CATO
NETWORKS

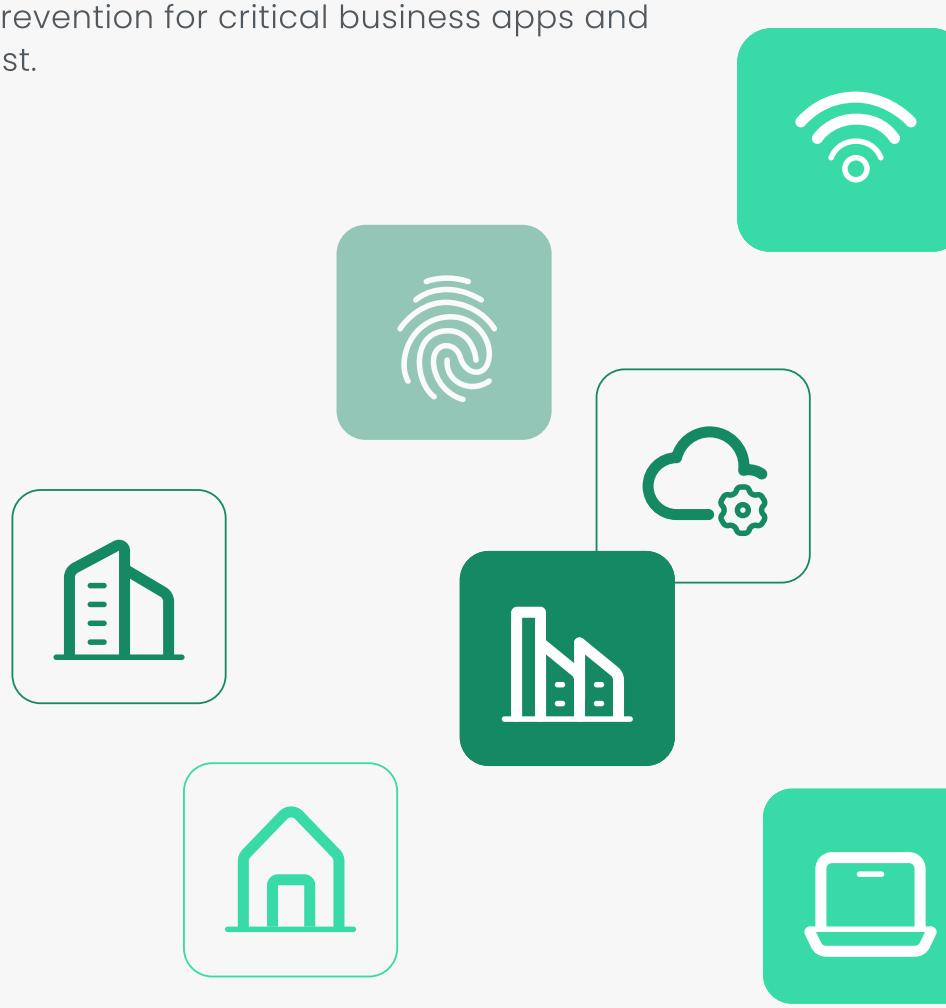
Deploying Zero Trust Security Using a SASE Platform

The Business Case for Zero Trust and SASE

The growth of cloud computing and work-from-anywhere (WFA) has introduced complex use cases that place pressure on an organization's security posture. This increased pressure on modern digital enterprises dictates new strategies for protecting sensitive business resources.

Gartner predicts that **by 2025, more than 60% of organizations will use Zero Trust** as the starting point for security. This re-evaluation is the driving force behind innovative approaches to enhanced security, with zero trust being one of them. Secure Access Service Edge (SASE) is another approach to overcoming legacy security architecture limitations.

SASE is a cloud-based security architecture consolidating network and security functions, including ZTNA (Zero Trust Network Access), into a single, global, cloud-native architecture. Implementing ZTNA within a SASE architecture helps to limit network entry points, providing identity-based access and advanced threat prevention for critical business apps and data. This is the core of zero trust.



Zero Trust Challenges

Zero trust represents a dramatic shift in how enterprises protect sensitive business resources, transitioning from implicit trust to identify-driven, data-centric access models. While it provides numerous benefits, many challenges remain that impact overall effectiveness. Integration is a major challenge because it must simultaneously maintain a consistent user experience while seamlessly integrating with existing architecture tools like:

- SIEM
- IAM
- EDR
- Numerous othersecurity tools

Another challenge is advanced threat prevention. Unfortunately, zero trust focuses on access security so preventing malware, zero-day threats, etc. is left to existing security tools. This risks inaccurate detection schemes and inconsistent enforcement for zero-trust traffic.

Performance will also impact the Zero Trust experience because most traffic is subject to the unreliable nature of the public internet. Encryption, authentication, and traffic inspection will impact this traffic, and latency-sensitive applications will suffer because of this.

Other challenges include scalability, policy management, and cost. While no individual challenge is a complete blocker, organizations face multiple challenges and this will disrupt their efforts, making full zero trust benefits difficult to achieve.

Zero trust secures access to business applications and resources, but gaps remain that do not address all challenges. These gaps leave organizations at risk and require a comprehensive architecture that consolidates multiple security technologies for full protection.

Zero Trust Deployment with a SASE Architecture

SASE compliments zero trust by providing a comprehensive, cloud-native architecture. It converges core technologies, provides consistent policy enforcement, and improves performance for an enhanced user experience.

SASE simplifies security while strengthening protections for business applications and data. It delivers threat prevention and trust across the entire enterprise without impacting user productivity, which is critical for zero trust.

Achieving the full benefits of zero trust depends on the chosen architecture deployed. There are different deployment approaches, but SASE stands out by delivering better outcomes. Deploying zero trust within a SASE architecture blends core Zero Trust principles with SASE's advanced security capabilities. These include:

Zero trust secures access to business applications and resources, but gaps remain that do not address all challenges. These gaps leave organizations at risk and require a comprehensive architecture that consolidates multiple security technologies for full protection.

- **Secure connectivity** via encrypted tunnels to ensure in-transit protection for all critical enterprise resources.
- **Dynamic policy enforcement** for real-time adaptation based on enterprise-defined criteria. This risk-based approach should enforce policies as close to the user or application as possible
- **Identity-based access control** takes advantage of the foundational element of zero trust (identity) and forms the basis for every secure action in SASE.
- **Least privileges and micro-segmentation** ensure the minimum permissions required to access specific resources. This reduces the attack surface and limits lateral movement.
- **Orchestration and automation** require a holistic view to ensure enforcement policies address security posture changes and reduce blind spots.

With SASE, it is easy to deliver these over a consistent architecture and ensure efficient security operations. While SASE architectures vary in deploying Zero Trust, it should take a risk-based approach to strengthening security that aligns with modern digital business demands.

Single-Vendor SASE Platform:

Holistic Zero Trust Security

Enterprises need simple access solutions that provide in-depth protection for all users, apps, and data and scales on demand with their business. They must align with Zero Trust principles, provide holistic threat prevention, and consistently enforce policies regardless of location.

A single-vendor SASE platform secures and optimizes access for everyone, everywhere. This is achieved by converging multiple security functions, including zero trust, into a single, cloud-native software stack with single-pass inspection. This provides a single contextual view of all traffic flows that only a true platform provides. This ensures all zero-trust traffic automatically receives advanced threat protection.

A common misunderstanding about zero trust is that it only applies to remote access. This overlooks physical office users and devices that require the same risk-based treatment as remote users, and a single-vendor SASE platform is uniquely architected to provide a consistent user experience. This is only possible because of three unique characteristics demonstrating the power of the SASE cloud platform: 1) Global Connectivity, 2) Holistic Threat Prevention, and 3) Unified Management at Scale.

Global Connectivity for Complete 360-degree Visibility

Visibility and control are necessary to provide complete security coverage. This requires a global private backbone built from the ground up to connect users, applications, and data regardless of location. For a single-vendor SASE platform, this backbone presents an innovative approach to improving enterprise networking and security. For zero trust with a single-vendor platform, this represents a risk-based approach to network access, least privileges, segmentation, and threat prevention.

Securing all users and applications from threats requires an in-depth layer of security visibility provided by a private backbone. This makes zero trust security possible by quickly and accurately identifying malicious activities to accelerate threat remediation.

This enhances the zero-trust experience and provides consistent enforcement for 360-degree security.

Reducing the Attack Surface with Holistic Threat Prevention

Threat prevention and reducing the attack surface are fundamental to zero trust security. This means limiting access with dynamic policies while employing threat prevention measures to block hidden or unknown threats. This is the basis of zero trust with SASE.

Single-vendor SASE platform goes beyond simple access security to seamlessly extend protections to all traffic. FWaaS controls traffic flow in all directions, enforcing core zero-trust principles everywhere. Advanced threat prevention provides real-time zero-day protection, while data protection tools implement identity-based access control policies.

Combining these security capabilities with single-pass scanning provides a single context for all zero-trust traffic. This enables simultaneous inspection and strengthens zero-trust policies. The result is risk-based access to specific applications and data, with consistent policy enforcement.

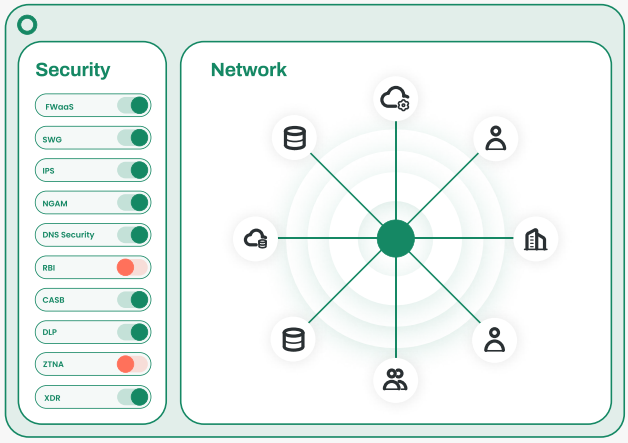
Unified SASE Platform Management

Managing security operations is extraordinarily complex and resource-intensive in mixed vendor environments. It makes correlating events and alerts a nightmare with most teams spending considerable time managing multiple technology stacks. Managing zero trust presents numerous challenges, including policy complexity when enforcement misaligns with other security tools. This impacts successful deployment.

A single-vendor SASE cloud platform, however, provides better security management because it handles all security through a single management application. All data is captured in a single repository for analysis, and the single dashboard streamlines policy management for all security. This provides IT teams full visibility to take appropriate actions to ensure zero-threat operations.

This is how zero trust with a single-vendor SASE was conceived and is a major benefit of a true platform approach.

Cato SASE Cloud Platform for Zero Trust



Cato SASE Cloud is the first and only single-vendor SASE platform purpose-built to converge network, security, and access technologies into a private global cloud network. This platform is built with enhanced tools to deliver flow control and segmentation, application and data protection, advanced threat prevention, and threat detection and response capabilities. This provides a consistent and secure user experience and is ideally suited to deliver advanced zero-trust security.

Cato's Single Pass Cloud Engine (SPACE), the core of the Cato SASE Cloud platform, enhances Zero trust. Via SPACE, all security technologies simultaneously process zero trust traffic flows to provide 360-degree visibility, control, and advanced threat prevention. This in-depth security inspection through SPACE utilizes techniques such as network and security enrichment, real-time machine learning, and threat intelligence feeds to produce a single context of all zero-trust activity. This ensures consistent, universal policy enforcement and provides an extra layer of security by ensuring all traffic is protected from zero-day threats. This provides continuous enterprise protection and helps mitigate all security risks across all physical, remote, and cloud locations. More details on Cato SPACE can be found here.

Managing zero trust and security deployments simple, regardless of the size is simple with Cato SASE Cloud Platform. It delivers current and future zero-trust security capabilities, with everything managed through a single Cloud Management Application. Policies are defined and seamlessly distributed across the entire SASE platform and Cato Clients for consistent global enforcement. Similarly, a single universal API can access all platform data to automate integrations with other business processes and 3rd party tools.

The Cato SASE Cloud is a future-proof, single-vendor platform designed to deliver on SASE's true promise. Its holistic on-demand threat prevention schemes and autonomous self-maintenance capabilities enable it to scale and adapt to technology innovation when businesses require it.

Learn more about Cato's SASE Cloud platform and how Cato enhances zero-trust security.

Cato's Single Pass Cloud Engine (SPACE), the core of the Cato SASE Cloud platform, enhances Zero trust. Via SPACE, all security technologies simultaneously process zero trust traffic flows to provide 360-degree visibility, control, and advanced threat prevention. This in-depth security inspection through SPACE utilizes techniques such as network and security enrichment, real-time machine learning, and threat intelligence feeds to produce a single context of all zero-trust activity. This ensures consistent, universal policy enforcement and provides an extra layer of security by ensuring all traffic is protected from zero-day threats. This provides continuous enterprise protection and helps mitigate all security risks across all physical, remote, and cloud locations. More details on Cato SPACE can be found here.

Managing zero trust and security deployments simple, regardless of the size is simple with Cato SASE Cloud Platform. It delivers current and future zero-trust security capabilities, with everything managed through a single Cloud Management Application. Policies are defined and seamlessly distributed across the entire SASE platform and Cato Clients for consistent global enforcement. Similarly, a single universal API can access all platform data to automate integrations with other business processes and 3rd party tools.

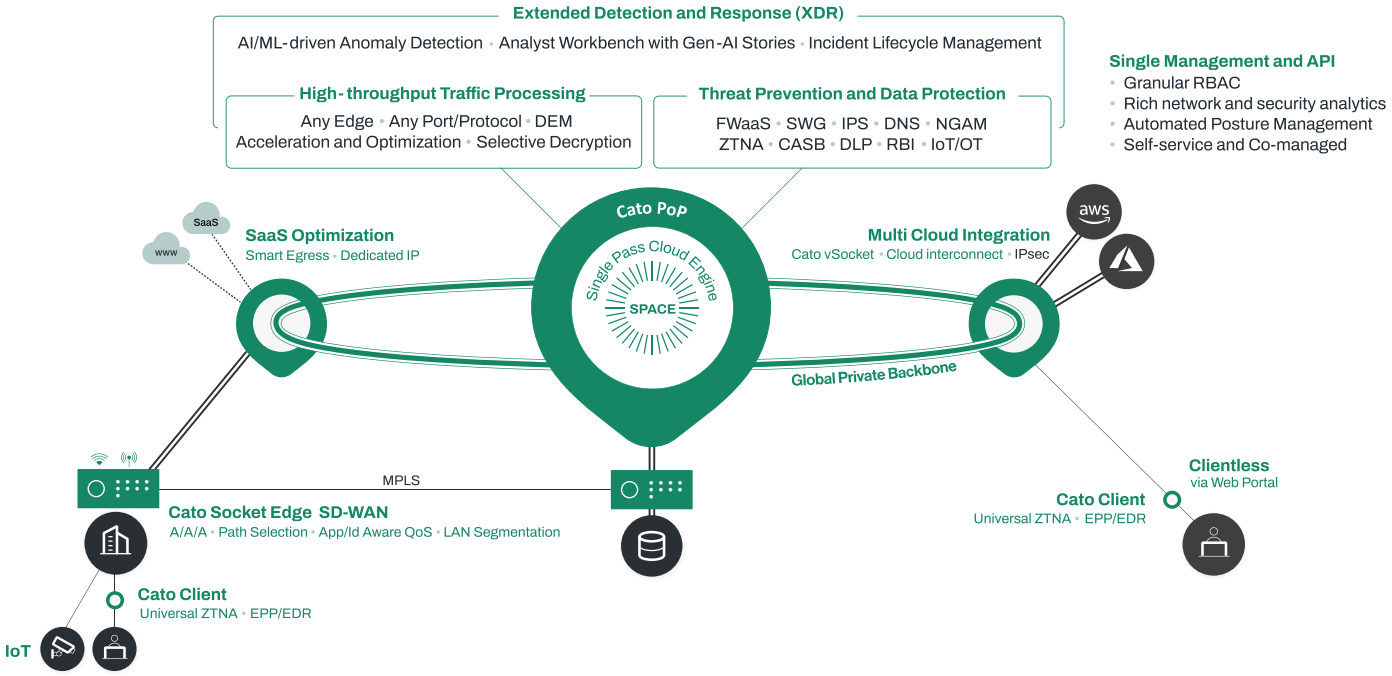
The Cato SASE Cloud is a future-proof, single-vendor platform designed to deliver on SASE's true promise. Its holistic on-demand threat prevention schemes and autonomous self-maintenance capabilities enable it to scale and adapt to technology innovation when businesses require it.

Learn more about Cato's SASE Cloud platform and how Cato enhances zero-trust security.

About Cato Networks

Cato Networks is the leader in SASE, delivering enterprise security and network access in a single cloud platform. With Cato, organizations replace costly and rigid legacy infrastructure with an open and modular SASE architecture based on SD-WAN, a purpose-built global cloud network, and an embedded cloud-native security stack.

Cato SASE Cloud Platform



Cato. WE ARE SASE.

Cato SASE Cloud Platform

Connect

Cloud Network

Cloud On-Ramps

Protect

Network Security

Endpoint Security

Detect

Incident Life Cycle Management

Run

Unified Management and API

Use Cases

Network Transformation

MPLS to SD-WAN Migration

Global Access Optimization

Hybrid Cloud & Multi-Cloud

Business Transformation

Vendor Consolidation

Spend Optimization

M&A and Geo Expansion

Security Transformation

Secure Hybrid Work

Secure Direct Internet Access

Secure Application and Data Access

Incident Detection and Response

Contact Us