SASE WHITE PAPER

The unification of network and security

Enterprise-level security in the cloud and beyond with SASE and SD-WAN

Organizations today require immediate and uninterrupted access to critical network and cloud-based resources in order to support the swift pace of digital business transformation. Spurred by the boom in remote work and the ongoing migration to cloud-based applications and services, consumption patterns are transforming traditional private and public networks into a single network of many end-users and devices scattered across the organization's footprint. As a result, there are growing security concerns with this rapidly changing environment—many traditional security solutions no longer provide the protection needed along with the flexibility to support businesses anywhere, anytime, via any device.

Enter SASE—short for Secure Access Service Edge and pronounced sassy—the unifying construct that converges network and security. This whitepaper accurately defines SASE, the challenges SASE aims to solve in today's evolving landscape and how, when leveraged with SD-WAN, it's the optimal method for delivering security in the cloud. Learn how a comprehensive, resilient SASE solution can help enable the most seamless, secure work in the cloud.

Executive takeaways

Here's what you'll learn from this whitepaper:

1. The complex modern-day landscape driving digital transformation and the acceleration of cloud-based application adoption.

2. The challenges enterprise IT faces in enforcing security, with a dispersed workforce in a cloud-based network environment.

3. The emergence of SASE and how it enables secure network access capabilities no matter where the users, devices or applications are located.

4. The ways SASE—delivered with SD-WAN—offers organizations the most flexible and reliable security in the cloud.

The cloud era: Redefining the business network

According to the IDC, 80% of enterprises will speed up their shift to a cloud-centric infrastructure by the end of 2021.[1] This acceleration can be accredited to the global pandemic driven surge in remote work and the coinciding need for secure access to network resources from anywhere, on any device. In this modern-day reality, enterprise migration to using resources in the cloud is happening at an unparalleled rate.

The migration to the cloud has made the network edge more dispersed and, in some cases, evaporated it completely. Digital business and edge computing have inverted access requirements, with more users, devices, applications, services and data now located outside of an enterprise rather than inside. In Gartner's Initial Secure Access Service Edge Forecast, Gartner analysts Joe Skorupa and Nate Smith write, “Network security architectures that place the enterprise data center at the center of connectivity requirements are an inhibitor to the dynamic access requirements of digital business.”[2] Because, from an enterprise IT perspective, the perimeter is no longer limited to a location, it's a set of dynamic edge capabilities delivered as a service when needed, from the cloud.

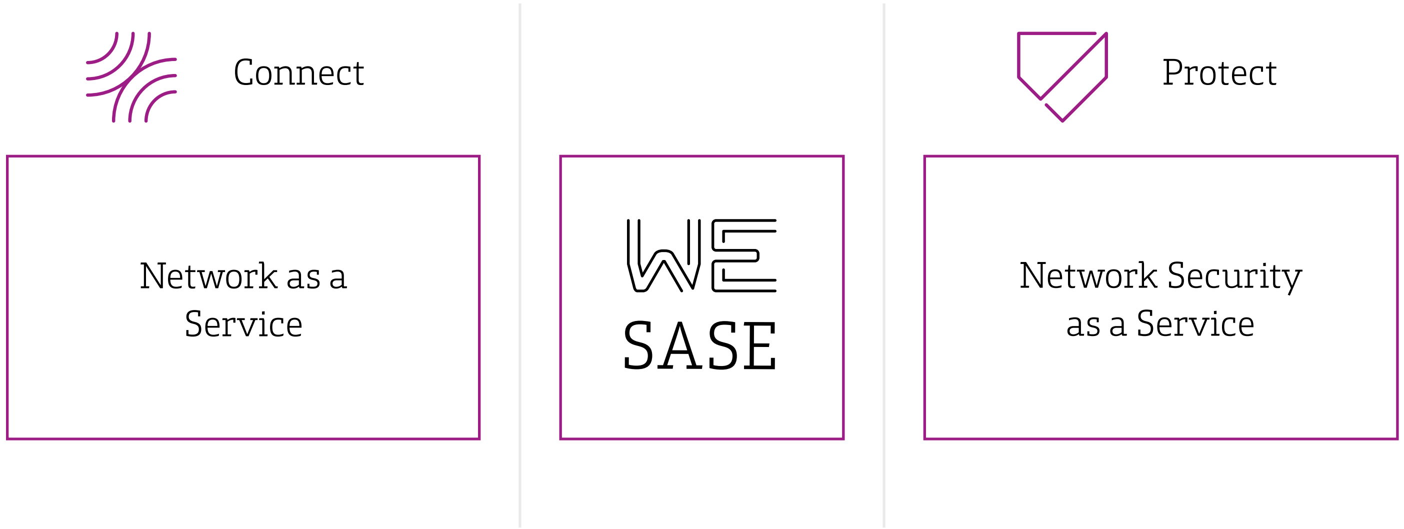
As networking and security becomes increasingly more complex within this new environment, organizations are turning to technologies like SD-WAN and now SASE to enable speedier and more agile digital business transformations and workforce mobility.

The emergence of SASE is rooted in the rise of distributed organizations and its accompanying workforce. It enables remote workers to gain full access to designated company applications and resources while offering a much simpler secure connectivity model for cloud-first enterprises, bringing security functions wherever they're needed.

According to Gartner, by 2025 at least 60% of enterprises will have explicit strategies and timelines for SASE adoption, up from 10% in 2020. This demonstrates the urgent need for flexible “anytime, anywhere” solutions that can deliver secure remote access (SRA) at scale.[3] SASE enables organizations to deliver protected networking and security services in a consistent way and support the unceasing movement towards digital business transformation and workforce mobility.

How SASE delivers

SASE consists of a layered, interwoven fabric of network and security technologies that protect an organization's data and systems from unwanted access. The architecture weaves into an ecosystem of “Network as a Service” and “Network Security as a Service” as depicted in the diagram below, resulting in a unified connectivity experience that is ubiquitously available anywhere and anytime.



Built upon a solid platform of SD-WAN technology, SASE dynamically extends the edge of the private network right up to multiple clouds such as AWS, Azure and Google Cloud Platform (GCP) and to popular Software as a Service (SaaS) applications such as Microsoft 365 and Salesforce. In doing so, SASE transforms the network into a virtual on-ramp to cloud providers' services.

Underpinning this streamlined access is software-defined connectivity—leveraging a dispersed network of Internet Exchange Points—where the SASE providers connect to cloud providers. At these cloud connection hubs are the provider-owned SASE gateways that terminate secure, dynamic tunnels from customer locations. Remote and mobile workers that are not at customer locations will connect to their private network through the closest service provider SASE gateways via the Internet.

Irrespective of the end-user location, their computing and communication devices are protected end-to-end by a full set of security technologies, including:

- Software-Defined Wide-Area Networking (SD-WAN)
- Firewall as a Service (FWaaS)
- Secure Web Gateway (SWG)
- Cloud Access Security Broker (CASB)
- Zero Trust Network Access (ZTNA)

Network security provided in the SASE framework is ubiquitously available anywhere and anytime. The security policies for an organization are managed and orchestrated from the cloud using an intuitive, self-service portal. These policies can protect both legacy and modern cloud-based computing resources that are either on private networks or on the Internet.

At the core of the SASE architecture, access controls with advanced authentication, authorization and accounting capabilities are based on the identity of the user, device and application. Leveraging these—and other controls such as CASB—SASE can provide next-generation secure remote access (SRA) capabilities, known as ZTNA. ZTNA moves away from providing end-users unfettered access to entire private networks. Instead, it delivers an access model that grants access to resources based on the identity of the user, and their permissions, while denying access to everything else.

The integration of these functions will expedite the digital transformation for organizations while enhancing security and minimizing complexity.

SASE transcends SD-WAN

When first introduced, hub and spoke WANs, often using multiprotocol label switching (MPLS), were an ideal option for organizations that ran multiple business-critical applications at their data center locations. But the traditional, data-center-centric network and network security architecture of hub and spoke private networks—with their virtual private network (VPN) connections into the data center are not equipped to handle today's widely distributed remote workforce and the increased volume of traffic traversing public, private, hybrid and multi-cloud environments. The process of routing traffic to and from a data center, through a centralized security stack and then out to the Internet, creates network congestion and hinders application performance, affecting productivity and end-user experience. As a result, SD-WAN—one of today's fastest-growing technology trends—took flight.

SD-WAN offers a much smarter, more efficient WAN model by adding a layer of software intelligence on top of the WAN infrastructure and access networks. Instead of routing traffic through the data center, SD-WAN can route traffic from the remote location securely to the cloud over the Internet —making it ideal for access to cloud-based resources. SD-WAN can steer traffic automatically in response to real-time network conditions by continually tracking the health and status of all connections and sending traffic down the best path available at that moment. Depending on the links that are available and based on each application's business policy, as defined in the SD-WAN orchestrator, SD-WAN routes traffic from the remote location to the desired location, such as to the enterprise data center on a private or public underlay, or to the cloud securely over the Internet. Optionally, SD-WAN can route traffic over dual Internet links either to the cloud or to the corporate data center.

Traffic steering over multiple Internet links at the remote location is done by the SD-WAN edge device at the remote location, which connects to the SD-WAN gateway and further directs the traffic to the cloud or to the data center.

SD-WAN technology gives users a much more efficient, higher-performing connection to cloud-based applications. And with its ability to chain in various cloud-hosted services, SD-WAN has evolved to a point where it can be used to deliver dynamic, user-centric SASE security services.

When transcending to a SASE architecture that leverages SD-WAN technology, essential security capabilities such as encryption, firewall, access control and others can be run in the cloud as Network Security as a Service, similar to any other SaaS cloud service. These solutions also free businesses from perimeter-based trust models. Using ZTNA, they grant trusted access based on the identity of the user—or application, or other entity—instead of their location or IP address as is done by legacy systems.

SASE DEFINED BY GARTNER[4]

SASE is an emerging offering combining comprehensive networking and security functions (such as SD-WAN, FWaaS, SWG, CASB and ZTNA) to support the dynamic secure access needs of organizations.

Agile, cloud-based security with SASE and SD-WAN

SD-WAN deployments within organizations have skyrocketed— to accelerate existing IT plans to use resources in the cloud and to provide IT with a more flexible and manageable network. Now, the industry is taking SD-WAN to the next level by pairing it with SASE that delivers ZTNA capabilities. This approach combines the efficiencies of SD-WAN with a more malleable, user-centric approach to securing remote workers and cloud applications.

The combination of dynamic, intelligent network capabilities of SD-WAN with advanced security functions, lays the foundation for a SASE transformation that can achieve comprehensive protection and necessary compliance for migrations to cloud architectures.

SD-WAN and SASE providers can build a fabric of cloud network and security services, as well as create partnerships with cloud providers to access their services. Together, this framework acts as an on-ramp to SaaS applications and other cloud services. When users, and devices connect to applications—from either a branch or from a remote location—the SASE service in the cloud location can apply any security functions that the enterprise requires. These include:

Firewall as a Service (FWaaS)
FWaaS is a new type of a next-generation firewall, it eliminates the appliance form factor, making network security capabilities such as URL Filtering, Intrusion Prevention System (IPS), next generation anti-malware (NG-AM) and Managed Detection & Response (MDR) available everywhere.

Secure Web Gateways (SWG)
SWG solutions protect users against malware, phishing and other web-borne threats. SASE offers SWG protection to all users, at all locations and eliminates the need to maintain policies across multiple point solutions.

Zero Trust Network Access (ZTNA)
ZTNA offers a modern approach to securing application access for users replacing legacy VPN. It embraces a zero-trust policy, where application access dynamically adjusts based on user identity, location, device type and more.

Cloud Access Security Broker (CASB)
CASB helps enterprises adapt and protect against new threats that come with cloud computing like when connecting to IaaS and SaaS. CASB applies security policies as users access cloud-based resources to protect against cloud security risks, comply with data privacy regulations and enforce corporate security policies.

The global SD-WAN market size was roughly $1.4 billion in 2019, and it is expected to reach

$43 billion

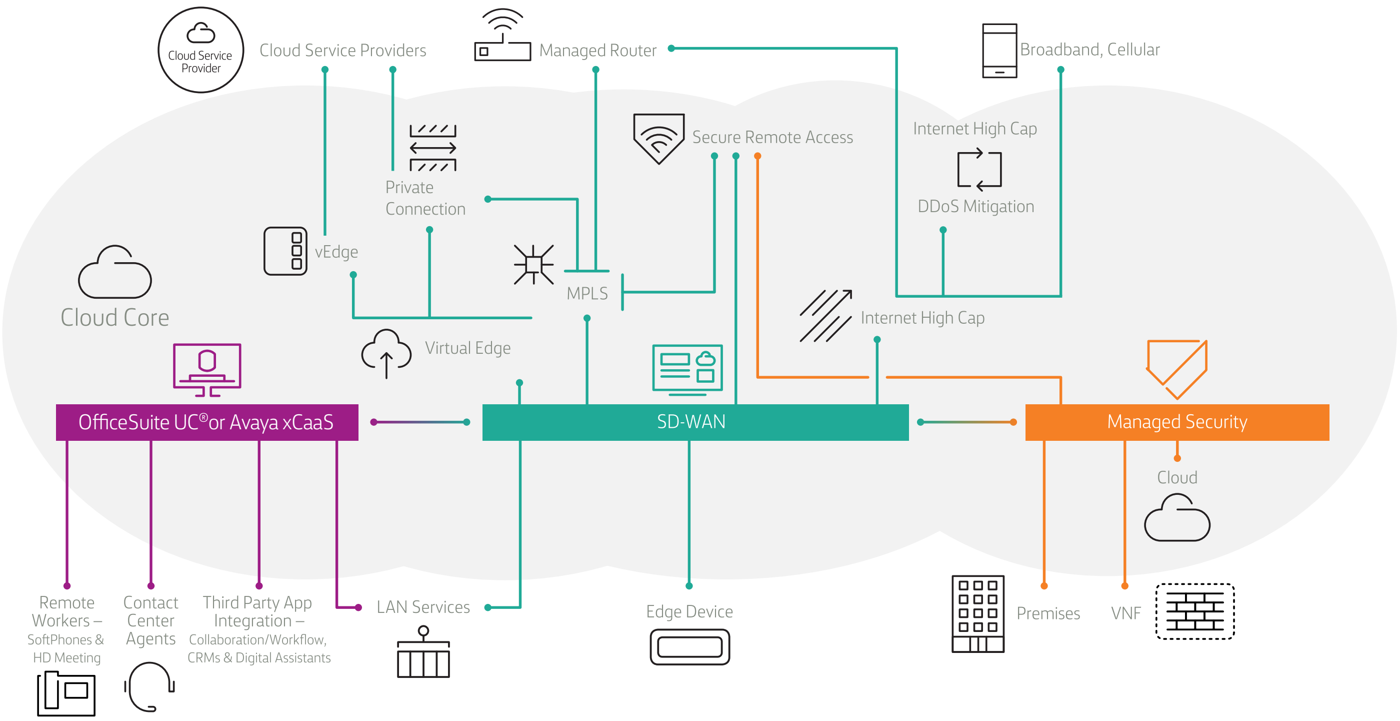
by 2030.[5]

Rethinking cloud security with Windstream Enterprise and VMware

Digital transformation coupled with the global pandemic has driven an unprecedented wave of remote work and use of cloud-based resources that has resulted in taxing legacy network models, accelerating network transformations to SD-WAN and driving new security challenges. To provide businesses with peace-of-mind that their network is highlight reliable, efficient and secure, Windstream Enterprise and VMware have partnered to create a unique cloud security solution that offers unparalleled visibility, uptime and control, along with a rich customer experience.

As the application access needs of the end-users evolve—as well as the IT resource consumption needs of the enterprise IT organization—so does the need for cloud security. Integrating these needs with the recent evolution in WAN management brought by SD-WAN requires a new best practice: don't look at WAN performance and cloud security separately, but as a unified entity. Security policies must now be integrated with functionally and operationally application polices to become part of the same field-of-view and workflow. This requires the SD-WAN and SASE providers to offer their clients with an integrated and real-time view, as well as some level of self-service control over the deployment, management and governance around all polices.

SASE architecture over SD-WAN



How it works

VMware SD-WAN edge devices provide the first hop from the branch locations to SD-WAN gateways for all traffic to the cloud services, offering enhanced security via encryption. The gateways deliver optimized performance in a redundant and scalable architecture to eliminate downtime and provide an ideal infrastructure for automating security based on policies the organization sets.

Windstream Enterprise delivers four core SASE capabilities:

Next-generation Unified Threat Management (UTM) firewall security that can be deployed as cloud-based Customer Premises Equipment (CPE) or virtual network function integrated into a single CPE.

SRA to ensure an encrypted connection over the Internet. WE Connect portal enables IT to manage end-users, control access to internal applications, systems and resources by defining which network and corporate resources are accessible to remote workers.

WE Connect, a true "single pane of glass" for all services and interactions with Windstream Enterprise, provides network visibility and management that leverages and incorporates big data to offer actionable insights.

A nationwide Cloud Core™ SASE architecture delivers rapid deployment, seamless integration, greater extensibility and higher uptime. It integrates SD-WAN with MPLS, UCaaS, cloud firewalls, remote access VPN and private hyperscale compute connections.

From there, Windstream Enterprise also brings these additional proprietary capabilities:

The award-winning WE Connect Insight Engine gathers and evaluates data across all network locations (or a set of sites defined by the user) and aggregates it to deliver enhanced visibility and reporting—quickly identifying noteworthy areas in the network, applications or devices.

Windstream Enterprise's Concierge service model offers network assessment and design for low-touch provisioning and deployment, proactive management of access service providers and ongoing guidance and support to help optimize the network.

Flexible, fully managed access options help achieve the highest bandwidth for the lowest possible cost. We support any combination of Windstream Enterprise-provided fiber Ethernet, broadband, cellular broadband or bring-your-own bandwidth utilizing public or MPLS underlay networks.

PCI DSS compliance for SD-WAN is validated by a third-party Qualified Security Assessor (QSA). Windstream Enterprise provides an annual Attestation of Compliance (AOC) report to reduce customer costs.

When multiple connections are deployed in active/active configuration, Diverse Connect virtually eliminates downtime and offers 100% uptime SLA.

Conclusion

Windstream Enterprise has partnered with VMware—a recognized industry leader named in Gartner 2021 Magic Quadrant for WAN Edge Infrastructure[6]—to deliver the most sophisticated and resilient SASE solution available to simplify and consolidate security elements in the cloud. SD-WAN Concierge™ from Windstream Enterprise is powered by VMware SD-WAN™ to provide a high-performance network with integrated security. While SASE continues to evolve (and will for quite some time), Windstream Enterprise has deep experience in providing all the foundational elements of a SASE architecture. We will continue to develop and expand our SASE capabilities as this technology unfolds. To learn more about our managed communications solutions, visit windstreamenterprise.com.

Cloud-enabled connectivity, communications and security—guaranteed.

Windstream Enterprise drives business transformation through the convergence of our proprietary software solutions and cloud-optimized network to unlock our clients' revenue and profitability potential. Our managed services streamline operations, enhance productivity and elevate the experience of our clients and their end users while securing their critical data and brand reputation. Analysts certify Windstream Enterprise as a market leader for our product innovation, and clients rely on our unrivaled service guarantees and best-in-class management portal. Businesses trust Windstream Enterprise as their single-source for a high-performance network and award-winning suite of connectivity, collaboration and security solutions—delivered by a team of technology experts whose success is directly tied to our clients' complete satisfaction.

1. Network World, "With COVID-19 hanging on, migration to the cloud accelerates." Andy Patrizio. November 12, 2020.
2. Gartner, "Forecast Analysis: Gartner's Initial Secure Access Service Edge Forecast." Joe Skorpa and Nate Smith. August 26, 2020.
3. MacDonald, Neil, et al. "2021 Strategic Roadmap for SASE Convergence." Gartner. March 25, 2021.
4. Andrew Lerner. "Say Hello to SASE (Secure Access Service Edge)." Gartner. 13 Dec. 2019.
5. "SD-WAN Market Research Report." P&S Intelligence. August 2020.
6. Gartner, Magic Quadrant for WAN Edge Infrastructure, Jonathan Forest, Naresh Singh, Andrew Lerner, Evan Zeng, September 20, 2021.

Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

To learn more about network solutions, visit windstreamenterprise.com

vmware | WINDSTREAM ENTERPRISE