Publication date:
May 2023
Author:
Cindy Whelan
Adeline Phua

Enterprise Experiences Untangling WAN Complexity

Brought to you by Informa Tech

Omdia commissioned research sponsored by Verizon

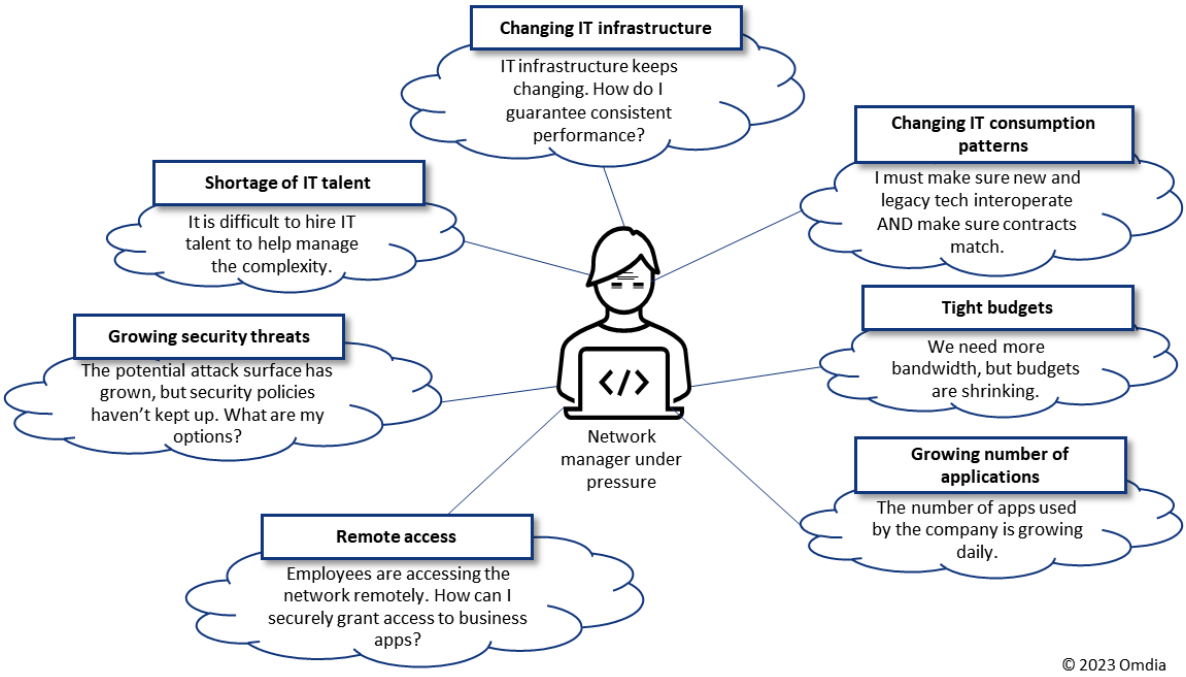
Contents

Summary

The network manager's struggle is real

Technology and IT architectures are not static. Neither are business models. IT managers are under pressure to adapt networks and application management that are agile for the business, delivering the performance businesses need while protecting the network and enterprise data. **Figure 1** shows why network management is becoming more challenging for IT managers.

Figure 1: What is causing the struggle?



Source: Omdia

In today's multicloud-driven business environment, enterprise network managers must ensure that employees, partners, and other stakeholders have secure, reliable access to the applications they need to support business objectives. The network must be built to support the capacity and performance required to support the enterprise's IT needs.

Enterprises need a solid network underlay to support modernization initiatives

Private connectivity services such as virtual private networks (VPNs), private circuits, dedicated internet access, and MPLS that include strong network security and delivery guarantees continue to be preferred solutions for many enterprises to transport workloads to locations such as cloud services on-ramps, colocation facilities, and critical offices. However, getting superior performance can come at an additional cost. Private connectivity services are often more expensive than services delivered over contended public networks such as broadband.

Enterprises today need agile and flexible networks that can adapt quickly to changes in the environment caused by internal business decisions that affect operations and the network or by external disruptions that need a response. Network managers must adapt the network to meet this need for increased agility while reducing capital and operational costs. They must also deliver a good user experience, consistent network performance, and strong security. Enterprises are considering new network solutions to cater to these needs.

Software-defined wide area networking (SD WAN) has emerged as a network approach that allows enterprises to retain their private connectivity services and service guarantees and connect locations via broadband (cable, DSL, or fixed wireless access such as LTE or 5G) for less mission-critical workloads. Enterprises can align network connectivity with the needs of each location so that they can manage service costs and performance needs granularly.

Although SD WAN is becoming a popular solution, enterprises need to take a step back and consider the entire network. SD WAN has many solid use cases and can add new capabilities, but it is not a silver bullet in all circumstances. The network underlay is the foundation that will underpin the success of network modernization. Networks must be flexible and reliable to meet today's enterprise needs. They must seamlessly integrate private and public connectivity services. Enterprises need to rethink how they build their networks: an inadequate foundation will lead to problems in the future.

Expectations for some SD WAN scenarios may not always align with reality

Software-defined networking (SDN) is a technology that operators use to separate the control plane (overlay) from the data plane (underlay). SD WAN is the application of these SDN principles to the WAN to control and manage applications over the network underlay. SD WAN is not the same as SDN. SD WAN lets enterprises set policies, but it is not responsible for the quality of the network underlay. The underlay could be high-quality private connectivity services or best-effort public broadband.

SD WAN platforms do provide hybrid connectivity capabilities, include granular management tools that set policies prioritizing specific applications and provide network visibility. However, they sometimes fall short of enterprise expectations, particularly when established in do-it-yourself (DIY) implementations. Typically, SD WAN adopters expect the following:

- Improved application performance

- Simplicity in managing SD WAN
- Reduced network costs
- Improved security

Organizations use hundreds of applications. The policies set for each application are limited by the ability of the underlay to support them. Large organizations also have hundreds of sites. They must consider an optimal mix of underlay network services for each site. Further, some organizations use multiple SD WAN platforms and therefore need to deal with multiple management tools. Enterprises can find themselves entangled in complex issues if they lack the expertise, vision, or discipline to formulate, set, and follow a strategic plan for their network modernization.

Omdia surveyed more than 300 enterprise executives in the fourth quarter of 2022 to understand their perspectives on SD WAN. The survey found that the post-deployment experience does not always match enterprise expectations.

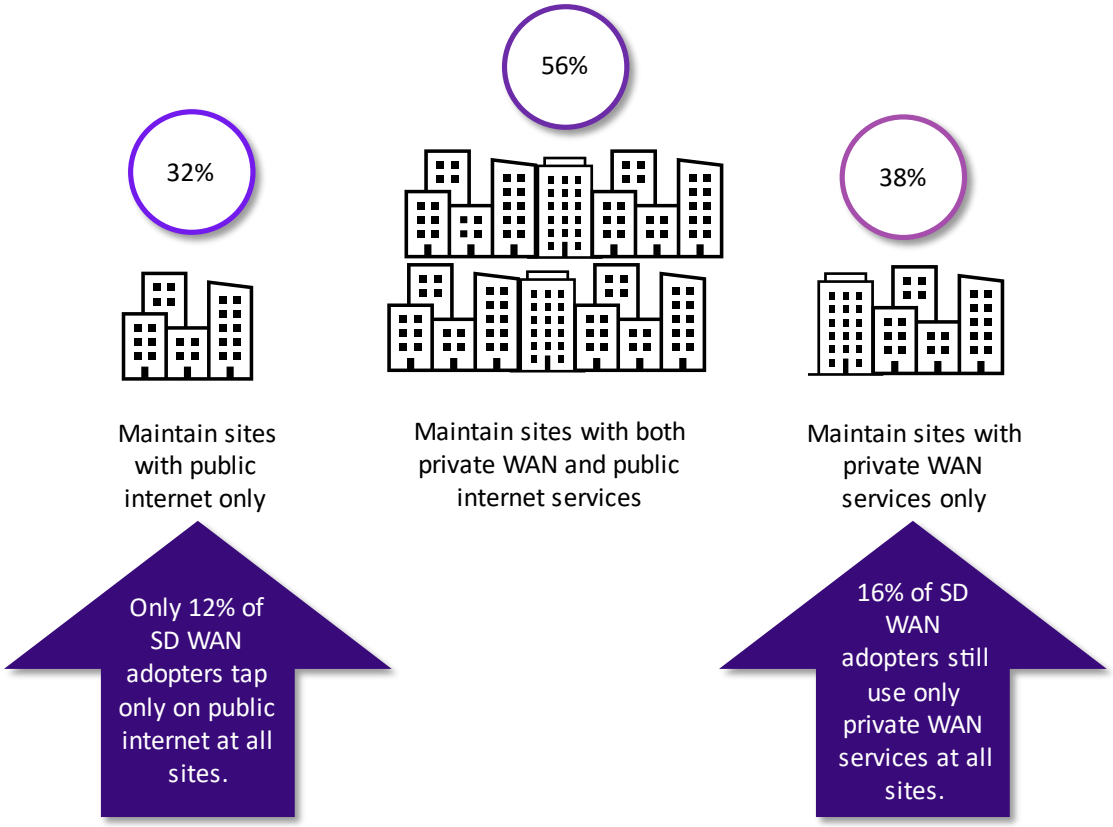
Enterprises have doubts about the performance of services delivered over traditional broadband

One of the main benefits of SD WAN is its ability to replace some private connectivity services with broadband, creating hybrid networks that do not diminish the reliability and performance of core applications that users require and have come to expect. The success of an SD WAN deployment depends both on the overlay—the SD WAN platform used to manage the workloads—and the underlay network that routes traffic.

Applications are taking center stage as companies increasingly rely on business applications hosted in the cloud. Poor application performance can disrupt business operations and result in a flood of complaints to IT managers. Under such circumstances, IT managers are under immense pressure to troubleshoot and resolve application-related issues and return to business as usual quickly.

Application performance, however, is only as good as the weakest link, which often is the broadband underlay network component. Enterprises recognize this, and most continue to send critical workloads over private connections to reduce the risk of poor application performance. Omdia's survey found that 55% of companies surveyed have deployed SD WAN for at least some locations. However, as shown in **Figure 2**, 32% of enterprise SD WAN adopters have some of their sites connected only by broadband, and only 12% use broadband over public internet across all locations. Even with SD WAN deployed, 88% of enterprises still opt to keep the more secure and higher-performing private connectivity services for their primary connection, using broadband for secondary or temporary connectivity. The survey found that 16% of SD WAN adopters still maintain *only* private WAN services across all sites.

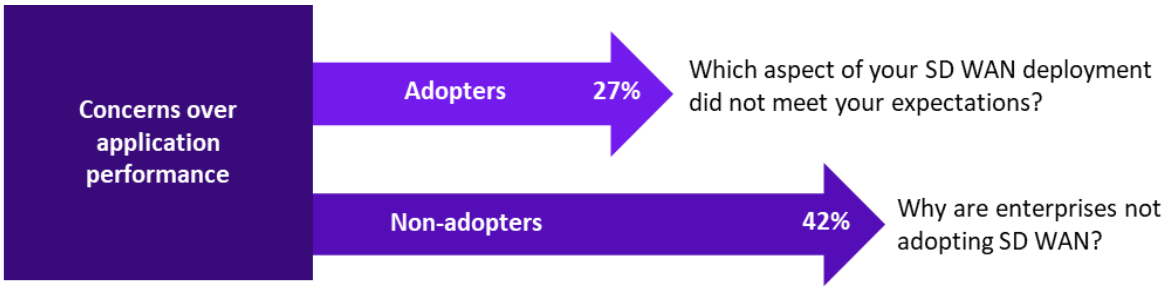
Figure 2: Few enterprises with SD WAN deployments rely on broadband services only



Source: Omdia

The survey also found that concerns about degraded application performance were a deterrent to enterprises considering SD WAN. As shown in **Figure 3**, 42% of survey respondents that had not yet deployed or did not plan to deploy SD WAN had concerns that SD WAN would not meet their application requirements. These concerns are valid: 27% of adopters noted that after deploying SD WAN, application performance was below expectations. Reasons for this performance impact point to the quality of the underlying service and the complexity of application policy configuration and maintenance.

Figure 3: Concerns about application performance are not unfounded



Note: adopters n=170; non-adopters n=137

Source: Omdia

> *Even with SD WAN deployed, 88% of enterprises surveyed still opted to keep the more secure and higher-performing private connectivity services for their primary connection to ensure consistent application performance.*

Managing SD WAN from end to end is not always easy

SD WAN offers greater control over traffic prioritization regardless of the underlying transport, allowing IT staff to manage workloads closely and route noncritical workloads over lower-cost broadband services. But continuous monitoring, management, and fine-tuning can be complicated. Further, relying on a collection of public broadband service providers, each with its own service characteristics, makes it more complicated to manage services across different geographies.

Enterprises that have taken a DIY approach to SD WAN confront implementation challenges including figuring out the best platform and architecture for the organization, configuring the platform properly for their site connectivity and supported applications, and issues of interoperability with existing services.

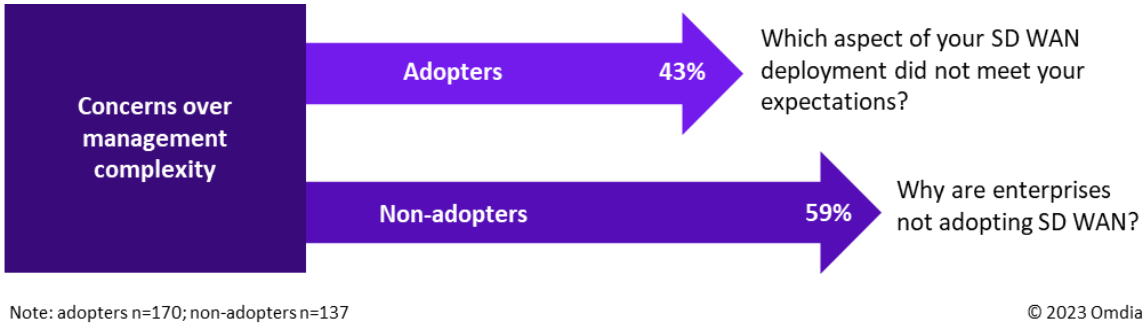
These examples contradict early enterprise perceptions of SD WAN as a solution that would be easy for enterprises to implement and manage by themselves. Those that do initially manage their SD WAN implementations internally often end up looking to partners for assistance to scale and operate the migration.

Complexities of managing SD WAN, including orchestration and service chaining, overseeing multiple endpoints, and application management, are common problems experienced by SD WAN adopters

(**Figure 4**). Enterprises must contend with different requirements at different sites ranging from headquarters to the cloud, branches, and remote locations in different geographies.

Concerns over management complexity also hold some enterprises back from adopting SD WAN. Management complexity issues that concern SD WAN non-adopters include a lack of interoperability of the SD WAN solution with existing network infrastructure and unexpected complications in deploying and managing SD WAN. Based on the experiences of SD WAN adopters, there is some justification for these concerns: 43% highlighted that management complexity continued to exist after deployment. These enterprises found that they still needed to fix issues on site and found it challenging to provision network services, change site configurations, or scale the network.

Figure 4: Management complexity of SD WAN is often higher than expected



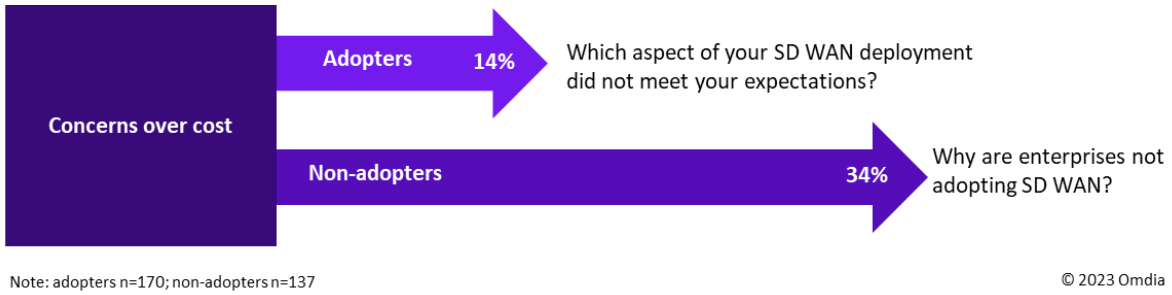
Source: Omdia

> *Forty-three percent of SD WAN adopters still needed to fix issues on site and found it challenging to provision network services, change site configurations, or scale the network.*

Cost is always a consideration

Cost has receded as a primary driver behind SD WAN, but some enterprises still are disappointed when they find SD WAN cost savings are below their expectations (**Figure 5**). Enterprises expect to reduce network costs by increasing their broadband use and reducing private connectivity. They move sites from dual-router / dual-MPLS networks to less expensive hybrid MPLS VPN / internet VPN or all-internet access. They expect that SD WAN's traffic prioritization and application policy capabilities will allow them to maintain network performance.

Figure 5: Cost savings do not always materialize



Source: Omdia

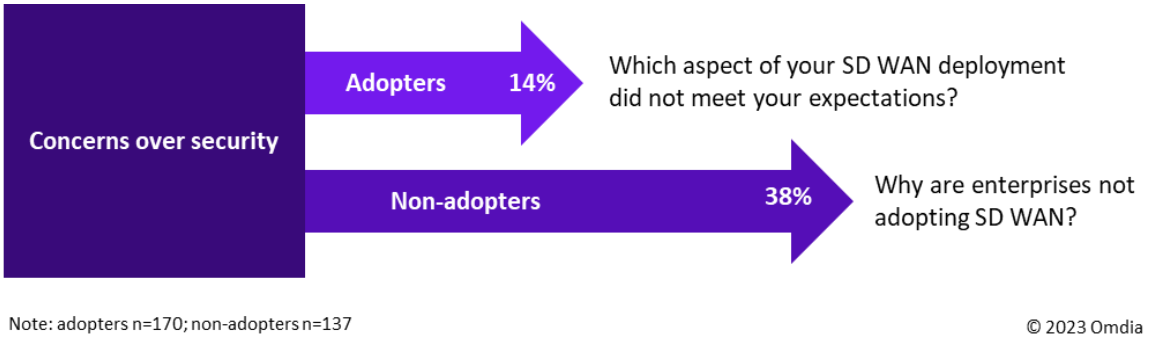
When enterprises replace private connectivity such as MPLS VPN ports for broadband, they often buy faster, shared, asymmetrical speeds on less reliable circuits (no SLAs) or even add circuits such as a second internet service or additional 4G wireless backup to make up for the use of lower-quality underlay broadband services. That reduces some of the savings. The enterprise also needs to review its security measures and may need to increase investment in security tools. That too takes a bite out of expected cost savings. There is also the overhead cost of managing multiple service provider contracts and guarantees, which further reduces potential cost savings.

> *By increasing their broadband use and reducing private connectivity, enterprises expect to reduce network costs, but this is often not the case. Enterprises may need to buy faster and more expensive broadband speeds or add a failover circuit, which reduces cost savings.*

Security is top of mind during a network transformation

Omdia surveys across service areas consistently find that security is a top expectation of modern IT initiatives, and network modernization efforts are no different. Security concerns figure prominently for enterprises, regardless of how they have proceeded with their SD WAN implementations. There is a noticeable difference in perception between respondents that have implemented SD WAN and those that have not: **Figure 6** shows that security is a more significant concern for those companies that are holding back from moving to SD WAN than for those that have progressed further and now have post-implementation experience. Few enterprises in the latter group express discontent with actual security capabilities relative to their expectations for simplification and application performance.

Figure 6: SD WAN adopters understand that additional tools are required for comprehensive security



Source: Omdia

SD WAN platforms can use internet VPNs that ignore traffic outside the VPN. Platforms include built-in firewalls and can configure application management policies and path restrictions. Some SD WAN vendors draw on their security background or incorporate unique security features into their platforms. But not all SD WAN is inherently built to detect and protect from threats intelligently.

Enterprises implementing SD WAN accept that if they require security tools beyond the basic policies supported by their SD WAN platform, they need to look to additional sources. They understand that they must procure services for capabilities such as zero-trust network access (ZTNA), cloud access security broker (CASB), firewalls, and other security options that they might have to find separately from their SD WAN solution.

> *Security is seen as a critical benefit of SD WAN. Though SD WAN often includes firewall and UTM capabilities and policy-based routing, enterprises may still find that they need to procure additional tools to establish a comprehensive security posture.*

Considering options

Before making the leap to a new network solution, enterprises must consider what they want to achieve and prioritize critical objectives. Is the main objective to optimize application performance, to have better visibility and controls over the network, to simplify management of the enterprise network, to lengthen the lifespan of existing solutions, to be access agnostic, or to lower cost? Considering the trade-off between cost and performance, enterprises need to identify their desired outcomes and study a range of hybrid network transformation options to find one that best suits their needs. SD WAN is one option; it is not necessarily always the best solution for every enterprise environment.

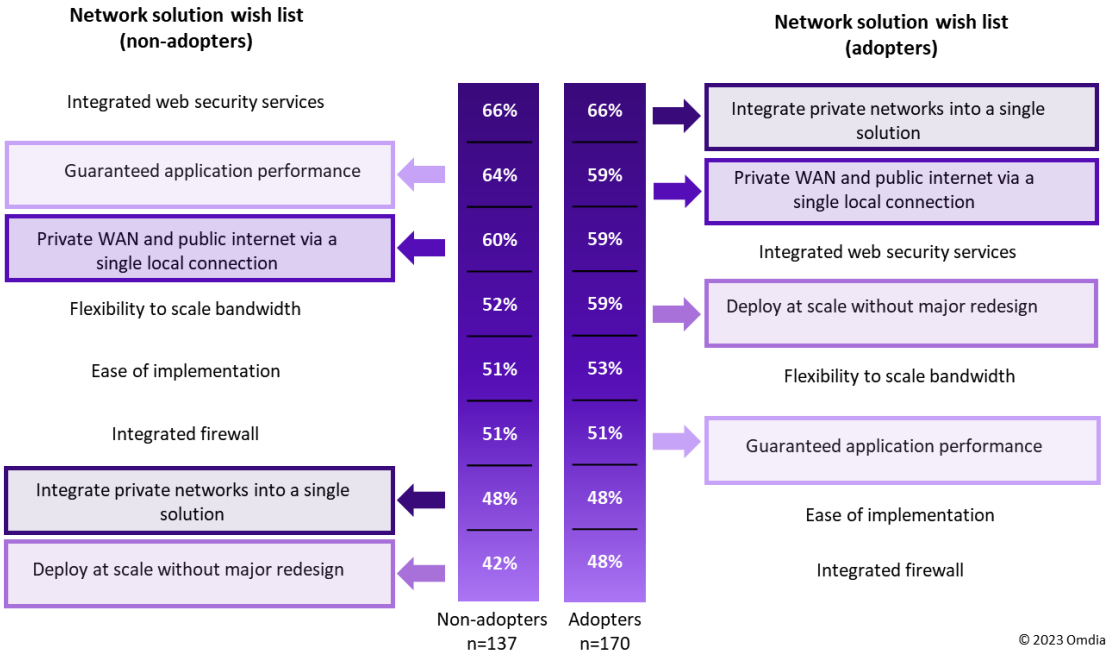
Network managers' requirements, and the discussion below, are a starting point to broaden the conversation beyond SD WAN to what the organization needs.

What do enterprises really want?

Omdia's survey of enterprise executives asked respondents to rank features they considered most important when migrating away from conventional offers. What does the ideal solution include?

Enterprises want the flexibility and scalability of newer technologies such as SD WAN, but moving to new technologies can be a difficult process. Large enterprises often have extensive legacy network estates that are difficult and risky to turn down, and they may wish to retain secure, private WAN services for mission-critical traffic. At the same time, these companies want to connect some locations via public internet services to manage costs. Ultimately, they want to merge their private WAN and public internet estates, with the entire network solution managed via a single pane of glass. And though cost is not always the primary element in evaluating a solution, it is always important. A transparent cost structure is ideal for enterprises that need visibility to plan their budgets.

Figure 7: Perspectives shift once an enterprise undertakes network transformation



Source: Omdia

Figure 7 illustrates the shift in "must-have" priorities between enterprises that have not yet undertaken network transformation such as SD WAN and those that have deployed SD WAN. SD WAN adopters acknowledge the challenges they face in managing disparate networks and the difficulty in scaling to new sites. The key takeaway is the lessons learned by enterprises after they have network transformation experience, which include valuing solutions that simplify scaling and managing the network.

In a perfect world, a network transformation solution is flexible and scalable and integrates disparate legacy networks such as private WAN or public internet connectivity. It should draw on the best of both worlds, supporting reliable application performance based on site needs. Network security should also be embedded in the service. A partner that supports a hybrid network solution with these attributes can help enterprises build new solutions out of existing private network services such as MPLS while meeting business needs and budgets.

Should your service provider own the underlying network?

Enterprises have several options when it comes to assembling the network best suited to connect their sites. They can work with multiple internet service providers (ISPs) to cover their sites, work with a single provider that partners with many ISPs to aggregate coverage, or work with a single provider that has both networks and partners.

- **The benefit of working directly with multiple ISPs is the option to partner with an ISP for each enterprise location with the best on-the-ground connectivity and quality.** This option comes

with the complexity of managing multiple ISP contracts, service level agreements, and management platforms. Omdia's surveys find that this complexity slows implementation progress for 58% of adopters and even has an impact on business operations for 21% of adopters.

- **The benefit of working with a single provider that does not own or operate their network but instead partners with many ISPs is minimizing the number of contracts to manage.** However, these providers rely on third-party networks, and there may be delays in troubleshooting as problems are routed to different partners for resolution. In addition, there may be fewer ISP choices: the enterprise relies on a local ISP in each market preferred by its provider.

- **The most significant benefit of working with a single provider that owns most of the network and has partners is avoiding the pain of managing multiple suppliers and, therefore, multiple contracts.** There is one contract, one bill, one support contact for troubleshooting, and one pane of glass to manage the entire network. These providers have control over the quality and reliability of their network and the freedom to work with partners to serve off-net enterprise locations.

An enterprise accustomed to using private WAN connections will naturally be more familiar with dealing with fewer suppliers. Managing multiple ISPs across the globe introduces a new level of complexity. Surveyed enterprise SD WAN adopters highlight the challenges that can accompany the first two models. The enterprise faces a lot of new complexity or else is limited to the provider's ISP partners and may have to pay higher prices for middling service quality in some markets.

The cloud and network services landscape has many players

Just as enterprises have several partnering models for sourcing network services, they also have several models available for overlay solutions. Each model has benefits and drawbacks:

- **Solutions from SD WAN platform vendors are widely available to enterprises today.** Platforms from these suppliers feature high availability and dynamic traffic management with application-aware routing to ensure user experience. The benefits of these solutions include end-to-end visibility, enterprise choice in selecting the underlay network services to meet budget needs, and the ability to configure policies to manage applications and secure traffic. However, these services can be complicated to implement, especially when an enterprise must source and manage a complex network underlay to connect locations. SD WAN platforms also feature proprietary hardware and software; enterprises may face additional challenges in getting their hands on equipment because of supply chain disruptions and vendor lock-in because interoperability between vendor solutions is often an issue.

- **Cloud-based SD WAN solutions deliver solutions over the public internet.** The companies providing these services do not own or operate their networks. Instead, they have partnerships with many ISPs and source SD WAN network services for the enterprise based on these partnerships. The benefits of this type of supplier include a single contact and "one throat to choke" if there are problems with the service. The downside is that enterprises must work with the service provider's local partner selection. That may not always be the best option for the

enterprise. These players also rely on best-effort internet and third-party networks. Network performance is hard to guarantee, and limited low-layer network visibility can complicate troubleshooting.

- **Multicloud networking simplifies the management and delivery of workloads between multiple clouds.** These providers highlight the simplicity and speed of provisioning connectivity. They scale to manage network needs on demand. They offer consumption-based models with portal access that require no hardware or software deployment. However, there may be limitations in the ability to address performance problems.

- **Conventional hybrid networking allows the enterprise to deploy different network technologies based on the needs of each location.** This solution addresses the cost and performance dilemma but introduces management complexity. Network managers must deal with a complicated topology of connectivity profiles across sites to route each of dozens or even hundreds of applications over the correct network. On its own, hybrid networking offers limited visibility across the network.

Network modernization must start with a solid foundation

There are many options for enterprises that want to modernize their network, but these solutions are only as good as the underlying network. Enterprises evaluating network solutions must strike a balance between managing costs and ensuring optimal network performance. However, they also need to ensure that the underlay meets security, reliability, and performance needs, regardless of the network overlay technology.

Integrating multiple networks into a single solution, utilizing a single connection for private WAN and broadband, and deploying and scaling a solution without major redesign were apparent desires of both enterprises that had adopted SD WAN and those that had not. These responses highlight the need for a new approach to building networks, a strategy that delivers an integrated, flexible solution that can support whatever services the enterprise deploys over them.

KEY TAKEAWAYS

- **Expectations for some SD WAN scenarios may not match reality**

  SD WAN is often positioned as a way for enterprises to extend reach to distributed enterprises while reducing network costs and without sacrificing application performance. However, adopters find that while they can move to lower-cost network services, there could be a price to be paid in terms of impact on application performance and management complexity. Careful consideration must be given to exactly what type of SD WAN or hybrid connectivity solution is chosen and what kind of underlay networking elements will work best.

- **Private connectivity still has a place in private networks**

  Despite the move by some enterprises to connect more locations via broadband, the need for private connectivity remains. Enterprises cannot take risks when it comes to critical communications. Private connectivity solutions continue to deliver traffic between critical locations such as company headquarters, essential facilities, data centers, and cloud service providers.

- **One solution may not always be the best fit**

  SD WAN is a popular enterprise solution, but it is not always the best-fit solution. Enterprises should explore all options available to identify their most effective solution. There are alternatives to SD WAN in the market for companies wanting a solution that packages reliable, consistent application performance regardless of the underlying technology without increasing management complexity.

Appendix

Author

Cindy Whelan
Practice Leader, Service Provider Enterprise Network and Wholesale Services
customersuccess@omdia.com

Adeline Phua
Principal Analyst, Network Transformation
customersuccess@omdia.com

Get in touch

www.omdia.com
customersuccess@omdia.com

Omdia consulting

Omdia is a market-leading data, research, and consulting business focused on helping digital service providers, technology companies, and enterprise decision makers thrive in the connected digital economy. Through our global base of analysts, we offer expert analysis and strategic insight across the IT, telecoms, and media industries.

We create business advantage for our customers by providing actionable insight to support business planning, product development, and go-to-market initiatives.

Our unique combination of authoritative data, market analysis, and vertical industry expertise is designed to empower decision-making, helping our clients profit from new technologies and capitalize on evolving business models.

Omdia is part of Informa Tech, a B2B information services business serving the technology, media, and telecoms sector. The Informa group is listed on the London Stock Exchange.

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Omdia's consulting team may be able to help your company identify future trends and opportunities.

Copyright notice and disclaimer

The Omdia research, data and information referenced herein (the "Omdia Materials") are the copyrighted property of Informa Tech and its subsidiaries or affiliates (together "Informa Tech") or its third-party data providers and represent data, research, opinions, or viewpoints published by Informa Tech, and are not representations of fact.

The Omdia Materials reflect information and opinions from the original publication date and not from the date of this document. The information and opinions expressed in the Omdia Materials are subject to change without notice and Informa Tech does not have any duty or responsibility to update the Omdia Materials or this publication as a result.

Omdia Materials are delivered on an "as-is" and "as-available" basis. No representation or warranty, express or implied, is made as to the fairness, accuracy, completeness, or correctness of the information, opinions, and conclusions contained in Omdia Materials.

To the maximum extent permitted by law, Informa Tech and its affiliates, officers, directors, employees, agents, and third-party data providers disclaim any liability (including, without limitation, any liability arising from fault or negligence) as to the accuracy or completeness or use of the Omdia Materials. Informa Tech will not, under any circumstance whatsoever, be liable for any trading, investment, commercial, or other decisions based on or made in reliance of the Omdia Materials.