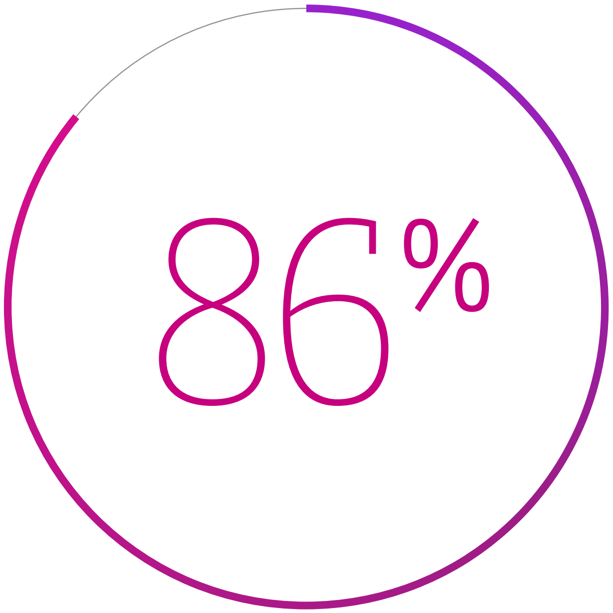
Deliver Protected Networking and Security Services Anywhere, Anytime

How to Bring a Robust SASE Solution to Your Organization

WINDSTREAM ENTERPRISE | vmware®

More than ever, the landscape driving digital transformation is increasingly complex. The acceleration of cloud-based application adoption and the rising risk of cybercrime create new challenges for enterprise IT teams who need to ensure easy access and absolute security for an often dispersed, remote workforce.

What's inside?



86% of organizations expect to be impacted by a cyberattack within a year.[1]

New era, new challenges

Following a surge in remote work at the beginning of this decade, organizations have become more reliant on systems and technologies that operate outside of an official office structure. From an enterprise IT perspective, the organizational perimeter is no longer limited to a location. Now, it’s a set of diverse locations and capabilities delivered from the cloud when needed.

At the same time—and not by coincidence—cyberattacks have become a more dangerous and imminent threat. Breaches are no longer a question of “if” but “when,” and organizations that fail to adequately protect their cloud-based devices, applications, services and data are playing with fire.

As a result, the intersection of networking and security is quickly becoming more complex than ever. While workplace flexibility provides new opportunities for organizations and their employees it also presents heightened security risks, with remote workers logging on from home or any public WiFi hotspot using a mixed bag of personal and company devices.

Forward-looking organizations are turning to emerging technology frameworks to deliver protected networking and security services and support the persistent movement toward digital transformation and workforce mobility.

> “The assumptions underlying legacy WAN architectures—that most users work from branches, that almost everything lives in a central data center—no longer apply.”[2]

SASE & ZTNA For Dummies

Why yesterday’s networks won’t cut it

Traditional hub-and-spoke networks and their associated security architecture were built for a set purpose: using Multiprotocol Label Switching (MPLS) made them an ideal way for organizations to run multiple business-critical applications from their own data centers.

However, in today’s environment, the “data-center-centric” approach is showing its limitations.

Geography

With Virtual Private Network (VPN) connections into the data center, these networks aren’t equipped to serve a remote workforce that’s more geographically distributed

Security

Traditional network security models were designed to accommodate employee devices and systems that were located within a physical perimeter, assumptions that no longer hold true

Traffic

These networks also aren’t built to scale with the increased volume of traffic that traverses public, private, hybrid and multi-cloud environments en route to its destination

Flow

Constantly routing traffic to and from data centers through a static centralized security stack and ultimately out to the Internet creates network congestion

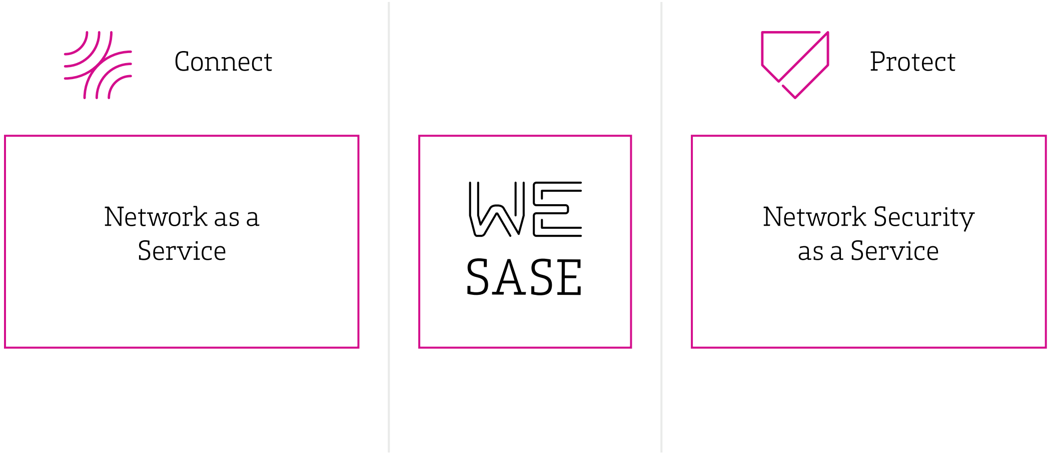
Speed

All these factors and the resulting congestion combine to hinder application performance, which affects end users’ experiences and productivity

Networking and security converge

To enable secure and reliable access to cloud-based assets, enterprises are turning to Secure Access Service Edge (SASE)—an emerging “as a Service” network and security framework.

SASE is more than a single technology: It’s a layered, interwoven fabric of network and security technologies that work together to protect an organization’s data and systems from unwanted access.



Connect

Network as a Service

WE SASE

Protect

Network Security as a Service

Through its five components, SASE dynamically extends the edge of the private network right up to multiple clouds (such as AWS, Azure and Google Cloud Platform) and to popular SaaS applications. For end users, this provides a virtual on-ramp to those cloud providers’ services.

The computing and communications devices in the hands of those end users are also protected end-to-end by a full set of network security technologies. The policies for those technologies can be managed and orchestrated by the organization from the cloud using an intuitive self-service portal, reducing complexity and simplifying management.

The convergence:
Network as a Service and Network Security as a Service

In short, SASE offers a unified, secure connectivity solution that is available anytime and anywhere.

The 5 components

SASE is a complement of five components that bring networking and security capabilities into a single-service, cloud-native model.

1 **Software-Defined Wide-Area Networking (SD-WAN)**

SASE is built upon a solid foundation of SD-WAN, intertwined with software intelligence, which enables optimal WAN management. SASE leverages SD-WAN capabilities to provide optimized application performance, network routing, global connectivity, WAN and Internet security, cloud acceleration, and remote access. SD-WAN also provides an ideal platform to secure unified communications applications including voice, video and chat.

2 **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.

3 **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.

4 **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.

5 **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 real boost to your business

A robust SASE solution can not only positively impact your end users' experiences, but also reduce your IT team's management complexity and increase your organization's bottom line.

Enterprise-level security for users that allows access to apps and data over any connection type with peace of mind that security is in place

Centralized operations that put policy management in the cloud and distributed enforcement points close to the user, app or device through a "single pane of glass" portal

Device consolidation via the reduction of the amount of single-purpose customer premises equipment (CPE) at a branch to a single agent or SD-WAN device, reducing cost and complexity

Secure Remote Access (SRA) that helps ensure encrypted connections and bases network access on the identity of the user, device or application, enabling a work-from-anywhere model

Hybrid WAN that can seamlessly run security over the top of both existing private MPLS connections and public Internet bandwidth without requiring a network rip and replace

Improved performance leveraging multiple access connections to improve resiliency and performance for critical applications including latency-sensitive apps

Lower operational overhead with SASE providers fully managing, monitoring and maintaining security software and devices, so IT doesn't need to constantly update, patch, upgrade and replace appliances

Limitations and opportunities

Standing up a SASE solution isn’t like flipping a switch, and not all vendors are created equal. Organizations may be limited by legacy network and security point solutions, or their provider’s capabilities and readiness to deploy SASE technologies. Barriers to adoption may include:

Vendor focus
Your provider’s capabilities and offerings may be focused exclusively on networks or on security, but it’s possible they aren’t proficient in both areas

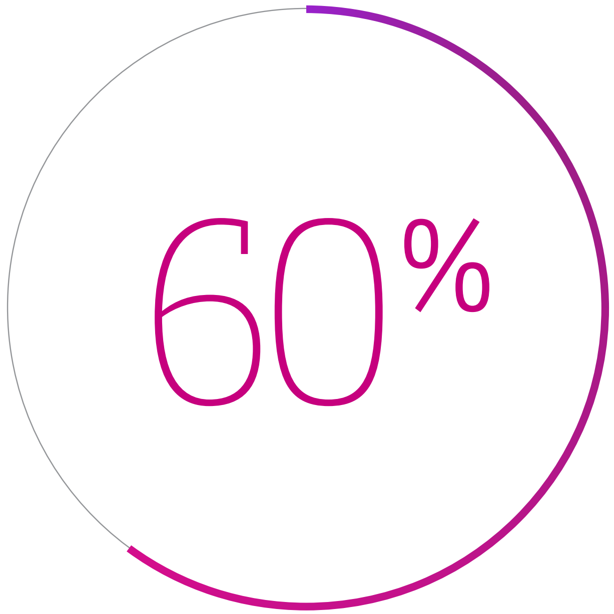
Vendor approach
Well-integrated features, in-line proxy experience and context awareness are all key to successful SASE implementation. If a vendor lacks them, it can increase costs and decrease performance

Vendor history
Your provider’s legacy experience may be with on-premises hardware in the “data-center-centric” approach, which can create resistance to a cloud-native mindset

Are you ready for a SASE solution?

If these trends and challenges apply to you, a SASE solution may be right for your organization:

- Need protection from malware and exposure to security vulnerabilities
- Disjointed management of siloed security and networking technologies
- Applications reside in the cloud
- End users connect to your network from outside a controlled environment
- Limited visibility to cloud compute and end-user resources
- End user performance experience is degrading
- Unable to control all device connection to your network
- Increased network complexity
- End users expect more direct access to resources



By 2025, at least **60%** of enterprises will have explicit strategies and timelines for SASE adoption, up from 10% in 2020.[3]

Why get started with Windstream Enterprise today?

The cloud era is redefining the business network. SD-WAN deployments are skyrocketing around the world, and SASE capabilities will enable organizations to deliver protected networking and security services as the landscape continues to evolve.

In partnership with VMware, Windstream Enterprise delivers the most sophisticated and resilient solution. With SD-WAN Concierge™ from Windstream Enterprise, powered by VMware SD-WAN™, you can provide a high-performance network and integrated security that will help your organization consolidate security elements in the cloud. And with our deep experience in providing all the foundational elements of a robust SASE solution, you can count on Windstream Enterprise to continue developing our SASE capabilities as this technology unfolds.

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.

Sources:

[1] Liu, Nancy. "Trend Micro: 86% of Orgs Expect a Serious Cyberattack." SDxCentral. August 4, 2021.

[2] SASE & ZTNA For Dummies—VMware Special Edition (2020).

[3] MacDonald, Neil, et al. "2021 Strategic Roadmap for SASE Convergence." Gartner. March 25, 2021.

To learn more about SASE, visit windstreamenterprise.com

WINDSTREAM
ENTERPRISE