

SD-WAN and SASE Managed Services Survey Report

June 2023



Sponsored by:



Highlights and Key Findings

- **For this report, we surveyed 196 qualified enterprise networking and security users, director-level and above.** The goal was to find key needs for software-defined wide-area networking (SD-WAN) and secure access service edge (SASE) in managed services.
- **Survey respondents indicate strong demand for SD-WAN and SASE managed services.** Our survey data and discussions with end users indicate SD-WAN/SASE technology helps professionals with network and security challenges, including the growing complexity created by distributed applications, cloud connectivity, and sprawling security risks.
- **Managing network complexity is the largest challenge driving managed services demand.** When asked about the largest challenges in managing WANs, 85% of respondents identified complexity, followed by expertise and knowledge (68%). Rounding out the responses were cost (60%) and time (47%). (Multiple responses were allowed.)
- **Hybrid work and the need for zero-trust network access (ZTNA) are key drivers of SD-WAN/SASE technology.** In the survey, 98% of respondents said that hybrid work has increased demand for SASE and ZTNA, **with 92% considering ZTNA** a crucial component.
- **Hybrid (cloud/edge deployment) and single-pass architectures will be important components of SASE/SD-WAN services going forward.** When respondents were asked if they wanted a hybrid solution that can accommodate networking and security both on premises and using cloud points of presence (PoPs), 98% said yes. In addition, 94% of respondents said they prefer a single-pass architecture.
- **There will continue to be a diversity of SD-WAN/SASE deployment models.** The two most popular models for deployment are best-of-breed combination (34%) and single-vendor (23%), but survey results show a wide diversity of deployment models.
- **Companies covered in this report:** Aryaka, Amazon, AT&T, British Telecom, Cato Networks, Check Point Software, Cisco, Colt, Comcast, Deutsche Telekom/T-Systems, Forcepoint, Fortinet, HPE (Aruba), Hughes, Juniper Networks, Lumen Technology, NTT, Orange, Palo Alto Networks, Tata Communications, Telefónica, Telstra, VMware, Verizon, Versa Networks, Vodafone, Windstream, Zscaler

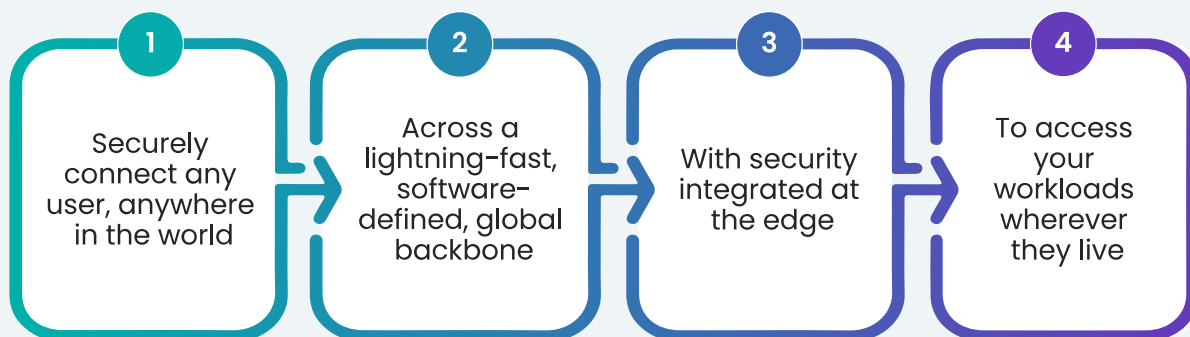
Aryaka SASE

It's time to evolve to a better
Network and Security
Services Experience



Why Aryaka

- ✓ True converged Network & Security via Aryaka Single-Pass Architecture
- ✓ Multi-Cloud Connectivity to hundreds of IaaS, SaaS and UCaaS
- ✓ Reliable Network Performance for onsite and remote users
- ✓ Single security policy enforced across Hybrid Edge
- ✓ Global SLAs with up to 99.999% Uptime
- ✓ Single Point of Contact



SD-WAN and Security
Delivered-as-a-Service



Enterprise Network Transformation
Survey Report 2023



Table of Contents

Introduction: Identifying Key Needs for Networking and Security Management	4
Survey Background & Demographics	5
Trends in SD-WAN/SASE: Key Survey Takeaways	7
A Drive Toward Integration	7
Key Challenges Faced	8
Hybrid Work and Zero Trust Are Key Drivers	9
SD-WAN and SASE Architectures Can Be Diverse	12
Deployment Models Will Vary	13
Single-Pass Architecture Can Be Important	16
SD-WAN/SASE Is Part of the NaaS Movement	16
Key Partnerships in the SD-WAN/SASE Managed Services Ecosystem	19
SD-WAN and SASE Vendors Targeting Managed Services	19
Independent Providers of SD-WAN/SASE Services	20
Changing Landscape of SD-WAN/SASE Services	20
Major SASE Platform and Service Provider Partnerships	23

1. Introduction: Identifying Key Needs for Networking and Security Management

Software-defined wide-area networking (SD-WAN) and secure access service edge (SASE) have been evolving to help networking and cybersecurity professionals with many new challenges, including the growing complexity created by distributed applications, cloud connectivity, and sprawling security risks.

What's needed more than ever are software-based platforms for integrating the management of network and security functions at the same time. This approach was first initiated by SD-WAN, which separated the software control from the hardware for branch-office networking. SD-WAN evolved and grew by adapting security functionality (SASE), which could be integrated into the network platform.

This unique approach of melding software-based control of SD-WAN and SASE has driven broad adoption across both enterprises and service providers, with service providers adopting the technology to deliver enterprise managed services.

Some of the problems that SD-WAN/SASE managed services solve:

- They can help enterprises adapt more flexible network architectures for secure connectivity to cloud services and multicloud applications;
- They help in integrating a growing number of cybersecurity functions, which need to be integrated with networking;
- They respond to the need for flexibility in enterprise architectures and work environments such as hybrid work.

Of course, this process can be complicated and not without challenges, many of which we will identify in this report. A managed services approach can help enterprises implement SD-WAN/SASE managed services by consuming services and communications networks in an integrated, fully managed package. Service providers and SASE vendors can work together to qualify, integrate, and deploy the services. These new markets have been successful because they help enterprise network and security managers implement a wide array of networking and security services at once, using software-based control and management.

In this report, we will update you on the evolution of SD-WAN/SASE managed services, anchored to a detailed annual survey of enterprise users of SD-WAN and SASE technology. The report includes the following:

- Full survey results from 196 IT networking professionals, including details on their challenges, needs, and desires for SD-WAN/SASE managed services.
- International survey with respondents from the U.S., Germany, and India.
- An overview of recent news in SD-WAN/SASE managed services.
- Key partnerships and offerings in the market.

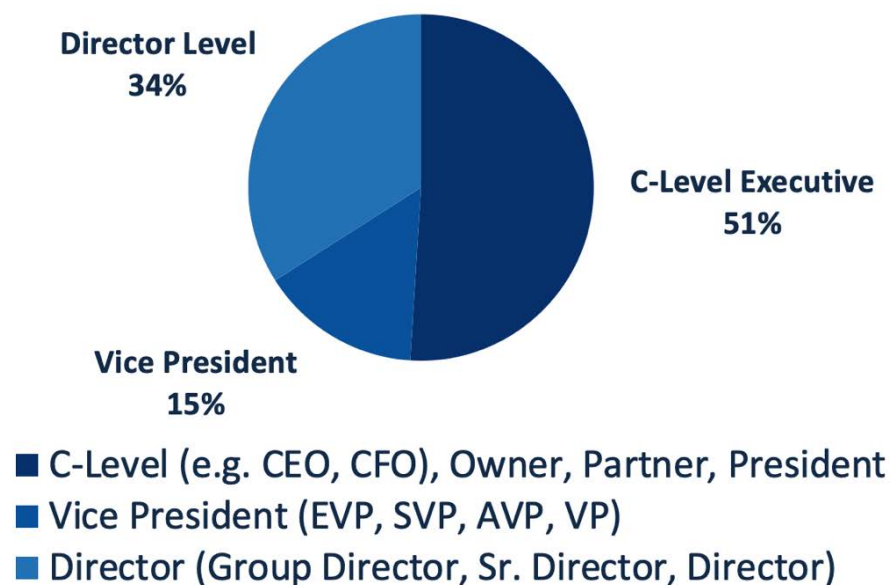
We also detail trends in consumption of managed network services – and why SD-WAN/SASE technology is naturally suited to delivery as a managed service. We have interpreted the results and tied them to ongoing trends in the industry, as the market for SD-WAN/SASE managed services evolves.

Survey Background & Demographics

Our survey took place in March and April of 2023. The total audience of 196 respondents came from three countries: the U.S. (127 respondents), Germany (37), and India (32).

We qualified the audience by asking filter questions to ensure respondents were director-level and above employees managing network and cybersecurity services at companies with more than 200 employees. In addition, we qualified respondents for networking and cybersecurity budget authority. The majority of respondents were C-level executives (51%), with the next largest groups comprising director level (34%) and vice president level (15%).

Survey Demographics – Job Title



N=196

We found that this survey delivered key insights into many of the trends we have been following in the market, and it backs up some of the conclusions we have about the direction of the SD-WAN/SASE market, which we will detail in this report. So read up – as usual we look forward to any thoughts and feedback!

R. Scott Raynovich
Founder and Principal Analyst
Futuriom

2. Trends in SD-WAN/SASE: Key Survey Takeaways

Networks have gotten complicated over the past few years. Network managers and architects are looking for more flexible ways to manage their networks and applications. This has served as the foundation of the growth in SD-WAN/SASE, which we expect will continue for many years to come.

The explosion of connectivity to cloud services, often using a combination of enterprise networks and the Internet, triggered the need for SD-WAN and SASE. In the early days, SD-WAN emerged to build networks that could leverage the best of both worlds – combining aging enterprise networking technologies such as multiprotocol label switching (MPLS) in addition to Internet-based broadband. Enterprises found it a more efficient way to manage branch connectivity.

With more people using the Internet to access the cloud, SD-WAN was needed to provide better intelligence and security for access to both enterprise and cloud software-as-a-service (SaaS) apps. For example, the network needed to know which services users needed in order to access better control and provide security for apps, especially those accessed outside of the enterprise on the Internet. The market expanded to include SASE functionality, which provided cybersecurity functions such as secure web gateway (SWG), cloud access security broker (CASB), firewall-as-a-service (FWaaS), intrusion detection, zero-trust network access (ZTNA), and many others to protect enterprise access to public networks and SaaS apps.

The SASE market was accelerated by the COVID pandemic, which triggered a long-term shift to hybrid work – and shifted the center of gravity of networks from enterprise sites to remote and hybrid environments. This demanded a more flexible, software-based architecture for delivering users network and security services – any network, all security, anywhere – on demand.

A Drive Toward Integration

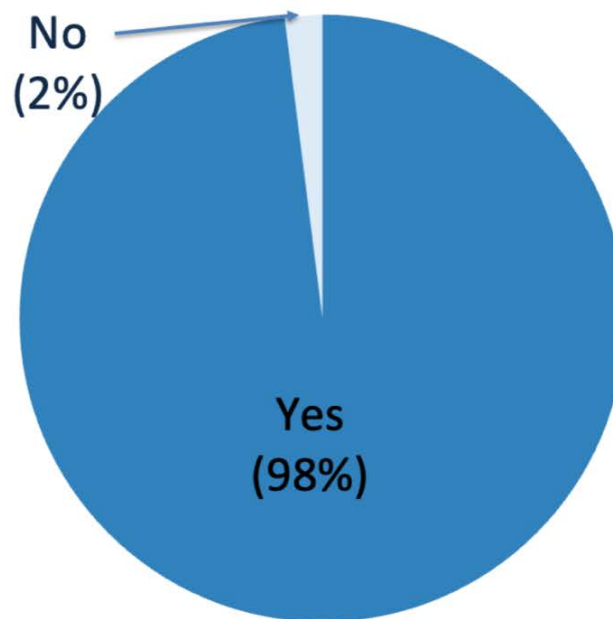
The easiest way to think about the evolution of SD-WAN and SASE is that it's about integrating discrete security and networking functions that can be more easily managed with software-based orchestration and cloud-based distribution.

The core value of SASE is a network and security framework that can deliver secure access to applications and data from anywhere. It's a comprehensive platform for integrating network security functions. These include some of the major ones we have discussed – such as CASB, SWG, FWaaS, IDP, and ZTNA – as well as many others.

The factors fueling SD-WAN/SASE adoption are not always easy to figure out. Many organizations

would like to buy these technologies from either an integrator or a managed service provider (MSP). As seen in the survey result below, 98% of respondents said they saw the benefits of combining SD-WAN with SASE. This trend has been strong driver of rapid expansion and integration of SD-WAN and SASE services over time.

Do you see the benefits of combining SD-WAN technology with security services at the edge (SASE)?



N=196

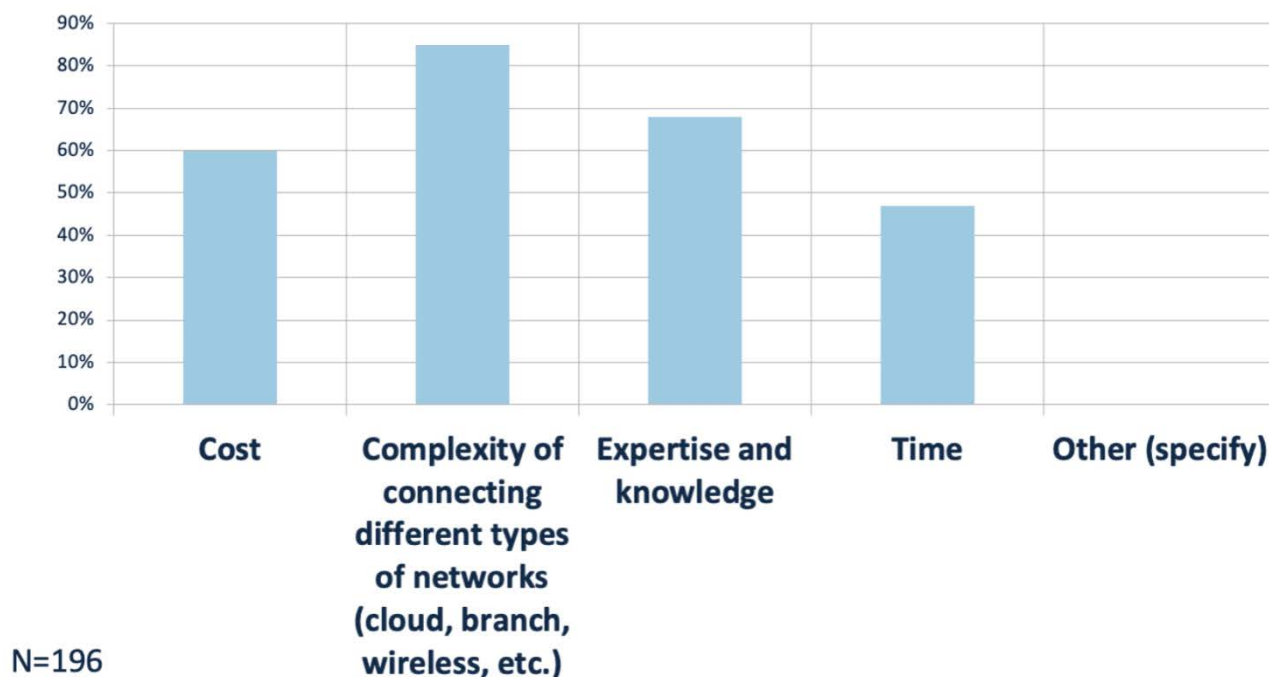
Key Challenges Faced

The complexity of cloud networking, cybersecurity markets, and worker patterns these days has brought many challenges to network managers. Whether it's figuring out from which of the hundreds of vendors to purchase network security products or how best to build a secure, cloud-friendly network for end users, they have a lot of choices.

The complexity is demonstrated in one of our survey questions, which asked respondents to detail the largest challenges they face in managing WANs and enterprise networking connectivity.

The largest challenge identified was network complexity, identified by 85% of respondents (multiple responses were allowed), followed by expertise and knowledge (68%). Rounding out the responses were cost (60%) and time (47%).

What are the largest challenges you face managing wide-area networks (WANs) and enterprise network connectivity?



Hybrid Work and Zero Trust Are Key Drivers

The impact of the COVID pandemic on the technology world was widespread, accelerating many digital services. In addition, the large-scale shift had enormous impact on network architectures, which were largely built for a different world – one in which most of the workers worked within the safety of an enterprise security perimeter.

With the expanded use of the Internet, SaaS, and remote work, enterprise perimeters have largely broken down, requiring a new security architecture that can secure access to any applications from any location. The general description of this approach is the term zero trust, which means that networks and applications can't trust access by anyone or anything and must use a more sophisticated set of identifiers and authentication methods to ascertain that access is non-hostile.

In the context of hybrid work, where employees may work from different locations, SASE offers several security and zero-trust benefits:

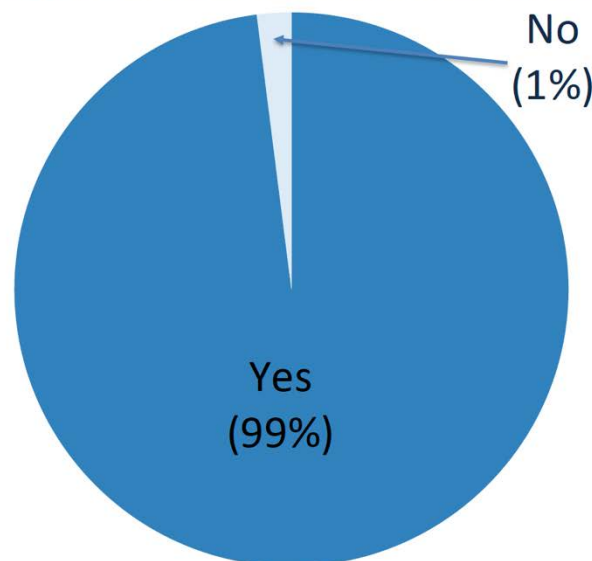
- Simplified network architecture: SASE consolidates multiple network and security functions into a unified service that can be managed either from the cloud or in an enterprise environment, simplifying network management and reducing the complexity of hybrid work environments.

- Secure access: SASE enables secure access to applications and data regardless of the user's location, improving productivity and flexibility for remote and mobile workers.
- ZTNA: The zero trust approach assumes that no user or device can be inherently trusted, regardless of their location. Instead, it verifies and enforces strict access controls and authentication for each user and device attempting to connect to network resources.

As seen in the responses to the survey question below, 99% of respondents say that hybrid work has increased demand for SASE and ZTNA.

FUTURIOM

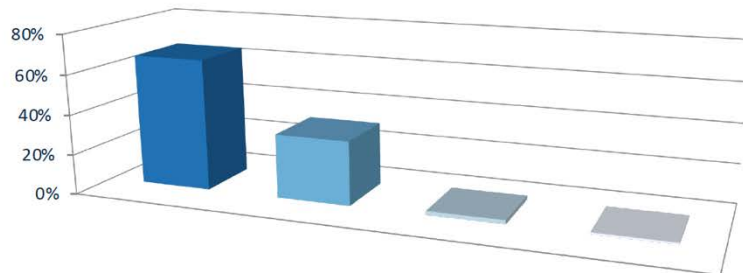
Has the advent of hybrid work and remote work increased demand for secure, software-based networking and security technology such as SASE and zero-trust networking?



N=196

In another question, we asked survey respondents about whether they are managing end users from an on-premises or hybrid scenario.

Has the recent evolution toward hybrid work changed how you view managing networks and security across on-premises versus remote users?

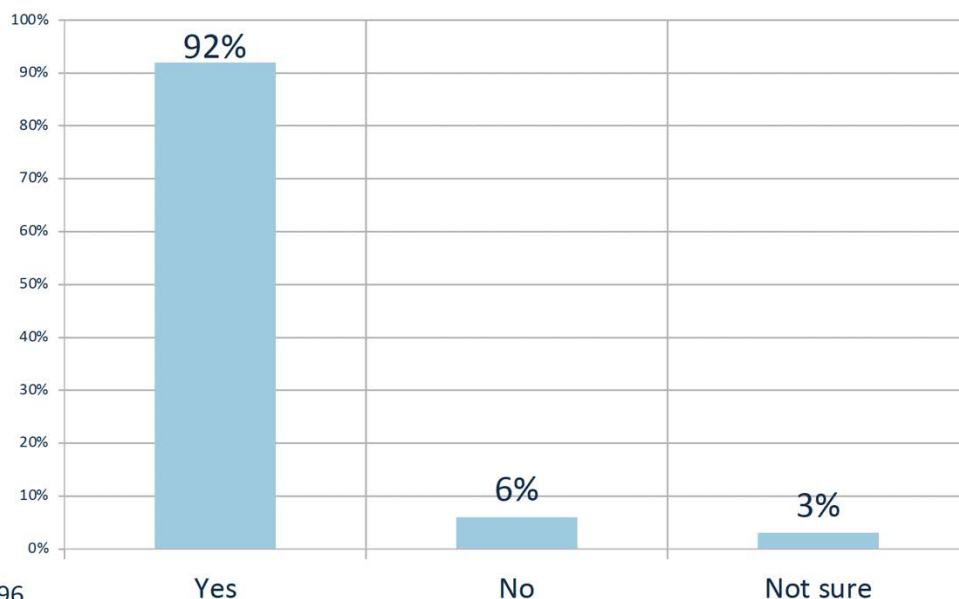


- Yes, we now have immediate plans for hybrid scenarios of on premises and remote connectivity
- Yes, we have to plan for hybrid scenarios of on premises and remote connectivity in the next 6-12 months
- Yes, we have to plan for hybrid scenarios of on premise and remote connectivity in 12-18 months
- No, there has not been a meaningful shift

N=196

It's clear from these results that there is a strong pull toward hybrid work deployments: 66% of organizations already having immediate plans or capabilities for hybrid work scenarios, and 32% of them are planning on rolling hybrid capabilities out over the next 6-12 months. And when we asked respondents if ZTNA is a crucial component of SASE and SD-WAN offerings, 92% said yes.

Do you consider zero-trust security a crucial component of SASE and SD-WAN offerings?



N=196

SD-WAN and SASE Architectures Can Be Diverse

There are several architectures associated with the implementation of SD-WAN and SASE. These architectures vary depending on different vendors and their specific offerings, but mostly they come down to where the functions are hosted and how they are orchestrated and managed across networks and hardware. Here are the three most common SASE architectures:

Cloud-hosted architecture: This architecture is focused on a cloud-native approach, where all SASE services are delivered as a unified, cloud-based platform. The network and security functions, such as SD-WAN, SWG, FWaaS, CASB, and others, are hosted and managed in the cloud. This architecture offers agility and ease-of-use, with the primary benefit of enabling end users to adopt the services right away from the cloud. In addition, some of these services are often integrated into “best-of-breed” platforms through partnerships among SD-WAN/SASE vendors and service providers.

A 100% cloud-hosted architecture does have some drawbacks, however. In larger deployments or those involving large networks over great distances, it can become unwieldy, because all traffic must be diverted to the cloud rather than being processed on local hardware.

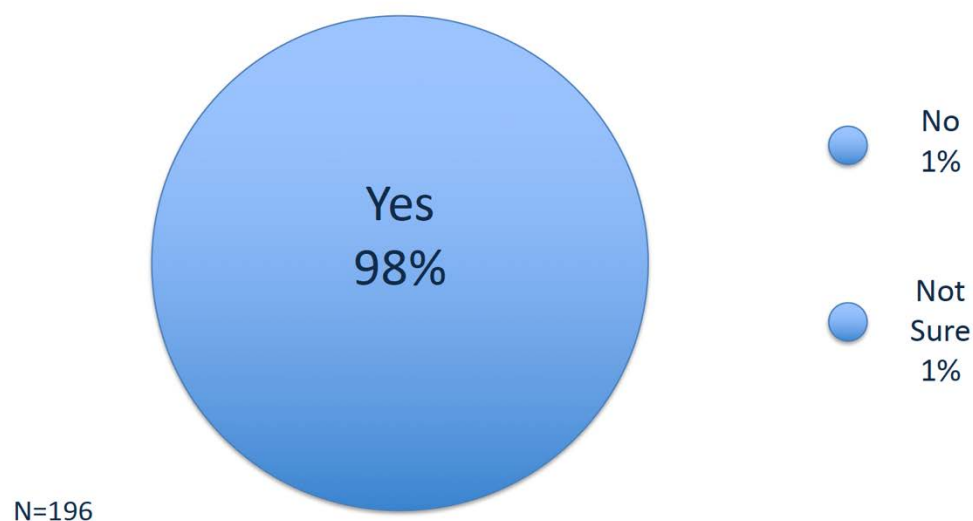
Local appliance architecture: In this architecture, SASE services are delivered through physical or virtual appliances deployed at the network edge, such as branch offices or datacenters. These appliances consolidate various network and security functions into a single device. This architecture suits organizations that prefer on-premises control or have specific compliance requirements that restrict cloud usage, but it is often associated with past enterprise security perimeter architectures – such as putting firewalls around the users.

Hybrid architecture: As the name suggests, a hybrid architecture combines elements of both cloud-hosted and appliance architectures. It allows organizations to deploy certain SASE services in the cloud while retaining some on premises. For example, an organization may opt to utilize cloud-based SD-WAN and SWGs from the cloud while keeping certain security functions within their local infrastructure. This architecture offers flexibility and allows organizations to leverage the benefits of both cloud and on-premises solutions.

Interestingly, when we asked respondents if they wanted a hybrid solution, 98% said yes. This may be the case of the solution sounding easier to find than it is, as hybrid solutions tend to be more difficult to build. But it’s clear that the respondents are looking at hybrid architectures (see following page).

FUTURIOM

Are you interested in a hybrid solution that can accommodate network and security convergence at on-premises and branch installations as well as SASE cloud points of presence?



Deployment Models Will Vary

Not only do organizations have to determine which architecture they would like, but they also need to establish how they are going to deploy the technology.

For example, the most common deployment models are:

Single-vendor solution: The organization purchases a SD-WAN/SASE platform from a single vendor and seeks their assistance in implementation.

Best-of-breed solution: The organization purchases SD-WAN/SASE components from different vendors, using an integrator, MSP, or platform partner for deployment.

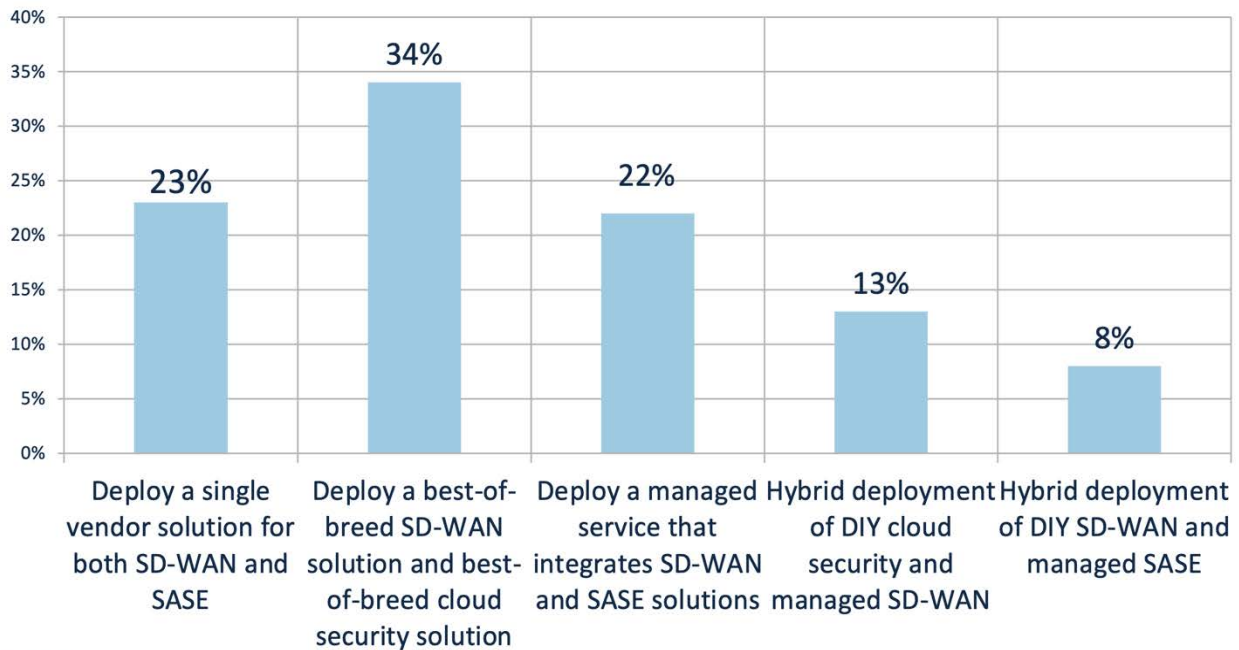
Integrated managed service: The organization purchases SD-WAN/SASE components and connectivity or transport services from a managed service provider.

Hybrid DIY: In this model, the organization does most of the integration themselves, choosing services and features from MSPs and vendors.

In our questions on this topic, it became clear that there is large diversity among organizations in how

they seek deployment of SD-WAN/SASE. This makes sense, as the demands, architectures, and configurations of organizations vary widely. The largest group, 34%, picked a deployment scenario of separate best-of-breed SD-WAN and SASE solutions. However, the next-largest groups were split equally among single-vendor solution (23%) and managed services with integrated SD-WAN and SASE (22%).

Which one of the following deployment options would you prefer to implement for SD-WAN and SASE?

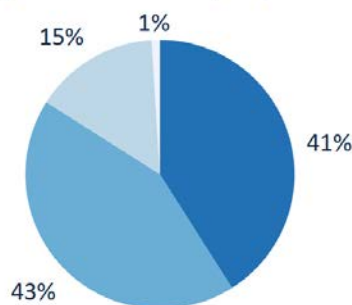


N=196

Another consideration is network transport. Enterprises must also acquire bandwidth, or transport

FUTURIOM

In considering an SD-WAN managed service, which type of provider would you prefer?



- Underlay and SD-WAN all from an incumbent telco
- Underlay and SD-WAN all from an alternative provider
- Underlay and SD-WAN from different providers
- Other (specify)

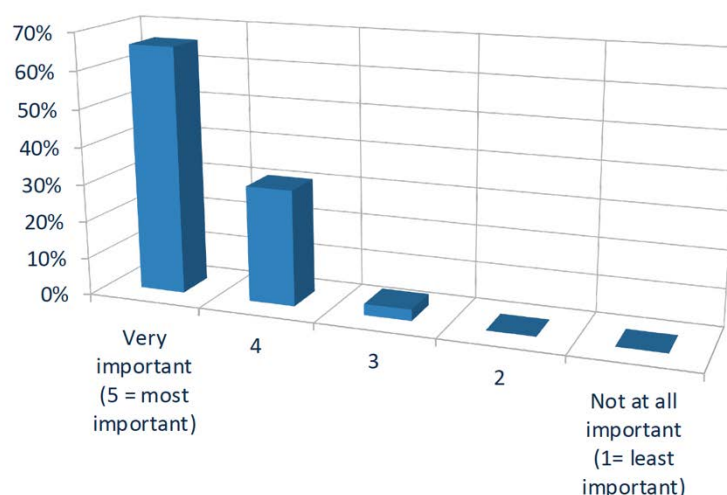
N=196

(underlay), in the form of network services such as broadband, Ethernet, MPLS, or wireless connectivity. In our survey results, 43% of respondents would like to buy underlay and SD-WAN together from an alternative provider; 41% would like to purchase both from an incumbent provider. A smaller percentage, 15%, would purchase from different providers.

Finally, there's the issue of global connectivity for SD-WAN. When asked to rank the importance of global connectivity, a majority (61%), ranked it as very important and 31% ranked it as important, while zero respondents said it wasn't important at all.

FUTURIOM

What is the importance of global connectivity in an SD-WAN managed service?



N=196 ■ Very important (5 = most important) ■ 4 ■ 3 ■ 2 ■ Not at all important (1 = least important)

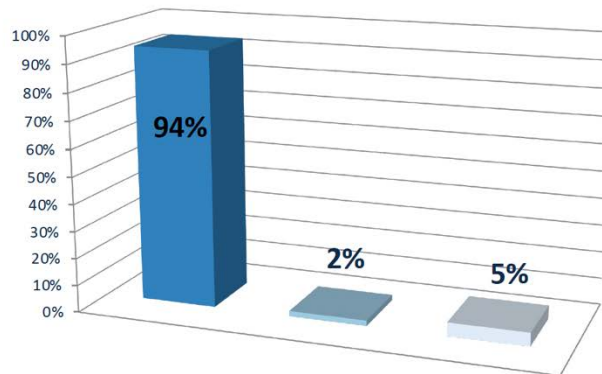
Single-Pass Architecture Can Be Important

One of the innovations of SD-WAN and SASE is to integrate the examination and processing of packets to identify network applications and security risks. The challenge is that this is technologically challenging – as a SASE architecture must implement packet processing in specific points of the network, which can introduce processing overhead and performance hits.

One of the considerations in the architectural decision is whether a single-pass architecture is preferred. In a single-pass architecture, packet-processing for applications and security are generally done in the same place – for example, the packets can be inspected at one point locally in a hybrid scenario or at a local PoP. The advantage of a single-pass architecture is that it can improve efficiency and speed. Rather than sending the same packets to different locations for processing (for example, sending apps for inspection in different places for SWG, CASB, and FWaaS), they can be processed once, at a centralized location. When we asked our survey audience, they clearly demonstrated a preference for a single-pass architecture, with 94% selecting it.

FUTURIOM

Do you believe that a single-pass architecture, which enables packet inspection for traffic analysis and security both on-premises and in the cloud, is an important element SASE solution?



N=196

■ Yes ■ No ■ Not sure

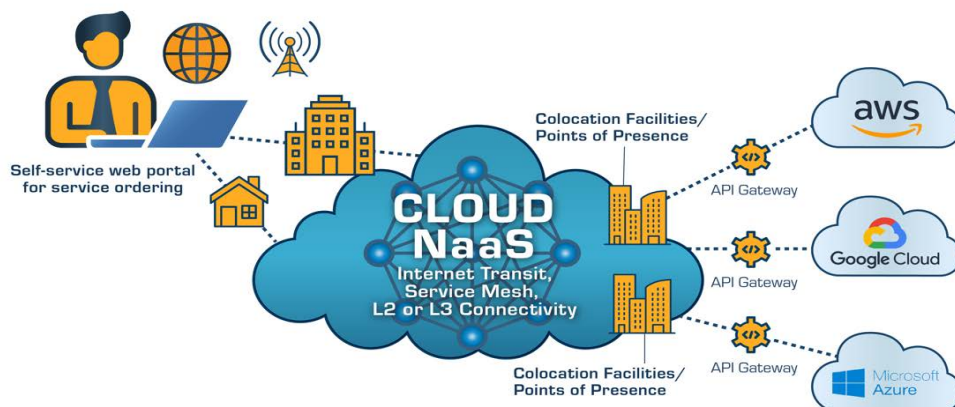
SD-WAN/SASE is Part of the NaaS Movement

Another conclusion we can reach based on our survey results and discussions with end users is that the network-as-a-service (NaaS) has wide appeal and that SD-WAN/SASE is part of that trend.

What is NaaS? It's the model in which customers consume networking as a service, rather than being consumed with building it themselves. In the NaaS model, the MSP or the integrator, rather than the end user, takes on more of the weight in building and deploying the service. The end user simply uses the service. This business model has been the great driver of enterprise software through the SaaS model – and it's now becoming part of the infrastructure model.

From the CxO's perspective, NaaS is great because it falls as an operating expense rather than a capital

Building the Virtual NaaS

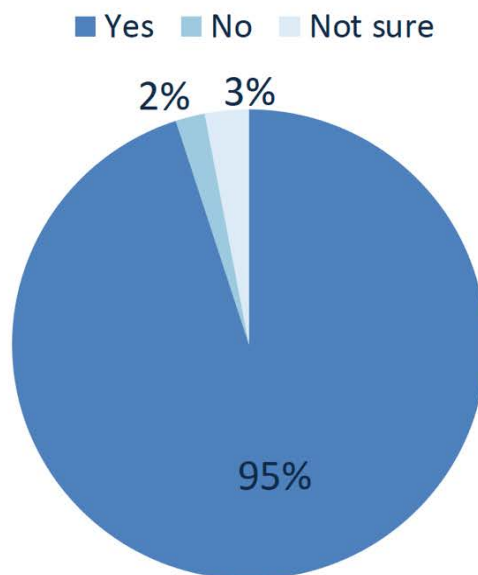


expense. It's also more flexible, because services can be added on demand without requiring a heavy up-front investment. NaaS is becoming increasingly popular for a wide variety of enterprise networking services – such as transport and cloud connectivity. One could argue that SD-WAN was the first NaaS service, enabling enterprises to buy software-defined WAN services that could be sold and orchestrated from the cloud. SASE showed that NaaS has many other possibilities in areas such as cybersecurity and policy control.

Futurium's vision of the future is that any network service can be consumed as a service and that someday most network services will be run by operators rather than end users. Indeed, our survey confirms this, with 95% of respondents saying that managed services and NaaS will play a greater role in how they manage network and global connectivity.

FUTURIUM

Will managed services and NaaS play a greater role in how you manage network and cloud connectivity services in 2023?



N=196

3. Key Partnerships in the SD-WAN/SASE Managed Services Ecosystem

There are many suppliers of SD-WAN/SASE technology solutions and services that are consumed by both enterprises and service providers. At last count there were upwards of 50+ SD-WAN and SASE vendors.

However, when you narrow the providers down to managed services, the list drops rapidly. Building an enterprise-class SD-WAN/SASE managed service requires a lot of work on both the service provider and vendor side, and it requires companies that have significant scale and expertise. It's true that many individual vendors can build a fully integrated solution, but as our survey points out, many end users would also like the service to be integrated with transport and underlay as well, with global connectivity. In the cases of the leading providers, the service is a cooperative effort between a service provider and a vendor or several vendors.

At the end of this section we offer a summary of some of the leading global SD-WAN/SASE managed services. These ecosystems have been built up over many years of partnership, and we would describe them as reaching maturity.

SD-WAN and SASE Vendors Targeting Managed Services

There are dozens of SD-WAN and SASE providers, but only a few have the scale and platforms designed specifically for use by the major service providers to roll out managed services. The market can be segmented by the varied approaches to deploy SD-WAN/SASE platforms and services: best-of-breed solution, DIY by enterprise customer, and integrated managed service. Some of the leading SD-WAN and SASE vendors have platforms targeting enterprises for DIY as well as service providers for managed services.

For the purposes of this report, we have focused on vendors that have specific platforms targeted at SD-WAN/SASE managed services. The leaders, by partnership count, include Cisco, Fortinet, HPE (Aruba EdgeConnect), Juniper Networks, VMware (VeloCloud), and Versa Networks. Nokia (Nuage) was once a significant player in this market but has pulled back significantly in recent years and is no longer actively marketing SASE solutions.

On the service provider front, some of the leading service providers for SASE/SD-WAN managed services include AT&T, British Telecom, Deutsche Telekom, Tata Communications, Telefónica, Telstra, Verizon, and Vodafone. They typically build services using the platforms from the

vendors, although there is usually further integration work involved – for example, they may need to connect to separate billing and support Systems (BSSs) or operations support systems (OSSs) from vendors such as Amdocs, Ericsson, Netcracker, and Nokia (the BSS and OSS leaders).

Independent Providers of SD-WAN/SASE Services

In addition to the major incumbent service providers, there are a handful of independent cloud-based providers with SD-WAN and SASE offerings. These include Aryaka Networks, Cato Networks, and Cloudflare, all of which have built their own networks to compete with incumbent service providers.

These independent cloud service providers take different approaches. In the case of Cato and Cloudflare, they offer primarily over-the-top overlay solutions leveraging the Internet, with network underlay purchased separately. Aryaka is one of the few independent providers packaging overlay and underlay services with the expansion of its new FlexCore offerings, which include layer 2 and layer 3 options for connectivity.

Changing Landscape of SD-WAN/SASE Services

Among the service providers as well as the leading SD-WAN/SASE platform vendors there is fierce competition to have fully featured platforms. Technology as well as partnerships are constantly shifting. M&A remains busy.

Compared with last year, news on the partnership front has slowed a bit, but there is still quite a bit of activity. Here are some of the highlights we have seen in the market in the past few months:

- Aryaka Networks in 2021 launched a major upgrade of its SASE and SD-WAN services using both L2 (Ethernet) and L3 (routed IP) infrastructure services, called Aryaka FlexCore. In 2021 Aryaka also purchased Secucloud to augment its SASE capabilities. More recently, Aryaka in April 2023 announced the availability of basic FWaaS delivery in a hybrid edge model on-premises and via its global PoPs. Aryaka also announced it had expanded its partnership with Check Point Software to combine Aryaka's global WAN with Check Point's Harmony Connect for cloud security, as well as on-premises security with Quantum Edge, Check Point's virtualized next-generation firewall. This combination is geared to delivering managed SASE services.

- Cato Networks has been steadily adding additional security features to its SASE service. In 2022, Cato added CASB functionality to its SASE services. The Cato CASB was built into the Cato Single Pass Cloud Engine (SPACE). More recently, at the RSA Conference in San Francisco in April, Cato announced the addition of Cato Remote Browser Isolation (RBI) to its Cato SASE Cloud platform. The company also recently claimed to be among the fastest-growing enterprise network security startups with \$100 million in annual recurring revenue, a target reached in just five years.
- Cato also recently announced a partnership with Windstream Enterprises to deliver a single-vendor secure service edge (SSE) solution. Cato says that SSE provides the benefits of enterprise-level security along with constant visibility and maximum protection for users, devices, applications, and data across any device or location.
- Cisco's Viptela SD-WAN platform recently drew the wrong sort of attention when the company announced that some vEdge devices were at risk of failing due to expirations of security certificates. Thousands of customers scrambled to patch or replace devices. We view this as a significant hit on Cisco's brand in the SD-WAN space.
- Fortinet recently touted better automation and integration among SD-WAN and SASE in the release of its FortiOS version 7.4. It implements Fortinet Security Fabric and includes firewalling, access control, zero trust, and authentication in addition to managing SD-WAN, switching, and wireless services. The company said it also added enhancements to FortiSASE, its single-vendor SASE implementation, to give teams more granular control and flexibility to choose when to perform security on premises or in the cloud to optimize user experience.
- Kyndryl in May launched a SASE service with Fortinet. The solution combines Fortinet's cloud-delivered security and secure networking solutions with Kyndryl's network and security services to design, build, manage, and modernize mission-critical networking for customers across industries.
- NTT in February announced a partnership with Palo Alto Networks to launch a managed SASE offering. Managed Prisma SASE integrates security and networking with a full NaaS service.
- In April, Lumen Technologies adopted Versa Networks as one of the suppliers of its SASE managed services. While the two companies have been partners for eight years on SD-WAN, Lumen's addition of Versa SASE gives it a complete SD-WAN/SASE managed service offering. Lumen also offers Fortinet and VMware SASE.
- Versa Networks is one of the few remaining SD-WAN/SASE independents with scale (Cloudgenix, Silver Peak, VeloCloud, and Viptela were all acquired respectively by Palo Alto, HPE, VMware, and Cisco). It continues to have a heavy presence on the service provider side and differentiates itself by having a full SASE stack with a

single-pass architecture. After raising a \$120 million investment round in October of 2022, the company recently strengthened its management team, naming Dan Maier as Chief Marketing Officer, Gopal Bhagia as VP of Demand Generation, and Kevin Sheu as VP of Product Marketing. In addition, the company recently expanded in the Latin American region by choosing Calculus as its distributor in Mexico and other areas in the region.

- Tata Communications has one of the largest global reaches of all service providers, as well as the widest slate of partners. Its IZO SDWAN is a platform-based, fully managed service enabling the entire secure network transformation life cycle from design to delivery, including support for ongoing management and day-to-day operations. It offers its customers with choices from technologies include Cisco (SD-WAN and Meraki), HPE Aruba, Fortinet, and Versa. It assesses its customers' requirements and provides the best-fit SASE solutions by leveraging its global SASE points of presence and using technology and hardware solutions of its partners, including Fortinet, Palo Alto Networks, Zscaler, Versa Networks, and Netskope. It has also developed a unique "thin-branch" on-premises solution to offer zero-trust network access to corporate applications.
- At Mobile World Congress in March, VMware announced deployment of the VMware Telco Cloud platform by NTT Data and Samsung Electronics.

Major SASE Platform and Service Provider Partnerships

Below is our updated list of major SD-WAN/SASE partnerships among service providers and vendors:

SD-WAN Managed Services Leader	Notable Technology Partners	Strategic Approach
Aryaka	Alibaba Cloud, Amazon Web Services (AWS), Check Point Software, Cisco (Webex and Umbrella), Microsoft (Azure, Office365), NCP, Oracle Cloud, Google Cloud, Salesforce, 8x8, Zoom, RingCentral, Palo Alto Networks, Symantec, Wasabi, Zscaler	Aryaka is a leading provider of managed SD-WAN and SASE services operating its own network. Connectivity services include a premium global L2-over-fiber service with performance guarantees and a white-glove service experience. This is now coupled with an L3 fully managed enhanced Internet service that delivers predictable performance at a much lower price point. An AppAssure capability delivers better observability and control vs. traditional overlay solutions and includes rich co-management. The company's SASE offering leverages the service sophistication of Aryaka's global services PoP footprint, including application optimization and automated multicloud connectivity.
AT&T	Cisco, Fortinet, HPE (Aruba/Silver Peak), Palo Alto Networks, VMware	AT&T offers many different flavors of managed services targeting application-aware dynamic routing and integration of legacy networks, including MPLS, LTE, and Internet. The various services are offered both via AT&T's traditional network including SD-WAN services based on its FlexWare platform as well as services using Cisco, HPE, and VMware's VeloCloud. It has also launched a wide variety of new SASE managed services through its AT&T Cybersecurity division, adding products from Cisco and Fortinet in the last couple of years.
British Telecom	Cisco, Fortinet, Nuage Networks, Infovista	BT offers several flavors of managed services that include services such as Layer 3 MPLS, IP VPN, DIA (dedicated Internet access), Layer 2 Ethernet VPN, and Ethernet private lines. It also facilitates direct connections to the major cloud service providers using technology platforms from its partners.
Colt	Versa Networks	Colt has been one of the more aggressive moves in the SD-WAN market and recently expanded its program with the launch of a new universal customer premises equipment (uCPE). Colt also provides a sophisticated self-service portal. It recently partnered with Versa to offer the Versa platform to customers.

Comcast	Comcast doesn't specifically disclose its SD-WAN vendors, but it is known to have integrated technology from Versa Networks and Fortinet.	Comcast Business launched its ActiveCore SDN platform in 2017, which is a carrier-class, cloud-based, fully orchestrated platform with a multitenant architecture that supports multiple VNFs (e.g., SD-WAN, Managed Router, Advanced Security). Comcast Business also designs and deploys managed Fortinet, Cisco Meraki, and Cisco Viptela SD-WAN solutions, particularly for large enterprises. Comcast Business added Advanced Security solutions to its portfolio with Versa and Palo Alto in 2020. In 2021, Comcast Business completed its acquisition of Masergy, an independent SD-WAN managed services company.
Deutsche Telekom/ T-Systems	Aryaka Networks, Juniper Networks, HPE (Aruba), Versa Networks	Deutsche Telekom (DT) has partnered on SD-WAN services with Versa Networks. The service includes integrated routing, application prioritization, security features, analytics, and monitoring for insight into datacenter and cloud traffic. T-Systems, a DT subsidiary, also has a range of SD-WAN services partners including Aryaka Networks, Juniper, and HPE (Aruba/Silver Peak).
Hughes	Fortinet, VMware	Hughes provides managed SD-WAN services for enterprise customers, including end-to-end turnkey managed services networks that can leverage the Hughes global satellite network. Features include dynamic load sharing across multiple connections for better traffic flow, the capability to dynamically allocate traffic across two active paths, 24/7 WAN management, zero-touch configuration, and Web-based management.
Lumen Technology (formerly CenturyLink)	Cisco, Versa Networks	Lumen offers a variety of SD-WAN managed services with multiple connectivity options reaching 100 countries. Offerings include dedicated internet, broadband aggregation, and 4G/5G LTE. Lumen offers customers a choice between the Cisco and Versa platforms. Services can run from the cloud or on a uCPE.
Masergy (Comcast)	Forcepoint (CASB), Fortinet, and HPE (Aruba)	Masergy (owned by Comcast) is a network service provider offering fully managed, best-of-breed SASE solutions covering core security and networking capabilities, including FWaaS, CASB, SWG, SD-WAN, and ZTNA. Masergy provides these solutions through a combination of different service models and packages. Masergy's fully managed CASB, SWG, and FWaaS solutions are turnkey services covering deployment, integration, ongoing policy management, monitoring, incident response, and issue mitigation from three global 24x7 security operations centers (SOCs) supported by an extensive security team.

NTT	Cisco, HPE (Aruba)	NTT offers a broad SD-WAN Service Portfolio with solutions available in 190 countries. Services include SD-WAN features such as application prioritization, firewalling, advanced security features including malware and IPS, integrated path routing, and hybrid SD-WAN services. The platform is also transport independent and can use Ethernet, Internet, broadband, fixed wireless, and 4G/LTE, as well as connectivity to NTT's 75+ global Local Cloud Centers (LCCs)
Orange	Cisco, Fortinet, Juniper Networks, Nuage Networks (Nokia)	Orange and Orange Business Services work with several partners to deliver a variety of SD-WAN services that the carrier calls Flexible SD-WAN. Features and services include enhanced application performance, simplified management, best-of-breed security, and native cloud connectivity.
Tata Communications	Cisco, Versa Networks, Fortinet, Palo Alto Prisma Access, Zscaler	Tata Communications is one of the largest global providers of managed SD-WAN services. Its IZO SDWAN is a platform-based, fully managed service enabling the entire secure network transformation life cycle from design to delivery, including support for ongoing management and day-to-day operations. It offers its customers with choices from technologies include Cisco (SD-WAN and Meraki), HPE Aruba, Fortinet, and Versa. It assesses its customers' requirements and provides the best-fit SASE solutions by leveraging its global SASE points of presence and using technology and hardware solutions of its partners, including Fortinet, Palo Alto Networks, Zscaler, Versa Networks, and Netskope. It also leverages its IZO Internet WAN predictable Internet in over 150 countries to ensure end-to-end performance.
Telefónica	Fortinet, flexiWAN, Nuage Networks	SD-WAN by Telefónica enables the remote management of global enterprise networks. It includes a fully managed and centralized solution. The company is also using flexiWAN technology on white-box customer premises equipment (CPE) for businesses that require throughputs ranging from 50 Mbit/s to 1 Gbit/s of encrypted traffic. Additional partners have included Fortinet and Nuage Networks.
Telstra	Cisco, VMware	Telstra offers managed SD-WAN that it calls "Adaptive SD-WAN" that is transport agnostic and includes enhanced secure connectivity, application-aware routing, fixed wireless services, and central orchestration. Telstra's primary partners are Cisco and VMware.

Verizon	Cisco, HPE (Aruba), Versa Networks	Verizon provides several flavors of SD-WAN using technology from several vendors. Recently, it has emphasized the co-management trend by launching a Co-Management Service that employs an intent-based networking (IBN) management platform to control policy changes.
Vodafone	Cisco, Juniper Networks, VMware	As a major global CSP with services in Europe, Africa, and the APAC region, Vodafone offers managed SD-WAN services from Juniper Networks, Cisco, and VMware from on-premises devices and hosts 16 SD-WAN gateways. Vodafone has touted automation and plans to use AI to enhance operational capabilities.
Windstream	Fortinet, VMware, and Versa Networks	Windstream is considered a leading provider of SD-WAN services and recently branched out to provide a wide variety of SASE technologies, including virtual next-generation firewall (NGFW). Its primary partners are Fortinet and VMware, but it recently added Versa to its roster of single-vendor SASE platforms.