



Cato Solution Brief

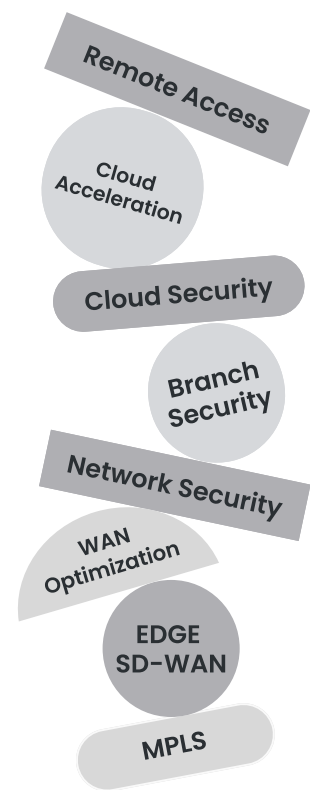


The Network and Security Challenges of Digital Transformation

Your business is now AI-powered and digital-first. It depends on optimized, secure global access to applications, data, and AI services across on-premises, cloud, and edge environments for an increasingly hybrid workforce. Rigid, appliance-centric network and security stacks stitched from point solutions cannot keep pace with dynamic AI workloads, continuous

The result is lower business agility and increased risk, made worse by a shortage of resources and scarcity of critical skills, as well as the high cost of outsourced support. All this legacy burden leads to increased technical debt.

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 strains legacy architecture and IT resources because:

- Disjointed point solutions now amplify operational drag, overloading IT and widening the attack surface with fragmented, inconsistent controls. To increase agility and responsiveness, CIOs must consolidate and converge into cloud-delivered, self-healing, self-maintaining architectures that abstract underlying complexity rather than merely outsourcing it.
- Legacy networks are built around a physical data center and WAN access. However, modern business needs require a resilient network platform that encompasses LAN, WAN, the Internet, and the Cloud to support cloud DCs, SaaS, and enterprise applications, while also enabling significant capacity increases.
- A hub-and-spoke security model inhibits SaaS, AI, and cloud access, degrading experience and resilience. Branches, remote users, and edge locations need local, identity-aware Internet access with full SSE/SASE controls consistently enforced everywhere.
- Legacy WANs were not designed for an AI-era workforce that moves across homes, offices, and edges. Today, architectures must be identity-, device-, and posture-centric, delivering secure, optimized access from anywhere as the default state, not the exception.

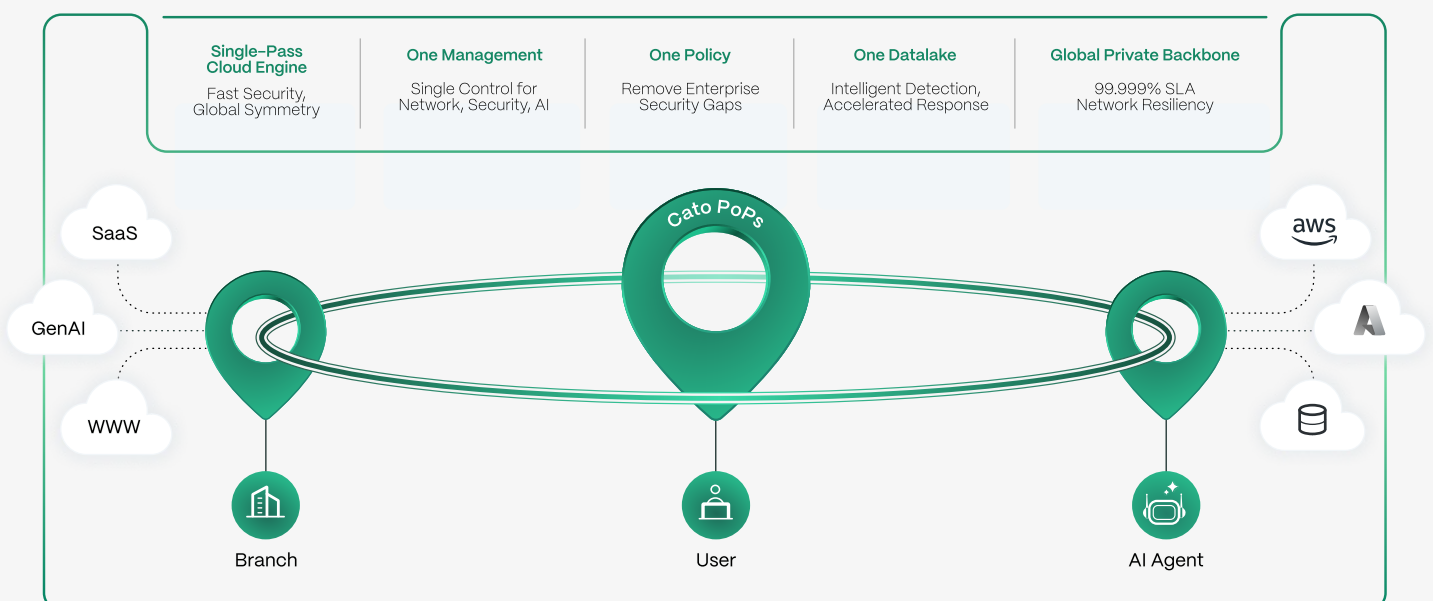
The World's First SASE Platform

The world's first single-vendor SASE platform, converging SD-WAN, SSE, Universal ZTNA, AI Security, XDR, AIOps, DEM, EPP in to a global cloud-native architecture. Each consumed on its own and yet leveraging the power of a platform..

Cato was the first single-vendor implementation of the Gartner secure access service edge (SASE) framework, which identified global, cloud-native platforms as the way to deliver secure, optimized access to all users and applications. With Cato, enterprises can modernize their network architectures with a global, secure, agile, and affordable platform that future-proofs their business.

The Cato SASE Platform connects every enterprise resource, branches, hybrid workers, data centers, clouds, and edges, through a global, secure, cloud-native SD-WAN platform. By converging WAN and Internet traffic into a single, AI-driven security and networking platform, Cato delivers continuous, enterprise-grade protection and optimized access for all users, applications, and locations, everywhere.

The Cato SASE Platform



Global Private Backbone

The Cato global private backbone is comprised of 85+ PoPs worldwide servicing customers in 200+ 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.

Cato SASE Cloud Global Private Backbone of 85+ PoPs



North America (27):

Ashburn, VA
Atlanta, GA
Austin, TX
Boston, MA
Charlotte, NC
Chicago, IL
Cincinnati, OH
Dallas, TX
Denver, CO
Detroit, MI
Honolulu, HI
Houston, TX
Kansas City, MO
Las Vegas, NV
Los Angeles, CA
Miami, FL
Minneapolis, MN
New York, NY
Phoenix, AZ
Portland, OR
Salt Lake City, UT
Santa Clara, CA
Seattle, WA
Calgary, CA
Montreal, CA
Toronto, CA
Vancouver, CA

Europe (21):

Vienna, AT
Brussels, BE
Prague, CZ
Copenhagen, DK
Helsinki, FI
Marseille, FR
Paris, FR
Frankfurt, DE
Munich, DE
Dublin, IE
Milan, IT
Rome, IT
Oslo, NO
Warsaw, PL
Bucharest, RO
Spain, Madrid
Stockholm, SE
Zurich, CH
Amsterdam, NL
London, UK
Manchester, UK

Asia (22):

Melbourne, AU
Perth, AU
Sydney, AU
Beijing, CN
Shanghai, CN
Shenzhen, CN
Urumqi, CN
Hong Kong, HK
Chennai, IN
Mumbai, IN
New Delhi, IN
Jakarta, ID
Osaka, JP
Tokyo, JP
Kuala Lumpur, MY
Auckland, NZ
Manila, PH
Seoul, KR
Singapore, SG
Taipei, TW
Bangkok, TH
Ho Chi Minh City, VN

Latin America (10):

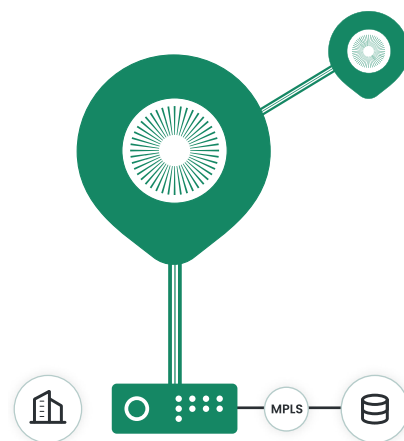
Buenos Aires, AR
Fortaleza, BR
Sao Paulo, BR
Santiago, CL
Bogota, CO
San Jose, CR
Quito, EC
MexicoCity, MX
Monterrey, MX
Lima, PE

Middle East & Africa (6)

Tel Aviv, IL
Nairobi, KE
Casablanca, MAR
Lagos, NG
Johannesburg, SA
Dubai, UAE

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 backbone), 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 three series: XI500 and XI600 for branch offices, and XI700 for datacenters. All are continuously monitored and updated by Cato's network operations center (NOC).



Features and benefits 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.

Zero Trust Security (SSE)



Cato SASE Cloud is powered by cloud-native security service edge (SSE), Cato Zero Trust Security. Cato Zero Trust Security 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)
- Firewall as a Service (FWaaS) with Autonomous Policies
- Threat Prevention (IPS, DNS, NGAM, Threat Intelligence, TLSi, AI/ML anti-phishing)
- Advanced Threat Prevention (TP, Dynamic Prevention, Sandboxing and RBI)
- All 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 can exclude privacy-sensitive applications, such as banking and healthcare, from inspection. In addition, Cato complies with PCI 4.0, SOC 2, and ISO 27001, 27017, 27701, and 27018.

Features and benefits include:

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:

- **AI-driven policy optimization** performs continuous ruleset analysis to autonomously identify misused and expired rules. This reduces policy sprawl, ensures Zero Trust enforcement, simplifies audits, and sustains compliance, with no added overhead for security teams.
- **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.
- **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.
- **Complete visibility**, inspecting all LAN, WAN, and Internet traffic for fixed and mobile users. There are no blind spots, no need to deploy multiple security appliances or tools.
- **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.

Secure Web Gateway

Secure Web Gateways (SWGs) protect against phishing, malware, and other Internet-born 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 CASB provides depth visibility into SaaS usage and enables IT leaders to better cope with Shadow IT. Cato's DLP enables granular control over the extraction of sensitive enterprise information in order to protect from potential data breaches.

- **Cloud Access Security Broker (CASB)** Cato's CASB provides IT managers comprehensive insight into their organization's cloud application usage, covering sanctioned and unsanctioned (Shadow IT) applications. It enables the assessment of each application to evaluate its potential risk and define highly granular and flexible access rules to ensure the least privileges and minimal risk exposure. Using both inline inspection and APIs enables a comprehensive assessment of a SaaS application to evaluate its potential risk to the enterprise. Highly granular and flexible access rules are defined to ensure the least privileges and minimal risk exposure. Behavioral analytics (UEBA) adds another layer of protection against rogue users.
- **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 Protection 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.

Features and benefits include:

- **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. Safe TLS Inspection is Cato's automated, data-driven approach to decrypting and inspecting only traffic that is safe to inspect, enabling full threat prevention, CASB, and DLP coverage without breaking applications or require manual bypass management. Cato inspects all TLS-encrypted traffic flows without impact on user experience or application performance.
- **Intrusion Prevention** Cato IPS uses layered defenses to block network attacks. It validates protocols to detect malformed or manipulated traffic and applies context-aware signatures to stop exploits tied to known CVEs, suspicious behaviors, and network scans. Internal and external reputation feeds enhance detection, while geo-based controls reduce exposure. Unlike legacy IPS, which requires constant signature tuning, performance checks, and risk validation, Cato IPS is fully managed by the Cato Security Research Lab and SOC. Rules are validated, optimized, and updated automatically. Customers simply enable IPS in the Management Application to gain immediate protection.
- **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 always updated 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 SentinelOne 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. Cato Sandbox provides detailed forensic reports for security teams needing in-depth malware investigation, enhancing threat intelligence and response.
- **Sandboxing** Cato Sandbox automatically sends any suspicious or malicious files for sandbox analysis, executing them in a controlled, isolated environment. This generates rich, detailed forensic reports, including Indicators of Compromise (IOCs) and insights into attack behavior. Security teams can download these reports directly from the Cato Management Application (CMA) to accelerate incident response and enhance forensic investigations, improving their ability to detect, analyze, and mitigate advanced threats.

- **Dynamic Prevention**

Cato Dynamic Prevention correlates network behavior across hosts and networks to identify risky patterns over time. By linking signals that seem benign on their own, it detects behavior-based threats that point-in-time inspection misses. When risk conditions are met, it automatically enforces restrictions. Policies adapt as behavior changes, stopping advanced threats earlier and reducing dwell time. Built natively into Cato's Single Pass Cloud Engine (SPACE), Dynamic Prevention creates a context-based baseline for every network entity and delivers inline, real-time prevention at scale. It requires no agents or additional tools. The result is stronger prevention, fewer false positives, and less investigation effort for IT and SOC teams.

- **Remote Browser Isolation**

The Remote Browser Isolation (RBI) service provides secure browsing by streaming web pages through a virtualization layer to the user's device. Page code is executed remotely, keeping users safe from ransomware, phishing and other threats. The RBI gives IT managers an 'Isolate' option that lets users browse unknown sites safely, rather than disrupt productivity by blocking. It adds another layer of protection against new sites and attacks that are not yet documented, and user error.



AI Security

Cato AI Security secures and governs every AI interaction across the enterprise. Available as a standalone solution or as part of the Cato SASE Platform, it provides governance, data protection, and runtime policy enforcement across the tools employees use and the applications organizations build. As organizations adopt third party AI tools, homegrown AI-powered applications, and AI agents, security teams need visibility and control that traditional web and cloud security controls are not built to provide. Cato AI Security extends the same centralized visibility, policy enforcement, and reporting that teams already use for network and security operations to every AI interaction.

AI Security for Users

Cato AI Security delivers visibility and control over AI tools accessed and used across the enterprise.

- **Shadow AI Discovery** Cato discovers sanctioned and unsanctioned AI applications in use across the organization, including embedded AI features inside SaaS applications.
- **Data Protection** Cato inspects prompts and AI generated responses in real time, detecting sensitive information and applying enforcement actions including blocking, redacting, alerting or monitoring.
- **Agentic AI Governance** Cato provides visibility into AI agents operating across the enterprise, allowing security teams to monitor automated behavior and apply policy controls.
- **Runtime Guardrails** Cato enforces enterprise policies on what employees send to and receive from third party AI tools, ensuring AI usage aligns with organizational and regulatory requirements.

AI Security for Applications

Cato AI Security extends governance and control to homegrown applications and agents that are deployed and managed across the organization.

- **Visibility** Cato provides audit trail and reporting across homegrown AI applications, giving security teams an accurate record of AI activity and enforcement actions.
- **Runtime Protection** Cato protects enterprise-built AI applications by enforcing security and safety guardrails that detect and prevent AI-specific attacks such as prompt-injection and jailbreaks.
- **Security and Compliance Guardrails** Cato enforces regulation and compliance controls across AI applications, supporting enterprise governance requirements with audit reporting and configurable data privacy settings.
- **Homegrown Agent Governance** Cato provides visibility into AI agents and their associated tools, enabling security teams to monitor agent activity and apply policy controls across enterprise systems.

Endpoint Protection Platform (EPP)

Cato Endpoint Protection Platform (EPP) protects endpoints from attack, using software on the endpoint that connects to the Cato platform and is managed from within CMA.

The Cato EPP protects endpoints in multiple ways. The File Protection engine scans every file opened or created on the endpoint, to protect against malicious files. The Behavioral Protection engine analyses running processes for malicious behavior, using heuristics to protect against unknown and zero-day threats. Cato EPP provides:

- **Clear Visibility**

Admins see their endpoints directly within the same console they use to manage their network, security and users, giving them better visibility of their infrastructure.

- **Improved Control**

Admins can set endpoint policies and rules in the same console and in the same way as for the rest of their infrastructure. The familiarity, accessibility and consistency give them better control of their endpoints than with a separate EPP.

- **Better Understanding**

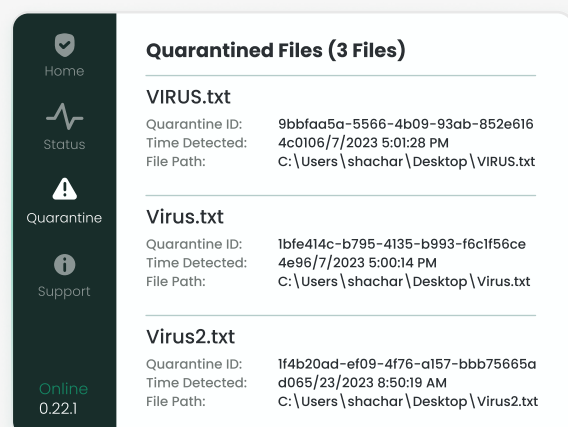
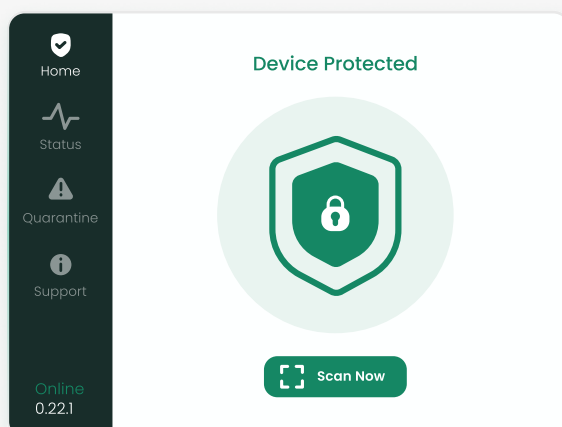
Admins see Endpoint events alongside network, security and user events, giving them a single context and allowing them to correlate events. This gives them better understanding than with a separate EPP.

- **Faster Remediation**

Admins deal with endpoint threats right within CMA. And they don't just see device information in endpoint events: they see user information too. So, they can isolate the affected user account within CMA, helping them counter threats before they spread beyond the device.

- **Better XDR integration**

Cato EPP provides rich, native data to Cato XDR, including the user identity used throughout Cato's service, making Cato XDR even more powerful.



Cloud Access and Optimization and Remote Access

Cloud Datacenter Integration

Cato tightly couples cloud data centers 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 is routed along the optimal 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 Direct Connect or Microsoft Azure ExpressRoute.



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, avoiding additional VM costs and 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 the performance of public cloud applications, including Microsoft 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 with Universal ZTNA

Cato extends the full range of its network and security capabilities down to remote and mobile users. Using a Cato Client, Browser Extension, Enterprise Browser, or clientless portal access, users connect to the nearest Cato PoP and have their traffic routed optimally over the Cato global private backbone to on-premises or cloud applications. Cato provides remote and mobile users with Cato Universal ZTNA, allowing the most granular user access control down to specific applications all enforced through a single, unified security policy shared across users, sites, and cloud environments. By contrast, legacy VPN solutions limit access to entire subnets and require separate policy definitions across appliances and access tools. All user activity is protected by Cato's built-in security stack, with one centrally managed policy consistently applied everywhere, ensuring enterprise-grade protection to all users.



Private Application Access with Cato AppConnector

For organizations that want to deliver secure private application access without changing their existing network architecture, Cato offers AppConnector. AppConnector provides private application access to Cato UZTNA users while allowing customers to retain their current networking configuration, including existing SD-WAN deployments. Instead of requiring site connectivity changes or SD-WAN replacement, AppConnector is deployed near the private application environment and establishes a secure outbound connection to the Cato SASE Cloud. Remote and mobile users authenticate through Cato’s ZTNA framework and are granted least-privilege access directly to the specific application. The internal network remains non-routable and never exposed to the Internet.

XOps (XDR and AI Ops)

Cato XOps is an AI layer that provides customers with the insights and actions they need to quickly detect and resolve network and security issues. Cato XOps transforms millions of raw events into consumable incident stories, correlated across users, devices, and locations. These stories provide full context and are prioritized by risk, enabling security teams to act quickly, reduce alert fatigue, and respond with confidence. The XOps license includes Cato's security (XDR) and network (AI Ops) capabilities. It automatically processes events from all licensed Cato products, add-ons, and connected third-party tools, with no manual setup required.

Extended Detection & Response (XDR)

Cato XDR helps security teams detect and respond to incidents, to make them more effective and efficient. It surfaces threats that real-time engines can't see, shows analysts the top-priority issues, and helps them remediate quickly, with simple, appropriate guidance from within CMA. Cato XDR is the first to leverage power of SASE. It performs better because it uses the broadest range of native network and security inputs, from Cato's SASE platform, along with hundreds of Threat Intelligence sources.

Cato XDR, a core component of the Cato XOps AI layer, uses AI to create actionable stories, at scale, finding the most important issues while reducing noise. It reduces alert fatigue by surfacing the most important Block alerts from the real-time prevention engines. It finds threats that those engines cannot see, by correlating signals with heuristics and machine learning. It detects suspicious behavior, by finding anomalies with advanced statistical models and UEBA. Cato XDR helps SOC teams to:

- **Find more threats, with high quality native data**

Unlike XDRs that take native data just from endpoints, Cato XDR is SASE-based. It takes the broadest range of native data inputs directly from Cato single pass processing engines. This native data suffers no loss from normalization, improving the ability to identify hidden threats and minimize false positives.

- **Detect more, with powerful correlation**

Our advanced AI and Data Science algorithms were built by ex-military security researchers, trained on petabytes of data and trillions of events and proven over tens of thousands of confirmed incidents. Our native data is enriched with hundreds of proprietary and third-party sources and millions of records of valid Indicators of compromise (IoCs).

- **Investigate faster with guided information**

Detected incidents contain all the information required for an in-depth investigation. The information is rich, accurate, easy to analyze, all in one place and presented in a guided order, reducing the time to investigate and thus increasing analyst capacity.

- **Remediate faster, with one tool**

Cato XDR uses Cato's single management platform that manages network, security and endpoints. All remediation is done in the same place, using a single toolset that avoids the need for third-party integrations, reduces time and enables collaboration between teams.

- **Deploy faster, with all inputs instantly ready**

With Cato XDR, all native sensors are part of the same SASE platform and instantly ready. No sensor integration, setup or baselining is required, eliminating costly delays to deployment.

Detection & Response Story

Attack Detected:	Engine Type	Analyst Severity	Analyst Verdict	Type	Compromised...	Missing...	Story Duration	Status
Suspicious Network Activity	Threat Hunting	N/A	N/A	Reputation	1	26	8 days	Open

Timeline:

- 1 Oct 30, 2023 08:00 am: Story created, Suspicious Network Activity
- 2 Nov 06, 2023 04:00 pm: Added 2 Targets, www.swixil.com +1

Details:

Generate AI Summary

Story Summary (Powered by AI)

In this incident, there were 11 flows detected with a duration of approximately 9 days. The flows were flagged as suspicious outbound network activity related to DNS protection blocks. The threat names associated with the blocks were "Domain reputation based signature - Malicious" and "IP reputation based signature - CnC Communications". The incident occurred on a Linux operating system and the site type was identified as a regular site. The analyst feedback classified the threat as "CnC Communications" and the predicted verdict was "Suspicious". The incident timeline spanned over multiple days, with flow start times ranging from 1698735600000 to 1699279200000. The server ports involved in the incident were 53, which is commonly used for DNS communication. The specific IPs and domains involved in the incident were not provided in the data.

This summary was generated with AI, and therefore, its accuracy may vary due to the inherent limitations of artificial intelligence algorithms.

Related Events:

Target	Type	Action	Related Events
quicklyseek.com	N/A	N/A	N/A
www.simpli.com	N/A	N/A	N/A
www.pcmptuner.org	N/A	N/A	N/A
simpli.com	N/A	N/A	N/A

AIOps

Cato AIOps, a core component of the Cato XOps AI layer, helps IT teams detect and respond to network incidents, and presents them as Network Stories. It surfaces issues within prioritized incident stories and helps remediate them quickly with simple, appropriate guidance from within the Management Application. AIOps continuously collects and correlates real-time data across SD-WAN, ZTNA, and Digital Experience Monitoring (DEM). Events are analyzed using Alto detect performance issues, anomalies, and potential service disruptions proactively, and to help IT teams remediate them. By embedding this functionality into XOps, Cato eliminates the need for separate AIOps tools, simplifies operations, and supports a proactive IT model.

Digital Experience Monitoring (DEM)

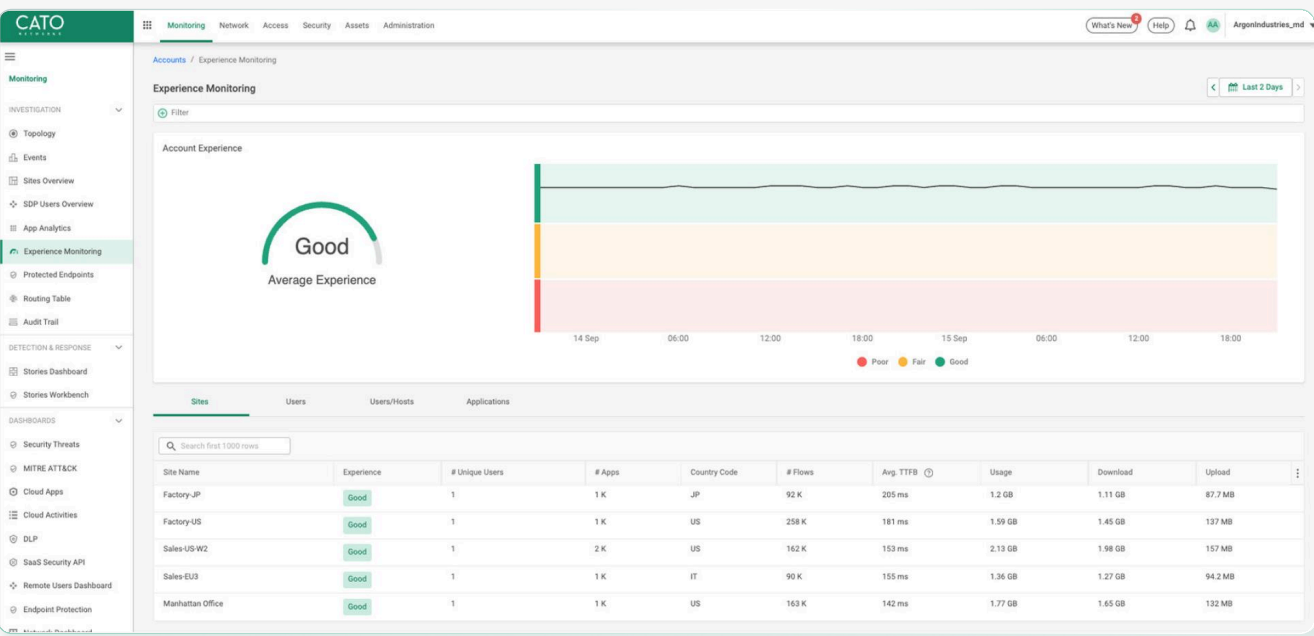
Unacceptable user experiences can impact productivity, and ultimately, the business. IT Teams need network insights to quickly pinpoint and resolve issues while preventing potential problems. Cato DEM provides these insights, enabling IT teams to deliver on strategic digital transformation projects, ensure optimal user experiences, reduce disruptions, and streamline IT operations. As a native part of the Cato SASE Platform, DEM uniquely delivers unparalleled end-to-end network visibility leading to actionable insights using both real-time and historical network data. IT teams can address experience issues more efficiently, improving user productivity and satisfaction.

- **Identify experience issues with in-depth visibility**

Cato DEM offers hop-by-hop visualization of both endpoint and network performance issues, providing IT teams with actionable insights to optimize performance. Using Real User Monitoring (RUM) and SyntheticProbe Monitoring (STM), Cato DEM delivers rich data without the need to deploy dedicated sensors, simplifying deployment and reducing costs. As a native part of the Cato SASE Platform, it monitors and analyzes traffic in all directions, supporting 10,000+ applications, helping businesses identify and resolve issues faster, improve application performance, and enhance overall user experience.

- **Increase efficiency to deliver exceptional user experiences**

Cato DEM allows IT teams to seamlessly prioritize, investigate, and remediate issues within CMA to gain a complete picture. This eliminates the need to switch between multiple tools, streamlines workflows, and enhances operational efficiency. With historical data retention of up to 3 months, IT teams perform trend analysis to identify recurring issues and optimize performance over time. Additionally, Cato's ready-to-use, proven XOps playbooks minimize the need for specialized expertise, guiding IT teams to resolve issues quickly and effectively, further improving response times and reducing downtime.



IoT/OT Security

Cato IoT/OT Security is a native feature of the Cato SASE platform and does not require complex integrations or special configurations. It quickly enables security teams to manage and secure IoT/OT devices with simplicity and precision in three key areas.

Discovery and Classification

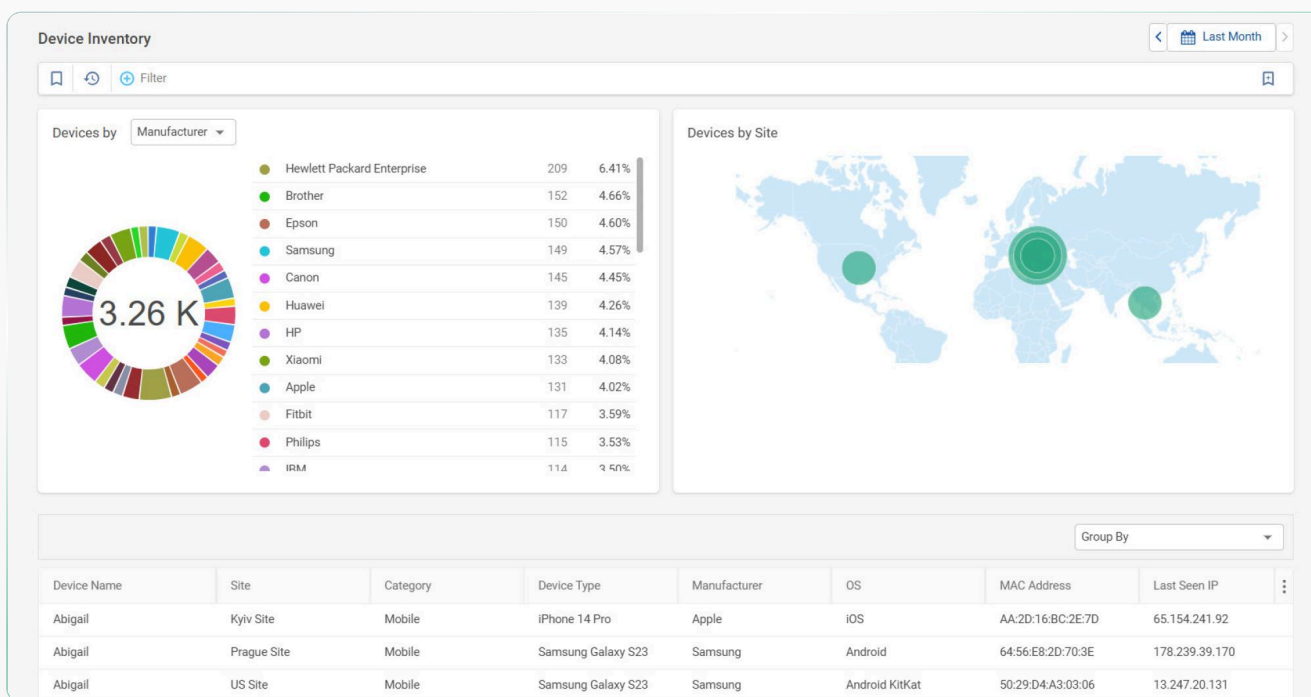
Unlike XDRs that take native data just from endpoints, Cato XDR is SASE-based. It takes the broadest range of native data inputs directly from Cato single pass processing engines. This native data suffers no loss from normalization, improving the ability to identify hidden threats and minimize false positives.

Policy Enforcement

IoT/OT requires more than visibility to help IT teams efficiently control IoT/OT device access. Cato IoT/OT security empowers IT teams to define and enforce granular access policies based on specific device characteristics or device groupings.

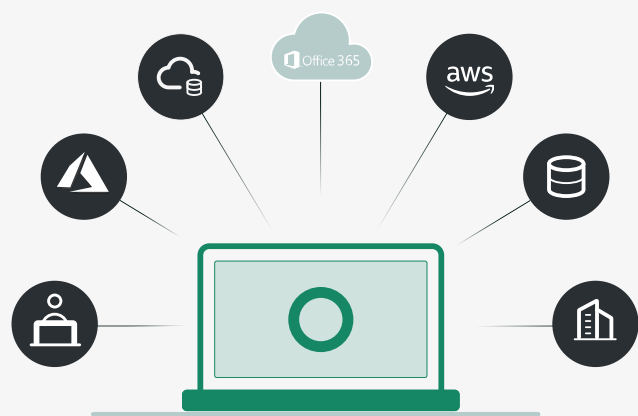
Threat Prevention

Cato IoT/OT Security benefits from the prevention capabilities of the Cato SASE platform. Beyond policy enforcement, Cato's advanced threat prevention fully protects IoT/OT assets, providing consistent protection against known and emerging threats.



Cato Management Application (CMA)

Cato provides customers 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 Application 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.**

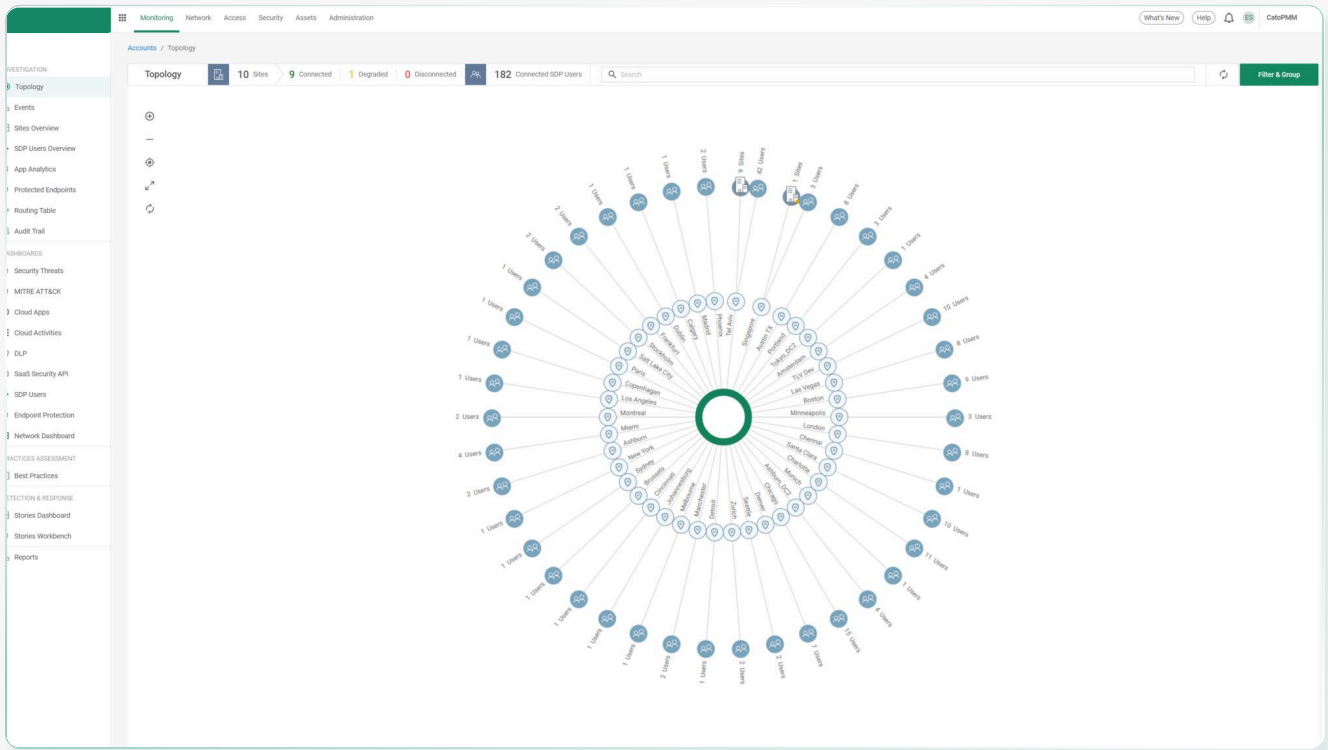
Provides comprehensive network visibility, solving key challenges of access control, user experience, troubleshooting, and Shadow IT.

- **Collection and delivery of full network and security logs.**

Integration with external analysis solutions, such as SIEMs, is available, offering the unique benefit of 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 Application provides a single-pane-of-glass, showing all connected sites, cloud resources, and users:**



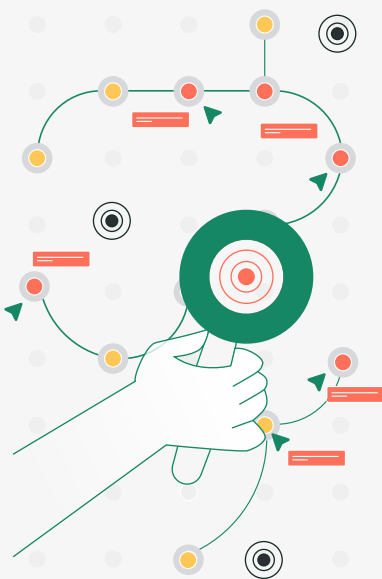
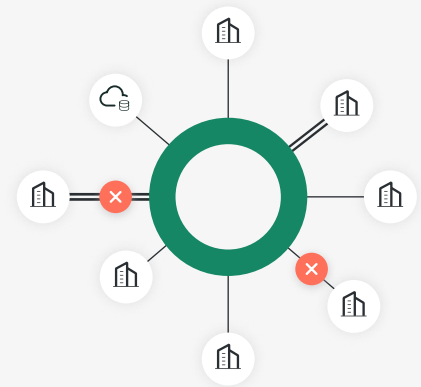
Managed Services

Cato offers a suite of managed services depending on the management model that best meets customer requirements. In all cases, Cato maintains the underlying platform, freeing customers from the associated costs and complexities of scaling, upgrading, and otherwise managing the networking and security infrastructure.

With self-service management, customers control all aspects of their own networks. With co-management, customers can delegate configuration and troubleshooting tasks to the Cato NOC or a regional partner. Fully managed puts responsibility for monitoring and managing the customer's network on a regional partner.

Intelligent Last-mile Management

Cato provides customers with a premium service to continuously monitor last-mile ISPs. In case of an outage (blackout) or performance degradation (brownout), Cato works with the ISP to resolve the issue by providing pertinent and detailed network information around the incident. This service helps customers that migrated from a fully managed MPLS network to quickly resolve network issues across multiple, global ISPs without expending precious internal IT resources.

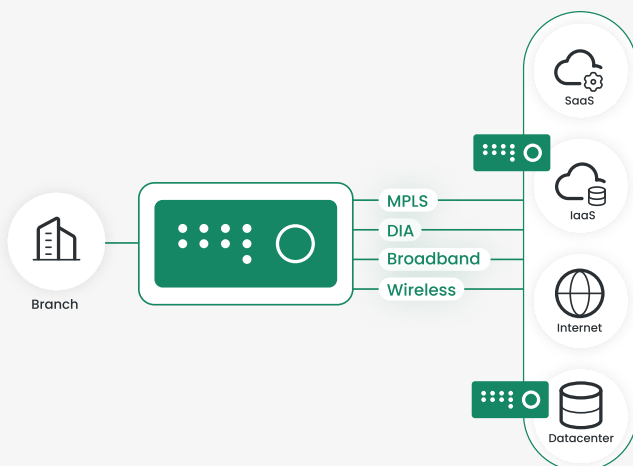


Managed Detection and Response (MDR)

Cato XDR can be managed by the customer, by a Cato Partner, or by the Cato MDR service. With Cato MDR, customers offload the responsibility to detect, investigate and remediate threats to the Cato SOC team. The Cato SOC reviews flagged threats and assesses risks, alerting only on actual threats. These can then be contained by configuring network policies or disconnecting compromised machines or users. The Cato SOC will advise on the threat level and the recommended remediation. It will follow up until the threat is eliminated. A monthly report summarizes threats detected, risk levels, and impacted endpoints.

Hands-free Management

Customers can choose Cato or one of its partners for complete hands-free management of their network. Expert staff will perform all changes to networking and security policies as needed to accommodate changing business and technical requirements. A co-management model between the customer, a partner, and Cato is also available. In all cases, Cato maintains the underlying Cato Cloud platform so customers do not need to upgrade, patch, or otherwise maintain any Cato software.

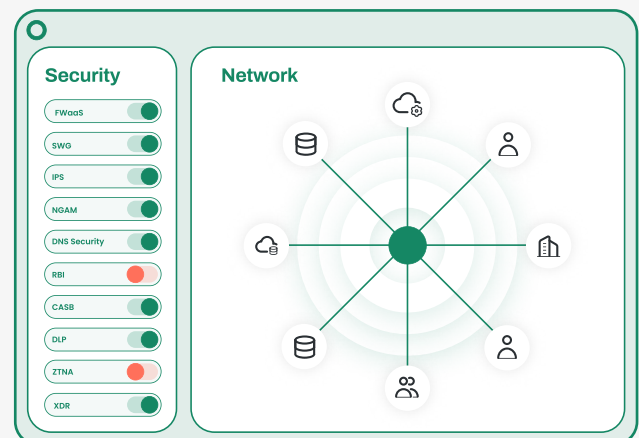


SASE Transformation Services

Cato's Professional Services can guide you through configuring the Cato SASE platform with your organization's unique security and connectivity requirements in mind. Whether deploying Cato Sockets across multiple locations, onboarding mobile users, or setting security and networking policies to secure and enable your workforce, Cato Networks is your dedicated partner on your unique SASE journey.

Customer Success Engineer (CSE)

A Cato Customer SuccessEngineer is a named Cato engineer who acts as the customer's single point of contact and subject matter expert. The CSE is deeply familiar with the customer's account and provides hands-on technical guidance, architectural expertise, proactive analysis, and consultation on the Cato platform.



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 Zero Trust Security, converged into the Cato SASE Cloud. By connecting all locations and users to Cato SASE Cloud through Cato edge SD-WAN devices and Cato ZTNA Clients, all traffic, both Internet and WAN, is fully protected by Cato Zero Trust Security. 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 to a single user's laptop, smartphone, or tablet. Using a Cato ZTNA Client, Browser Extension, or clientless portal, 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.

CatoZero Trust Security 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.



Secure AI Adoption

Cato enables enterprises to safely adopt public GenAI by providing full visibility into AI interactions across web, API, and applications. By discovering and categorizing "Shadow AI" usage, it enforces granular, intent-based policies that detect and block sensitive data violations in real time, preventing leakage while supporting innovation.

For homegrown AI applications and agents, Cato provides specialized runtime protection against emerging threats such as prompt injection and jailbreaks. Whether deployed as a gateway or via API, it centralizes security and response across cloud, on-prem, and edge environments, ensuring that proprietary AI remains resilient and compliant without slowing down development.



Sensitive Data Security

Cato Zero Trust Security'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 Zero Trust Security 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.



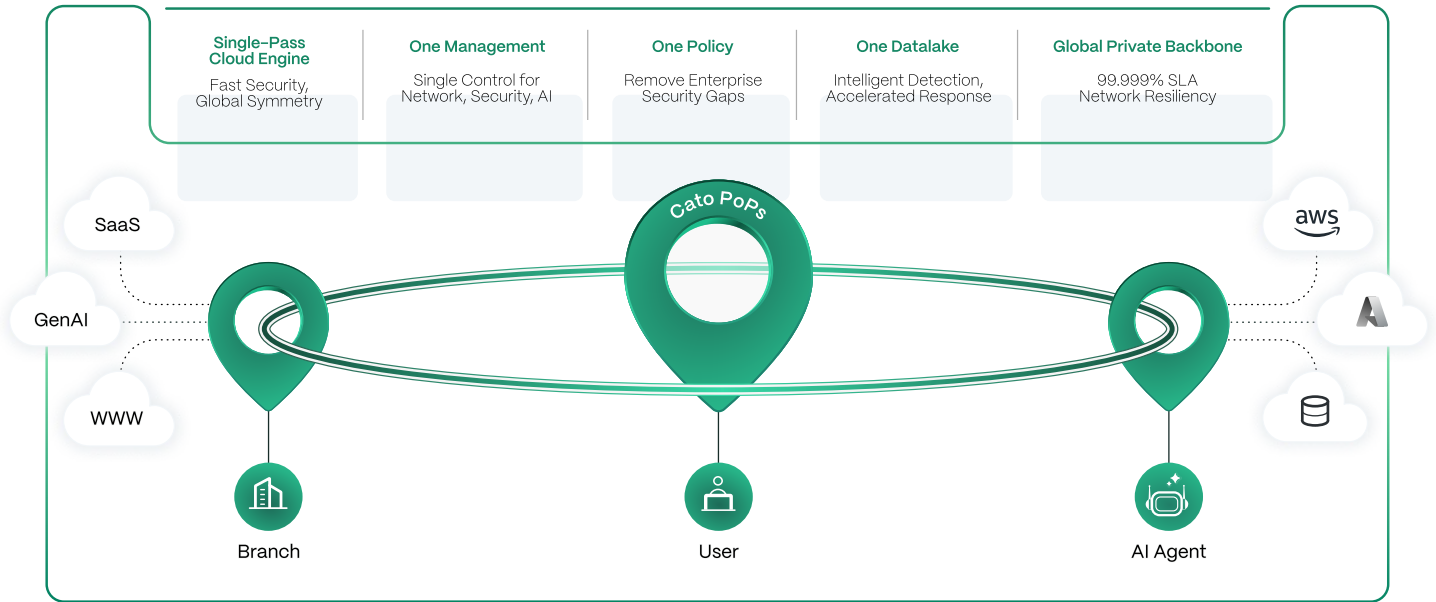
Global Application Access

CatoSASE 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.

About Cato Networks

Cato Networks, a leader in SASE and AI security, delivers secure, zero-trust access everywhere to thousands of customers worldwide. Built for organizations operating across all cloud and hybrid environments, the Cato Platform unifies networking, security, and access, providing them as elastic, modular capabilities that organizations can easily adopt and grow over time. Cato combines the Cato Cloud, a purpose-built global network, with simplified operational experience, all delivered across a robust, AI-driven platform. With Cato, organizations modernize confidently, operate with greater resilience, and innovate faster, without added complexity or risk.

The Cato SASE Platform



Cato. WE ARE SASE.

Cato SASE Cloud Platform

Connect

Cloud Network
Cloud On-Ramps

Protect

Network Security
AI Security
Endpoint Security

Detect

Incident Life Cycle Management

Run

Management, Analysis,
and Integration

Use Cases

Network Transformation

MPLS to SD-WAN Migration
Global Access Optimization
Hybrid Cloud & Multi-Cloud

Security Transformation

Secure Hybrid Work
Secure Direct Internet Access
Secure Application and Data Access
Incident Detection and Response

Business Transformation

Vendor Consolidation
Spend Optimization
M&A and Geo Expansion

Deployment Models

Regional Enterprises
Global Enterprises
Do It Yourself
Managed Service

Contact Us