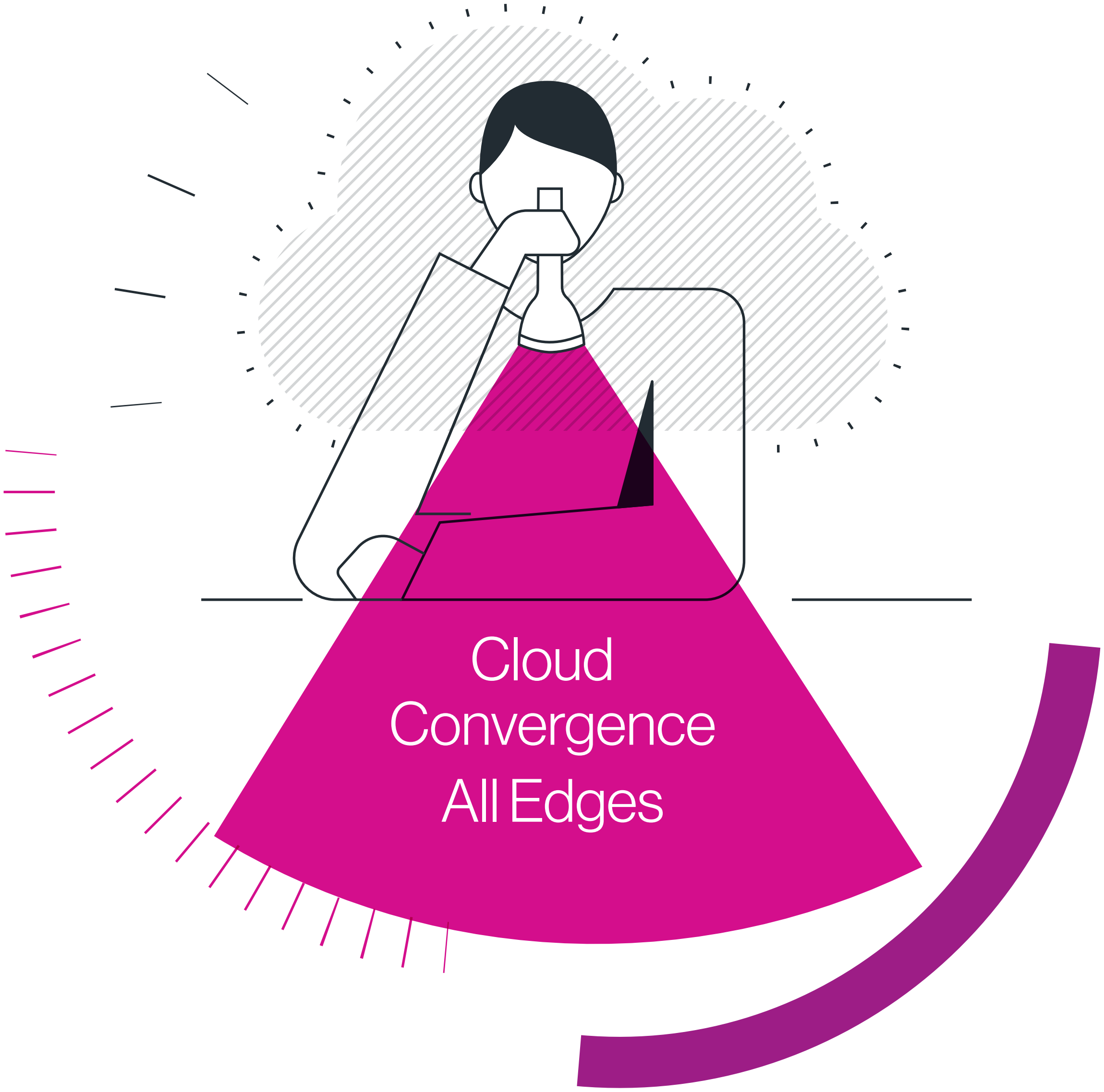
CATO NETWORKS | WINDSTREAM ENTERPRISE

What to Consider Before Renewing Your SD-WAN Contract or Service



The State of SD-WAN: Feature, Point Solution, or Platform?

Over the past few years, many enterprises deployed SD-WAN edge appliances to overcome the limitations and dated design of their MPLS networks. Capacity constraints, high costs per MBPS, and Internet traffic backhauling to the datacenter, all made MPLS a poor fit to support the ongoing migration to cloud services, work from home, and geographic expansion.

Enterprises expected SD-WAN to make their networks agile, secure, high performance, and cloud optimized. But the requirements for transforming the network go beyond the WAN edge alone.

Here are a few examples:

WFH and Remote Access

became a necessity with the onset of the COVID-19 pandemic that moved users away from the branch, rendering SD-WAN investments useless.

Geographically Diverse Locations

require a reliable transport to connect to physical and cloud datacenters that must be more reliable than the public Internet.

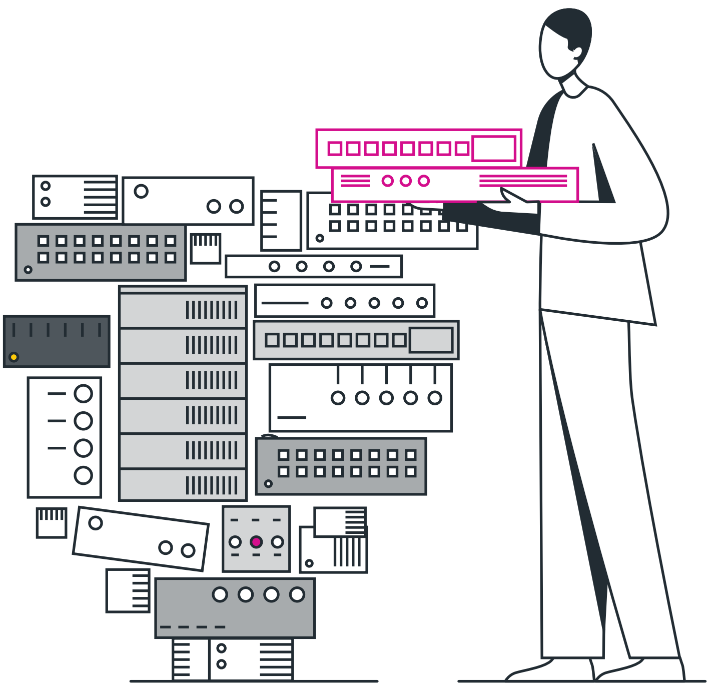
Secure Direct Internet Access

at the branch requires security everywhere – not in a specific location you backhaul traffic into.

Cloud Access

requires an optimal connection from anywhere in the world, not just premium connectivity from the datacenter.

While SD-WAN is a crucial element in the WAN transformation journey, enterprises still need to address **security, cloud, remote access, and connectivity requirements**. This "gap" led to the deployment of multiple point solutions, alongside SD-WAN, that in turn increase complexity and costs, and reduced agility, speed and responsiveness.



IT executives and professionals are now facing a simple, but difficult, choice. Should they renew the SD-WAN point solution for three or more years or reassess? Can the network evolve to holistically address the current and emerging needs of the business?

We think there is a powerful alternative. It is called the **Secure Access Service Edge (SASE)**. SASE is the convergence of SD-WAN, security, and remote access into a unified, cloud service. Reduce the number of point solutions, complexity, costs, and grunt work, and gain agility, security, speed, and efficiency.

SASE: The Convergence of SD-WAN, Security, and Access Control in the Cloud

SASE is a new technology category that took the market by storm. It is not just the latest shiny widget. Rather, it delivers existing networking and security capabilities you already know, via a new, converged and cloud-native architecture.

These are the attributes of the SASE architecture that help IT organizations to become faster, agile, and efficient while maintaining a high performing and secure network.

Convergence

SASE converges multiple capabilities such as Edge SD-WAN, Firewall as a Service (FWaaS), Threat Prevention (Anti-malware, IPS), Cloud Access Security Broker (CASB), Data Loss Prevention (DLP) and Zero Trust Network Access (ZTNA/SDP) into a single code base and a single pass engine.

Why it matters: Instead of selecting, testing, sizing, deploying, integrating and managing individual point solutions, a SASE platform enables gradual deployment of a wide range of capabilities with the same platform anywhere in the world and for any location or user. A single pass engine also eliminates the overhead of chaining multiple separate products to achieve the desired optimization and security outcome.

Cloud-native

SASE is a cloud-native architecture. We are all familiar with the benefits you get from a cloud solution. The cloud provider is responsible for maintaining the code so fixes and enhancements come faster. There are no worries about scaling and sizing the infrastructure to accommodate new growth. And, the cloud provider designs deep security and high availability measures to ensure service continuity.

Why it matters: Unlike legacy appliance-based solutions that you own and maintain, a cloud-native architecture reduces grunt work and infrastructure upkeep that slows IT's response to changing business needs.

Connectivity

The SASE cloud service can extend all its capabilities across all locations while maintaining optimum performance. This is dependent on the number and locations of PoPs that can actually deliver SASE capabilities. A SASE service with the right footprint, and the right private backbone, eliminates the need to build regional hubs that host networking and security functions, and all the complex capacity planning and high availability design that entails. In addition, a converged private backbone provides reliable transport for both WAN and cloud traffic and reduces the need to introduce a third-party carrier into the IT stack.

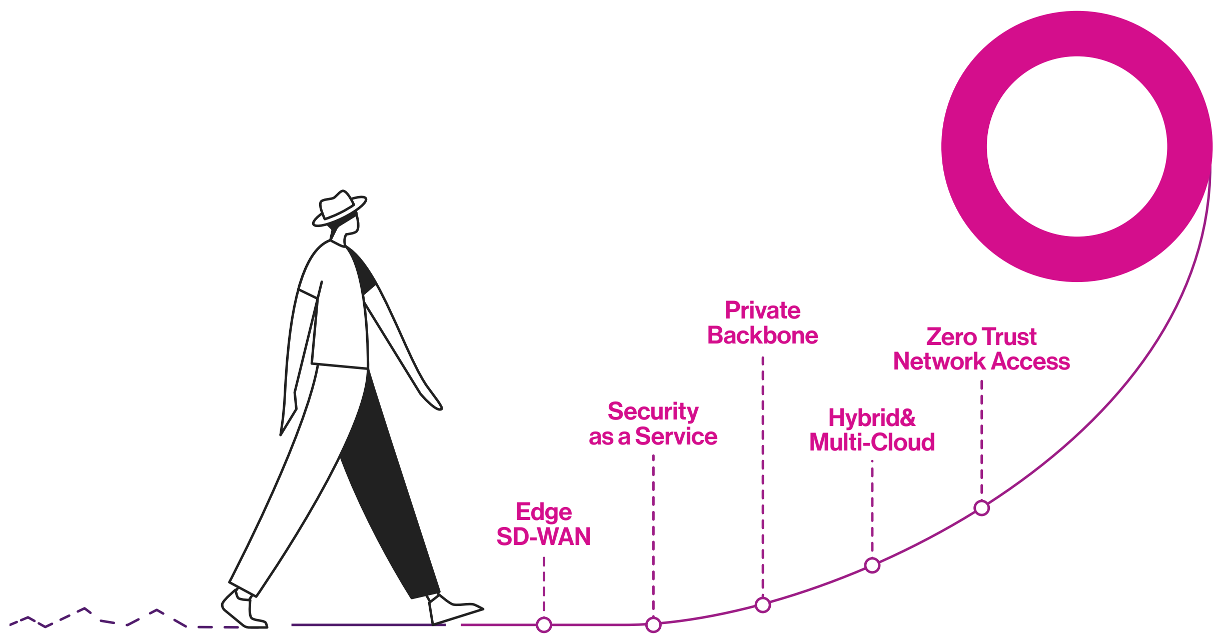
Why it matters: Legacy architectures force IT to design a custom delivery of the capabilities offered to the business. This is a complex and expensive effort, that complicates maintenance and troubleshooting, and could impact security and optimal connectivity for remote locations.

All edges

A real SASE architecture is designed from the ground up to serve all edges: sites, cloud, and people. The only way to achieve this with legacy approaches is by deploying separate point solutions for each edge: SD-WAN for the branch, ZTNA or VPN for remote access, and cloud accelerators for optimal cloud access.

Why it matters: By placing as many capabilities as possible inside the SASE cloud, SASE can equally and easily extend these capabilities to all edges. This reduces complexity and costs.

How SASE Covers the Full WAN Transformation Journey vs. SD-WAN



1 SASE Edge SD-WAN: Robust and Resilient Last-mile Access to Cloud and DC Applications

A complete SASE architecture includes a full edge SD-WAN solution. The objective of the SD-WAN edge is simple: ensure that branch traffic optimally flows to the SASE cloud and from there to the Internet, cloud datacenters and cloud applications, and applications hosted in physical datacenters. SD-WAN traffic steering is achieved using multiple active/active last mile links, prioritization of traffic by applications, and the mitigation of link degradation for loss-sensitive applications (i.e. voice).

Edge SD-WAN that is part of a SASE service provides similar capabilities to SD-WAN point solutions. However, policy management and analytics are fully managed through the SASE console alongside security, cloud and remote access.

2 Security as a Service: Pervasive Self-maintaining Security Stack for all Locations and Users

As branches and users connect to the Internet, all traffic must be secured against threats. This requirement for pervasive security was less important when most traffic was within the MPLS network. Those days are now gone. Today's traffic commonly goes to and from the cloud and the Internet—SASE places a wide range of security controls in the cloud to protect all traffic, both WAN and Internet, against phishing, malware, and other Internet-borne attacks. Cloud-native security helps reduce branch footprint and makes protection available for all edges: from the datacenter all the way to a single user anywhere in the world.

Most SD-WAN point solutions lack a full-blown security stack (other than a basic firewall with no threat prevention capabilities). Appliance-based products that combine SD-WAN and network security are subject to the same sizing, upgrades, patching, and maintenance challenges like edge firewalls and UTMs, and have no value for use cases such as remote access that require security outside the branch.

3 Private Backbone: Optimized Connectivity for Both WAN and Cloud Traffic

A private backbone provides a reliable transport for enterprise WAN and Internet traffic. When embedded inside the SASE cloud it handles traffic from all edges—physical, cloud, and user—to any destination—on-premises and in the cloud. The result is that ALL traffic is optimized and accelerated without the need to deploy edge-specific acceleration solutions (like WAN optimizers).

SD-WAN point solutions rely on the Internet as their "backbone." Third-party backbones, like MPLS or Azure Virtual WAN, are required to address high latency for users and locations that are far away from on-premises and cloud applications.

4 Hybrid and Multi-Cloud: Plug Your Cloud Datacenters into SASE for Seamless Migration

Cloud migration is a strategic project for many enterprises. As applications move to the cloud, the SASE cloud acts as an interconnect that optimizes traffic from branches and users to the cloud applications and datacenters. No other solution is required.

SD-WAN point solutions require premium cloud connectivity solutions like AWS Direct Connect and Microsoft Azure ExpressRoute to optimize access to the cloud.

5 Zero Trust Network Access: Cloud-scale Remote Access for the Entire Business

Remote access, and specifically work from home, has created an urgent need to extend corporate security and optimization capabilities to users outside the office. In turn, this created a need to scale up legacy infrastructure to support such access for all users at all times. The SASE cloud was designed to follow the user and provide the same capabilities inside and outside the office. In the office, the user benefits from the connection to the SASE cloud via the SD-WAN device. Outside the office, a lightweight device client continuously connects the user to the SASE service where its traffic is subject to the same security and optimization capabilities.

SD-WAN point solutions, as branch technology, have no bearing on the remote access requirement. Enterprises have to stretch their legacy VPN or deploy ZTNA-based remote access point solutions if they want to provide secure access to users at home.

The Checklist: What to Consider Before Renewing Your SD-WAN Contract or Service

Capability	Use Cases	How is it Achieved Today?	SD-WAN to SASE Upgrade Impact	
			Converged SASE Capability	**SASE Unified Management**
SD-WAN	MPLS alternative	SD-WAN + Internet	Full featured SD-WAN + Private Backbone	Zero touch provisioning
Security	Secure Internet Access for locations and users	Edge FW or cloud-based security	Enterprise-grade cloud-based security to all edges, full decryption and threat prevention	Self-maintaining, no upgrades, maintenance, scaling, sizing, integration
Remote Access	Work from home 3rd party access	Legacy VPN FW/VPN ZTNA product	Cloud-scale and optimized remote access with full threat prevention	Full visibility and control per user
Connectivity	Low latency and traffic optimization for real-time unified communications	Alternative backbones or the Internet	Private Backbone with built in WAN and Cloud traffic optimization	Full visibility and control to all locations
Cloud	Cloud migration, acceleration, security	Premium cloud connectivity, CASB or nothing	Multi-cloud optimization with full access control and threat prevention	Full visibility and control of all cloud traffic, smart egress policies to critical cloud apps traffic

Summary

SASE is a platform that can truly transform your IT networking and security infrastructure. IT made a crucial first step by deploying SD-WAN to augment or replace MPLS to address network resiliency and costs. It is time to think more broadly on what is next for your network. SASE can make your network more secure and optimized for connectivity, work from home and cloud migration.

For more details, visit
windstreamenterprise.com

0408 I 12.22