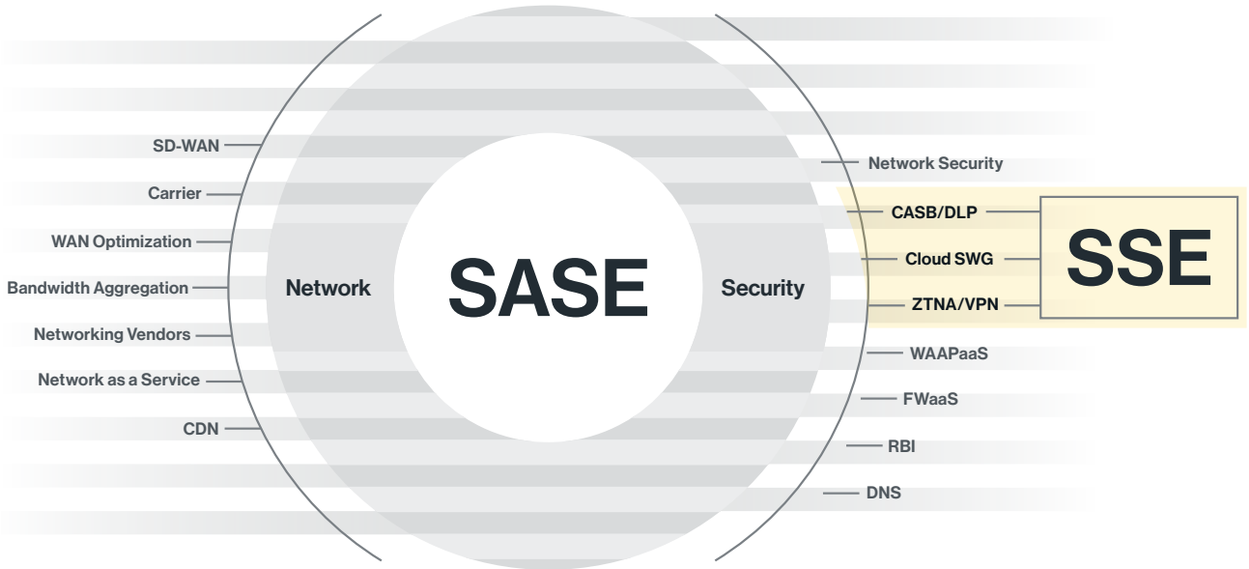
CATO NETWORKS | WINDSTREAM ENTERPRISE

SSE

Total visibility and control for all:
Traffic, users, and applications everywhere.

SSE, SASE, and the path to IT convergence



In 2019, Gartner introduced the Secure Access Service Edge (SASE) category. SASE defined the convergence of two distinct technology markets, the WAN edge (SD-WAN) and network security, into a global cloud service that enables secure and optimized access to any user, at any location, and to any application. The security pillar of SASE included Secure Web Gateway (SWG), Cloud Access Security Broker (CASB) with Data Loss Prevention (DLP), Zero Trust Network Access (ZTNA), and Firewall as a Service (FWaaS) delivered as a cloud service.

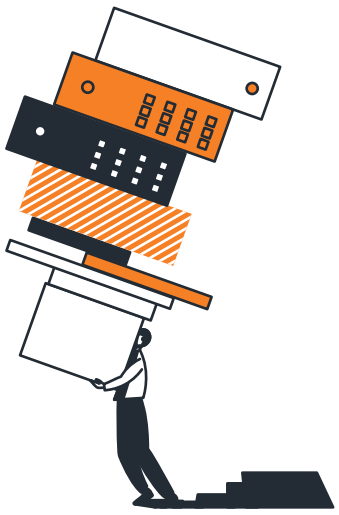
Two years later, Gartner introduced a new category called the Security Service Edge (SSE) to describe a more limited scope of convergence focused on network security. SSE converged three security components, SWG, CASB/DLP, and ZTNA into a single cloud service. SSE provides secure access to applications without directly addressing the end-to-end optimized network connectivity and east-west WAN security aspects of that access. These remain part of a separate technology stack including technologies such as SD-WAN, Next Generation Firewalls (NGFWs), and global network backbones.

Customers are now faced with a decision of how to approach the "converged future" of their IT infrastructure. Some organizations will go for the full SASE convergence from the outset. Others will approach the journey to full SASE convergence through multiple steps, starting with SSE-driven security transformation on top of the existing network infrastructure and proceeding to SASE with a network transformation project at a later stage. Keeping this full transformation path open, using a single vendor SASE, is a strategic decision for most enterprises. Simply put, the deeper the convergence, the better the visibility, security posture, operational simplicity, cost savings, and business agility.

In this paper, we will look at the capabilities, benefits and use cases covered by Windstream Enterprise SSE, powered by Cato, our implementation of SSE, and the path to full SASE transformation.

Legacy security architectures impact agility, risk, resources, and skills

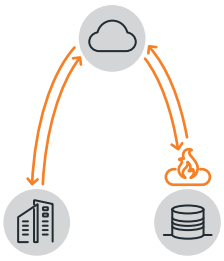
Businesses today depend on optimized and secure access to applications and data, on premises and in the cloud, by an increasingly hybrid workforce. Rigid security architectures built with disjointed point solutions and appliances, can't adapt to emerging business and technical requirements and the evolving threat landscape. The result is lower business agility and increased risk made worse by lack of resources, scarce cybersecurity skills, and high cost of outsourced support.



Key barriers to digital transformation created by legacy architectures

Legacy networks are built around physical corporate locations

This design pattern forces a re-architecture of the network to support internal applications in physical and cloud data centers, public cloud applications, and secure access by users anytime and anywhere.



Centralized (backhauling) security model slows down secure cloud access

As the volume of Internet and cloud-bound traffic increases, it no longer makes sense to drive all traffic through the data center firewalls. Direct secure Internet must be enabled at every location and down to a single remote user to extend full visibility and control to all application access without impacting the user experience.

Legacy security solutions can't scale to support work from anywhere

Supporting the hybrid workforce requires a flexible and scalable security architecture that can secure the entire workforce wherever they work from: in the office, on the road, and at home.

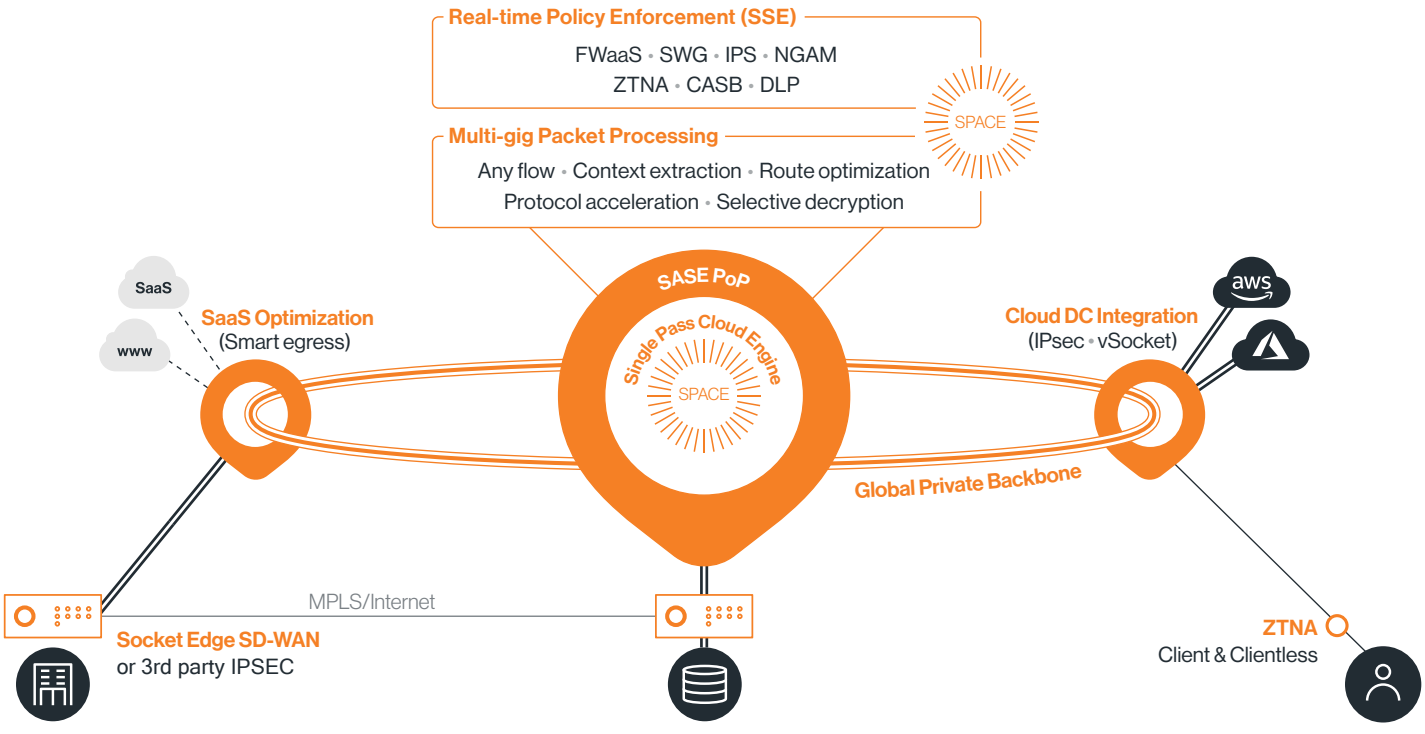
Disjointed solutions introduce fragmented and complex management

Security consolidation and architectural convergence in the cloud reduce the work required from IT to keep the security infrastructure up and running and in an optimal security posture. As the work shift to expert team running the cloud platform for all customers, the likelihood of a mistake or oversight due to workload is reduced.

These are all architectural and structural issues, that yet another point solution will not solve. Enterprises should consider security transformation using the right SSE architecture to address them.

Windstream Enterprise SSE: Beyond Gartner's SSE

The Security Service Edge (SSE) enables enterprises to move away from a rigid and disjointed IT architecture to a converged security platform delivered as a cloud service. With SSE, enterprise IT can rapidly address new business and security requirements such as cloud migration, adoption of public cloud applications, and work from anywhere. SSE's converged architecture reduces cost and complexity with simple management through single pane of glass, self-healing infrastructure, and automatically evolving defenses that seamlessly mitigates emerging threats. Customers can opt to manage their infrastructure themselves or co-manage it with their preferred partners.



Platform overview

Windstream Enterprise SSE takes SSE beyond the Gartner defined scope with the following components:

Cloud-native security service edge

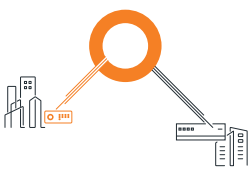
Our SSE is built using the Cato Single Pass Cloud Engine (SPACE) architecture that is the foundation of Cato's global, converged, cloud-native service. Current converged capabilities include not only SWG, ZTNA, and CASB/DLP but also full Firewall as a Service (FWaaS) with Advanced Threat Prevention (IPS, Next Generation Anti-malware) as well. Using FWaaS along with the other converged capabilities enables Cato to apply the full set of SSE controls to all traffic.

Private backbone

A geographically distributed, SLA-backed network of 26+ PoPs in North America, interconnected by multiple tier-1 carriers and Internet exchanges peered with multiple service providers. Each PoP runs the full set of SSE capabilities to ensure minimal latency for connected users and locations. In addition, the backbone provides routing optimization, self-healing capabilities, WAN and Cloud optimization for maximum end-to-end throughput and full encryption.

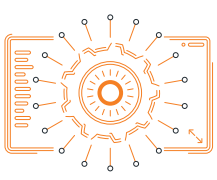
SDP clients

Lightweight clients connect user devices to SSE to optimally and securely access the Internet, internal applications, on premises and in the cloud, and global public cloud applications. Windstream Enterprise provides clients for laptops, smartphones, and tablets, as well as a clientless browser access option.



IPsec-enabled devices and Cato socket SD-WAN for locations

Physical and cloud locations connect to SSE using any IPsec enabled third-party device or Cato Socket SD-WAN appliances. The Cato Socket provides last mile resiliency and quality of service (QoS) and overcomes blackouts and brownouts using application-based dynamic path selection and packet loss mitigation.



Comprehensive management application for analytics and policy configuration

The Windstream Enterprise WE Connect portal provides customers with a management application for security and network analytics, as well as full granular policy configuration. As applicable, we offer managed service options, including site deployment, intelligent last-mile monitoring, configuration of network and security policy changes, and managed detection and response (MDR).

Key use cases, capabilities, and benefits

By using SSE, enterprises can address a wide range of use cases and gain multiple strategic capabilities. These include:

Scalable hybrid work

SSE provides secure and optimized access to all users, locations, and applications everywhere using SDP Clients, Sockets, or clientless access. All traffic is protected by SSE and optimized using the private backbone. SSE's elastic cloud-native architecture supports massive shifts in access patterns with users freely roaming between the office, travel, and their homes. Therefore, SSE overcomes the physical constraints of appliance-based VPN and security solutions. Customers use SSE to eliminate the cost and complexity of point solutions including appliances and cloud-based security services such as VPN, Firewalls, CASB, DLP, and Secure Web Gateways.

Gradual cloud migration

Windstream Enterprise easily connects physical and cloud data centers to SSE and optimizes access to public cloud apps. Traffic is inspected by SSE and optimized using the global private backbone across the "middle mile". This is achieved through a "smart egress" capability that allows customers to define an application-level rule to exit specific application traffic at a designated PoP that is the closest to the target instance serving the organization. With SSE, customers can eliminate premium cloud connectivity solutions like AWS DirectConnect and Microsoft ExpressRoute.

Secure sensitive data

SSE CASB and DLP enable full visibility and control of sensitive data. SSE enforces granular policies on data access from corporate and BYOD (bring your own devices), restricts access according to device posture and required level of access, and controls data sharing across applications. With SSE, customers can reduce the risk of sensitive data loss and reputation impact, and better comply with regulatory requirements.

Instant deployment of security capabilities

All security capabilities, present and future, are converged into SSE and can be deployed with a "flip of a switch" without complex integration, capacity planning, and multiple management consoles. All security policies and analytics are managed through a single pane of glass and are guaranteed to work at the geographies, capacities, and resiliency defined by current deployment without requiring further planning. Customers use Cato to eliminate the cost and complexity of point solutions including appliances and cloud-based security services such as VPN, Firewalls, CASB, DLP, and Secure Web Gateways.

Future-proof and zero maintenance security

SSE is self-maintaining, self-evolving and self-healing. Windstream Enterprise removes the grunt work associated with the upkeep of on-premises infrastructure and uses a cutting-edge team of security experts to maintain optimal security posture of SSE against emerging threats. MDR further augments customer resources and skills with on-going hunting and remediation of resident threats on the network.

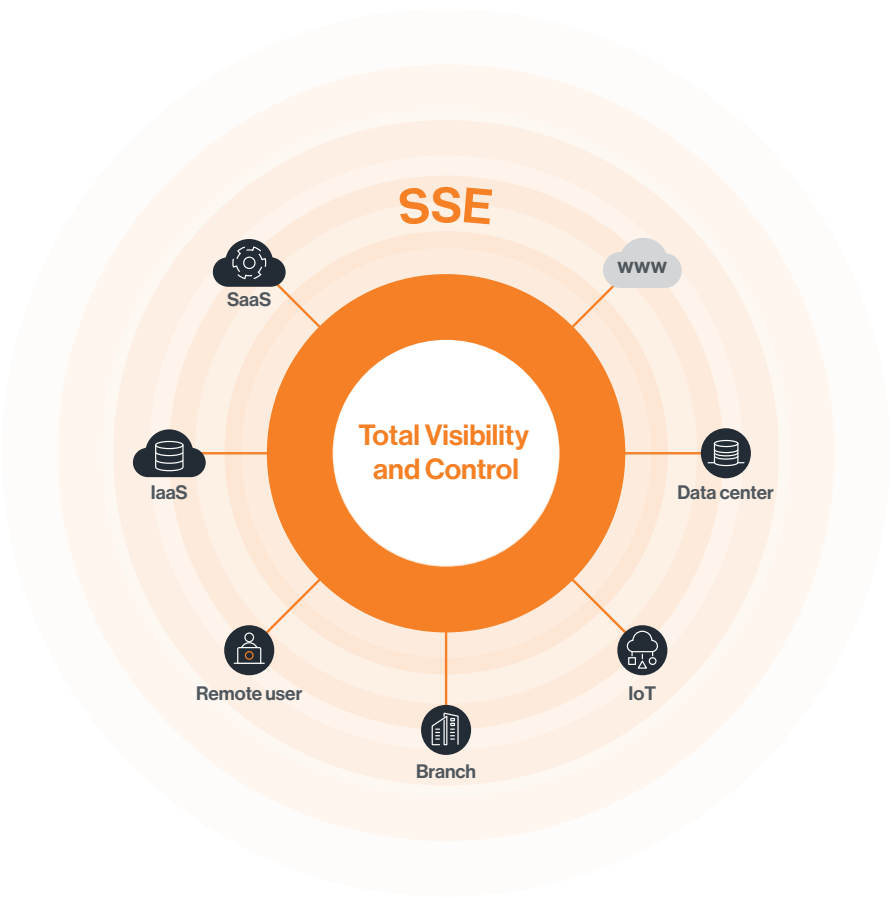
Extending SSE

Windstream Enterprise extends SSE by providing full visibility and control to all traffic, optimizing global application access without relying on the public Internet, and enabling a seamless path to a full single-vendor SASE deployment.

SSE provides full visibility and control across all traffic

Most SSE platforms are based on a web-proxy architecture that are built to inspect Internet and public cloud application traffic only. SSE can't inspect non-web traffic as well as ZTNA traffic supported through application connectors. As a result, it can't address risks associated with threats such malware propagation across the WAN and threats related to non-human generated traffic.

In contrast, our network-based architecture connects all enterprise resources into a secure cloud network. SSE was built to inspect all traffic across all ports and protocols that traverse our cloud network. As a result, Windstream Enterprise SSE enforces the full set of SSE capabilities, including access control, threat prevention, and data protection to all traffic regardless of the source (user, device, machine, application, etc.) or the destination (internal or external application, on premises or in the cloud). Our network-based architecture extends the visibility and control available to our security research and machine learning algorithms to a broader set of live traffic and increases our ability to detect and prevent the risk of data breach.



SSE optimizes global application access

SSE leverages Cato's private backbone to optimize application access, on premises or in the cloud, from anywhere. The backbone is a geographically distributed, SLA-backed network of 26+ PoPs in North America, interconnected by multiple tier-1 carriers and Internet exchanges peered with multiple service providers. Each PoP runs the full set of SSE capabilities to ensure minimal latency for connected users and locations. In addition, the backbone provides routing optimization, self-healing capabilities, WAN and Cloud optimization for maximum end-to-end throughput, and full encryption. Unlike typical SSE, our SSE can run application traffic across the backbone ("the middle mile") instead of dropping it to the Internet, to ensure optimized user experience.

SSE enables seamless path to full single-vendor SASE

Customers can start their SASE journey by deploying SSE for security transformation, leveraging existing WAN edge appliances for SSE connectivity. Extending the deployment to SD-WAN Socket devices enables the elimination of branch and data center WAN devices such as routers, firewalls, third-party SD-WAN, and WAN optimization. This extension enables the consolidation of networking capabilities and policies into the SASE Cloud including bandwidth management, last-mile resiliency and monitoring, and application Quality of Service (QoS) management. The convergence of cloud-based security and the WAN edge drives strong reduction of costs, complexity, and management overhead while improving resiliency, and end-to-end visibility.

Windstream Enterprise SSE vs. SSE: Choosing the right solution

Windstream Enterprise SSE includes white glove support at no extra cost. This key advantage comes at a premium from other SSE providers.

KEY
● Full Capability ◑ Limited/Partial Capability ○ No Capability

	Other SSE providers	Windstream Enterprise SSE
Core capabilities		
ZTNA	●	●
• Client + clientless	●	●
• Device posture	●	●
• MFA	●	●
• Continuous traffic inspection for threats	○	●
SWG	●	●
CASB/DLP	●	●
• Inline	●	●
• SaaS API	●	●
FWaaS with full threat prevention	○	●
Unified architecture for all capabilities	○	●
Management		
Connect with IPSec-enabled or SD-WAN devices	●	●
“Single pane of glass” management	●	●
Self-maintaining platform	●	●
Self-healing platform (cloud availability)	◑	●
Proven fast adaptation to evolving threats	◑	●
Traffic visibility		
Internet: Websites	●	●
Internet: Public cloud apps (Office 365)	●	●
WAN: Cloud DC apps (AWS, Azure, GCP)	● app-specific connectors	●
WAN: Physical DC apps	● app-specific connectors	●
All ports and protocols	○	●
Traffic control		
SSL decryption	●	●
Internet traffic	●	●
WAN traffic inspection	●	●
Max throughput with decryption + full inspection	1gbps	3gbps
Threat prevention		
Inbound (web)	●	●
Outbound (web)	●	●
WAN propagation	○	●
All ports + protocols	○	●
Threat detection		
Security events collection	●	●
Security events reporting an export	●	●
Managed detection + response	○	●
Access optimization		
Private backbone with “middle mile” control	○	●
Cloud applications access optimization	● peering	● egress
WAN applications traffic optimization	○	●
Path to SASE convergence		
Seamlessly expandable to single-vendor SASE	○	●
Appliance elimination for SD-WAN, firewalls, routers + WAN optimization	○	●
SD-WAN capable	○ partner	●
White glove support included		
Account setup	○	●
On site/remote deployment	○	●
Support engineer	○	●
Technical account manager	○	●
Technical project management	○	●
Training	○	●

The journey to full SASE transformation starts with SSE

SSE is transforming the fragmented security stack that is slowing down digital transformation in many enterprises. The convergence of ZTNA, SWG, and CASB is a right step in addressing this challenge. However, SSE itself is built on legacy technologies, that were architected to secure web-based applications. As a result, typical SSE products are blind to non-web traffic and non-human traffic from network devices, IoT, and applications, and have limited support for securing access to internal applications. Furthermore, they neglect the performance aspects of the access and rely predominantly on the unpredictable public Internet to serve as the application access transport.

Windstream Enterprise SSE offers total traffic visibility and control. Simply put, our SSE "sees" all traffic across all ports, protocols, sources, and destination, and applies the full range of its access control, threat prevention, and data protection capabilities to that traffic. Built on a private backbone, application access is fully optimized through a predictable and reliable transport that works equally well for application in physical data centers, cloud data centers, and the public cloud.

SSE creates a great foundation for customers to seamlessly complete their full SASE transformation on a single vendor platform. By extending the SSE implementation SD-WAN, customers can replace 3rd party routers, firewalls, SD-WAN, and WAN optimization appliances. This convergence of both security and networking further reduces costs, complexity, risk, and management overhead.

SSE, SD-WAN, SASE: Your journey, your way.