WHITE PAPER

Bringing It All Together: Managing SD-WAN With Campus and Branch Networks

Driving Operational Efficiency Across Wired, Wireless, and SD-WAN Environments

By Bob Laliberte, Principal Analyst
Enterprise Strategy Group

September 2023

Contents

Modern Network Environments Are More Distributed

Organizations are rapidly changing their businesses and underlying IT to better compete in a global economy. This shift is typically driven by digital transformation initiatives that deliver greater agility and flexibility. Research from TechTarget's Enterprise Strategy Group highlights that almost nine out of ten organizations (88%) are or have engaged in digital transformation initiatives and characterize them as just beginning, in process, or mature.[1] These initiatives have played a major role in modernizing IT and application architectures, which in turn has created highly distributed environments. Applications are no longer constrained by the four walls of private data centers and are increasingly being deployed across multiple public clouds and edge locations.
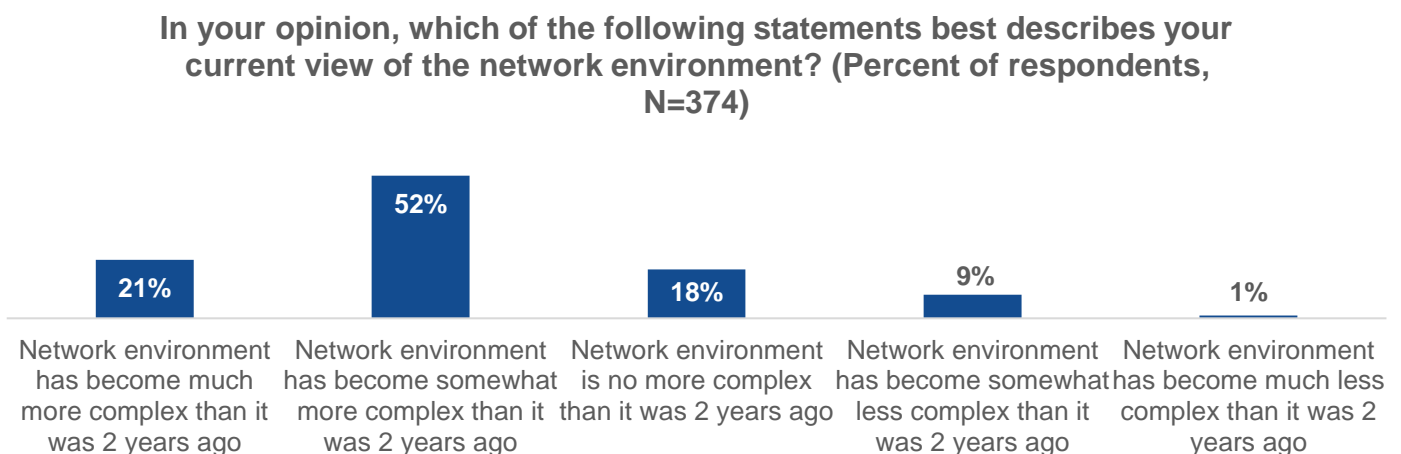
This transition to distributed applications has also made it necessary for organizations to connect employees working at branch and remote offices directly to the cloud. Legacy hub-and-spoke networks worked well enough when all the applications were in corporate data centers, but hairpinning traffic through the security stack results in increased latency and negative user experiences.

Fortunately, software-defined wide area network (SD-WAN) technology enables organizations to securely connect remote locations directly to these cloud environments, corporate data centers, and other remote offices, ensuring positive experiences. Today, the majority of organizations (55%) have either implemented or have begun to implement SD-WAN solutions.[2]

Challenges Created by Modern IT Environments

While the distributed nature of these modern applications and IT environments has led to increased agility for businesses, it has also led to more IT complexity. This is especially true for the network, with Enterprise Strategy Group research revealing that 73% indicated that their network environment has become more complex than it was just two years ago (see Figure 1).[3]

Figure 1. Network Complexity Over Time

In your opinion, which of the following statements best describes your current view of the network environment? (Percent of respondents, N=374)

Network environment has become much more complex than it was 2 years ago	Network environment has become somewhat more complex than it was 2 years ago	Network environment is no more complex than it was 2 years ago	Network environment has become somewhat less complex than it was 2 years ago	Network environment has become much less complex than it was 2 years ago
21%	52%	18%	9%	1%

Source: Enterprise Strategy Group, a division of TechTarget, Inc.

---

[1] Source: Enterprise Strategy Group Research Report, *2023 Technology Spending Intentions Survey*, November 2022.
[2] Source: Enterprise Strategy Group Complete Survey Results, *A Network Perspective on SASE and SD-WAN,* September 2023.
[3] Ibid.

A separate study explored why the network environment has become more complex, and organizations reported numerous causes, including new technology deployments (25%), the need for tighter security integration (24%), the need to ensure security between on-premises data centers and one or more public clouds (22%), highly distributed application environments (22%), and lack of visibility into the end-to-end network (20%).[4]

These challenges are amplified in organizations that are managing an end-to-end network with multiple vendors. Organizations may have one vendor for their wired environment, another for wireless access points, and yet another for rapidly emerging SD-WAN deployments. As a result, network operations teams are either forced to learn multiple management tools or they are divided into separate teams, each managing a single domain. Skilled IT resources are in short supply and budgets for new staff are extremely limited, creating additional problems, even as complexity is increasing with the deployment of new technologies and architectures.

Having separate management tools (and possibly vendors) for each domain only serves to increase the complexity and hinders moves, adds, changes, monitoring, and remediation efforts. Some of the challenges include:

- **Time to learn new tools.** Network operations teams have to dedicate time to learn and become proficient in each new network domain (wired, wireless, SD-WAN) management system that is deployed. Organizations need to send team members to training classes, which may incur additional fees.

- **Lack of end-to-end visibility and management.** Multiple network vendors provide limited snapshots of their specific domains, but operations teams lack a comprehensive view of the end-to-end network environment. It is important to note that, with the deployment of applications to the cloud, end-to-end environments now include the WAN connection to the public cloud.

- **Swivel chair management.** Leveraging multiple management tools requires operations teams to switch back and forth between screens to manage the end-to-end environment. This can be time-consuming and is prone to error.

- **Delayed troubleshooting and remediation efforts.** The ability to perform manual correlation of events across disparate network domains requires highly skilled resources and time. As such, organizations with multiple management tools are likely to experience slower problem isolation and remediation.

- **Lack of security integration.** Leveraging multiple management tools makes it more difficult to deliver consistent and correct security policies across all domains, as each separate domain may require different levels of integration. Security integration that is not properly aligned creates gaps in threat protection.

- **Lifecycle management.** Operations teams also need to consider the effort required to keep separate systems up to date with the latest code and security patches. Typically, on-premises appliances hosting the management software require their own patching and updating.

For these reasons, it shouldn't be a surprise that the objective most commonly cited over the last five years by respondents for their digital transformation initiatives is to drive operational efficiency.[5]

Modern Network Operations Require Unified Management

To become more operationally efficient, network operations teams need management solutions that provide visibility across more than one network domain. Some opt for unified management that network vendors increasingly are offering across their wired and wireless LAN solutions. However, as SD-WAN technology becomes more widely deployed, organizations need to extend their unified management across the wired, wireless, and SD-WAN environment to avoid diluting their efficiency gains.

Several key capabilities can help accelerate the delivery of this level of unified management, including:


- **Cloud-based management.** Because these modern environments are highly distributed, providing a centralized management portal in the cloud enables the timely collection of telemetry data from each network domain, regardless of where its solution elements are located. Being cloud-based also plays an important role in aggregating more data that is relevant, trusted, and of high quality in order to improve the efficacy of AI/ML capabilities. A cloud-based management portal gives remote workers easier access and eliminates the need to procure and maintain on-premises servers, including the application of software patches and upgrades as part of lifecycle management. Enterprise Strategy Group (ESG) research highlights that this is the preferred method for network management, with 73% of respondents stating that they prefer to use cloud-based visibility and management solutions (see Figure 2).[6]

Figure 2. Preference for Cloud-based vs. On-premises Unified Network Management

What is your organization's preference for where unified end-to-end network visibility or management solutions are located? (Percent of respondents, N=339)

Don't know/no preference, 1%

On-premises, 26%

Cloud, 73%
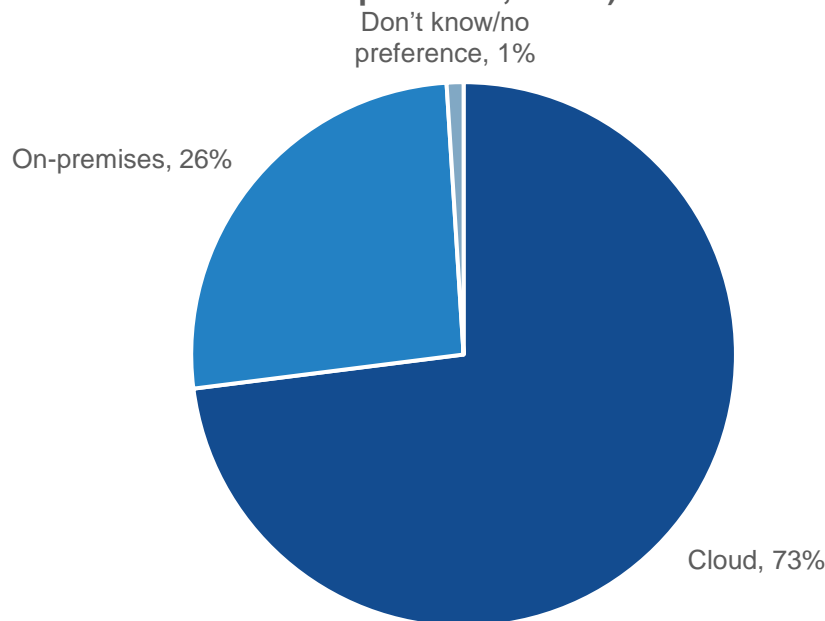
Source: Enterprise Strategy Group, a division of TechTarget, Inc.

- **End-to-end visibility.** To manage multi-domain environments effectively and efficiently, organizations first need to have visibility across all the domains, which can provide context to the events occurring in any one domain. The ability to detect and identify all the devices and how they are connected is instrumental in mitigating risk and delivering effective management. Thus, comprehensive visibility is extremely important in these highly distributed environments. According to ESG research, 81% of organizations indicate that end-to-end visibility is critical or very important (see Figure 3).[7]

---

[6] Source: Enterprise Strategy Group Research Report, *End-to-end Networking Visibility and Management*, April 2023.
[7] Ibid. Note: The total in this figure does not add up to 100% due to rounding.

Figure 3. Importance of End-to-end Network Visibility

How important is having unified end-to-end visibility of your organization's network environment? (Percent of respondents, N=339)

Not at all important, 1%

Critical, 13%

Somewhat important, 19%

Very important, 68%
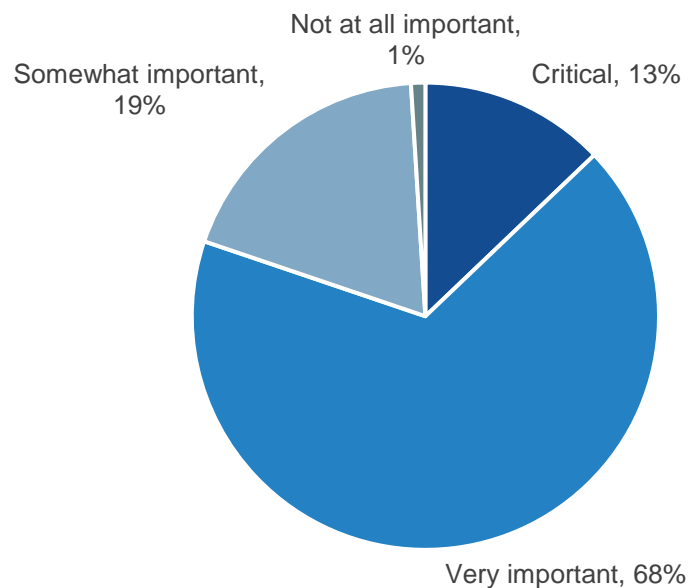
Source: Enterprise Strategy Group, a division of TechTarget, Inc.

- **AI/ML/GenAI.** The distributed and dynamic nature of modern IT environments makes it extremely difficult to manually correlate data and quickly determine the root cause of a problem. To keep up with these complex network environments, network operations teams are turning to AI/ML to rapidly detect a problem, provide recommendations to remediate, and, in some cases, even automate the correction. Given the distributed nature of SD-WAN deployments, ESG research has found that 97% of organizations believe it is either important, very important, or critical to have AI/ML technology driving automation in their SD-WAN environments (see Figure 4).[8] Applying these technologies across wired and wireless space will only provide additional value, as it will accelerate root cause identification and problem remediation. This will enable organizations to deliver networks with better performance, higher availability, and improved application and service experiences. Moving forward, operations teams should understand how newer generative AI solutions will be used to augment existing AI/ML solutions, providing natural language queries for network health or knowledge of the impact of simulated events on the network.

---

[8] Source: Enterprise Strategy Group Complete Survey Results, *A Network Perspective on SASE and SD-WAN,* September 2023.

Figure 4. Importance of AI/ML Across Wired, Wireless, and SD-WAN Environments

How important is it to have AI/ML technology driving automation in your organization's SD-WAN environment? (Percent of respondents, N=374)


Somewhat important, 2%

Not at all important, 1%

Critical, 17%

Important, 10%
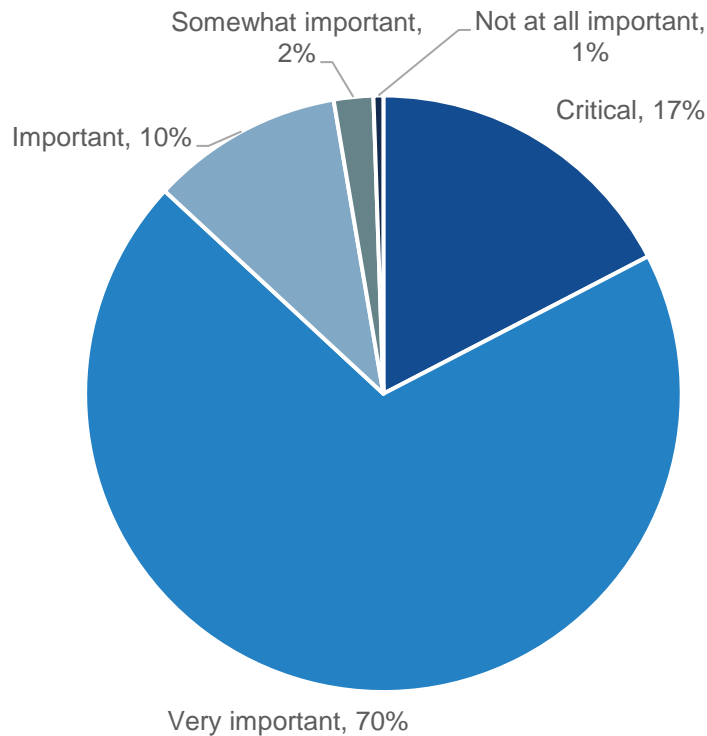
Very important, 70%

Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Organizations have recognized the importance of unified management for their network environments. In fact, according to ESG research, 93% of organizations state it is very important or critical to have unified wired, wireless, and SD-WAN solutions (see Figure 5).[9] Furthermore, rounding out the top three reasons, 38% of organizations stated that they would change SD-WAN vendors if it meant they could have unified management of the wired, wireless, and SD-WAN environment. The top two responses were providing higher levels of automation (42%) and improved visibility for faster troubleshooting (40%).[10] Having unified management enables operations teams to focus on a single management portal that is extensible across multiple network domains. Because adding a new network domain does not mean adding a new management tool, learning is faster and the need for manual correlation of data in the event of a problem goes away. It also makes it easier to deliver consistent and correct security policies across a distributed environment. Organizations can also mitigate risk by better understanding any vulnerabilities or exposures.

[9] Ibid.
[10] Ibid.

How important is it for your organization to have a unified wired, wireless, and WAN solution (i.e., common management platform for SD-WAN, wired, and wireless networks)? (Percent of respondents, N=374)

Somewhat important, 7%

Critical, 19%

Very important, 74%
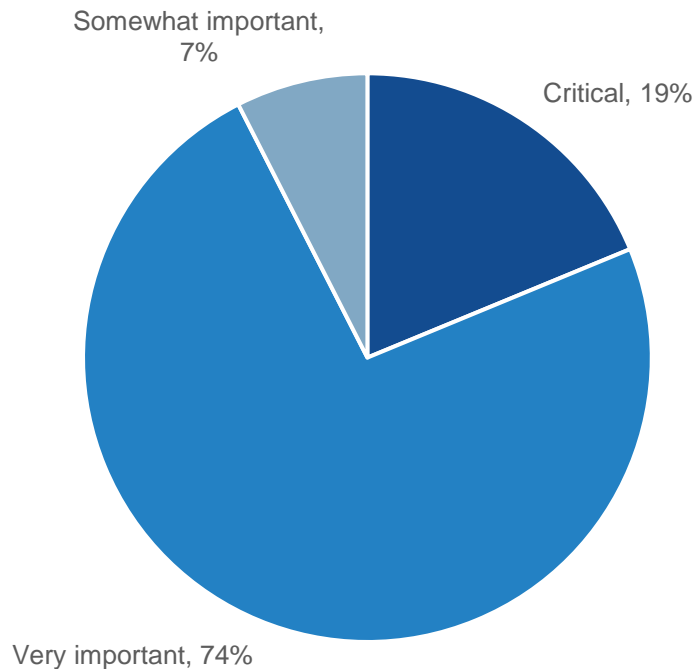
Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Juniper Networks Delivers Unified Network Management

Juniper Networks has been delivering network solutions to cloud, service provider, and enterprise customers for a number of years, and, as such, it has witnessed the shift of applications to the cloud and edge and the increased complexity of managing these environments. This perspective has driven them to build or acquire the technologies that create greater operational efficiencies, ensure positive experiences, and maximize availability. A significant part of reducing complexity for customers' network operations teams is delivering a unified network management solution across its wired, wireless, and SD-WAN portfolio.

Juniper Mist technology forms the foundation of its unified management strategy. Since acquiring the technology just a few years ago, Juniper Networks has tightly integrated the cloud-based platform across its wired, wireless, and SD-WAN portfolio. As a result, organizations can now take advantage of the cloud-based portal for full visibility across campus, branch, and WAN environments. It is cloud-based with well-developed AI/ML capabilities that enable organizations to accelerate problem identification and remediation across the wired, wireless, and SD-WAN stack.

Marvis, its conversational AI virtual network assistant, enables operations team members to use plain language to inquire about the status of the network or understand what may have changed without the need to learn and use CLI commands. Juniper has also integrated generative AI capabilities to make it easier to extract information from user manuals and troubleshooting guides. The widespread use of AI technology is part of Juniper's stated objective to deliver secure AI-driven network connectivity and is expected to eventually encompass the entire portfolio.

Leveraging Juniper unified network management will enable network operations teams to access a single cloud-based portal that provides end-to-end visibility and management of the wired, wireless, and SD-WAN domains. This drives greater operational efficiency and frees up the network team to spend more time working on strategic transformation efforts.

Conclusion

Modern application and IT environments are highly distributed and increasingly require direct cloud connectivity. For workers at branch and remote offices, SD-WAN technology is the de facto standard for direct internet connectivity to these apps and for enhancing their experiences.

As organizations transform to become more agile, the network needs to be an enabler. Simply adding SD-WAN as another domain to be managed with its own tools only slows their network operations teams by increasing complexity. Organizations need a management platform that simplifies end-to-end visibility and eliminates the "swivel chair" management and manual correlation of increasing amounts of network telemetry data.

Juniper understands the demands on the network operations teams supporting these modern environments and has built out its cloud-based Mist AI platform to provide unified visibility and management across wired, wireless, and SD-WAN environments, focused on driving operational efficiencies and ensuring positive experiences.

About Enterprise Strategy Group
TechTarget's Enterprise Strategy Group provides focused and actionable market intelligence, demand-side research, analyst advisory services, GTM strategy guidance, solution validations, and custom content supporting enterprise technology buying and selling.

contact@esg-global.com

www.esg-global.com

3200154-001-EN-Sept.2023