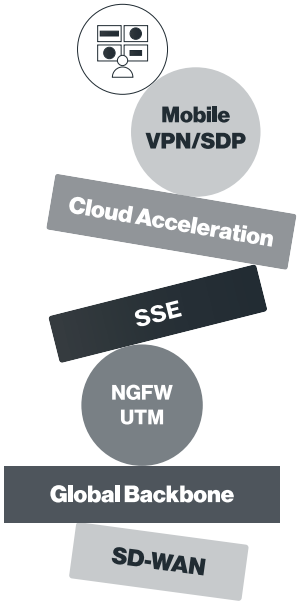
CATO
NETWORKS

Cato SASE Cloud: The World's Leading Single Vendor SASE Platform

Solution Brief

The Network and Security Challenges of Digital Transformation



Your business is going digital. It depends on optimized and secure global access to applications and data, on premises and in the cloud, and on an increasingly hybrid workforce. Rigid network and security architectures built with disjointed point solutions, 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 shortage of resources and scarcity of critical skills as well as the high cost of outsourced support. There must be a better way.

Digital business means a cloud-first, fast, and agile business, something that is incompatible with legacy telcos and network services.

Digital transformation pressures legacy architecture, IT resources because:

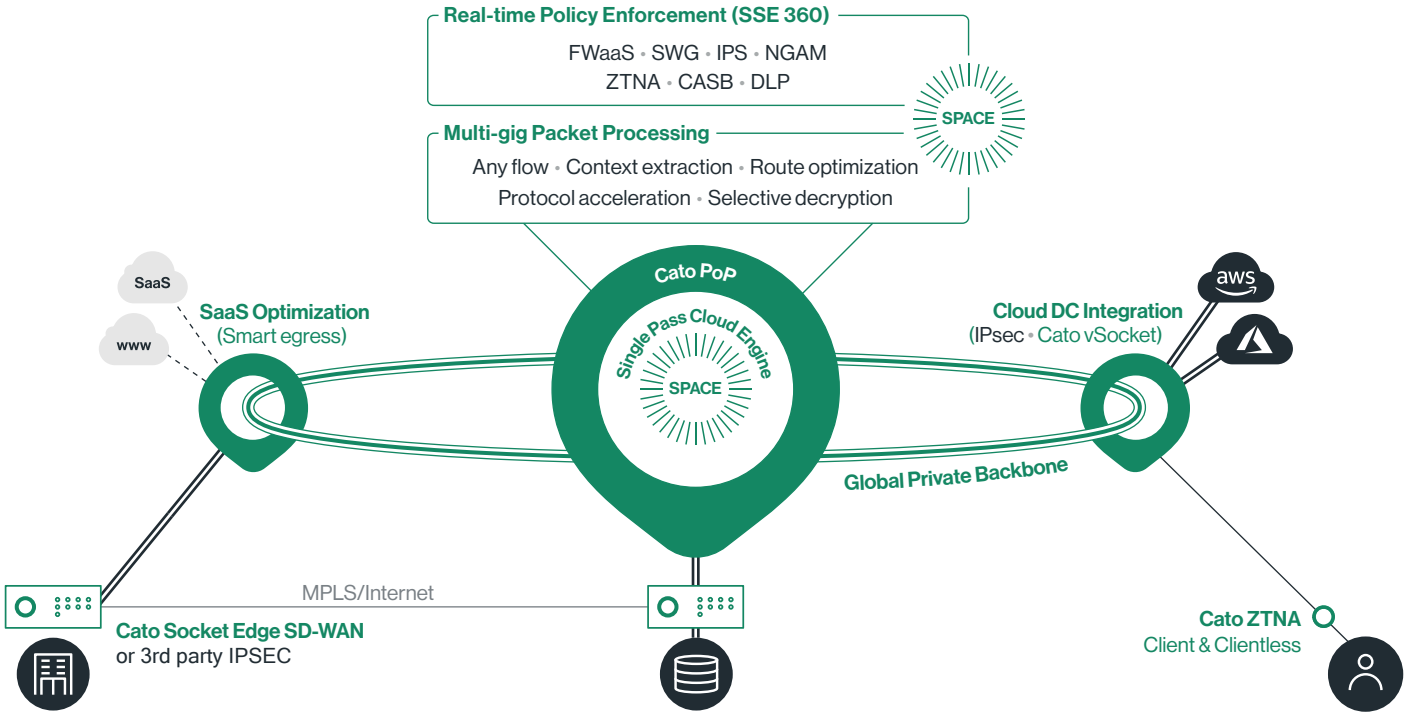
- **MPLS networks are built around a physical datacenter and WAN access.**
  The network must be rearchitected to encompass both WAN and Internet traffic to support the cloud DCs and applications along with big capacity increase.
- **Centralized (backhauling) security model creates a chokepoint for secure cloud access.**
  Direct secure Internet access at the branch must be enabled while extending full security capabilities to all branches and users.
- **The legacy WAN doesn't extend beyond physical locations.**
  Supporting the hybrid workforce to accommodate work from anywhere requires a flexible architecture that is user- and location-centric.
- **Disjointed solutions increase complexity, IT workload and security risk with fragmented management and expanded attack surface.**
  Increasing agility and improving responsiveness require solution consolidation. And, convergence into the cloud, with self-healing and self-maintaining architecture can help reduce the load on IT. There is no way to escape complexity: either you bear the costs and the business impact, or you pay outsourced service providers. Either way, underlying complexity is the root cause of rigidity and slow responsiveness.

The World's First SASE Platform

The world's first single-vendor SASE platform, converging SD-WAN and network security into a global cloud-native service.

Cato is the first single-vendor implementation of the Gartner secure access service edge (SASE) framework, which identified a global and cloud-native architecture as the way to deliver secure and optimized access to all users and applications. With Cato, enterprises move from legacy networks built with point solutions and expensive MPLS services to modern networks that are global, secure, agile, and affordable.

Cato SASE Cloud connects all enterprise network resources, such as branch locations, the mobile workforce, and physical and cloud datacenters, into a global and secure, managed SD-WAN service. With all WAN and Internet traffic consolidated in the cloud, Cato applies a suite of security services to protect all traffic at all times.



Global Private Backbone

The Cato global private backbone is comprised of 75+ PoPs worldwide servicing customers in 150+ countries. All PoPs are interconnected by multiple SLA-backed tier-1 providers, and every PoP runs Cato's cloud-native software stack. It's fully multitenant, scalable, and ubiquitous, performing in a single pass all network functions — such as global route optimization, dynamic path selection, traffic optimization, and end-to-end encryption — as well as implementing the inspection and enforcement functions needed by Cato security services.

WAN Optimization

WAN optimization is an integral part of the network software stack, utilizing TCP proxies and advanced congestion management algorithms to maximize throughput in key operations, such as file transfers.

Global Route Optimization

Cato's proprietary routing algorithms factor in latency, packet loss, and jitter. Unlike Internet routing, Cato routing always favor performance over cost, selecting the optimal route for every network packet.

Encryption

End-to-end encryption, using the strongest industry-standard cipher suites, assures data confidentiality, privacy and secure multitenancy.

Self-healing Architecture

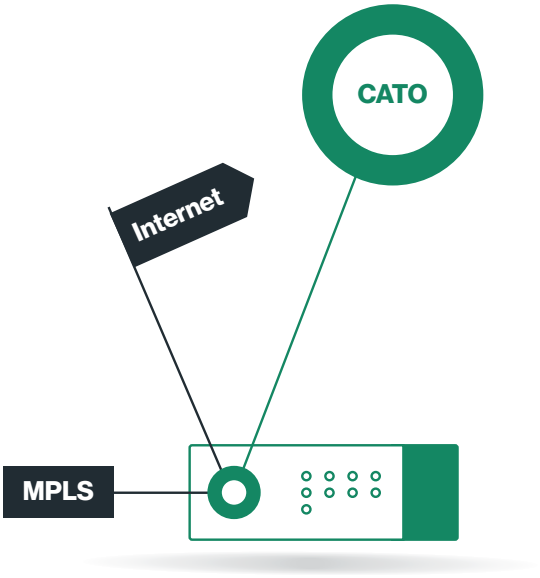
The Cato backbone is continuously monitored and measured. Self-healing capabilities guarantee 99.999% service availability. Elastic, scale-up cloud software design principles assure seamless service infrastructure growth without service downtime or disruptions.

Locations connect to the Cato global, private backbone by establishing encrypted tunnels from a Cato Socket, Cato's zero-touch, edge SD-WAN appliance, or any device that supports IPsec tunnels. Cloud datacenters connect through an agent or agentless configuration; mobile users connect clientless or by running a Cato Client.

Edge SD-WAN

Cato Edge SD-WAN works with multiple Internet circuits, providing reliable, high-performance access to Cato's global, private backbone. Traffic can also be routed over MPLS, directly between sites (not through the Cato PoP), and across IPsec tunnels to third-party devices.

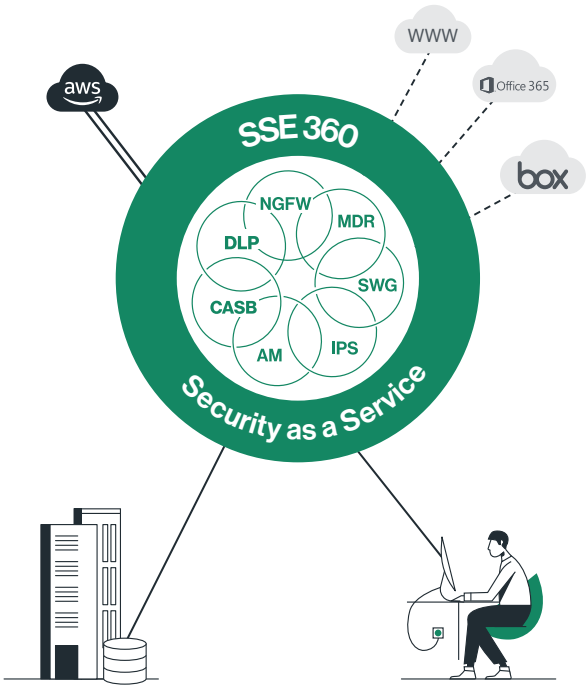
The Cato Socket, Cato's Edge SD-WAN device, is a zero-touch device ready to work in minutes once it has power and Internet connectivity. Sockets come in two models: X1500 for branch offices and X1700 for datacenters. Both are continuously monitored and updated by Cato's network operations center (NOC).



Cato Sockets include:

- **Link Aggregation** that balances inbound and outbound traffic across MPLS and multiple Internet circuits (fiber, DSL, cable, 4G/LTE or 5G) to maximize bandwidth (active/active) and availability.
- **Dynamic Path Selection** that routes traffic across the optimum transport based on application, user, and real-time link quality (jitter, latency, and packet loss).
- **Application Identification** that uses Cato's advanced Deep Packet Inspection (DPI) engine to automatically identify thousands of applications and millions of domains on the first packet.
- **Bandwidth Management Rules** ensure that more critical applications always receive the necessary upstream and downstream capacity, serving other applications on a best-effort basis.
- **Packet Loss Mitigation** techniques dynamically switch traffic to alternate, better performing link(s) and proactively duplicate packets on a per application basis. Cato's architecture eliminates middle-mile packet loss.
- **Routing Protocol Integration** that leverages BGP to make informed real-time routing decisions, easily integrating a company's existing routing infrastructure with Cato Edge SD-WAN.
- **High Availability (HA)** that carries no additional recurring charge and deployment is simple and completed in minutes. Sockets automatically connect to the best available Cato PoP. Should the connection degrade or fail, the Cato Socket automatically reconnects to the best available PoP.

Security Service Edge (SSE)



Cato SASE Cloud is powered by a cloud-native security service edge (SSE), Cato SSE 360. Cato SSE 360 is built using the Cato Single Pass Cloud Engine (SPACE) architecture and converges the following capabilities: Secure Web Gateway (SWG), Cloud Access Security Broker (CASB), Data Loss Prevention (DLP), Zero Trust Network Access (ZTNA), and Firewall as a Service (FWaaS) with Advanced Threat Prevention (IPS, Next Generation Anti-malware), which is managed by the Cato SOC (Security Operations Center). These security capabilities form the basis of a comprehensive Managed Threat Detection and Response (MDR) service that is provided as part of Cato's managed services offering. All capabilities seamlessly scale to process all customer traffic, encrypted and unencrypted, without the need for sizing, patching, or upgrading appliances and point solutions. Cato protects user privacy and fully complies with GDPR. Inspected data is never stored on Cato servers or shared with third-parties. Customers are able to exclude privacy-sensitive applications, such as banking and healthcare, from inspection. In addition, Cato complies with SOC 1 and 2, and ISO 27001, 27017, 27701, and 27018.

Next-generation Firewall

The Cato NGFW operates across every Cato PoP, protecting the entire organization with a unified application-aware and user-aware security policy — all without the cost and complexity of upgrading and maintaining individual firewall appliances. Cato's NGFW uniquely provides:

- **Complete visibility,** inspecting all WAN and Internet traffic for fixed and mobile users. There are no blind spots, no need to deploy multiple security appliances or tools.
- **Unlimited scalability,** applying security policies and inspecting any traffic mix (encrypted and unencrypted) at line rate. We ensure processing power and network capacity always meet committed service levels.
- **Unified security policy,** enforcing one granular policy and rule base that extends from one user to the entire business. The rule base is common to all security functions and traffic types. There is no need to associate policies with distinct appliances or point products.
- **Simple lifecycle management,** eliminating the need to size, upgrade, patch or refresh firewalls. Customers are relieved of the ongoing grunt work of keeping their network security current against emerging threats and evolving business needs — or being forced into paying more so their telco will do it for them.

Secure Web Gateway

Secure Web Gateways (SWGs) protect against phishing, malware, and other Internet-borne threats. Cato converges SWG with NGFW, eliminating the need to maintain policies across multiple point solutions and the appliance life cycle. Cato's integrated SWG provides dynamic site categorization, which includes an always current URL database enriched with information about phishing threats, malware delivery, botnets, and other malicious content. Customers can set and enforce one set of web access policies for mobile and fixed users based on visibility into user activity, reducing organizational risk.

Cloud and Data Security

Cato's SASE Cloud enables enterprises to gain better visibility and control over their cloud-hosted applications. Cato's Cloud Access Security Broker (CASB) provides in depth visibility into SaaS usage and enables IT leaders to better cope with shadow IT. Cato's Data Loss Prevention (DLP) enables granular control over the extraction of sensitive enterprise information in order to protects form potential data breaches.

Cloud Access Security Broker (CASB)

Cato's CASB provides IT managers with comprehensive insight into their organisation's cloud application usage, covering both sanctioned and unsanctioned (Shadow IT) applications. Cato's CASB enables assessment of each SaaS application in order to evaluate its potential risk, and definition of highly granular and flexible access rules to ensure least privileges and minimal risk exposure.

Data Loss Prevention (DLP)

Cato's Data Loss Prevention (DLP) enables enterprises to protect sensitive information from being uploaded to, or extracted from, cloud or physical datacenters. The solution inspects traffic to detect sensitive data or file types and takes the defined action when a match is found. DLP helps enterprises achieve regulatory compliance, for example with the General Data Protect Regulation (GDPR), by detecting Private Identifiable Information (PII), as well as with industry specific standards such as Payment Card Industry (PCI) and Health Insurance Portability and Accountability Act (HIPAA).

Advanced Threat Prevention

Advanced Threat Prevention is a collection of network security and related defenses deployed to address current and emerging threats. IT organizations face the daunting task of maintaining complex infrastructure to identify and prevent advanced threats from penetrating the network. Cato Advanced Threat Prevention solves that problem, inspecting encrypted and unencrypted traffic at line rate for malware and network-based threats.

TLS Inspection

With most Internet traffic encrypted, detecting and preventing threats delivered within SSL/TLS traffic is critical. However, inline SSL/TLS traffic inspection consumes significant processing resources. Appliance-based security solutions face resource limitations as their hardware is often inadequate, forcing hardware upgrades outside of the budgetary cycle. As noted, Cato security services benefit from infinite compute power of cloud. Cato inspects all TLS-encrypted traffic flows without impact on user experience or application performance.

Malware Protection

Cato's network-based malware protection leverages multiple, multilayered and tightly-integrated anti-malware engines running in all Cato PoPs. The first layer includes a signature and heuristics-based inspection engine, which is kept up-to-date at all times based on global threat intelligence databases, scans files in transit across the Cato backbone to protect against known malware. The second layer applies proven machine-learning algorithms from SentinalOne to identify and block unknown malware, such as zero-day attacks or polymorphic variants of known threats that are designed to evade signature-based inspection engines. With both layers, connected endpoints are deeply protected against network-delivered malware.

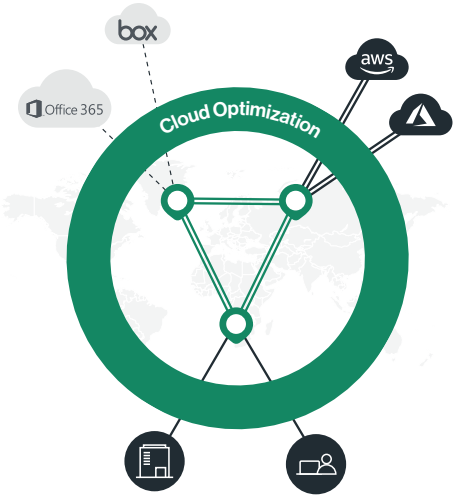
Intrusion Prevention

Cato's IPS leverages multiple layers and technologies to block network attacks. **Network protocol validation** detects protocol manipulations and malformed packets. **Context-aware signatures and rules** block attacks based on known CVEs, unknown attacks based on network traffic behavior, and network scans. Internal and external **reputation feeds** enrich IPS intelligence. **Geographic-based restrictions** minimize the threat landscape.

Legacy IPS technology requires extensive skills and management effort. IT teams need to evaluate new signatures, determine which ones to activate, validate they won't disrupt the business, and consider the performance impact on the IPS appliance and the network. Those concerns simply don't exist with Cato IPS. Like all Cato security services, the Cato Security Research Lab and SOC manage the Cato IPS for you and ensure appropriate rules are applied against emerging threats with the proper validation and capacity analysis. Activation is simple. Cato customers only need to enable the IPS from their management console to benefit from its prevention power.

Cloud Access and Optimization and Remote Access

Cloud Datacenter Integration

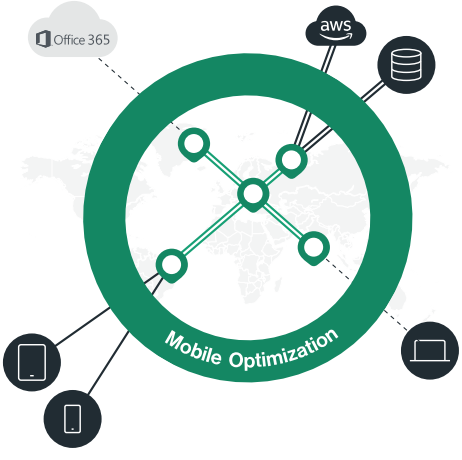


Cato tightly couples cloud datacenters into the SD-WAN, effortlessly. All cloud providers — Amazon AWS, Microsoft Azure, Google Cloud, and others — connect into the Cato global private backbone by establishing redundant IPsec tunnels, which typically only have to cross the physical datacenter shared with the Cato PoP. In this way, Cato delivers the optimum cloud experience. Cloud datacenter traffic routes over the optimum path across the Cato global private backbone to the Cato PoP. From there, traffic is typically sent across the datacenter network to the cloud datacenter. This architecture eliminates the need for premium cloud connectivity services, such as AWS DirectConnect or Microsoft Azure Express Route.

The integration is **agentless, requiring no virtual appliances.** For those who prefer a virtual appliance, Cato also offers its vSocket. Agentless configuration leverages the IPsec gateway connectivity available from all cloud providers avoids additional VM costs as well as the risk of modifying production server network configurations. Like all other traffic, cloud datacenter traffic is subject to full security inspection by Cato security services.

Cloud Application Acceleration

Cato also improves public cloud application performance, such as Office 365, Cloud ERP, UCaaS, and Cloud Storage. Latency is reduced by optimally routing cloud application traffic across Cato's global, private backbone to the Cato PoP closest to the cloud application provider's datacenter. Cato's built-in WAN optimization maximizes end-to-end throughput to improve application performance, especially around bandwidth-intensive operations, such as file transfers. All traffic and files exchanged with the cloud application are subject to full security inspection within the Cato SASE Cloud.



Secure Remote Access

Cato extends the full range of its network and security capabilities down to remote and mobile users. Using a Cato Client or clientless browser access, users connect to the nearest Cato PoP and their traffic is routed optimally over the Cato global private backbone to applications on on-premises or in the cloud.

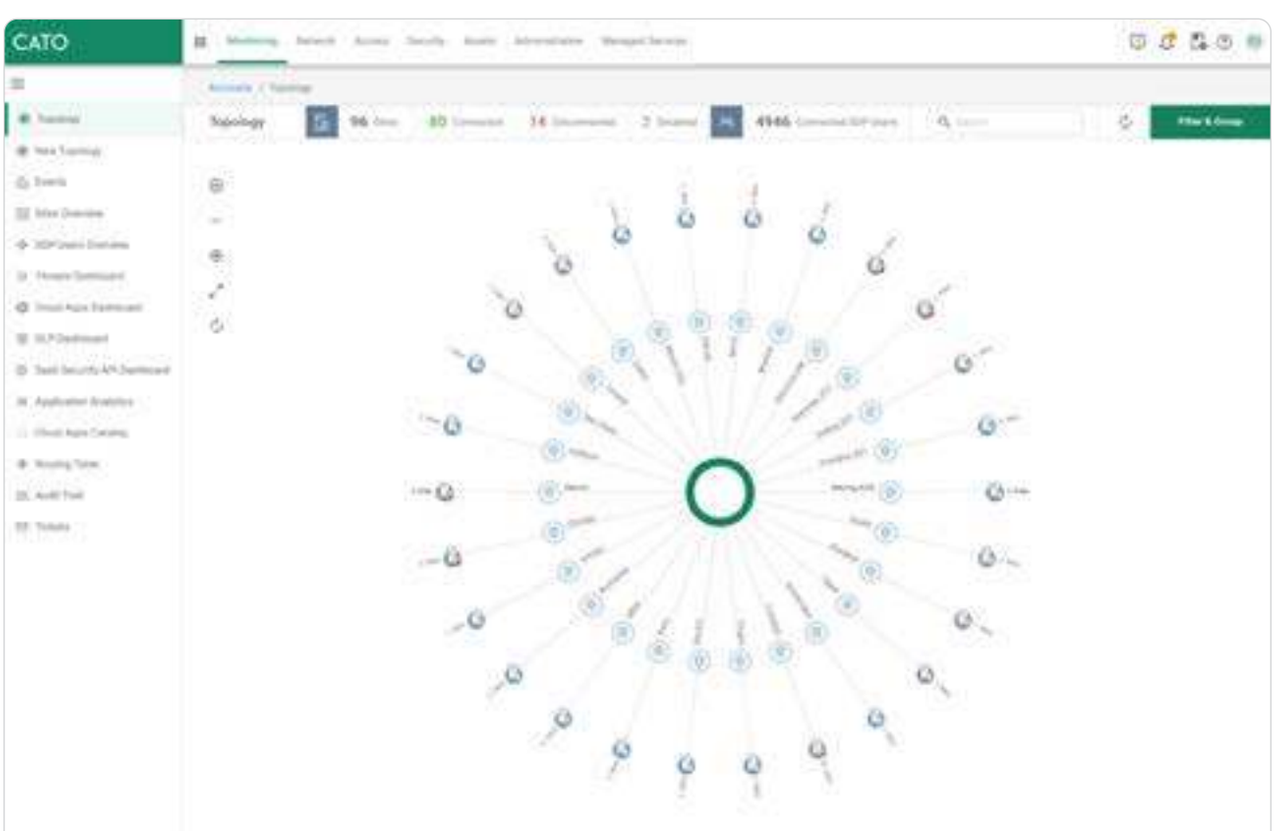
Cato provides remote and mobile users with Zero Trust Network Access (ZTNA/SDP), allowing the most granular user access control down to specific applications. By contrast, legacy VPN solution limit access to entire subnets. All user activity is protected by Cato's built-in network security stack, ensuring enterprise-grade protection to all users everywhere.

Cato Management Application

Cato provides customers with a self-service management application for events, analytics and policy configuration. As applicable, Cato or its partners offer managed service options including site deployment, intelligent last-mile monitoring, configuration of network and security policy changes, and managed detection and response (MDR).

- **The Cato management console combines power and simplicity.** Administrators define granular network and security policies without a long learning curve or repetitive manual operations now simplified by an intent-driven user interface.
- **Real-time and historical, analytics and reports** provide comprehensive network visibility, solving key challenges of access control, user experience, troubleshooting, and shadow IT.
- **Collection and delivery of full network and security event logs** to external analysis solutions like SIEM is available, with a unique benefit of using a single interface for all events rather than manually aggregating data from multiple appliances and sources.

The management application is web-based and accessible over the Internet with multi-factor authentication. All access and configuration changes are recorded in a centralized audit log.



Cato's management console provides a single-pane-of-glass, showing all connected sites, cloud resources, and users.

Use Cases

MPLS Migration to SD-WAN/SASE

Cato enables customers to move away from expensive, rigid, and capacity constrained MPLS to a high-capacity and resilient modern network. Using Cato Edge SD-WAN and multiple Internet links, customers boost capacity and improve resiliency for lower cost per Mbps. Customers with a global footprint leverage Cato's affordable global private backbone to replace global MPLS services to reduce cost, meet service levels, improve performance, and deliver security everywhere. Ultimately, most customers can increase capacity, resiliency, and improve overall network performance and security with the same network spend.

Secure Direct Internet Access

Cato provides a cloud-native security service edge, Cato SSE 360, converged into the Cato SASE Cloud. By connecting all locations and users to Cato SASE Cloud through Cato edge SD-WAN devices and Cato SDP Clients, all traffic, both Internet and WAN, is fully protected by Cato SSE 360. With Cato, customers can eliminate or avoid the cost and complexity of multiple firewall appliances and standalone cloud security services.

Work From Anywhere

Cato extends global networking and security capabilities down to a single user's laptop, smartphone, or tablet. Using a Cato SDP Client or clientless browser access, users dynamically connect to the closest Cato PoP, and their traffic is optimally routed over the Cato global private backbone to on-premises or cloud applications. Cato SSE 360 enforces granular application access policies, protects all users against threats, and prevents data loss. Customers use Cato to eliminate the cost and complexity of point solutions including appliances and cloud-based security services such as VPN, Firewalls, CASB, and Secure Web Gateways.

Sensitive Data Security

Cato SSE 360's CASB and DLP capabilities enable full visibility and control of sensitive data. Cato enforces granular policies on data access from corporate and BYOD devices and data sharing across applications. With Cato, customers can reduce the risk of sensitive data loss and reputation risk, and better comply with regulatory requirements.

Gradual Cloud Migration

Cato easily connects physical and cloud datacenters to Cato SASE Cloud and optimizes access to public cloud apps. Traffic is inspected by Cato SSE 360 and optimized using Cato's 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 Cato, customers can eliminate premium cloud connectivity solutions like AWS DirectConnect and Microsoft ExpressRoute.

Global Application Access

Cato SASE Cloud leverages Cato's a global private backbone with built-in WAN and cloud optimization to deliver an SLA-backed, predictable, and high-performance application access everywhere. Customers that suffer from poor application access for remote locations and users, use Cato to deliver a great user experience for both on-premises and cloud application access.

Cato SASE Cloud: Complete WAN Transformation

Cato is the world's first single-vendor SASE platform, converging SD-WAN and SSE into a global, cloud-native service. Cato optimizes and secures application access for all users and locations, including branch offices, mobile users, and cloud datacenters, and allows enterprises to manage all of them with a single management console with comprehensive network visibility. Cato's SASE platform has all the advantages of cloud-native architectures, including infinite scalability, elasticity, global reach and low total cost of ownership.

Connecting locations to the Cato SASE Cloud is as simple as plugging in a preconfigured Cato socket appliance, which connects to the nearest of Cato's 75+ globally dispersed points of presence (PoPs). Mobile users connect to the same PoPs from any mobile device via a simple piece of software that is easy to install and use. With Cato, new locations or users can be up and running in hours or even minutes, rather than days or weeks.

At the local PoP, Cato provides an onramp to its high-performance global private backbone and security services. Cato monitors traffic and selects the optimum path for each packet across the backbone for performance that is as good or better than legacy MPLS. Since mobile users run across the same backbone as all other resources, the remote access experience is no different from working at the office.

With Cato, customers can easily migrate from MPLS to SD-WAN, optimize global connectivity to on-premises and cloud applications, enable secure branch office Internet access everywhere, and seamlessly integrate cloud datacenters and mobile users into a high-speed network with a zero trust architecture.

Whether its mergers and acquisitions, global expansion, rapid deployments, or cloud migration, with Cato, the network and your business are ready for whatever is next in your digital transformation journey.

Cato SASE Cloud

- SSE 360
- Secure Remote Access
- Edge SD-WAN
- Global Private Backbone
- Multi-cloud / Hybrid-cloud
- SaaS Optimization
- Cato Management Application

Use Cases

- MPLS Migration to SD-WAN
- Secure Remote Access
- Secure Branch Internet Access
- Optimized Global Connectivity
- Secure Hybrid-cloud and Multi-cloud
- Work From Home

Cato. Ready for Whatever's Next.

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