CATO NETWORKS | WINDSTREAM ENTERPRISE

Achieving Zero Trust Maturity with SSE

The Need for Zero Trust

Zero Trust is a significant topic today and with just cause. Enterprises continue to experience cyber threats from all vectors, which doesn't appear to be waning anytime soon. These never-ending risks are detrimental to technical and business viability in the Digital Transformation era because existing architectures are designed on implicit trust. To remedy this, they must either be rebuilt or replaced; neither option is straightforward or inexpensive.

This conundrum was a driver of several maturity model proposals to enable organizations to transition to Zero Trust at their own pace. Most notable is the proposal put forth by the US government's Cybersecurity and Infrastructure Agency (CISA), which defined a five-pillar model that outlined guidance for organizations to achieve Zero Trust Maturity.

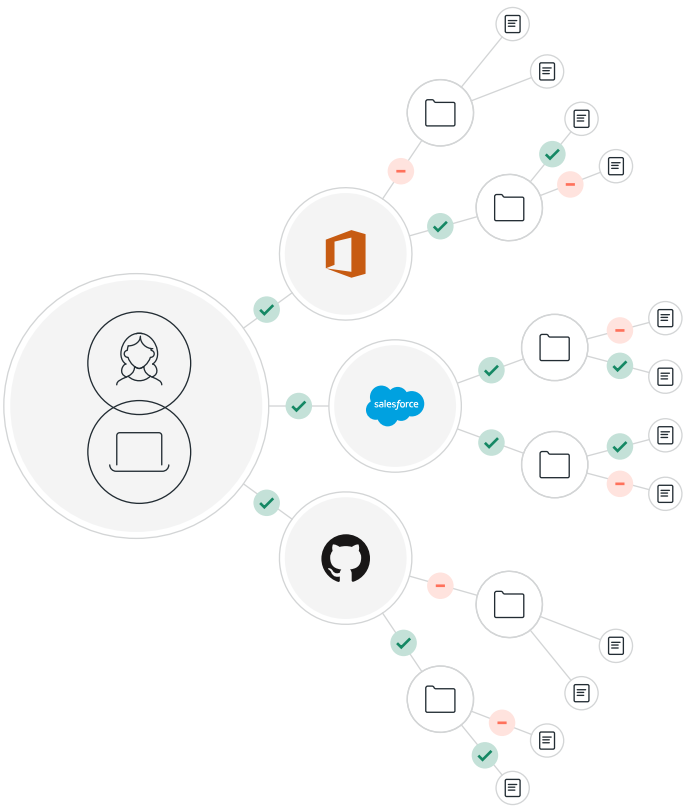
Zero Trust is a journey; having the right tools and architecture will help smooth and expedite this journey. Cato Networks, the world's first and only converged cloud-native SSE platform with Zero Trust built-in, provides a dynamic, scalable, and secure architecture. This paper will discuss how Windstream Enterprise SSE, powered by Cato, can help facilitate Zero Trust Maturity.

Trust is No Longer Implied

Zero Trust is a dramatic paradigm shift away from the traditional perimeter-centric security model, which is no longer adequate for today's dynamic Work-From-Anywhere (WFA) environment, to models emphasizing unique data access requirements. "Implicit Trust," the nemesis of perimeter-centric architectures, renders them ineffective because all entities, regardless of intent, are granted equal access upon authorization.

A Zero Trust Architecture (ZTA) removes the implicit trust model in favor of a per-session-based (explicit trust) model that enables secure access to applications and data without requiring complex network segmentation. Complex network segmentation can create more work for security and operations teams without producing significant additional benefits. However, a well-designed ZTA overcomes these flaws, and foundational to facilitating this is adherence to key ZTA principles:

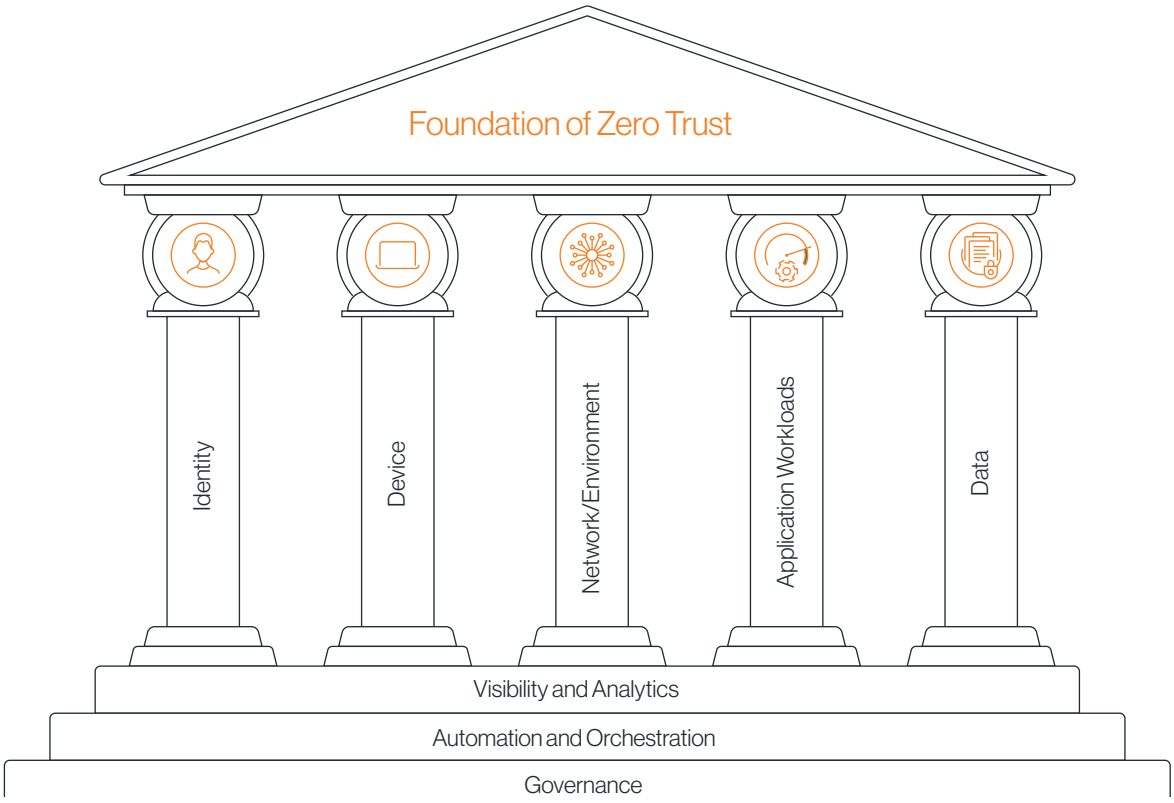
- Secure communications regardless of location
- Dynamic policy access to resources
- Continuous monitoring and validation
- Segmentation & least privileges
- User & device fitness is determined before granting network access
- Contextual automation to improve security posture



Zero Trust aims to ensure that access to data and applications is granted only after users and their devices have proven they can be trusted. This approach logically reduces the attack surface, which is desired to reduce threats to applications and data. Unfortunately, many organizations are challenged in understanding how and where to begin their Zero Trust journey, and this is where the **CISA Zero Trust Maturity** begins to provide clarity.

CISA Zero Trust Maturity and Windstream Enterprise SSE, Powered by Cato

Many organizations are realizing that understanding Zero Trust requirements is one thing, but adapting and implementing it is a challenge of its own. The path to Zero Trust is an incremental process that will take time to implement. Considering this and the ongoing risk from cyber threats, CISA proposed its Zero Trust Maturity Model as a flexible template for enterprises to measure their journey to Zero Trust while improving their overall security posture. The CISA model, as depicted below, is broken into 5 pillars: Identity, Devices, Networks, Applications, and Data.



Source: Cybersecurity and Infrastructure Agency (CISA)

Windstream Enterprise SSE, powered by Cato, is crucial in helping organizations transition to Zero Trust by facilitating maturity across all five pillars. Mapping these pillars to SSE highlights the depth of this coverage and the collaboration with external tools to deliver Zero Trust.

Pillar 1:
Identity

This pillar emphasizes the core functions of Authentication, Identity Stores, and Risk Assessments. This is core to Zero Trust. User credentials must be verified as belonging to the correct individual, and this pillar ensures proper credentials are applied when an action is requested. However, these user attributes should not grant permissions in every circumstance. It requires continuous validation and global awareness to ensure proper access is given when warranted.

SSE and Identity

As identity is a foundational element of Zero Trust, it forms the basis for every secure action taken across our SSE solution. Our SSE works in concert with enterprise Identity architectures by leveraging your existing Identity Provider (IdP) and enforcing strict user identity criteria. Identity and context are consumed via TLS to securely import over LDAP or auto-provisioning via Systems for Cross-domain Identity Management (SCIM).

Because user identity profiles exist everywhere across our SSE, we have global identity awareness. Consequently, the user's identity and behavior, combined with device attributes, determine permission to remain on the network.

Additionally, our SSE extends security to users by encrypting transport across our backbone and layering in Security-as-a-Service and advanced threat protection for each valid user session.

Pillar 2:
Device

This pillar manages device risk through Compliance Monitoring, Data Access, and Asset Management. This involves transitioning data access, regardless of device, to a risk-based access evaluation for every access request. This evaluation and validation include all networked devices, including IoT, mobile, servers, BYOD, etc. Constant monitoring for risky behavior of threats and device posture validation is crucial under this pillar.

Windstream Enterprise SSE and Device

Our SSE takes a risk-based approach to Zero Trust, combining Client Connectivity & Device Posture capabilities with 360-degree threat protection techniques. Typical enterprises will define posture criteria such as operating systems, software versions, disk encryption, geo-location, etc., to assess the worthiness of accessing network and application resources.

All data flows, threat intelligence feeds and user and device behaviors are accessed prior to granting access. This in-depth level of context allows us to determine client connectivity criteria and device suitability for network access and continually monitor and assess both the user and device.

Pillar 3:

Network/Environment

The Network pillar discusses secure digital communications within and across networks and clouds, focusing on Network Segmentation, Threat Protection, and Encryption. This requires a new, dynamic architecture encompassing LAN, WAN, Cloud, and Internet. Securing users from threats is a huge but achievable task. This includes identity-based network access with the least amount of privilege assigned, segmentation, holistic threat protections, and traffic encryption.

Windstream Enterprise SSE and Network Environment

Our SSE is your security architecture and your network infrastructure with its private backbone. Cato's extensive visibility into network traffic flows allows 360-degree security with FWaaS, IPS, SWG, CASB, DLP, and NextGen Anti-Malware to protect all apps from malicious intent. Cato enforces all Zero Trust policies at the cloud edge to ensure consistency, performance, and holistic security throughout.

Our SSE enables micro-segmentation for more granular access control within and between data centers and clouds. This prevents east-west lateral movement and contains attackers within a microsegment if there is a breach.

Our SSE provides modern encryption to secure traffic flows across the entire cloud backbone. Additionally, we use AI & Machine Learning to continually mine the network for indications of malware or other advanced threats to deliver extended protection. We will proactively block these threats to minimize the potential damage inflicted upon the network, users, devices, and applications.

Pillar 4:

Application Workloads

This pillar mandates Access Authorizations, Threat Protections, Accessibility, and Application Security for all enterprise and cloud applications regardless of location. Secure access to critical enterprise and cloud apps is fundamental to Zero Trust, regardless of their location. Authorization based on user, device, and contextual profiles ensures that those requesting access only gain permission on an as-needed basis. Requiring advanced security along the entire path will identify anomalous behavioral indicators.

Windstream Enterprise and Application Workloads

Cato built the architecture to protect all enterprise and cloud applications. Our SSE provides full application awareness to classify standard and non-standard applications and their relevant context to ensure consistent access policy enforcement regardless of the app location, user & device identity, or access method. This enables our SSE to control access where the user connects and where the application lives. Our SSE also includes threat hunting to extend security by identifying hidden threats to applications and data.

This cross-pillar collaboration extends to SecDevOps, which integrates security testing throughout the software development lifecycle (SDLC) and regularly tests deployed applications. FWaaS segments testing networks from production environments to protect live applications. NextGen Anti-Malware protects all enterprise and cloud applications from malware and other advanced threats.

Pillar 5:
Data

Inventory Management, Access Determination, and Encryption define this pillar. It mandates data protection across devices, apps, and networks. Access to data must be provided on the least privileged basis, and this data must be protected at rest and in transit (encryption). Data leak prevention is also mandated.

Windstream Enterprise SSE and Data

Securing critical data is always top-of-mind when deploying Zero Trust with our SSE. Users and devices are always inspected for risk before gaining application access and are continuously evaluated for fitness to maintain this access.

Like the application itself, advanced threat protection through SSE helps eliminate risks. We employ tools like CASB to prevent misuse of application data, combining IPS and NextGen Anti-malware to detect advanced threats, FWaaS to enforce security and access policies, and DLP to protect sensitive data, which is always the center of Zero Trust in our SSE.

Cross-pillar Mapping

Mapping across these pillars, we have visibility, analytics, and automation to facilitate dynamic policy changes and enforcement and security automation to accelerate threat response.

Our SSE provides a nice wrapper around this model by supporting or facilitating maturity across each pillar. For example, from an Identity perspective, Cato, being a global cloud-delivered network, can ensure global identity awareness for consistency of user and device access, security policy enforcement, and threat prevention no matter where the user or resource resides.

Finally, our SSE will also automate threat responses by enriching the data on ingress with context from all security tools, providing enhanced security analytics to extend protection for all applications and data.

Zero Trust is the Start, Not the Finish

> **60% of organizations will embrace Zero Trust as a starting point for security by 2025. More than half will fail to realize the benefits."**
>
> Source: Gartner's 8 Cybersecurity Predictions for 2022 Through to 2026

The foundation of Zero Trust is based upon 3 core functions:

1. **Identity** – Who are you, and why are you on my network?
2. **Device** – Is your device safe to access network and application resources?
3. **Network Security** – Can you securely connect users and devices to applications while securing data everywhere?

The beauty of Windstream Enterprise SSE, powered by Cato, is that it takes a risk-based approach to Zero Trust. It helps organizations identify, assess, control, and continuously evaluate the potential risk posed by users, devices, apps, and services, then adapt accordingly with minimal effort or impact on the user experience.

Our SSE provides complete security coverage while supporting many attributes across the Zero Trust Maturity pillars. Additionally, our SSE private network gives organizations the visibility of all user, application data, and network flows for richer security analytics to automate and adapt the security posture and reduce potential blind spots.

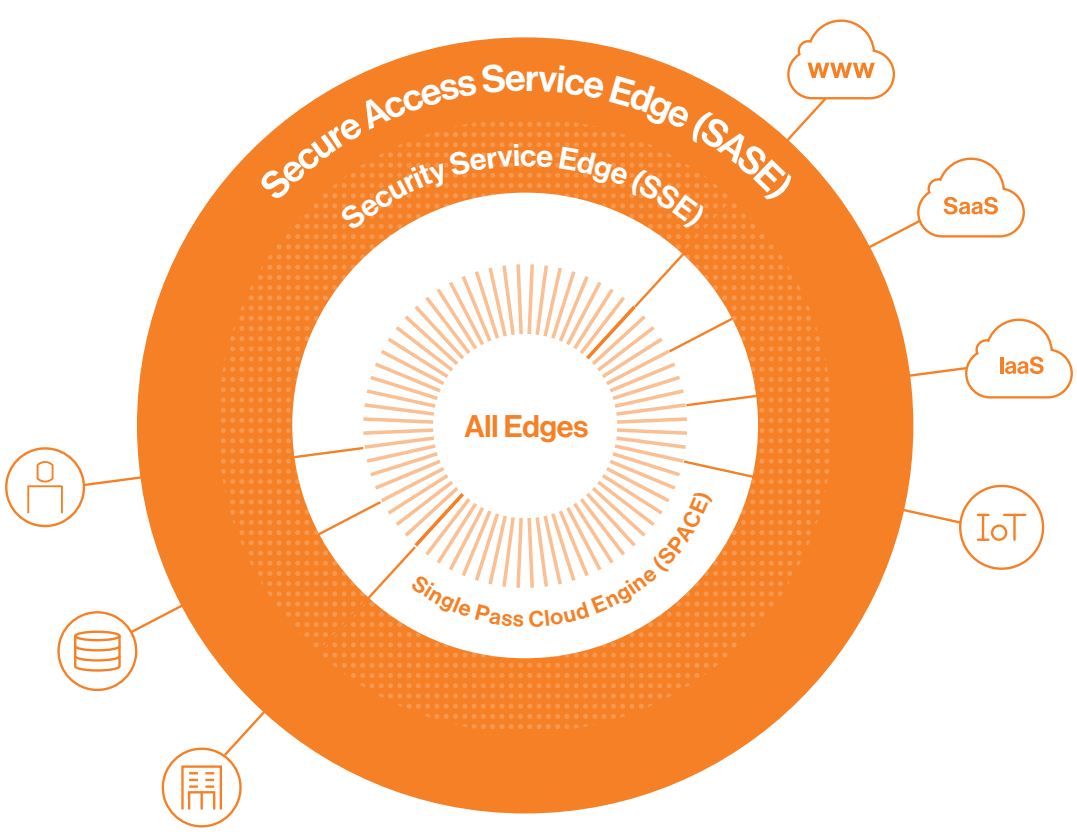
It must be noted that Zero Trust is not a single-product solution, and SSE does not address every aspect of Zero Trust. For example, tools like Privileged Identity Management (PIM) and Privileged Access Management (PAM) aren't native technologies of SSE solutions. However, our SSE integrates with Identity Service Providers (IdP) to enforce Zero Trust policies and help smooth the path to full maturity by supporting and facilitating Zero Trust across several pillars of the Maturity Model.

Zero Trust Maturity with SSE

Transforming from implicit trust to Zero Trust is building momentum, but it will take time for most organizations to achieve full maturity. The core of Zero Trust is an identity-driven default-deny approach to improving security postures, and applying the CISA Zero Trust Maturity Model helps map out any Zero Trust projects' current and future states. Organizations must then select the appropriate tools for achieving Zero Trust Maturity and ensure holistic security is part of this process.

Our SSE is a secure digital transformation platform that facilitates Zero Trust Maturity. Cato's cloud-native architecture approach to Zero Trust places user and device identity with global consistency at the center of its protection model to build coverage across all pillars of CISA's Zero Trust Maturity Model.

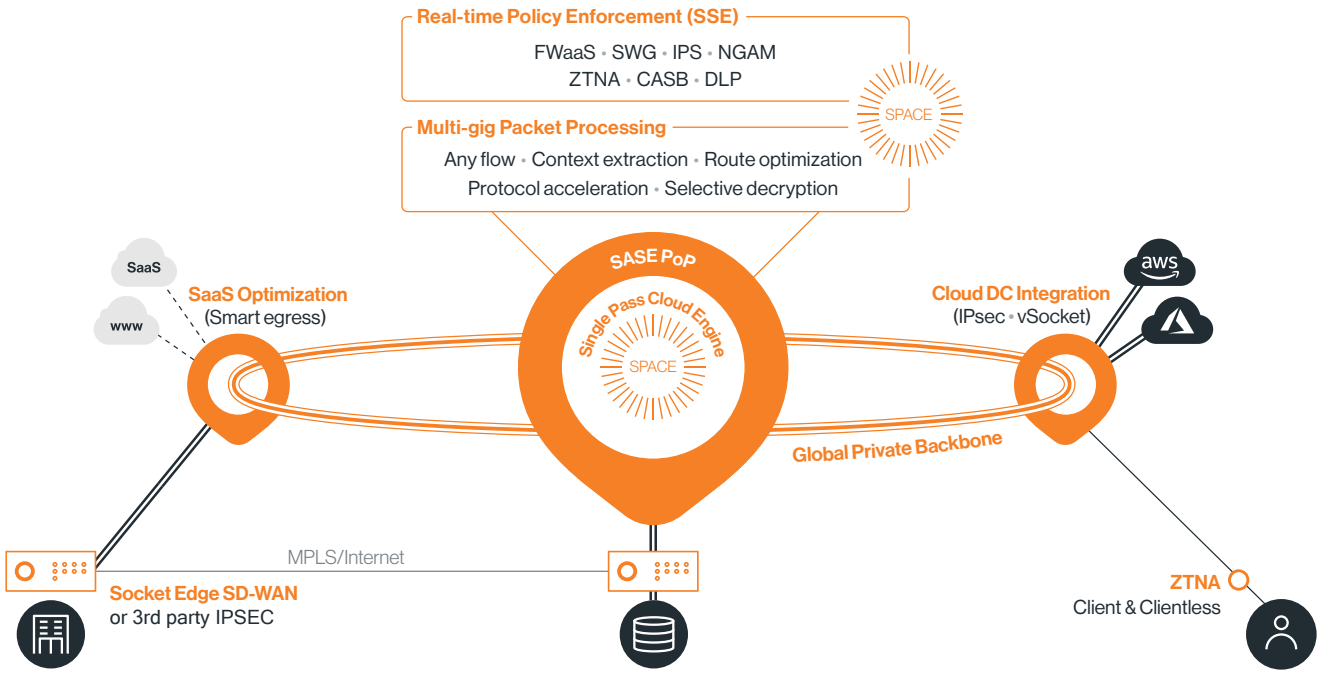
Our SSE controls and protects access to all edges—sites, mobile users and devices, and enterprise and cloud resources—in compliance with Zero Trust principles.



Why SSE from Windstream Enterprise

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.

SASE Cloud with SSE



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