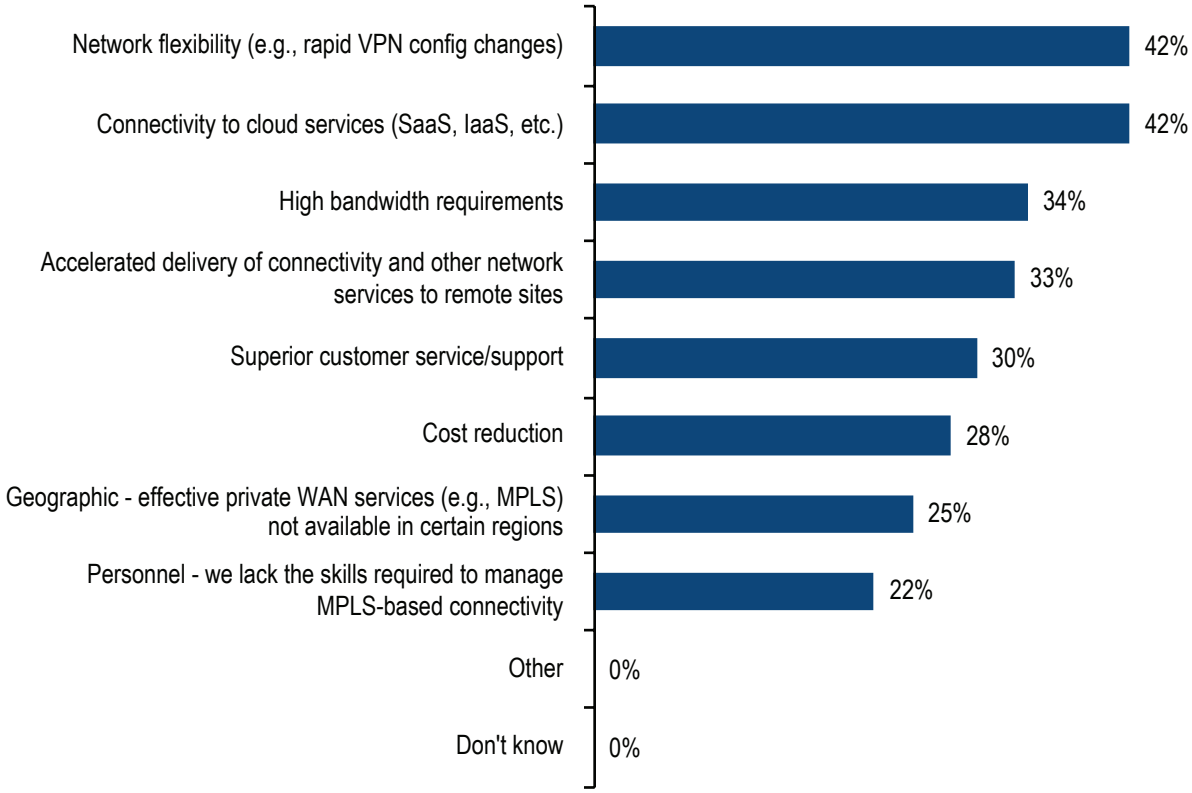

Figure 9. Primary drivers behind using the Internet as a primary WAN connectivity option for remote sites

The need for high bandwidth connections (34 percent) is also an important driver. In many geographies, network operators simply don't offer private WAN connections at speeds that are comparable to what many broadband ISPs offer. The Internet is very important to those who need to open up more bandwidth.

Accelerated delivery of connectivity (33 percent) rounds out the top four drivers of Internet use. Enterprises can connect sites faster with ISPs, which can usually light up a new site within days. New MPLS service can take weeks or months to set up.

Cost reduction (28 percent) is a relatively low priority. When it comes to the Internet, enterprises are trying to build a better network—not a cheaper one. Organizations that spend less than 15 percent of their annual IT budget on the WAN are the most likely (41 percent) to cite cost reduction as a driver. In contrast, organizations that spend more than 25 percent of their budget on the WAN are the most likely (52 percent) to target faster delivery of network services with their Internet use.

Roadblocks to Internet-Based WAN

Ninety-six percent of research participants said they encountered at least one challenge to successfully leveraging the Internet for their primary WAN option. **Figure 10** shows those challenges in detail.

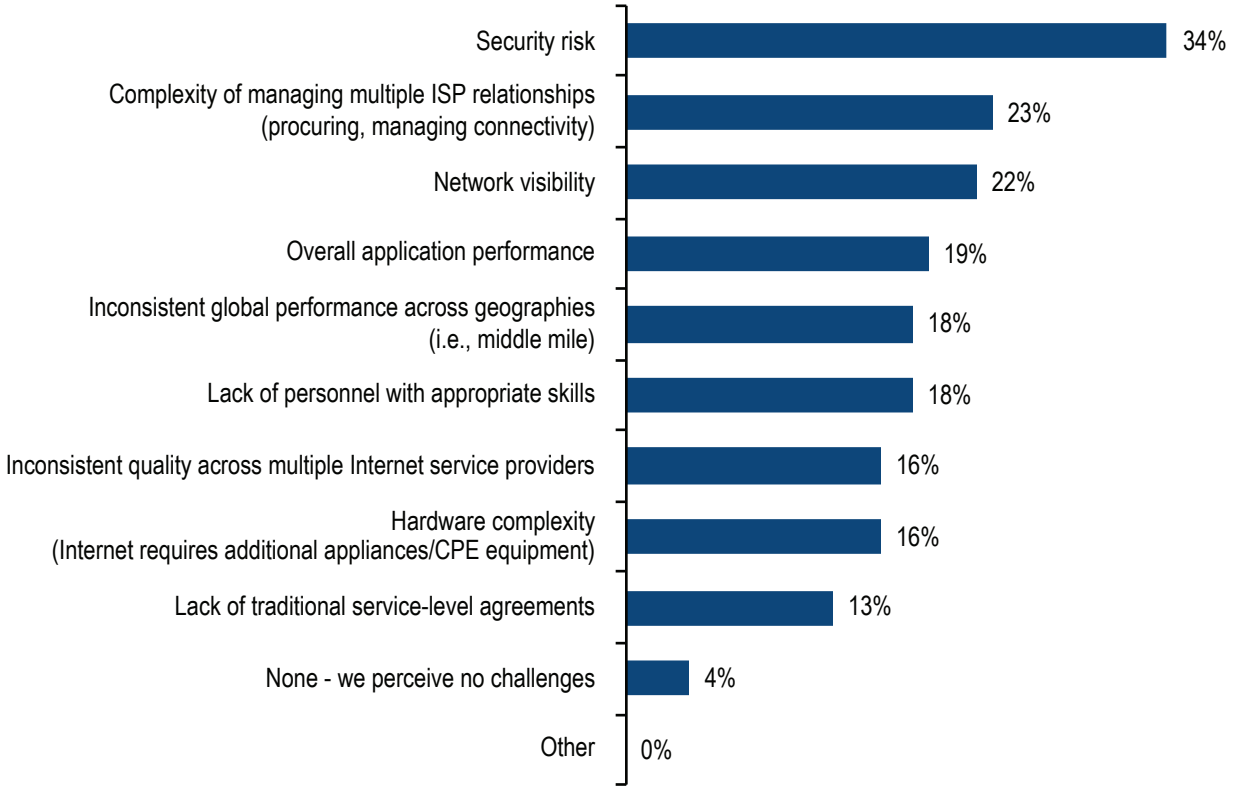

Figure 10. The biggest challenges to using the Internet for primary WAN connectivity

Security risk tops the list. The Internet is a shared resource, unlike private WAN services, where service providers are able to isolate customer traffic. Thus, the Internet will usually require encrypted, site-to-site VPN connections. Also, Internet links will need secure web gateways to separate non-business traffic that is going directly to the web. With more sites, this security will need to scale. It can get expensive and complex. Respondents from education (55 percent), healthcare (47 percent), and transportation (57 percent) businesses all say security is a major issue.

The complexity of managing multiple ISP relationships is a secondary challenge. ISP relationships will be especially hard to manage for global enterprises in which ISP quality varies and the central infrastructure team may have limited knowledge of the local market. Network visibility is also a secondary challenge. Visibility on the Internet is relatively low compared to private WAN services, given that MPLS providers usually deliver reports on network performance and service-level agreement compliance, but ISPs do not. Enterprises with more than 400 sites connected to the WAN were the least likely (14 percent) to struggle with network visibility, which suggests they are doing a better job of investing in operational tools to address this problem.

More Endpoint Devices Connecting in the Branch

Overall, 79 percent of enterprises in this survey reported that the number of endpoint devices connecting to their networks via remote sites is growing, and 30 percent say that growth is significant. North Americans (35 percent) are more likely than Europeans (22 percent) to report significant growth. **Figure 11** shows that only one percent of enterprises are seeing endpoints decrease in their remote sites.

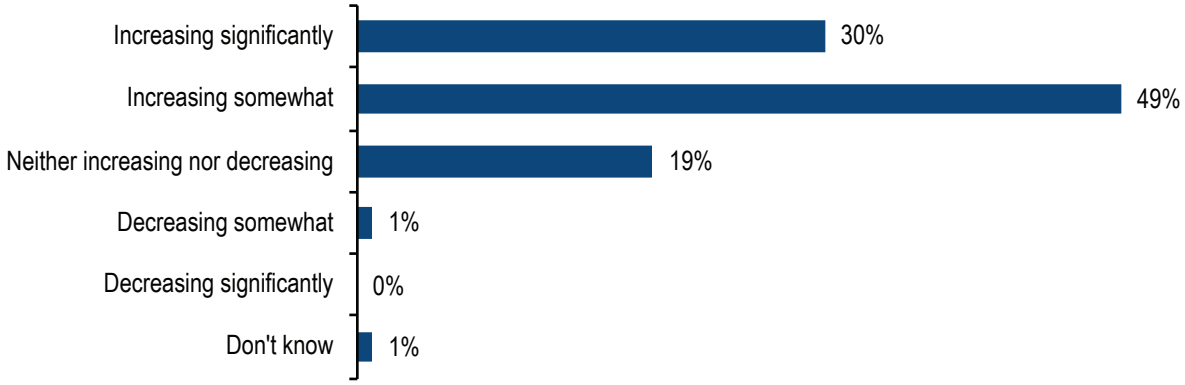

Figure 11. Is the number of network-connected endpoints in your organization's average remote site increasing or decreasing?

Organizations that are very successful with the WAN are very likely (69 percent) to report significant growth in endpoints, versus just three percent of organizations that are less than successful. Part of this might be a network visibility problem. Less successful organizations will sometimes have poor visibility and control over who and what is connecting the network. Also, organizations with poorly performing networks are going to be more conservative about allowing new devices to connect to networks that are already overwhelmed. WAN spending, which corresponds with WAN success, also matches this pattern. Organizations that spend more than 25 percent of their IT budgets on the WAN are the most likely (64 percent) to see significant endpoint growth.

Figure 12 reveals the most significant sources of endpoint growth. The majority of enterprises are dealing with more smartphones and PCs. Large enterprises (64 percent) are seeing more growth from PCs than medium enterprises (42 percent). These findings reflect the fact that individuals generally bring multiple devices to work, and they want to connect all of them.

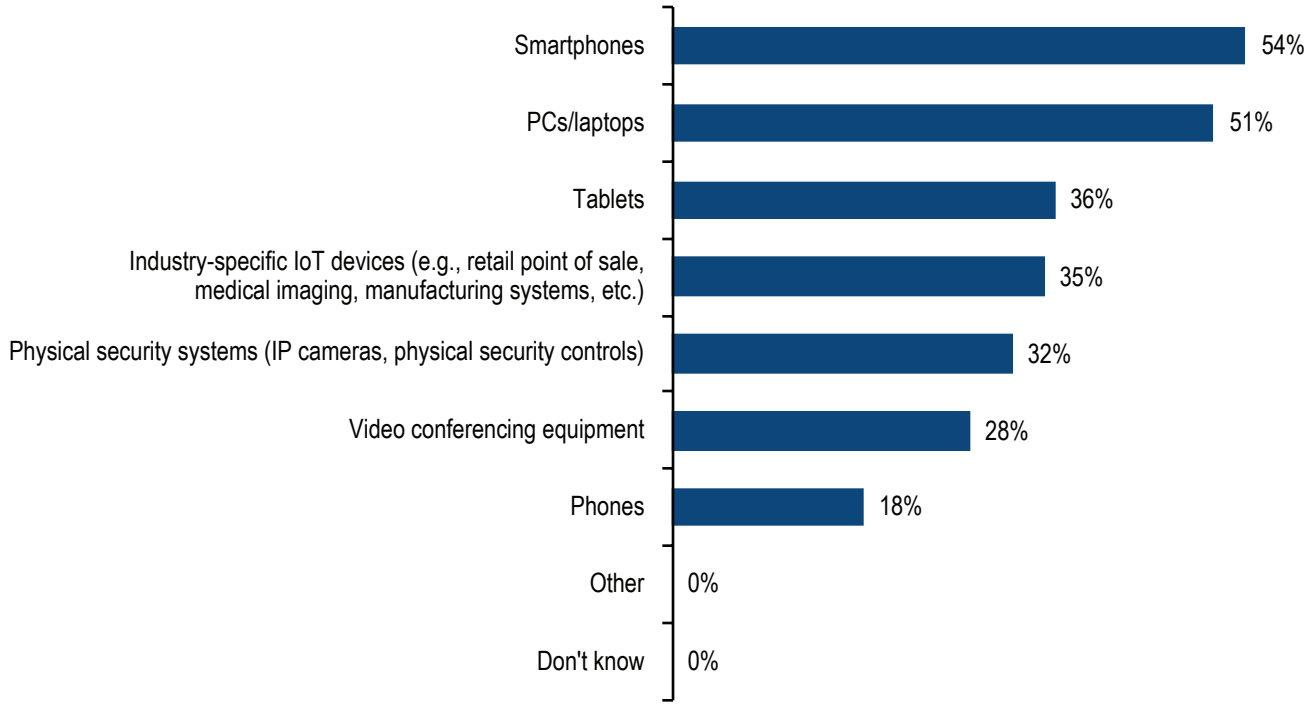

Figure 12. Devices most responsible for the growth of network-connected endpoints in remote sites

Tablets (36 percent) and industry-specific IoT devices like point-of-sales systems, medical imaging, and manufacturing systems are having a significant impact on more than one-third of enterprises. The IoT devices will be a particular challenge, and a likely driver of new network access management systems and network security systems.

The WAN Management Team

EMA asked research participants to reveal how many full-time equivalent (FTE) personnel their organizations devote to WAN management. **Figure 13** reveals a bell curve in the responses. In general, the typical company has four to 15 FTEs on the WAN. The largest group reports having eight to 15 FTEs, and nearly another quarter of them have four to seven FTEs. Very few enterprises are extremely lean with personnel. Just five percent have four or fewer people on the WAN team.

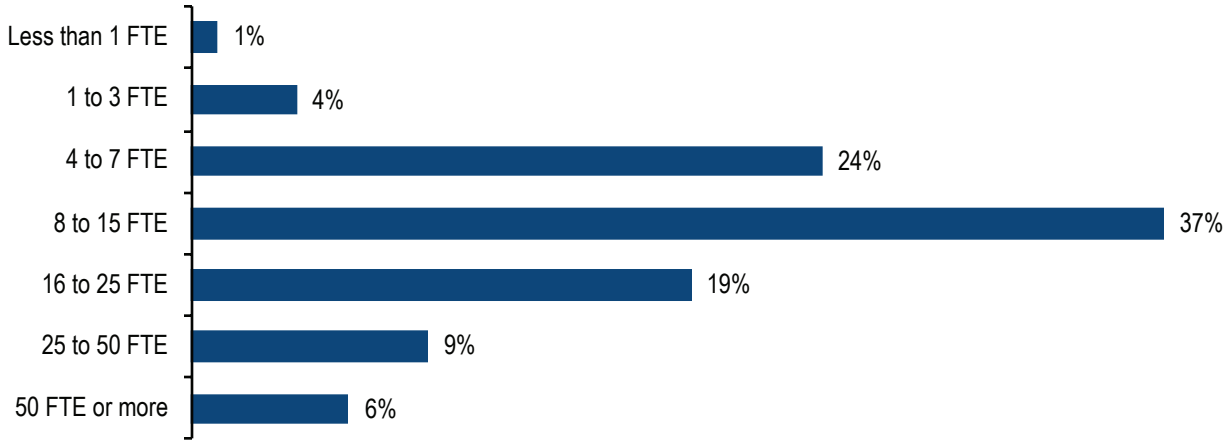

Figure 13. Full-time equivalent (FTE) personnel devoted to managing WAN infrastructure and services

Obviously, the size of a company has some impact on the number of FTEs it has. Medium enterprises were more likely (24 percent) to have 16 to 25 FTEs, while small enterprises were less likely (13 percent). Only large enterprises (22 percent) are typically able to sustain a team of 50 or more FTEs, versus only two percent of medium enterprises and one percent of small ones.

Speaking of remote sites, EMA investigated how many sites on the WAN have technical staff capable of supporting network-related tasks. **Figure 14** shows another bell curve. Enterprises rarely staff 100 percent of their sites, and they almost never staff fewer than 20 percent of sites. Every enterprise and every industry is different, but the mainstream approach to this staffing issue appears to fall between 40 and 80 percent of sites staffed with network personnel.

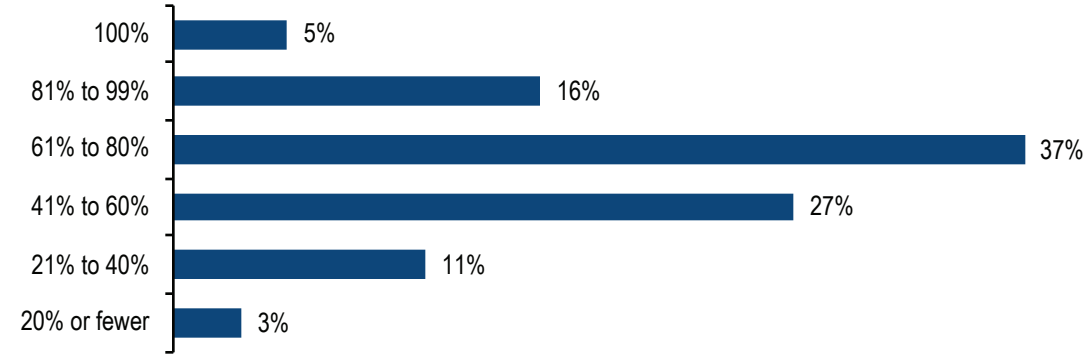

Figure 14. Percentage of WAN-connected remote sites/branch locations that have onsite, full-time technical IT staff capable of supporting network engineering and operations tasks

Enterprises Want End-to-End WAN Management Platforms

In recent years, EMA observed that network infrastructure teams are interested in centralized management systems for the WAN. There is a desire to move away from box-by-box management to a system that allows them to orchestrate network services across different places in the network and across different scopes of management tasks. The burgeoning popularity of SD-WAN is an expression of this requirement, but it is not the end-all-be-all of the issue. SD-WAN is about WAN connectivity at the remote site, but there's more to the network, such as local LAN services, the data center, security, and more.

In this research, EMA asked enterprises about their interest in an end-to-end management tool for WAN infrastructure and services. **Figure 15** reveals that 47 percent are looking for such a solution right now. Forty-three percent claim to already have such a tool. Only nine percent have no interest.

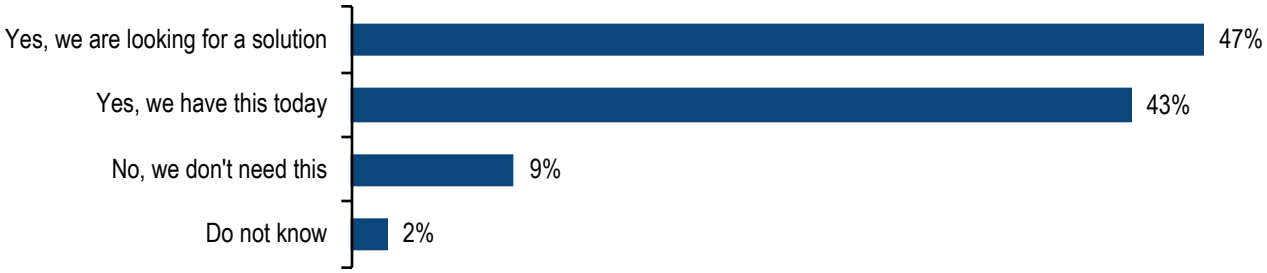

Figure 15. Does your networking team require or need a tool for end-to-end management of WAN infrastructure and services?

The percentage of enterprises that claim to have such a tool is quite high, since EMA considers this to be an emergent technology. It's possible that many of the enterprises that claim to have such a tool are referring to the centralized management capabilities of an SD-WAN solution.

Such an end-to-end tool appeals to enterprises with large number of remote sites Companies with 30 to 100 sites are the most likely (13 percent) to say these solutions aren't needed, versus five percent of those with 101 to 400 sites. IT executives are more likely to be looking for a solution (52 percent), versus just 42 percent of staff.

Figure 16 reveals the places in the network that enterprises want to include in the end-to-end management tool. Branch site WAN infrastructure is most critical. This includes routing, WAN optimization, and SD-WAN functionality. IT executives (56 percent) are much more interested in this element than staff (41 percent). This disparity is probably a reflection of network engineers who prefer a CLI-based management approach with routers. Organizations with more than 400 sites on the WAN were more likely (61 percent) to have this requirement. These managers of larger networks also need public cloud gateways managed by these tools (56 percent, versus 34 percent of those with 30 to 100 sites).

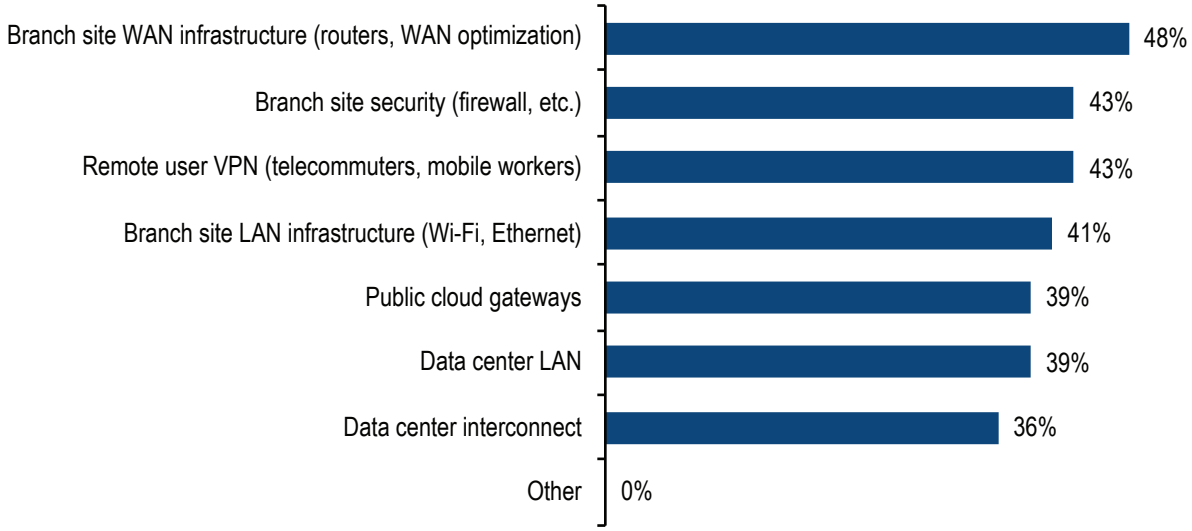

Figure 16. Places in the network that enterprises want within the scope of end-to-end WAN management

Branch site security is also very important to these enterprises. This is something that many SD-WAN solutions will cover with their management console, which reinforces EMA's theory that many enterprises that claim to already have an end-to-end tool are referring to their SD-WAN solution.

The third-most important element that they want to manage is the remote user VPN. This response suggests that enterprises want to manage connectivity for telecommuters and mobile users alongside their management of WAN infrastructure. Here is a gap in the SD-WAN-based approach to WAN management. In general, SD-WAN solutions completely ignore how remote users connect to the network.

Branch site LAN infrastructure management, such as switching and Wi-Fi, is also a priority for 41 percent of enterprises. The branch LAN is another place in the network rarely addressed by SD-WAN. Some SD-WAN vendors offer LAN solutions that are integrated with and managed by their SD-WAN products. Others offer LAN infrastructure products, but they haven't yet integrated them with SD-WAN solutions.

Nearly two in five enterprises need this end-to-end management solution to include the data center network in its scope. EMA's previous interactions with the industry also revealed emerging interest in integrating WAN and data center LAN management, particularly from a policy management and network segmentation perspective.

Figure 17 details the most important functional capabilities required in these end-to-end WAN management tools. Security management, network segmentation, and troubleshooting/ diagnostics are all top priorities. North Americans (52 percent) selected security management more often than Europeans (32 percent).

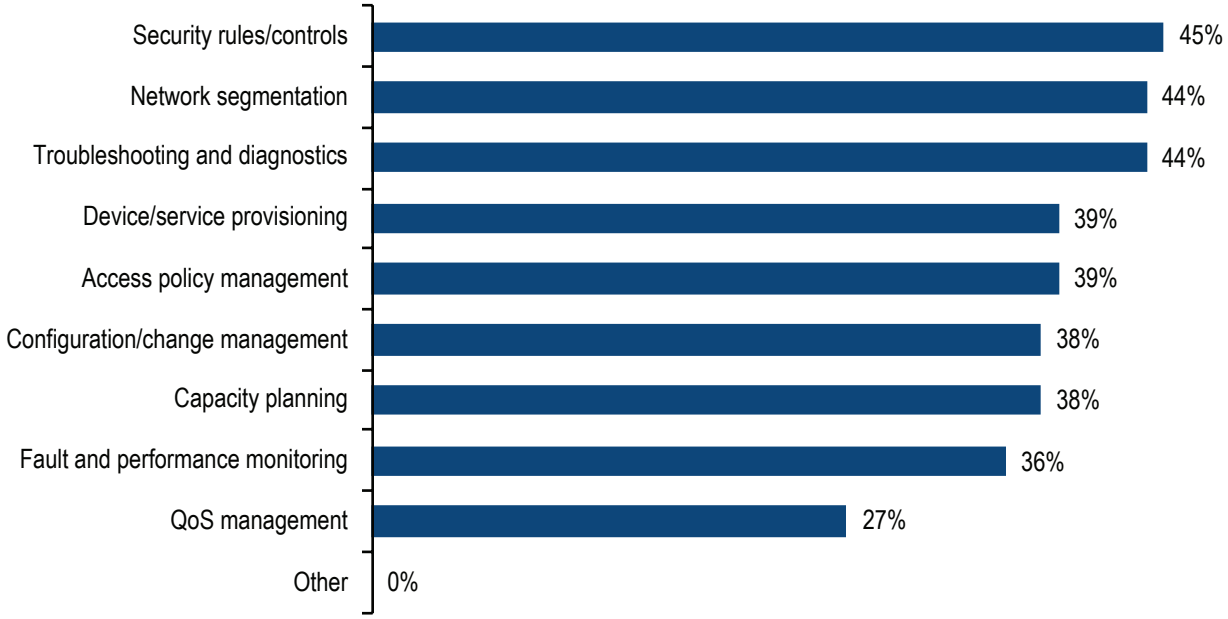

Figure 17. Management capabilities required in an end-to-end management environment

Network segmentation will become increasingly important, especially with IoT device growth at remote sites. Enterprises need will need to manage multiple VLANs and subnets to handle new services and devices. These segments will need to be managed end-to-end, all the way to the data center or the cloud.

Device and service provisioning, access policy management, and change management are all secondarily important. Capacity planning and fault and performance monitoring are also secondary, which suggests that some enterprises want these end-to-end management systems to absorb some of the capabilities they usually get from third-party network monitoring and performance management vendors.

Clearly, enterprises have an emerging need for tools that support end-to-end management of the WAN and reach into data centers, the cloud, and remote user VPNs, too. SD-WAN solutions offer some help here, but EMA suspects other tools may develop that can serve as a network manager of managers.

SD-WAN: WAN Transformation in Action

This research looked at many of the major factors that drive how enterprises transform the WAN, including cloud connectivity, security, infrastructure virtualization, Internet migration, and network management tool requirements. In this section, which forms the heart of this research, EMA examines SD-WAN, a technology that can enable much of that transformation.

Figure 18 reveals what stage of adoption enterprises are in with SD-WAN today. Bear in mind, these are companies with at least 30 remote sites connected to the WAN and a minimum of 500 employees, so these are distributed companies that will have a stronger demand for SD-WAN. The chart shows that 97 percent of these companies are actively engaged with SD-WAN in some way. The largest group of them are in the midst of implementing SD-WAN, with initial deployments completed, and 28 percent have fully implemented the technology.

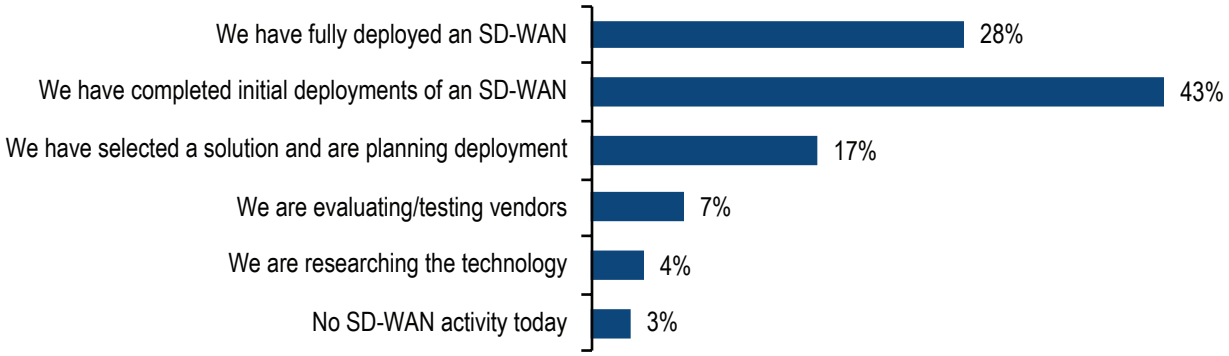

Figure 18. The state of SD-WAN in today's distributed enterprises

Enterprises with more sites to connect to the network are more aggressive with adoption. Enterprises with more than 400 remote sites are most likely (37 percent) to have completed their SD-WAN deployment already, versus 20 percent of companies with 30 to 100 sites. North Americans (30 percent) are also more likely to be fully deployed with SD-WAN, versus 20 percent of Europeans.

Business Drivers of SD-WAN Adoption

Enterprises identified three primary business drivers for their adoption of SD-WAN. They are trying to solve skills gaps within the IT organization, enable cloud computing, and improve network security, as shown in **Figure 19.**

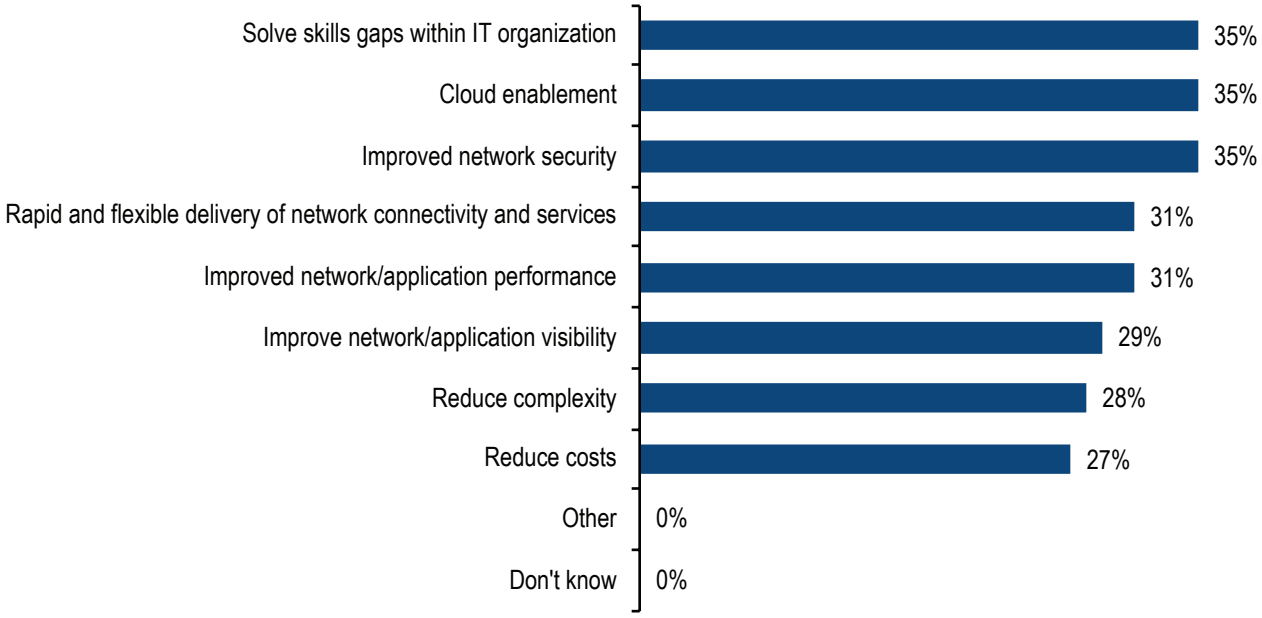

Figure 19. Primary business drivers for implementation or planned implementation of SD-WAN

SD-WAN solutions are typically managed via a GUI console, which allows enterprises to leverage their lower-skilled administrators for tasks that once required a certified engineer with CLI skills, deep knowledge of routing protocol knowledge, and other areas of expertise. SD-WAN not only addresses skills gaps, but it can also enable senior, certified engineers to focus on tasks that are more strategic to the business, such as supporting digital business transformation.

The strong drive for cloud enablement was expected, given the amount of cloud traffic on WANs today and the number of enterprises that want to connect their remote sites directly to the cloud. SD-WAN technology can remove a lot of the challenges associated with the cloud with a distributed, integrated security architecture, centralized control, and cloud gateways. Very successful organizations were more likely (41 percent) to prioritize cloud enablement with SD-WAN than less successful enterprises (24 percent).

The prevalence of security as a driver also makes perfect sense, given that security is the single most influential technical initiative on WAN strategy today.

There are many secondary drivers of SD-WAN today. Rapid and flexible delivery of network connectivity and services edges out the others. SD-WAN solutions can sometimes take a while to implement, like any WAN technology. However, once it's in place, its centralized management capabilities allow enterprises to turn on new services rather quickly. Adding a new site to a mature SD-WAN implementation should become trivial.

SD-WAN Feature Requirements and Connectivity Strategies

EMA asked research participants to identify the SD-WAN features that are most critical to their networks. Their responses reflected their attitudes on SD-WAN business drivers. The most important feature, according to **Figure 20,** was integrated monitoring of applications and networks. This visibility is critical to performance management. It can also reduce complexity, since network managers have better insight into the end-to-end network. This visibility was more important to North Americans (40 percent) than Europeans (28 percent).

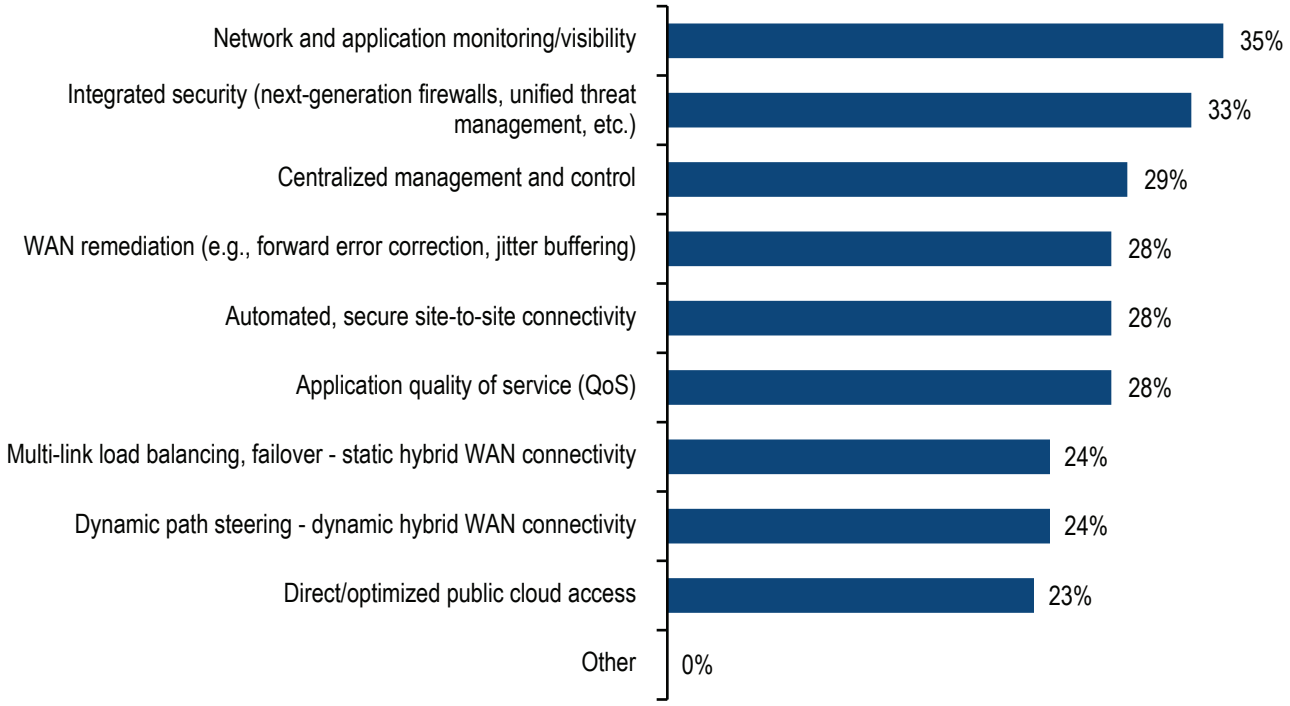

Figure 20. SD-WAN features most critical to enterprise networks

Integrated security is the other top-rated feature, which obviously addresses the security business driver, and more broadly it addresses the fact that security is the top technical influence on overall enterprise WAN strategies today. Security is a high priority for organizations with just 30 to 100 remote sites (39 percent). It is also a higher priority for education (50 percent), healthcare (47 percent), IT professional services (54 percent), and retail (40 percent).

Secondary features like centralized management and control via SD-WAN GUI consoles go a long way to reduce complexity and accelerate the delivery of network services, and WAN remediation techniques like forward error correction and jitter buffering help with improved performance. WAN remediation is less important to organizations with more than 400 remote sites (18 percent), but a priority for companies with 101 to 400 sites (35 percent).

Note that multilink load balancing, dynamic path steering, and direct and optimized public cloud access are the least important features. They are also table-stakes features. Almost every SD-WAN solution offers these capabilities today, although some vendors that focus on smaller companies lack dynamic path steering.

Multilink load balancing and dynamic path steering are also deeply associated with the notion of SD-WAN-enabled hybrid networks. The industry assumption is that enterprises use these products to support the expansion of Internet-based WAN. By load balancing and steering traffic across internet and MPLS links, network managers can mitigate the performance risks associated with the Internet. **Figure 21** looks at the type of aggregated connectivity enabled by today's SD-WAN deployments.

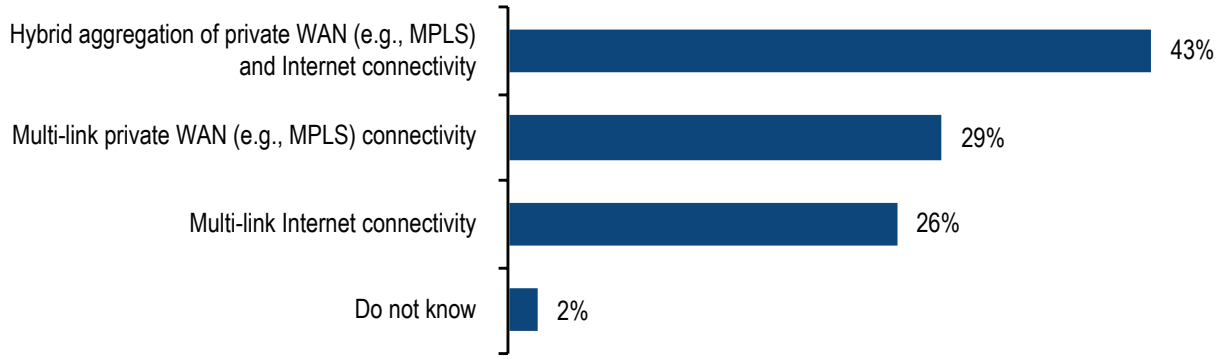

Figure 21. Enterprises identify the nature of the aggregated (load balanced) network connectivity enabled by their SD-WAN solutions

The most popular strategy is a hybrid network, with aggregation of MPLS and internet connections. Nearly one-third of enterprises are actually aggregating multiple MPLS connections at their remote sites with SD-WAN. Internet-only aggregated connectivity is slightly less popular.

Multilink MPLS is rarer among enterprises that have completed an SD-WAN implementation (21 percent) and most common with companies that are partially implemented (35 percent). There are two implications here. First, organizations that are less advanced with SD-WAN are more conservative. They are slower to rely on the Internet. Second, with experience, enterprises become more comfortable with the notion of transitioning to hybrid connectivity.

SD-WAN Management

SD-WAN solutions have a transformational impact on network management. Most vendors offer a GUI-based central management console in which most workflows are point-and-lick, rather than CLI-based. Depending on the nature of the implementation, some aspects of the WAN may continue to require legacy management approaches. For instance, if SD-WAN gateways do not displace a legacy router, those routers will continue to require legacy management approaches. This chapter examines how enterprises are managing this new technology.

Since many enterprises consume SD-WAN as a managed service, the scope of management responsibility may be narrow for many in-house network teams. **Figure 22** reveals the overall operational approach enterprises take with SD-WAN. It reveals that ten percent of enterprises prefer to outsource nearly all of SD-WAN management to their provider of managed SD-WAN. Another nine percent prefer to keep nearly all SD-WAN management tasks inside the enterprise.

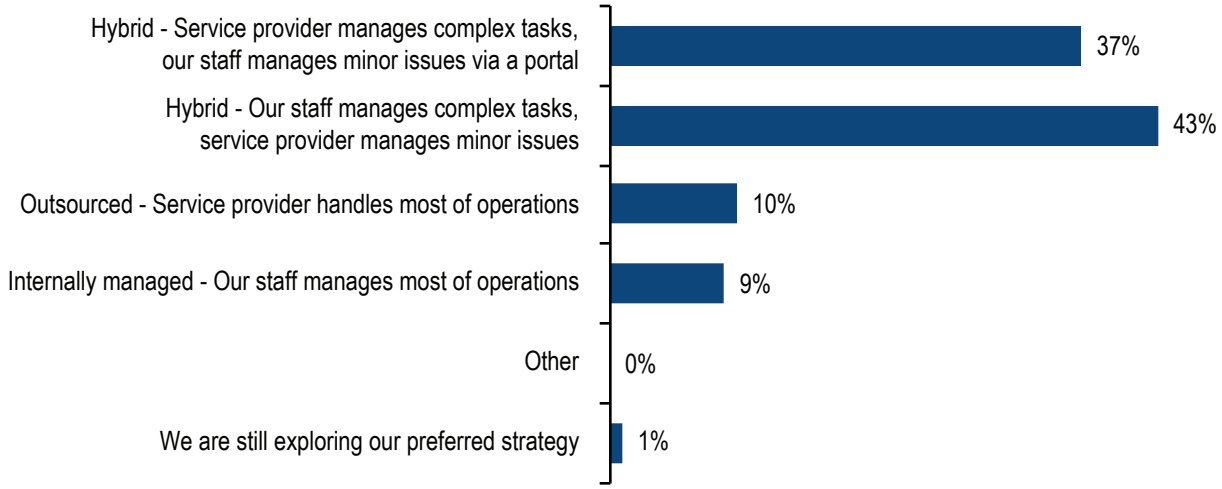

Figure 22. Preferred approach to SD-WAN operations (e.g., network change management, monitoring, troubleshooting)

The majority of research participants prefer a hybrid operational model, where internal network teams and a service provider or MSP share responsibility for the SD-WAN-based network. Eighty percent of enterprises plan to take a hybrid approach to operations with SD-WAN. The chart reveals a split in hybrid operations philosophy. Most prefer a hybrid approach in which the internal network team is responsible for complex tasks, and the service provider handles minor issues. A slightly smaller number want the service provider to do the heavy lifting while staff manages minor issues through a portal.

Enterprises that consider themselves very successful with the WAN are more likely (60 percent) to prefer a hybrid operational model that is led by the service provider, versus 29 percent of successful organizations and 24 percent of less-successful organizations. A staff-led hybrid operations approach is preferred by 50 percent of successful organizations, but only 31 percent of very successful ones. IT executives also reported a preference for a service provider-led hybrid approach (43 percent), versus just 32 percent of staff. Given that staff consider their ability to handle complex networking tasks as a guarantor of job security, it stands to reason that they're less inclined to hand that responsibility over to a network service provider or MSP.

Integrating SD-WAN with Enterprise IT Management Systems

EMA observed significant integration activity between SD-WAN vendors and network fault and performance management vendors over the last couple years. This integration is primarily aimed at collecting metrics from SD-WAN solutions so that enterprises can manage the technology's health and performance with their existing tools. However, network fault and performance management are not the only tools an IT organization uses to manage infrastructure and services. **Figure 23** reveals the management systems for which enterprises require integration with their SD-WAN solutions. Fault and performance management tools are actually tertiary priorities.

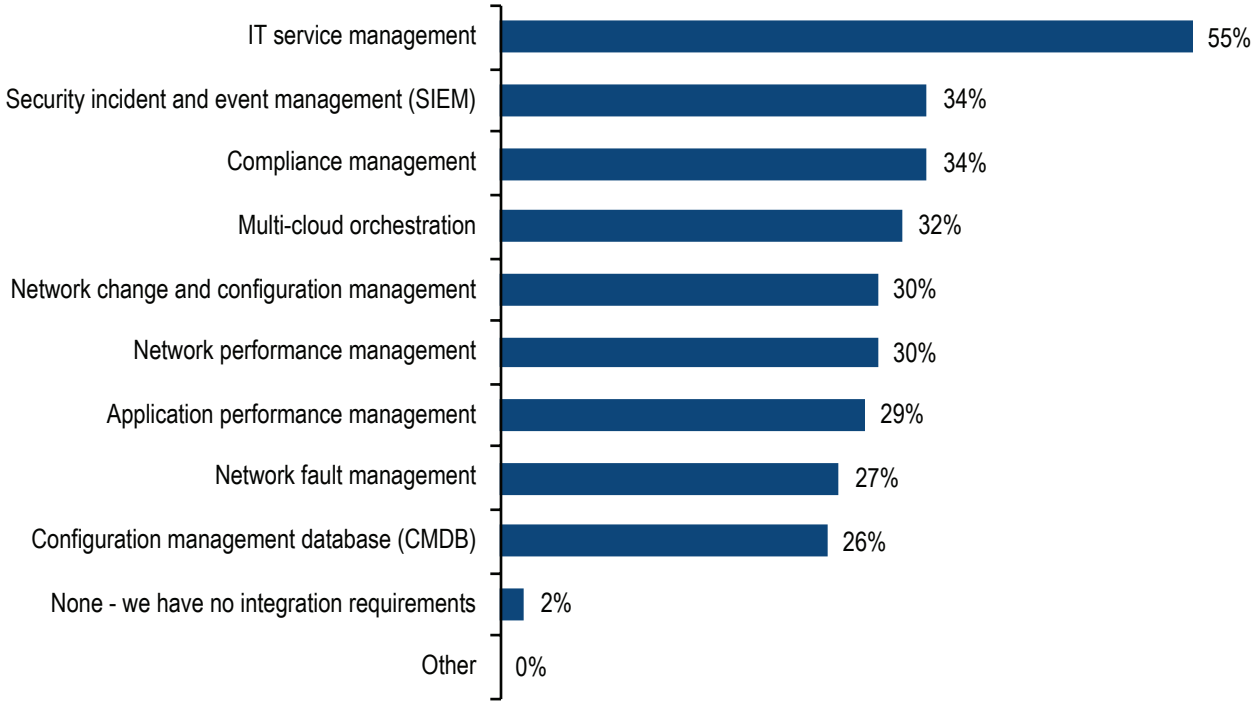

Figure 23. Enterprise requirements for SD-WAN integration with IT management systems

Overall, 98 percent of enterprises require at least one integration between SD-WAN and a management tool, and the average research participant identified three integration requirements.

The top integration requirement for SD-WAN is IT service management (ITSM). North Americans (60 percent) selected this requirement more often than Europeans (46 percent). ITSM systems are essential to mapping overall IT services to best practices and processes and aligning everything from IT operations to the help desk. Clearly, many enterprises have recognized that ITSM integration is important to integrating SD-WAN into their overall IT service portfolio, especially given the fact that SD-WAN is a major enabler of cloud connectivity from remote sites. Past EMA research found that the migration of applications to the public cloud often prompts increased collaboration between network management teams and ITSM teams. ITSM integration is an even more common requirement among enterprises that have completed an SD-WAN implementation (71 percent), versus just 49 percent of partially-implemented organizations and 43 percent of those that are still researching or planning SD-WAN. This disparity suggests that the importance of this integration becomes more apparent as enterprises get more experience with SD-WAN.

Security incident and event management (SIEM) systems and compliance management are the top secondary integration priorities, which demonstrates an emphasis on ensuring that SD-WAN implementations are secure and compliant. SD-WAN is a new class of technology that is fundamentally transforming how IT delivers network connectivity and services to remote sites. They need to ensure the integrity of their security and compliance controls amidst all this change. SIEM integration is more popular with healthcare companies (53 percent) and compliance management is more popular with financial firms (47 percent).

Multi-cloud orchestration was the next priority. These orchestrators will coordinate management of cloud infrastructure with the management of connectivity into the cloud from remote sites.

Although they are relatively low priorities overall, network change and configuration management systems (40 percent) and application performance management (37 percent) are more popular integration requirements among enterprises that are very successful with the WAN.

Enterprises with more than 400 sites connected to a WAN have a broader set of integration requirements. They are more likely to require integration with compliance management (46 percent), change and configuration management (42 percent), fault management (37 percent), and application performance management (46 percent).

Integrating Security into SD-WAN

This research established that security is an essential component of SD-WAN. It drives adoption, and it's a high-priority feature requirement. Most SD-WAN vendors are primarily networking vendors. Security is not their core business. Naturally, while enterprises want integrated security capabilities in SD-WAN, they may not always expect those security capabilities to be native. Many will consume third-party security services and functions that are integrated into their chosen SD-WAN product.

EMA asked enterprises to describe their SD-WAN integration requirements for six security functions: stateful firewall, next-generation firewall (NGFW), intrusion prevention/detection (IDS/IPS), malware protection, advanced threat protection, secure web gateway, and cloud application security broker (CASB). **Figure 24** shows the results. In general, many enterprises prefer vendors to deliver fully-native security features. However, plenty prefer third-party solutions integrated at the branch or third-party solutions that are cloud-based. Overall, at least 95 percent of enterprises had integration requirements for all seven of these security functions.

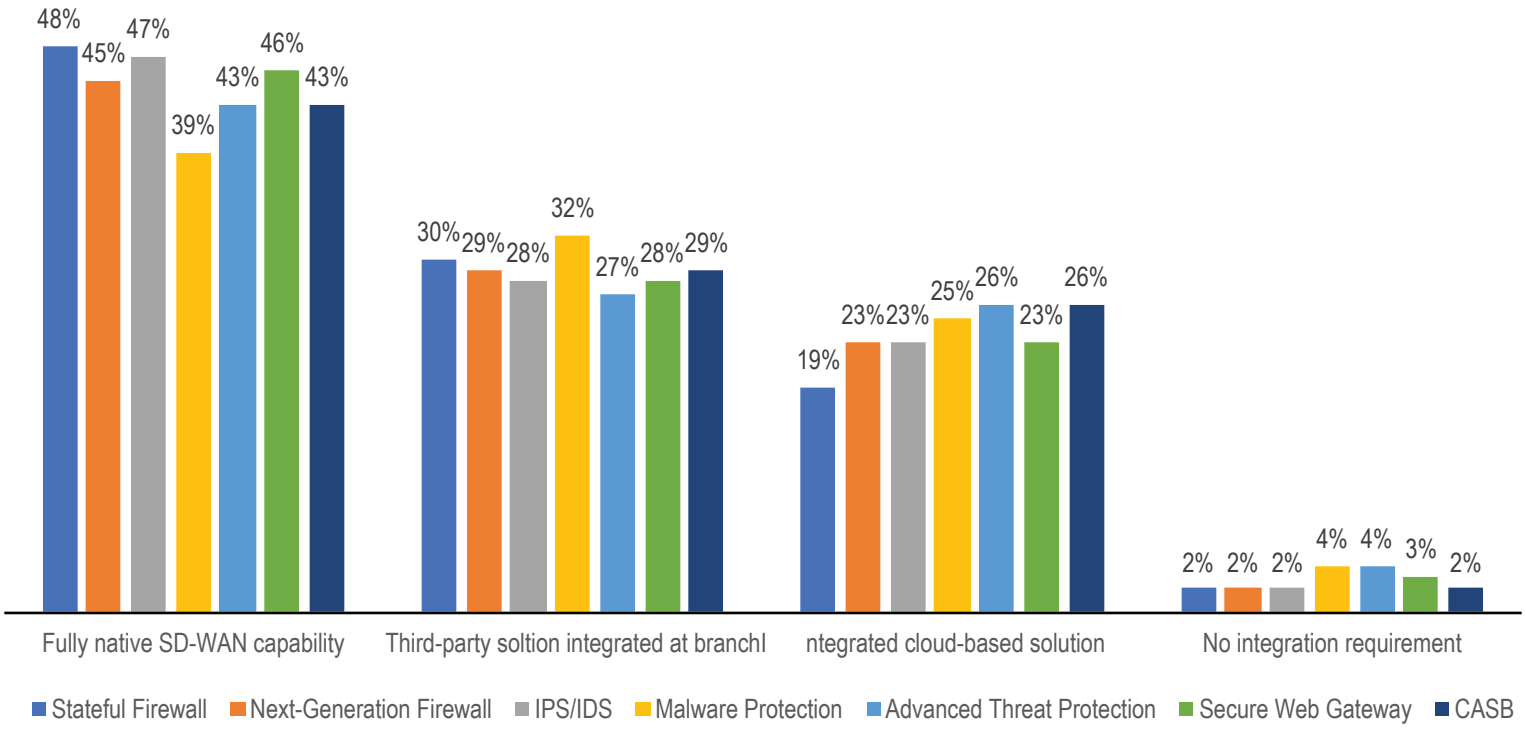

Figure 24. Security integration requirements for SD-WAN solutions

Cloud-based solutions are the least-preferred approach, even for CASBs. However, there is still significant interest, with at least one in five having a cloud-first approach for everything other than stateful firewalls. Third-party integration is slightly more popular than cloud services, especially for malware protection. They don't expect SD-WAN to be best-of-breed in this area.

The security functions for which enterprises have the strongest need for native capabilities are stateful firewall, NGFW, IPS/IDS, and secure web gateway.

Managing Security in SD-WAN

For many enterprises, the security group is responsible for managing many of the security functions that are integrating with SD-WAN. With this SD-WAN integration, it becomes unclear who will own management of these functions moving forward. EMA asked research participants to identify the two groups in their organization that are most responsible for managing security solutions once they are integrated with or absorbed by SD-WAN. **Figure 25** reveals that the ITSM group is essential to security management. This echoes an earlier finding that ITSM systems were the top priority for IT management tool integration with SD-WAN. ITSM is the group that defines service dependencies and maps best practices and processes to them. Clearly, enterprises recognize that they need ITSM to act as the enabler of security management within SD-WAN.

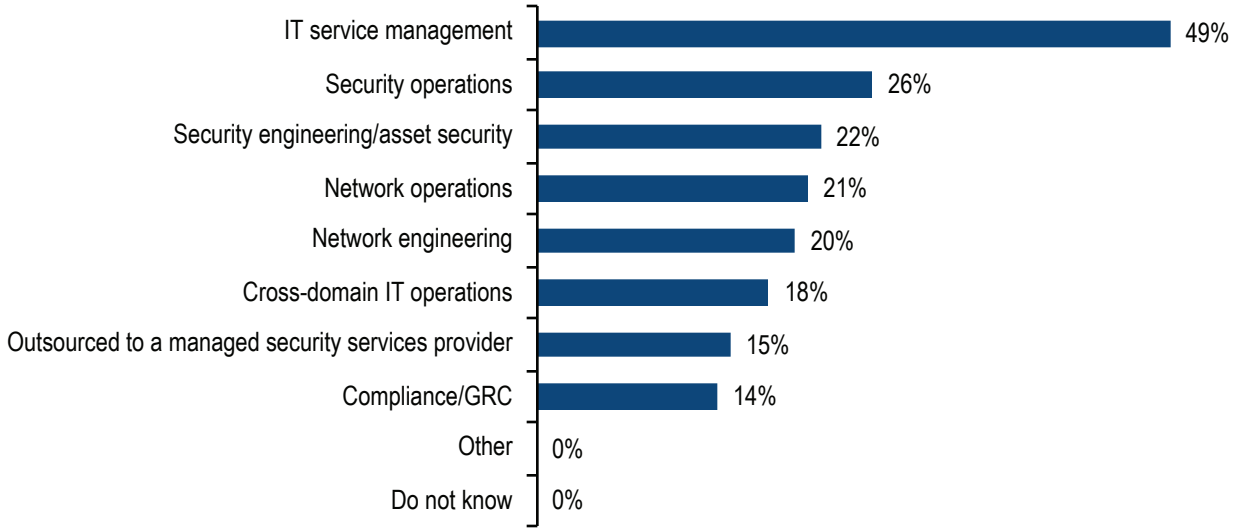

Figure 25. Groups primarily involved in managing security functions that are integrated with SD-WAN

After ITSM, security operations, security engineering, network operations, and network engineering are all tied for second. This suggests that enterprises are choosing from among these four groups and then partnering them with ITSM to manage the transition.

Success with SD-WAN

One of the strongest correlations throughout all the data in this research is between SD-WAN adoption and the level of success with the WAN. Enterprises that have fully completed an SD-WAN implementation are five times more likely to describe themselves as very successful than enterprises that have no SD-WAN plans or enterprises that are still researching or planning the technology. The patterns in **Figure 26** are hard to ignore. Overall, enthusiasm about the network goes steadily upward as enterprises move through the SD-WAN adoption process.

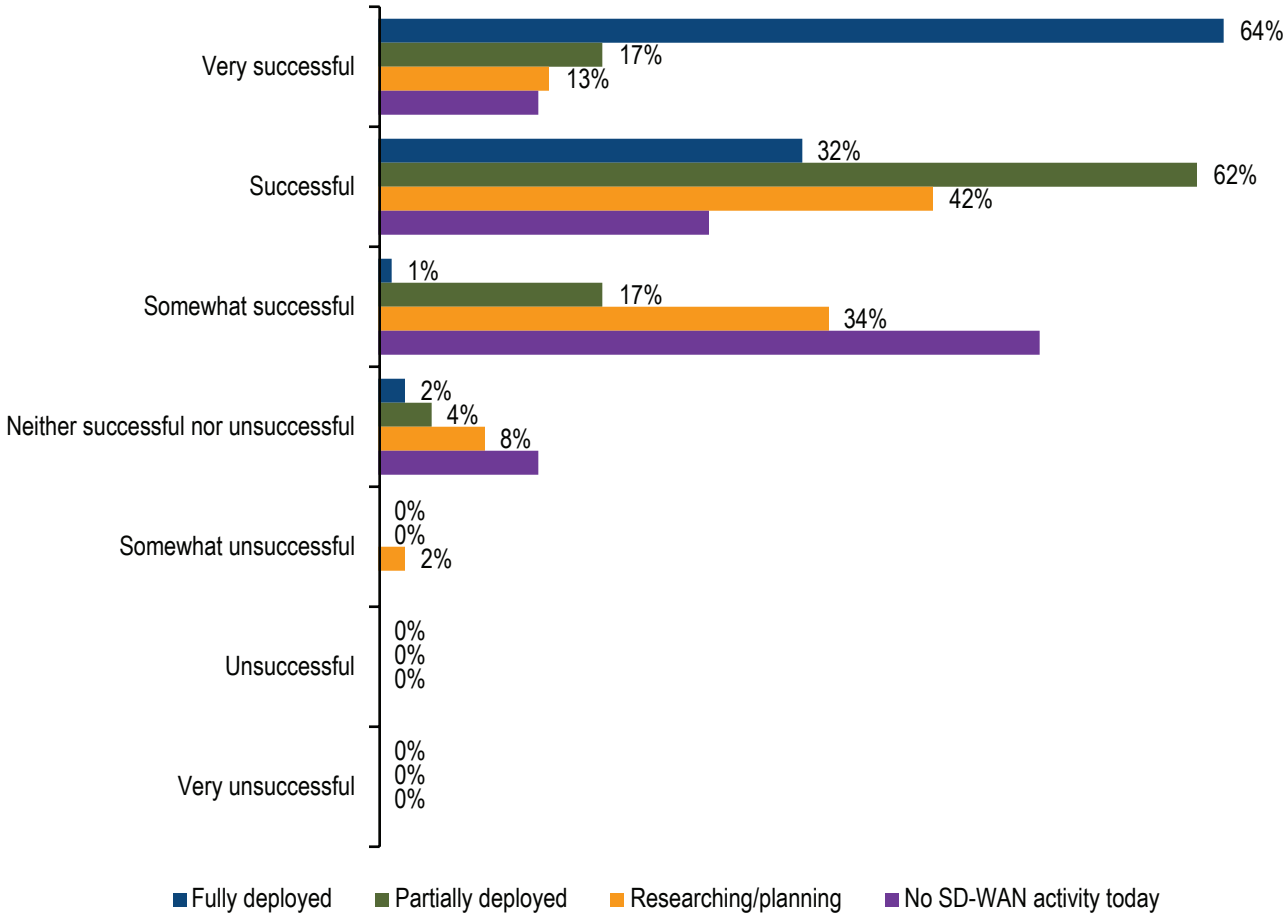

Figure 26. Overall WAN success correlates to completions of an SD-WAN implementation

The reasons for this pattern have been explored exhaustively in the previous sections of this research. Enterprises are reinventing the WAN, and SD-WAN solutions are a major enabler of change, from increased security requirements to internet migration to cloud enablement to digital experience management.

Enterprises are also earning an ROI with SD-WAN. Overall, 87 percent of enterprises say they are on track to earning ROI with the technology after three years, and 28 percent earn ROI within the first year, as **Figure 27** reveals.

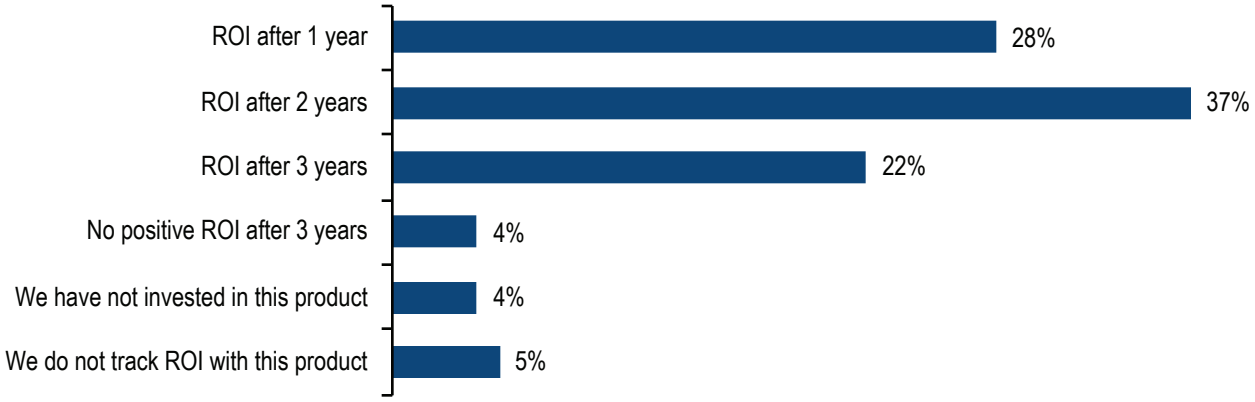

Figure 27. Enterprises report on expected return on investment with SD-WAN

There are pitfalls ahead. SD-WAN is a new, immature technology offered by a mix of startups, networking incumbents, and technology companies from adjacent markets expanding into the WAN. There isn't an undisputed roadmap for success. **Figure 28** reveals the most prominent challenges to SD-WAN implementation.

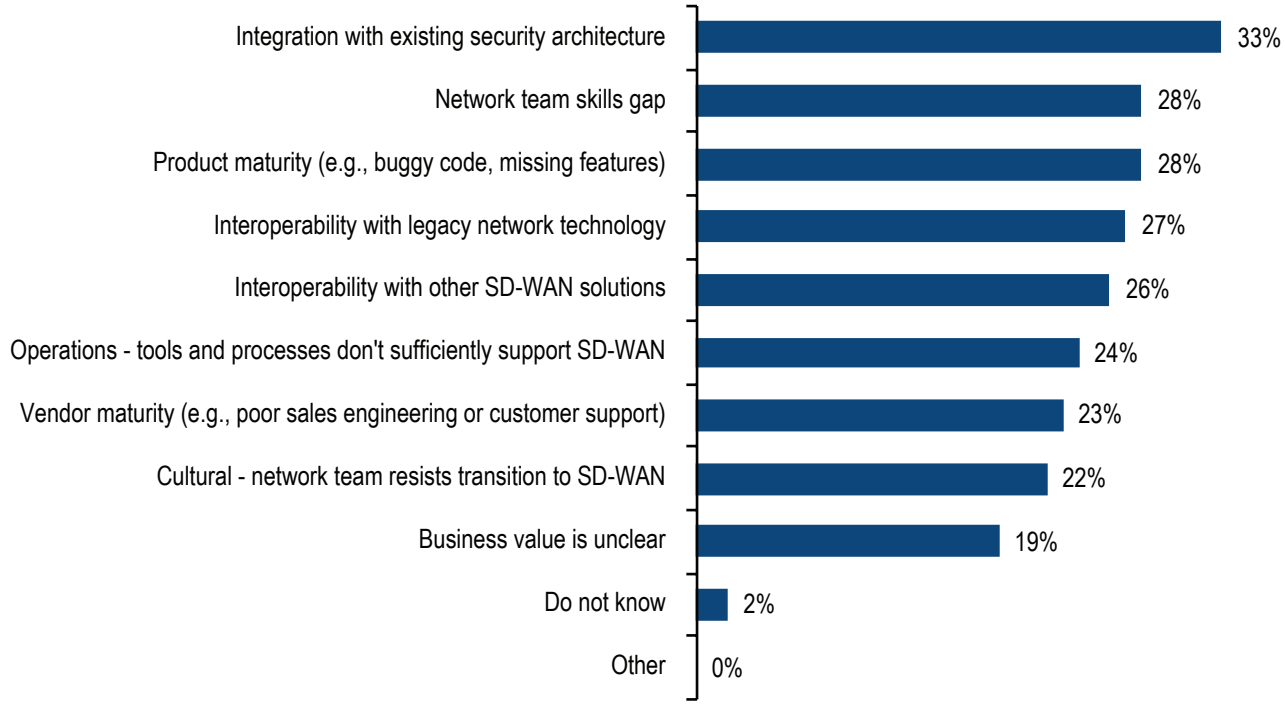

Figure 28. Most challenging aspects of SD-WAN implementation

The top issue is integration with existing security architecture. SD-WAN decentralizes architecture, and many of an enterprise's security systems are concentrated in central data centers. This will require careful changes to security architecture, which is why so many enterprises have broad requirements for integration between SD-WAN and security function and integration between SD-WAN and SIEM systems.

The network team skills gap is another prominent issue, which is concerning since the network team skills gap is also a driver for adoption. This contradiction suggests that some early growing pains will occur as the network team evolves to support a new technology. EMA has spoken with individual early adopters who reported that their network teams had to adjust to managing the network as a system of services rather than a collection of boxes.

Product maturity (28 percent) is another prominent challenge. Even many incumbent networking vendors are bringing entirely new products to market or acquiring startups. It will take time for these vendors to mature their products.

The prominence of interoperability with legacy network technology points to the fact that many enterprises are transforming gradually with SD-WAN. They will have plenty of legacy sites that will continue to use traditional network routing to connect to the WAN. For site-to-site communication, SD-WAN and legacy solutions will need to interact via traditional routing protocols.

Interoperability with other SD-WAN solutions is a challenge for slightly more than one-quarter of enterprises. Mergers and acquisitions might be the root cause of this problem, but there will be other instances where enterprises might switch vendors halfway through an implementation, or they might have different requirements for different types of sites on their network.

Enterprises struggle the least with unclear business value. This confirms that the majority of enterprises know how SD-WAN can support WAN transformation. It's notable given that previous waves of software-defined network solutions, particularly in the data center, have been slower to catch on with enterprises because of a lack of a killer use case. Organizations with more than 400 remote sites are more likely (31 percent) to struggle with business value, which is a warning sign that some SD-WAN solutions struggle to deliver value at scale.

Conclusion: SD-WAN is Essential to WAN Transformation, but Enterprises Need More

Enterprises are modernizing the WAN to support business drivers, like growth and digital transformation, and technical initiatives, like security and the cloud. Their networks need to be more agile, less complex, and have higher bandwidth.

On a fundamental level, this research revealed that enterprises are embracing changes like direct cloud access from remote sites. They are using the Internet and wireless WAN connectivity as replacements or supplements to MPLS. They are interested in consolidating branch office infrastructure with virtualization.

SD-WAN solutions address many of these requirements. They support changes in connectivity strategy, simplify transitions in network connectivity, and offer integrated security. Their centralized management consoles are easier to use than traditional network management approaches.

However, gaps remain. This research revealed that enterprises want to integrate mobile and remote user VPN access through their end-to-end WAN management tool. The vast majority of SD-WAN solutions ignore these requirements. Companies also want to coordinate management of WAN infrastructure and data center networks. Again, very few vendors offer this coordination.

Enterprises also have more vigorous requirements for integrating IT and security management with SD-WAN than the industry currently offers. Moreover, the data that SD-WAN vendors typically collect and share with IT management systems lacks granularity and insight into WAN transport and WAN hardware.

While this research shows that SD-WAN is delivering tremendous value to enterprises, there is still work to be done. Businesses must evolve to address all the requirements of WAN transformation. If they cannot address all their requirements with SD-WAN solutions, they will go elsewhere to fill the gaps, and that pivot toward other technologies could increase overall network complexity. Thus, this research should serve as a roadmap for the next generation of SD-WAN and WAN transformation technologies.

About Enterprise Management Associates, Inc.

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

Corporate Headquarters:
1995 North 57th Court, Suite 120
Boulder, CO 80301
Phone: +1 303.543.9500
Fax: +1 303.543.7687
www.enterprisemanagement.com

3785-Infovista-SUMMARY.121718