VERSA NETWORKS

WHITE PAPER

SD-WAN Foundations for a Successful SASE Implementation

Scott Raynovich, Founder and Principal Analyst

FUTURIOM
FUTURE OF CLOUD TECH

I. An Introduction to SASE

Secure access service edge (SASE) is a concept initiated by analyst research firm Gartner Inc. in 2019 as part of the technology "hype cycle." Recently, SASE has been embraced by the customer and vendor community more readily to solve a variety of modern networking and security challenges.

Enterprises and service providers are hungry for new models for deploying enterprise, branch, and cloud-based security services because of the growing threats and gaps. As we'll explain, software-defined wide-area networking (SD-WAN) is closely related to SASE because it helps SASE implementation run faster and more securely. SD-WAN and SASE work best when the services and products are conceived, built, and delivered as an integrated solution.

Security functions and services go hand-and-hand with modern networking technologies such as SD-WAN. Both depend on advanced packet inspection services, application-layer control, and granular visibility. A tightly coupled SASE and SD-WAN strategy provides an end-to-end, software-based networking platform that provides security and visibility of all applications on the network.

What Exactly Is SASE?

SASE does not apply to one specific product or feature. It describes a strategic approach to implementing security services that can be used to protect against different types of vulnerabilities and security challenges. That approach is appealing to organizations looking to build a unified security strategy that can be rapidly augmented with a variety of security functions built on a single platform and integrated into the network, from end to end.

Many of the security functions included in SASE existed before the term emerged, but SASE relies on the increased need to integrate security technologies with networking. To deliver superior performance for SASE, enterprise customers and service providers will need a robust SD-WAN platform to ensure that SASE services can run better, faster, and more securely.

A sound SASE architecture puts packet process and inspection at the core of the network and then integrates a variety of cybersecurity applications to help process, analyze, and automate responses to this networking data. By integrating all these functions on a single-pass platform, the network can protect all users, devices, and applications with one software architecture.

How does it work? In the case of Versa, a single operating system (VOS) is used, providing software that can be consumed in the cloud or by any device on the network. As packets pass through the network, they get inspected only once – rather than several times as in the case of using third-party cybersecurity functions in the cloud. This approach can have many benefits, including:

- Centralized management and control
- Minimized processing overhead
- Better throughput and lower latency
- Stronger security by reducing vulnerabilities from edge to cloud
- Lower operational costs

One of the key benefits for security operations is lowering the number of software components, appliances, and third-party services that need to be managed. Under one management console, an IT practitioner should be able to add and see any networking or security function to protect all of the devices, users, and applications within the organization. Some of the key networking and security services that should be included in SASE architecture are:

> **SD-WAN:** SD-WAN builds an abstracted, virtualized networking overlay that can be centrally controlled and orchestrated. It has the advantage of delivering application-level intelligence for routing, securing network communications over public Internet and cloud, and leveraging a variety of WAN connectivity including MPLS, LTE, and broadband internet services.
>
> **Cloud Access Security Broker (CASB)**: A CASB is a type of firewall that enables organizations to build security policies about how users reach and use services outside of the organization, such as cloud services. A CASB can also include many firewall services, such as identifying malware and preventing it from entering the network.
>
> **Zero Trust Network Access (ZTNA)**: ZTNA employs the concept of zero trust – which means that no connection can be trusted – to use several elements of context and application-aware authentication for applications and users accessing a network.
>
> **Secure Web Gateway (SWG)**: A secure Web gateway (SWG) protects users and organizations from Web-based threats, as well as enforcing policies for access to the Web. Often the SWG will be implemented as a proxy service that shields end users from harmful content on the Web.
>
> **Firewall-as-a-Service (FWaaS)**: FWaaS is a firewall solution delivered as a cloud-based service. It typically includes functions such as Web filtering, advanced threat protection (ATP), intrusion prevention system (IPS), and Domain Name System (DNS) security.

The major challenge for cybersecurity practitioners today is integration of security, not the lack of functions available. Some of the security operations folks we have spoken to have explained that they would prefer to have a better set of well-integrated cybersecurity tools to avoid the headaches of tool sprawl. By integrating these cybersecurity tools, you can overcome many security challenges such as lack of visibility and control into your users and devices.

II. What Is SD-WAN?

SD-WAN technology is one of the most transformative enterprise technologies to emerge in the past ten years. It simplifies management of networking infrastructure by enabling the management of the network using overlays which abstract networking functions into software.

Because SD-WAN uses programmable approach to interact with hardware, the networking can be managed and controlled easily, avoiding costly "truck rolls" to configure equipment and enabling automated updates using elements such as templates and policy orchestration across the entire network. In addition, the use of SD-WAN technology can increase the visibility, performance, and security of the networks through application-layer control and monitoring.

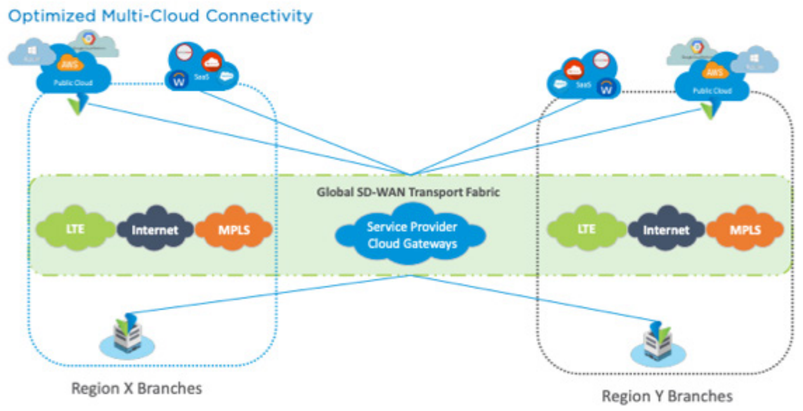
A key benefit of SD-WAN is that it can simplify the management of branch network and security equipment using standardized, commercial off-the-shelf (COTS) hardware with software-based management to simplify operations, lower costs, and provide greater control of the orchestration, monitoring, and visibility of WAN infrastructure.

How SD-WAN Can Improve Infrastructure Management

In the past, the traditional networking infrastructure was built with an "add a box" mentality, with new boxes added for discrete functions -- for example, a new box for a load balancer, packet filter, or a firewall. Because SD-WAN leverages scalable, COTS hardware, the same hardware can be used for many different functions, which can be added and managed using software modules.

The SD-WAN approach limits hardware sprawl, complexity, and lock-in to specific proprietary applications that can bring unnecessary cost and complexity to an organization. The SD-WAN approach enables IT and network managers to add applications and services with an automated and programmable cloud-native platform.

Another big advantage of SD-WAN is that by building secure networking overlays, it has the flexibility to use a variety of networking infrastructure – including the Internet, private MPLS networks, mobile networks, or even cloud networking infrastructure. SD-WAN can also be used to enable multi-cloud networking by routing applications to the closest cloud gateways or PoPs. These networking and multi-cloud connectivity options can be seen in the diagram below:



Source: Versa Networks

This flexible approach means that SD-WAN deployments can be used to manage networking connectivity to branch offices, in multiple clouds, or at private datacenters – all by using the same hardware and management. By combining SD-WAN with SASE services, a wide range of network and security functions can be managed from a single platform allowing for better administrative control.

III. Infrastructure Security Challenges

Why should you be considering a more integrated networking strategy? With the expansion of devices, applications, and security threats, it is more important than ever to have the most pervasive and operationally efficient cybersecurity strategy.

The ubiquitous availability of mobile devices, high-speed connectivity, and cloud-based services has permanently altered how and where people connect to networks, and these advances have introduced numerous security concerns. At the same time, applications have become fully distributed and connected to the cloud as well as the Internet.

Networks need to dynamically connect an evolving mix of users, devices, and applications in any physical location – and provide zero-trust security as part of this connection.

Traditional Networking Architecture Challenges

Enterprise IT architectural decisions no longer revolve around computing and storage resources residing in fixed, on-premises datacenters. With the movement toward the cloud, traditional networking and security approaches need a rethinking, and this has led to a serious rethinking of the value and utility of deploying proprietary on-premises networking and security tools. These tools need to be integrated with the cloud, using the broad-based data resources of application programming interfaces (APIs) and data to drive telemetry and analytics. Visibility of the entire network and applications has become more important than ever.

Traditional networking equipment and architectures were built for another era where client/server networking and compute infrastructure that was designed for when employees would physically come onsite to work. The network design was typically a hub and spoke, which routes all traffic back to a centralized location. In the hub-and-spoke architecture, all traffic inspection, application-level quality-of-service, and cybersecurity decisions are made in the central datacenter. This model is inefficient in a world where users are coming from anywhere in the world and leveraging different cloud services and mobile devices. Traffic needs to be able to have a direct connection to the Internet or to a cloud service and shouldn't require a costly and risky backhaul to the datacenter.

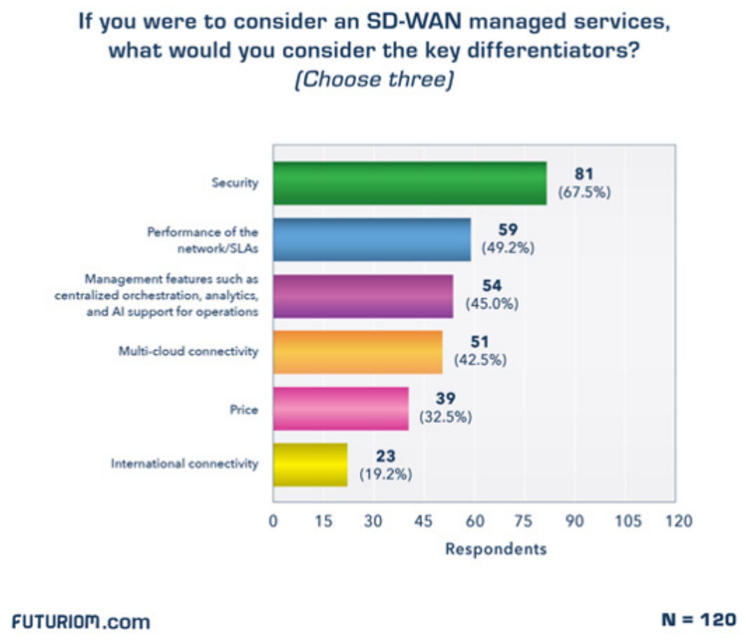
Additional challenges to legacy architecture include:

- Organizations must design a networking and security architecture that can protect traditional enterprise networks, branches, as well as private and third-party cloud connections.
- The security architecture should include provisions for processing packets on local devices in addition to cloud networks and at distributed points of presence (PoPs) around the world.
- IT administrators need to have full visibility of application usage and how to best connect users and devices to applications both inside and outside of the organization (Web, cloud) in a secure manner.

By integrating SD-WAN into a SASE framework, managers can change the game by driving operational simplicity for connecting devices, users, and applications to cloud computing and Internet environments.

IT Security Challenges

IT Security has always been top of mind for those building and managing IT networks, according to primary research from independent research firm Futuriom. For example, in the Futuriom 2022 SD-WAN Managed Services Survey, which targeted 120 director-level and above managers of networking services, security was deemed the key differentiator in an SD-WAN service by 67% of the respondents.



Cyber-attacks are on the rise, adding pressure to IT staff to maintain a secure environment. Here are some of the main challenges to solving cybersecurity:

- Attack vectors consistently increasing: Mobile, hybrid work, cloud services, and APIs present many security risks.
- Staffing: The cybersecurity industry is under-staffed, and companies are under immense pressure to secure networks with limited resources.
- With thousands of cybersecurity tools to evaluate and manage, cybersecurity professionals have a difficult time learning these new tools and managing them effectively.
- Lack of automation: A typical cybersecurity monitoring system generates thousands of alerts per day at most major organizations. Without automation, it is impossible to manually track all the alerts.

In the end, cybersecurity comes down to visibility, control, and automation for maintaining strong network and cloud security hygiene. An integrated SD-WAN and SASE solution can build these features directly into the networking platform, building security into the existing infrastructure for any environment: traditional enterprise, cloud, or hybrid cloud.

IV. Needs for Application Usage and Visibility

The move to the cloud has introduced new demands for networking technology, requiring a more modern, software-driven approach that can adapt to applications running in many different places.

To deliver the best secure networking experience, the network needs to have a detailed understanding of how to handle high-bandwidth applications – ranging from video, unified communications, real-time IoT, software-as-a-service (SaaS), and many others. New applications and usage needs have changed the requirements that many organizations are putting in place for their network infrastructure.

Application Visibility and Monitoring

SD-WAN provides packet-level visibility and security for applications running anywhere on the network: whether in the cloud, at the edge, or on-premises. To monitor and prioritize applications, traditional networking solutions have required a complex array of specialized hardware, software, and monitoring tools that need to be installed and managed separately. In addition, devices such as taps or monitoring devices were needed to gain visibility into the network, putting a tax on network operations.

The movement toward the cloud has led to a rethinking of traditional networking and security approaches, which often rely on proprietary on-premises networking hardware and security tools. These tools need to be more integrated with the cloud, using broad-based data resources of APIs and data to drive telemetry and analytics. Integrated SD-WAN and SASE platforms can build application-level visibility and security into the network without expensive add-on solutions or devices.

WFH and Hybrid Security Challenges

One of the biggest changes in the past five years has been the shift to hybrid work and mobility, accelerated by the COVID-19 pandemic. Businesses realized that employees could be productive in non-office environments, and employees realized there was more convenience in having a flexibility work location.

The challenges of catering to Work from Home (WFH) and hybrid environments are not limited to supporting demanding applications. Another key need is security. Digital workers accessing corporate environments or sending sensitive data must operate on a secure network that can segment work traffic. Virtual Private Networks (VPN) have been employed over time to secure connections across the Internet or from remote locations. However, VPNs are sometimes cumbersome to install and require the user's attention and cooperation. Modern, software-based security architectures such as ZTNA, which can be built into a SASE platform, assume that all connections are potentially hostile and build automated security into the network, deciding who and what can access a specific application using sophisticated authentication techniques based on identity and applications patterns.

SD-WAN and SASE solutions can be used to solve these problems from both a ZTNA and applications segmentation approach. With full applications visibility, the network can assign security policies as well as monitor for anomalies or high-risk activities. High-demand applications such as UC and video can be segmented on the network to be delivered the appropriate number of resources and security.

High-Usage Cloud Applications

Remote communications and cloud services have also changed the demands on networks. They have increased the need for more bandwidth to support high-bandwidth apps such as videoconferencing, unified communications, VOIP, and other real-time data streaming apps.

The modern network needs to be built to prioritize real-time applications on the network. In addition, when workers are using home networks, the network needs the capability to segment higher priority work traffic and route it to destination in the most efficient and secure manner possible.

V. Building Unified SASE Services

Over time, many of the SASE security functions have been developed as standalone functions delivered either as software products or cloud services. However, to achieve true visibility and control, organizations need to adopt a unified platform for all their SASE services so that they can achieve both optimal network performance and strong security hygiene.

Some of the key security functions and capabilities that are already associated with SASE include SD-WAN, SWGs, CASBs, FWaaS, and ZTNA. All these technologies are merging under a common policy management and security umbrella that supports secure connectivity between endpoints and physical locations or branches.

Many organizations are currently overwhelmed by the number and complexity of security services, which is why a unified SASE platform will be important to solving these problems. Most large, distributed networks have complicated security architectures. IT managers need to decide where to implement and place corporate security functions. For example, are separate security appliances needed at different branch locations? Should all traffic be routed back to the datacenter for inspection (often referred to as backhauling or hairpinning)? IT managers also need to implement the model of least privilege (which states that users should only have the minimal access rights to perform their duties) when setting access policies to remote users and contractors. When used effectively as an integrated platform, a unified SASE platform can help mitigate these challenges.

In short, unified SASE should provide enterprise-wide, consistent policy regarding access control, network security, cloud security, data protection, and more for all users and devices. A unified SASE architecture allows for flexible and scalable networks for managing and delivering security applications.

Why ZTNA and CASB Require SD-WAN Connectivity

Zero-trust security principles are part of the key goals for many SASE implementations. This has given rise to ZTNA products, which are designed to deliver secure, trusted connections to network users using a zero-trust security posture.

Zero trust, in general, is an approach to security that includes the following approaches: All connection or network requests should be considered potentially hostile; approved access should be restricted, with connections being set up based on a policy of least-privilege access; and any connections made should be continuously monitored and authorization reassessed as appropriate.

CASB is another security function designed to implement automated security policy enforcement by inspecting applications traffic and enforcing the policy for connections and data between a network and cloud services. CASB is often combined with other security functions such as Web application firewall (WAF). One function of a CASB solution is to identify high-risk applications running in the cloud and enforce the appropriate security access controls. CASB products can also use analytics functions to identify abnormal behavior and potential attack risks or data breaches in the cloud.

Why would functions such as ZTNA or CASB work better when integrated with SD-WAN? SD-WAN is a powerful network management tool that can manage both network and security policies – allowing for seamless interoperability between zero-trust policies and cloud data security policies. In addition, SD-WAN is actively monitoring all traffic data for which CASB and zero-trust policies can be enforced and analyzed.

An integrated SD-WAN product can monitor and control all network and applications traffic, connecting enterprise networks, cloud services, and hybrid networks. Because ZTNA and CASB require detailed understanding of applications traffic and policy, integrating these functions with SD-WAN can leverage an SD-WAN's understanding of the entire network to better enforce ZTNA and CASB policies. In addition, SD-WAN orchestration and automation can deliver ZTNA and CASB functions automatically to every user in a consistent and seamless manner.

How Does SD-WAN Improve Security for All SASE Services?

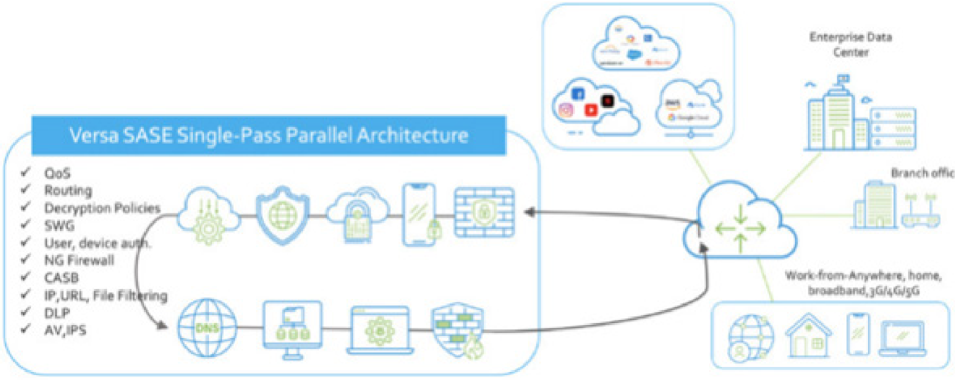
Implementing SD-WAN with SASE can improve the overall security and performance of the network by integrating functions in a single-pass architecture. As discussed, SD-WAN, CASB, and ZTNA services all require network access and applications data to make decisions about secure access.

Some of the key goals of implementing these network security functions include the following:

- Managing all network and security functions in one centralized location
- Improving performance of applications in the network
- Ensuring reliability of the data transfer within the network
- Reducing security risks and overhead by continuously monitoring traffic and applications
- Minimizing the processing overhead of examining packets for security and networking decisions
- Gaining visibility into users, devices, and applications
- Improving operations through more efficient IT management

A fully integrated implementation of SASE anchored on SD-WAN can address all these issues at once, providing centralized networking and security management and deep analytics. SASE anchored on SD-WAN provides more efficiency from both a management and a network performance perspective, as policy decisions can be made by examining traffic once, rather than by sending it across the network to multiple different services. By inspecting the traffic once and performing any necessary security and networking functions, an organization reduces the amount the attack surface all while improving the end user experience. This approach is known as a "single-pass" architecture, which processes all packets once for multiple security functions rather than chaining together or connecting disparate services.

The illustration below shows how an integrated SD-WAN platform can process, analyze, and route all applications traffic in a single-pass architecture:



Source: Versa Networks

VI. Real Life Use Cases – With or Without SD-WAN?

SASE services can be delivered with or without SD-WAN. In fact, that's how many of these security functions emerged – as discrete, cloud-based security services.

A variety of companies provide standalone SASE services such as CASB, FWaaS, and ZTNA without providing SD-WAN connectivity, assuming the customer has their own networking implementation.

SASE Without SD-WAN

In general, SD-WAN – management of the WAN network – is considered part of the SASE architecture. But in some instances, there are cases where SASE services might be delivered without SD-WAN.

One example would be a large group of remote workers that do not come into an office or use the traditional network. In this case, they may require cloud-based security services such as ZTNA, SWG, or FWaaS that can be used to secure remote connections and applications without hardware needed to access on-premises datacenters. WFH is in fact generating a lot of interest in ZTNA solutions that can be delivered without underlying SD-WAN connectivity. While SD-WAN connectivity will great increase performance of all network traffic, it is not needed in an organization that is fully cloud native and allows for 100% remote access to third-party applications.

SASE With SD-WAN

Use Case: Securing Networks for Branch Offices

The legacy branch office network is increasingly becoming the most plausible target for cybercriminals. The typical branch has evolved to become the hub of major digital services for both business productivity and customer services. Businesses across multiple industries are adopting direct Internet access to facilitate their multi-cloud services and are offering local guest network-based services, such as guest Wi-Fi. Branch offices are hubs of activity. While disruptive technologies, like the cloud and IoT, have broadened and diversified the attack surface, branch security architectures have not evolved at a similar pace.

IT teams can decide where to run each layer of required security – either on-premises in the branch office, or centrally in the datacenter or co-location PoP. SD-WAN enables centralized control and secure networking for all branch offices. For example, compute-intensive services such as malware sandboxing, intrusion prevention (IPS), and AV filtering can be run centrally, while key branch services such as firewall and secure Web gateway can be run locally, with the overall set of layered security services defined with a simple policy template. With SD-WAN delivered with SASE, organizations can protect their branch office and ensure services can be deployed and capacity can be increased and enhanced with additional functions automatically, without any on-site presence, hardware refreshes, or manual provisioning at every branch office.

Use Case: Enabling Hybrid Telework

The growing complexity of networks, especially hybrid networks that blend enterprise networks, cloud networks, and the Internet, is creating a new use case for SASE and SD-WAN to be delivered as one network – allowing for workers to work either on corporate premises or enabling remote teleworking.

An integrated SD-WAN and SASE platform can deliver secure, zero-trust networking to any device, any users, and any application – wherever they may reside. SD-WAN's natural position as a secure overlay can leverage the Internet to help deliver secure networks for hybrid work.

When using SASE without SD-WAN, applications are typically backhauled to either a private or third-party datacenter for traffic inspection and filtering. By using SD-WAN, organizations can provide a secure connection across the Internet that doesn't require any type of security backhaul and ensure that all traffic is using the most optimal path. An integrated SASE and SD-WAN service can build security and ZTNA services between the endpoint and the destination site, providing a fully secure connection with or without the Internet. In addition, policies that just pertain to remote teleworking will be applied based on the different types of connections: ensuring that the right security policy is applied to the right access attempt.

Use Case: Providing Unified Communications

Video collaboration and unified communications-as-a-service (UCaaS) have been the expected forms of communication for one-on-one and group meetings. As more employees go-to-office (GTO) and others continue to work from home, video collaboration will become the de facto standard for meetings inside and outside of the office. UCaaS will continue to be a driving factor in network transformation because these services are delivered to business offices and homes via the Internet, which is a best-effort network.

SASE integrated with SD-WAN helps segment this traffic by type and provide mitigation for packet loss, jitter, and delay using error-correcting technologies, dynamic jitter buffering, and link steering mechanisms that deliver a better user experience. Together, they create an expectational experience for video, VoIP, and UCaaS while steering this traffic over the highest capacity, lowest latency link, for superior performance. The availability of technologies such as secure SD-WAN will drive increases in UCaaS in corporate conference rooms and homes.

Use Case: Optimizing Application Experience for Cloud Services

By combining SD-WAN with a fully integrated SASE stack, organizations can improve the network experience for accessing applications over a variety of networks. SD-WAN with SASE can use a software overlay and application-level visibility to deliver the best experience over any network – whether it's the Internet, MPLS, or the cloud.

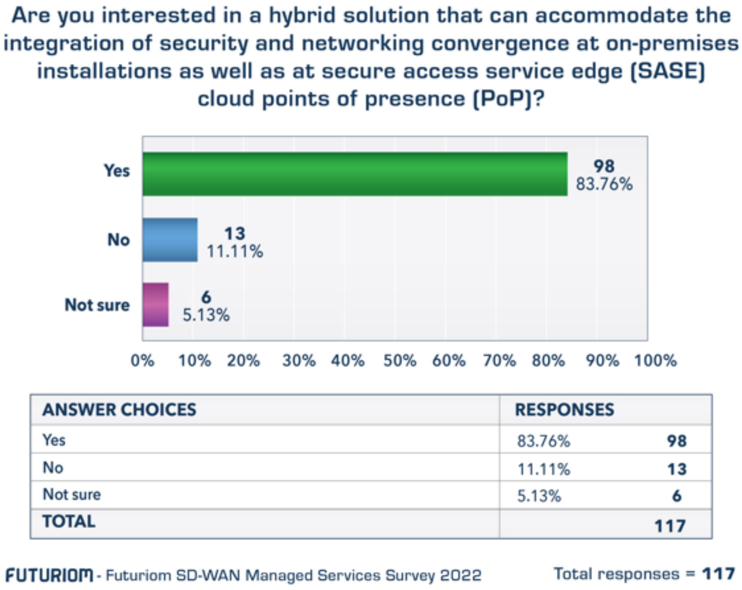
Organizations now have a wider range of network resources to reach both enterprise applications and applications in the cloud. They can use secure overlays over the Internet, private networks such as MPLS, or even cloud networks. SD-WAN functionality can be used to gain visibility into specific applications and services giving the potential to route applications over the best networks. By doing so, the application experience is delivered quickly and consistently, allowing the user to have the best experience. Ensuring easy and seamless user experience also promotes adoption of new technology, thus ensuring that shadow IT and human error are kept at bay.

Use Case: Delivering Multi-cloud Connectivity, Policy Consistency, and Interoperability

Today there is no unified hybrid cloud networking platform that provides optimal connectivity and security across complex multi-vendor ecosystems. Enterprises have been demanding a unified architecture that can normalize the different cloud environments and their respective network and security stacks.

Network managers are increasingly tasked with connecting a variety of networks to multiple clouds using PoPs and cloud on-ramps. By combining SD-WAN and SASE, network overlays can be used to connect diverse and disparate networks in a secure way. In addition, SD-WAN and SASE allow for easy interoperability between different cloud vendors and platforms, ensuring that there is consistent policy enforcement on data no matter where it resides.

As a 2022 Futuriom survey of 120 network managers indicates, respondents are interested in using SD-WAN as a solution for hybrid networking:



Are you interested in a hybrid solution that can accommodate the integration of security and networking convergence at on-premises installations as well as at secure access service edge (SASE) cloud points of presence (PoP)?

ANSWER CHOICES	RESPONSES	
Yes	83.76%	98
No	11.11%	13
Not sure	5.13%	6
TOTAL		117

FUTURIOM - Futuriom SD-WAN Managed Services Survey 2022 Total responses = 117

In addition to improving and optimizing access to specific cloud services, coupling SD-WAN with SASE can also be used to connect to and build hybrid networks using the best of cloud and Internet resources.

Use Case: Realizing Real-Time IoT and MEC

The explosion of 5G this past year has created transformational opportunities around smart manufacturing, augmented reality /virtual reality (AR/VR), and more. However, for low latency connectivity, multi-access edge computing (MEC) is an important paradigm to achieve many of these goals. MEC converges network, computing, storage, security, and application capabilities and delivers them seamlessly at the edge. This brings low latency compute as close as possible to users, devices, and things.

However, these advancements open the door to new potential threats and vulnerabilities such as kernel bypass, DDoS attacks on 5G service interfaces, and cyberattacks on the Internet-of-Things (IoT) ecosystem, leading to zero-day exploits, software tampering, and API exploits. Such attacks directly impact service availability, data exfiltration, and information integrity.

SD-WAN anchored SASE will help secure the MEC and IoT gateways in real time by requiring security hardening against API exploitation and the ability to detect privileged escalation within applications. SD-WAN integrated with SASE will help build zero trust holistically across MEC and IoT ecosystems and will be critical to guarantee end-to-end SLA management, contextual security, and visibility.

VI. Conclusion: Tightly Coupled SD-WAN and SASE Is the Future

A tightly coupled SD-WAN and SASE solution can solve many modern networking and security problems at once. Important security capabilities such as WAF, FWaaS, intrusion detection, URL filtering, and threat management can be implemented in the devices handling SD-WAN traffic, building the security capabilities directly into the network. In addition, an integrated SD-WAN and SASE approach is ideal for today's complex networking architectures because it provides visibility and control to IT administrators. By building secure overlays, traffic can travel more safely over Internet connections directly to cloud services, without the need for backhaul or hair-pinning to another datacenter.

When SASE is built into the SD-WAN, security is ubiquitous and consistent. Security inspection and policy enforcement are enforced across the traditional network, at enterprise branches, and at cloud providers' PoPs. Organizations will see an optimum implementation of SASE with SD-WAN as bringing together connectivity and network security into a single, integrated software solution that provides consistent, centrally managed access and security from anywhere in the world. Organizations will realize that deploying a multi-vendor approach for SASE introduces visibility gaps and security vulnerabilities, and by anchoring SASE to SD-WAN will they achieve optimal connectivity and protection.

Versa Networks, Inc, 6001 America Center Dr, 4th floor, Suite 400, San Jose, CA 95002
+1 408.385.7660 | info@versa-networks.com | www.versa-networks.com