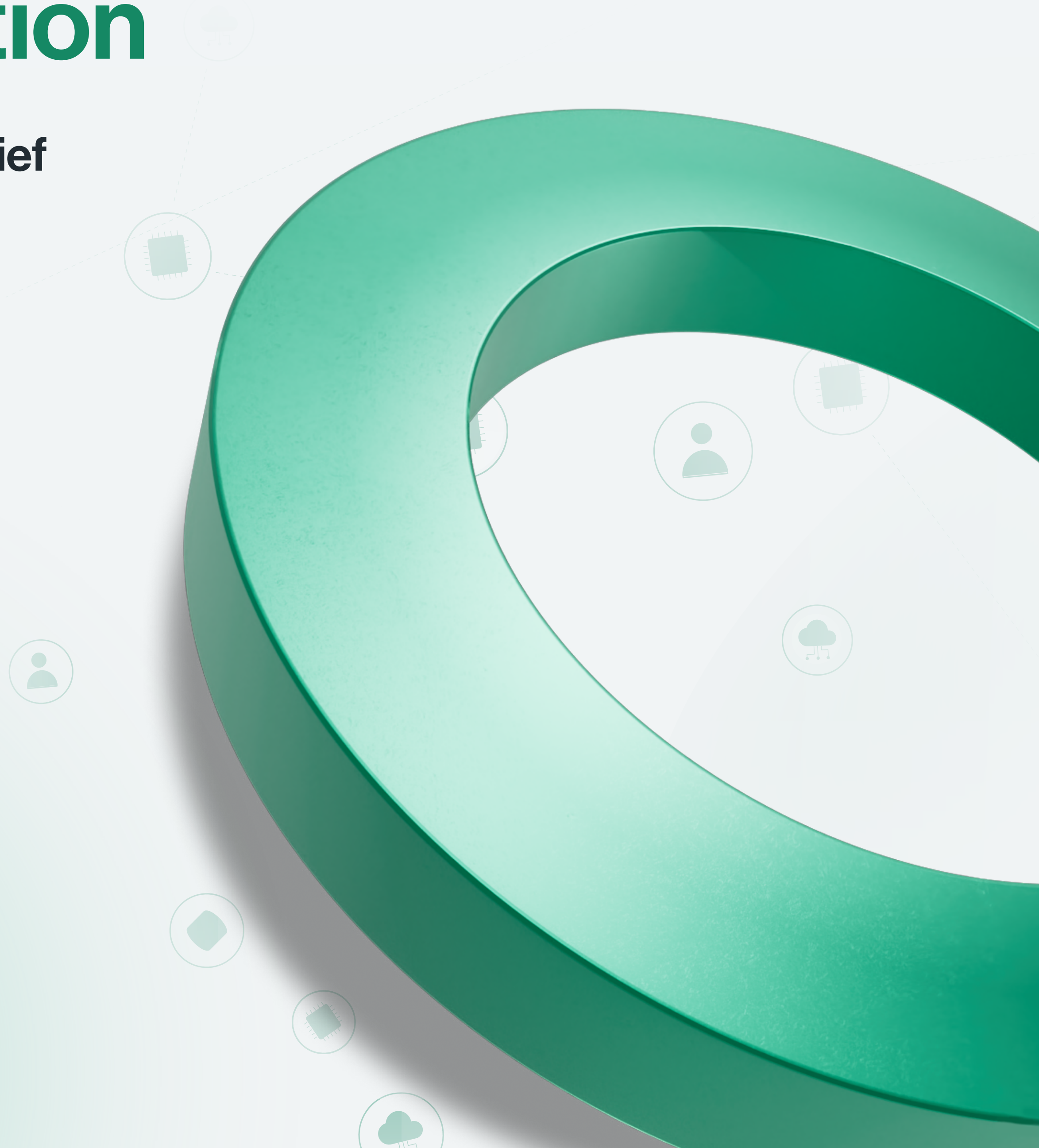
CATO
NETWORKS

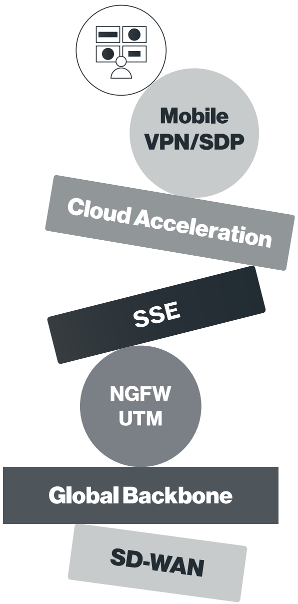
KONELYNK TECHNOLOGY
Networking Partner

Cato SASE Cloud Platform: The World's Leading Single-vendor SASE Solution

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. 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 pressures legacy architecture, IT resources because:

- **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.

- **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.

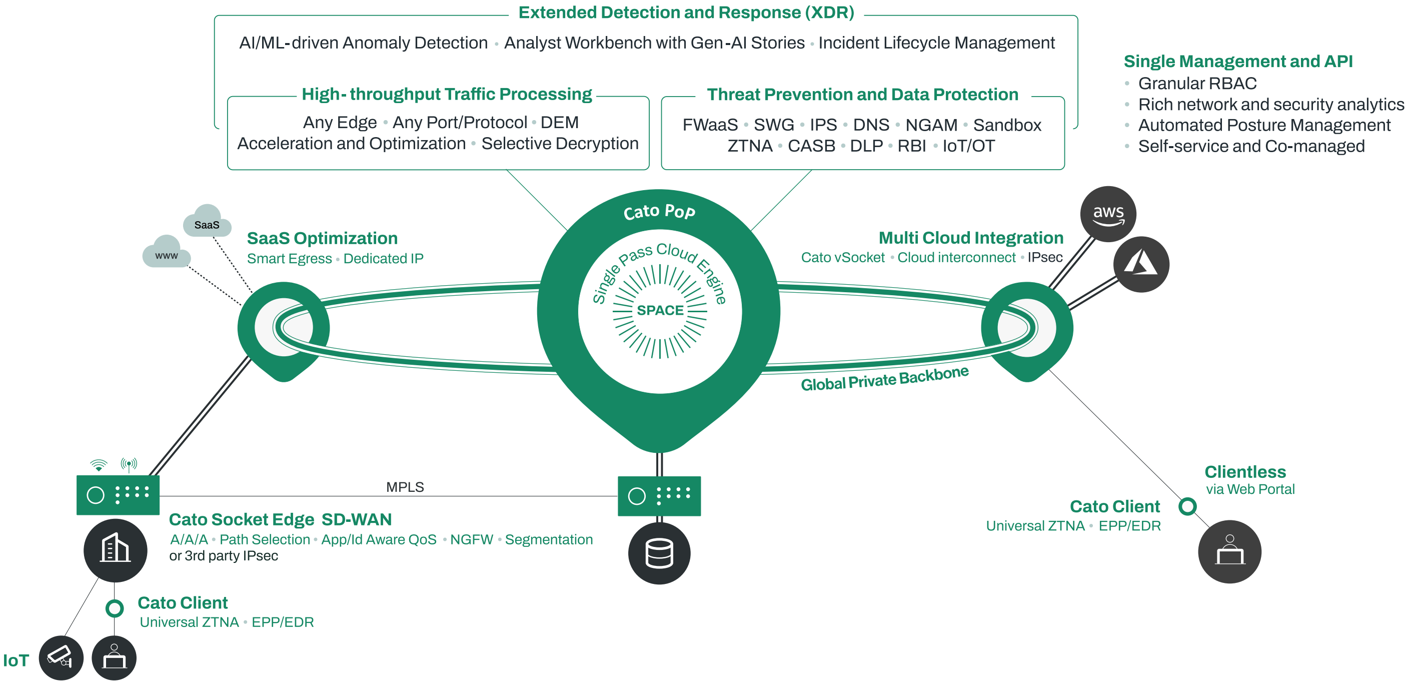
- **The legacy WAN doesn't extend beyond physical locations.**
  Supporting the hybrid workforce to accommodate work from anywhere requires a flexible architecture that is user- and location-centric.

The World's First SASE Cloud Platform

The world's first single-vendor SASE platform, converging SD-WAN, network security, XDR, DEM and EPP 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 security products 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 enterprise-grade security services to protect all traffic at all times.



Extended Detection and Response (XDR)

AI/ML-driven Anomaly Detection • Analyst Workbench with Gen-AI Stories • Incident Lifecycle Management

High- throughput Traffic Processing

Any Edge • Any Port/Protocol • DEM
Acceleration and Optimization • Selective Decryption

Threat Prevention and Data Protection

FWaaS • SWG • IPS • DNS • NGAM • Sandbox
ZTNA • CASB • DLP • RBI • IoT/OT

Single Management and API

- Granular RBAC
- Rich network and security analytics
- Automated Posture Management
- Self-service and Co-managed

SaaS Optimization

Smart Egress • Dedicated IP

Multi Cloud Integration

Cato vSocket • Cloud interconnect • IPsec

Cato Socket Edge SD-WAN

A/A/A • Path Selection • App/Id Aware QoS • NGFW • Segmentation
or 3rd party IPsec

Cato Client

Universal ZTNA • EPP/EDR

Clientless

via Web Portal

Cato Client

Universal ZTNA • EPP/EDR

Global Private Backbone

The Cato global private backbone is comprised of 85+ 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.

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
Canada, Calgary
Canada, Montreal
Canada, Toronto
Canada, Vancouver

Europe (21)

Austria, Vienna
Belgium, Brussels
Czech Republic, Prague
Denmark, Copenhagen
Finland, Helsinki
France, Marseille
France, Paris
Germany, Frankfurt
Germany, Munich
Ireland, Dublin
Italy, Milan
Italy, Rome
Norway, Oslo
Poland, Warsaw
Romania, Bucharest
Spain, Madrid
Sweden, Stockholm
Switzerland, Zurich
The Netherlands, Amsterdam
United Kingdom, London
United Kingdom, Manchester

Asia (23)

Australia, Melbourne
Australia, Perth
Australia, Sydney
China, Beijing
China, Shanghai
China, Shenzhen
China,Urumqui
Hong Kong
India, Chennai
India, Mumbai
India, New Delhi
Indonesia, Jakarta
Japan, Osaka
Japan, Sapporo
Japan, Tokyo
Malaysia, Kuala Lumpur
New Zealand, Auckland
Philippines, Manila
Republic of Korea, Seoul
Singapore
Taiwan, Taipei
Thailand, Bangkok
Vietnam, Ho Chi Minh City

Latin America (10)

Argentina, Buenos Aires
Brazil, Fortaleza
Brazil, Sao Paulo
Chile, Santiago
Colombia, Bogota
Costa Rica, San Jose
Ecuador, Quito
Mexico, MexicoCity
Mexico, Monterrey
Peru, Lima

Middle East & Africa (6)

Israel, Tel Aviv
Kenya, Nairobi
Morocco, Casablanca
Nigeria, Lagos
South Africa, Johannesburg
United Arab Emirates, Dubai

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

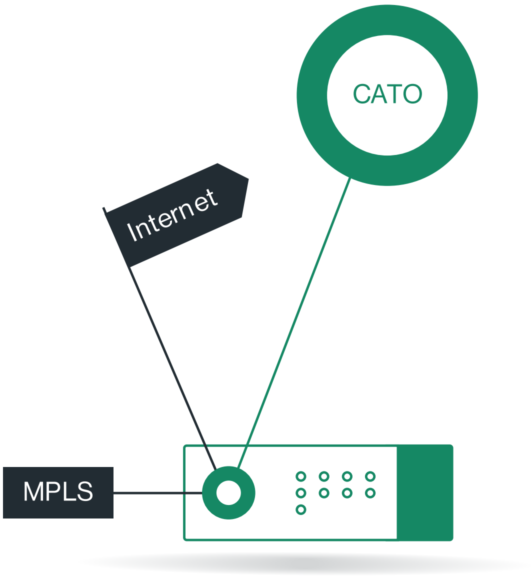
The Cato backbone is continuously monitored and measured. Self-healing capabilities guarantee 99.999% service availability. Elastic, scale-up cloud software design principles assure seamless service infrastructure growth without service downtime or disruptions.

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.

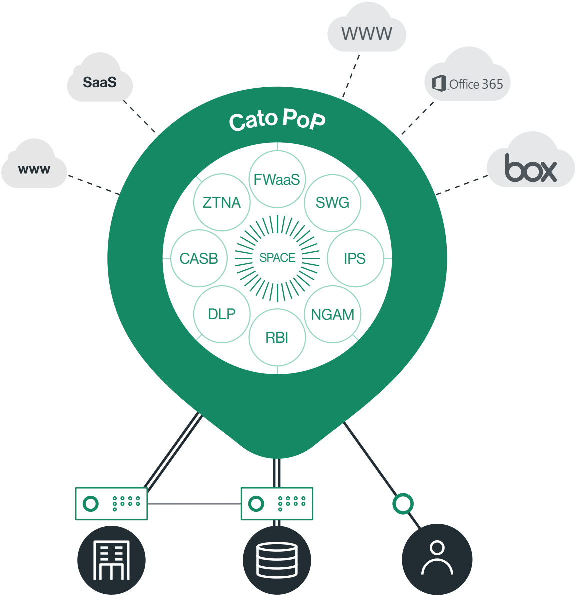
The Cato Socket, Cato's Edge SD-WAN device, is a zero-touch device ready to work in minutes once it has power and Internet connectivity. Sockets come in three series: X1500 and X1600 for branch offices, and X1700 for datacenters. Both are continuously monitored and updated by Cato's network operations 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, NGAM, Sandbox, DNS security & RBI) 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 PCI 4.0, 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.

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 CASB provides in 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 protects form 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 SaaS 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.

Remote Browser Isolation (RBI)

Cato's RBI provides secure browsing through a virtualization service that streams web pages safely to the user's device. Page code is executed remotely, keeping users safe from ransomware, phishing and other threats.

Cato RBI gives admins a new '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.

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 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 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. Cato Sandbox provides detailed forensic reports for security teams needing in-depth malware investigation, enhancing threat intelligence and response.

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.

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 Under standing

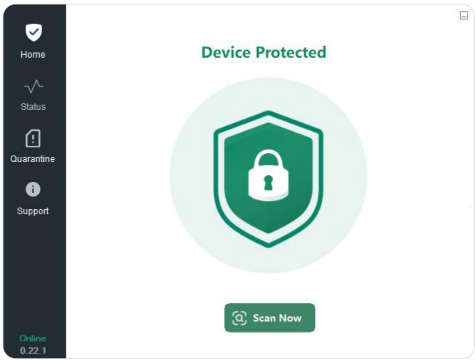
Admins see Endpoint events alongside network, security and user events, giving them a single context and allowing them to correlate events. This gives them better understanding than with a separate EPP.

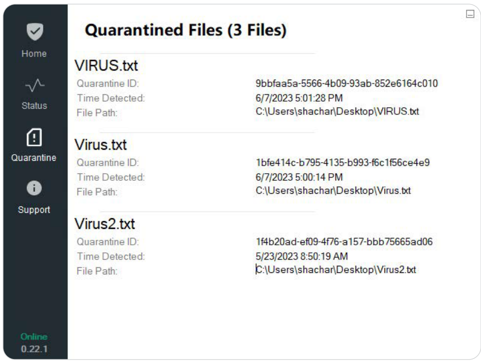
Faster Remediation

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.





Quarantined Files (3 Files)

VIRUS.txt

Quarantine ID: 9bbfaa5a-5566-4b09-93ab-852e6164c010
Time Detected: 6/7/2023 5:01:28 PM
File Path: C:\Users\shachar\Desktop\VIRUS.txt

Virus.txt

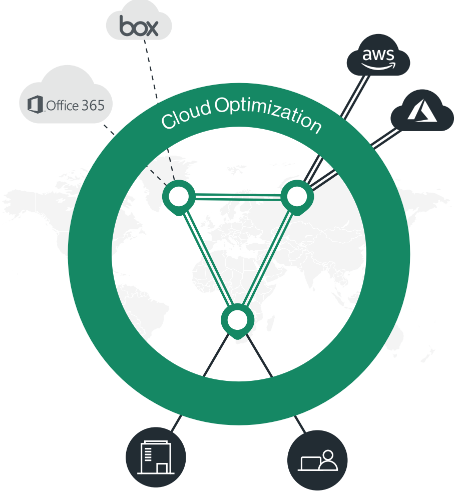
Quarantine ID: 1bfe414c-b795-4135-b993-f6c1f56ce4e9
Time Detected: 6/7/2023 5:00:14 PM
File Path: C:\Users\shachar\Desktop\Virus.txt

Virus2.txt

Quarantine ID: 1f4b20ad-ef09-4f76-a157-bbb75665ad06
Time Detected: 5/23/2023 8:50:19 AM
File Path: C:\Users\shachar\Desktop\Virus2.txt

Cloud Access and Optimization and Remote Access

Cloud Datacenter Integration

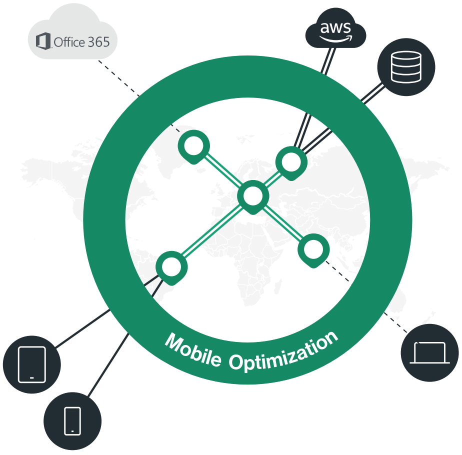


Cato tightly couples cloud datacenters into the SD-WAN, effortlessly. All cloud providers — Amazon AWS, Microsoft Azure, Google Cloud, and others — connect into the Cato global private backbone by establishing redundant IPsec tunnels, which typically only have to cross the physical datacenter shared 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 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 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 ZTNA, 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.

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 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

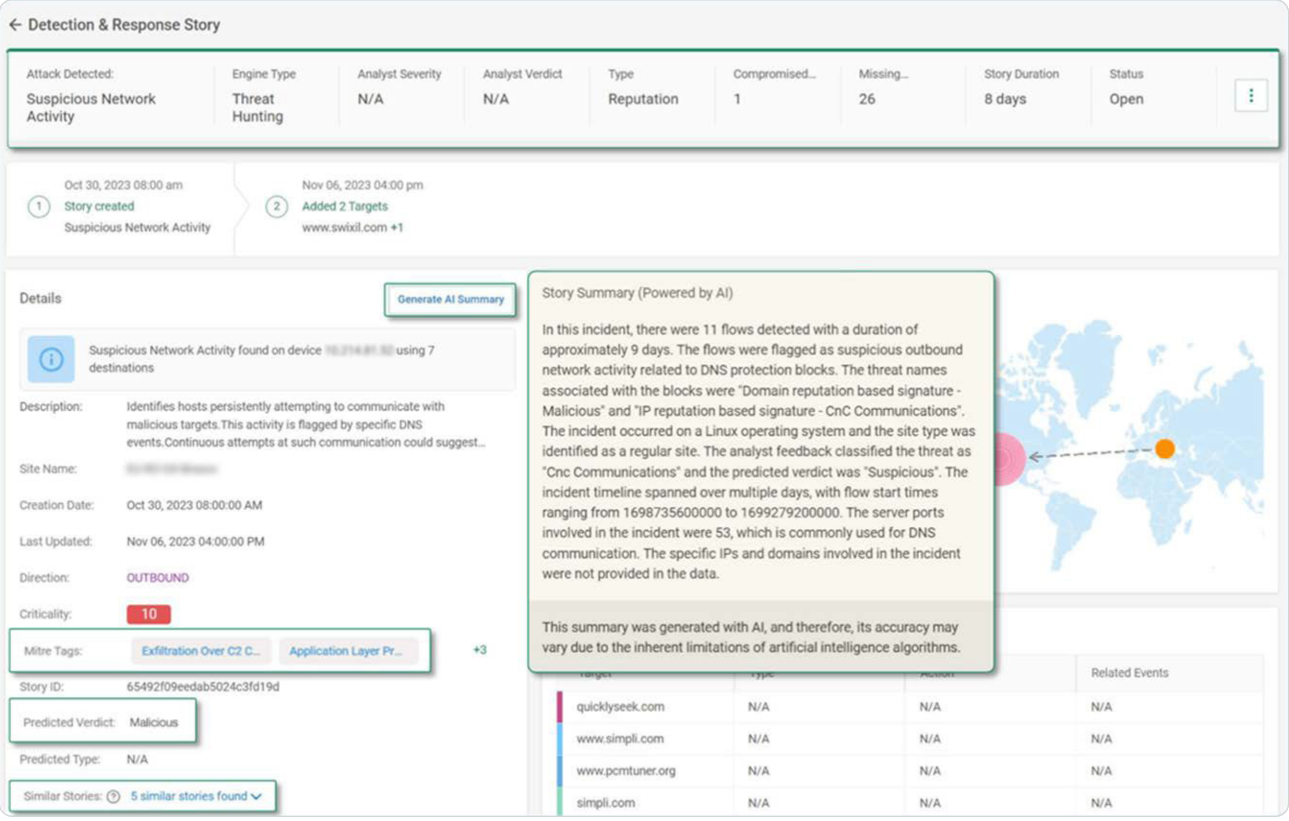
Detected incidents contain all the information required for an in-depth investigation. The information is rich, accurate, easy to analyze, all in one place and presented in a guided order, reducing the time investigate and thus increasing analyst capacity.

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

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

Suspicious Network Activity found on device [redacted] using 7 destinations

Description:	Identifies hosts persistently attempting to communicate with malicious targets.This activity is flagged by specific DNS events.Continuous attempts at such communication could suggest...
Site Name:	[redacted]
Creation Date:	Oct 30, 2023 08:00:00 AM
Last Updated:	Nov 06, 2023 04:00:00 PM
Direction:	OUTBOUND
Criticality:	10
Mitre Tags:	Exfiltration Over C2 C... Application Layer Pr... +3
Story ID:	65492f09eedab5024c3fd19d
Predicted Verdict:	Malicious
Predicted Type:	N/A
Similar Stories:	5 similar stories found

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.

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

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 Cloud 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

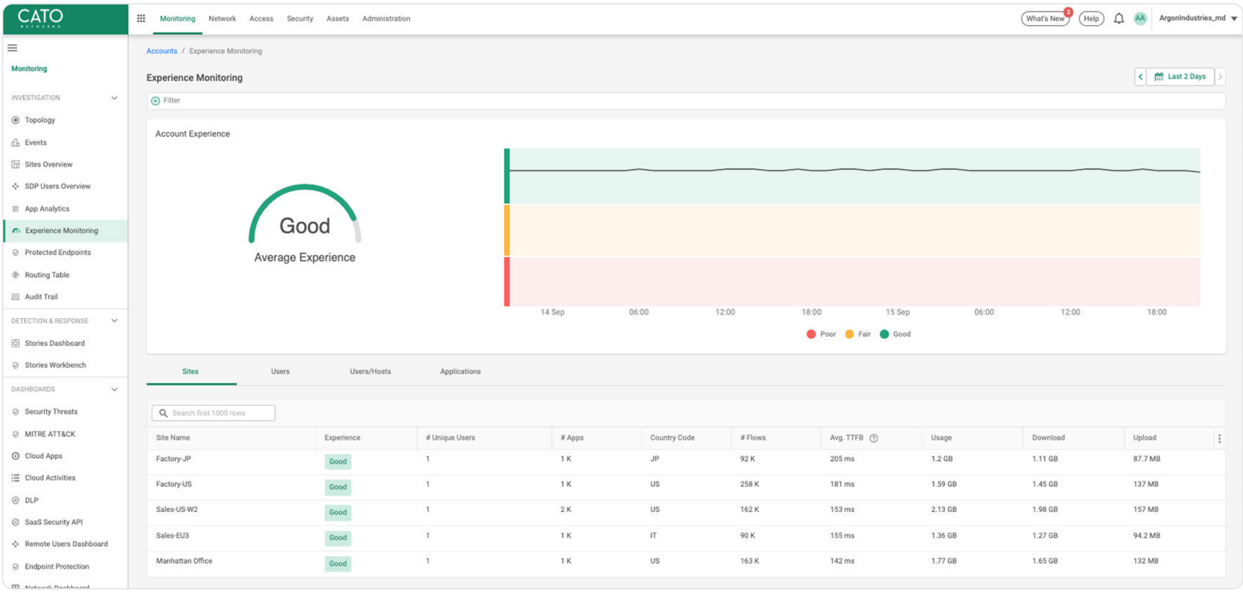
Cato DEM offers hop-by-hop visualization of both endpoint and network performance issues, providing IT teams with actionable insights to optimize performance. Using Real User Monitoring (RUM) and Synthetic Probe Monitoring (STM), Cato DEM delivers rich data without the need to deploy dedicated sensors, simplifying deployment and reducing costs. As a native part of the Cato SASE Cloud 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.

Proactively identify and anticipate potential issues

By continuously modeling, monitoring, and analyzing application performance, IT can pre-emptively anticipate and address user experience issues. AI-powered engines identify correlations between multiple RUM and STM generated events. Leveraging this data, IT gains full visibility into both the actual user experience and potential issues in the system that might not yet affect users but could lead to problems. This enables IT to investigate and remediate systematic problems before users become frustrated.

Increase efficiency to deliver exceptional user experiences

Cato DEM allows IT teams to seamlessly prioritize, investigate, and remediate issues within CMA, advantage of a single dashboard 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 can perform trend analysis to identify recurring issues and optimize performance over time. Additionally, Cato's ready-to-use, proven XDR playbooks minimize the need for specialized expertise guiding, IT teams to resolve issues quickly and effectively, further improving response times and reducing downtime.



Site Name	Experience	# Unique Users	# Apps	Country Code	# Flows	Avg. TTFB	Usage	Download	Upload
Factory-JP	Good	1	1 K	JP	92 K	205 ms	1.2 GB	1.11 GB	87.7 MB
Factory-US	Good	1	1 K	US	258 K	181 ms	1.59 GB	1.45 GB	137 MB
Sales-US-W2	Good	1	2 K	US	162 K	153 ms	2.13 GB	1.98 GB	157 MB
Sales-EU3	Good	1	1 K	IT	90 K	155 ms	1.36 GB	1.27 GB	94.2 MB
Manhattan Office	Good	1	1 K	US	163 K	142 ms	1.77 GB	1.65 GB	132 MB

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

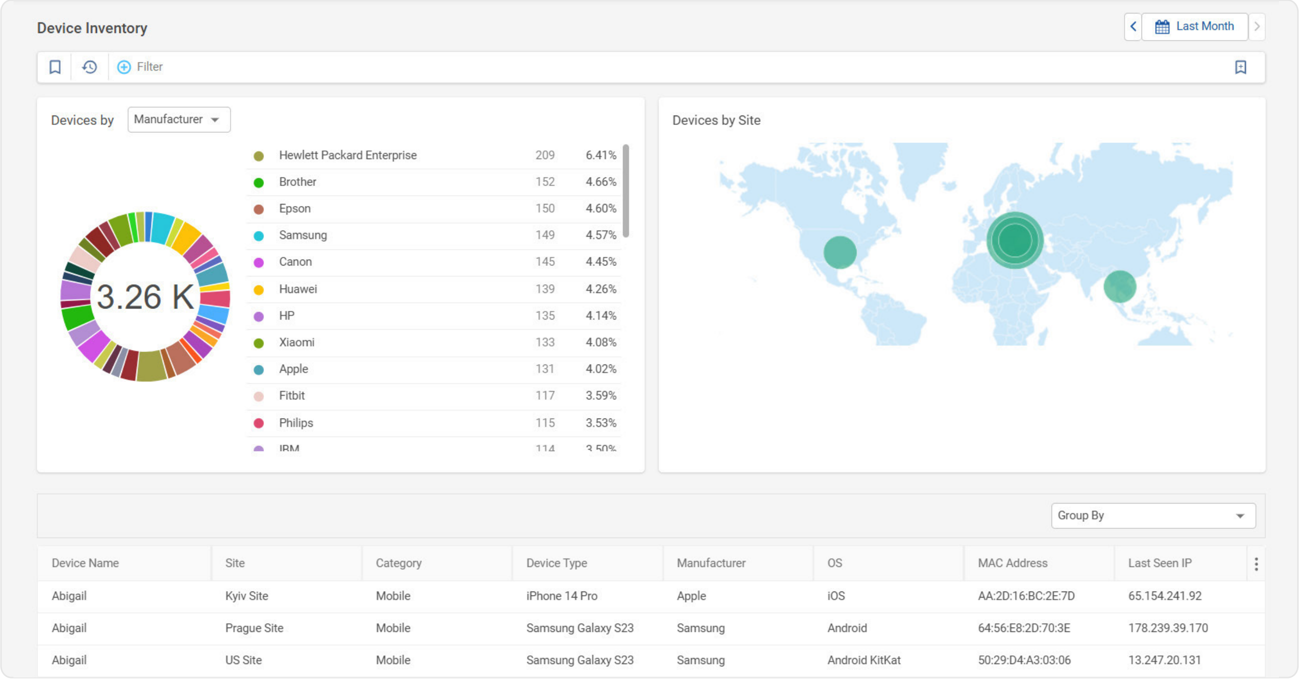
Cato IoT/OT Security delivers instant visibility across IT, IoT, and OT environments with no integration required. Purpose-built and trained AI and ML are used to fingerprint devices on the network, mapping their key attributes.

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

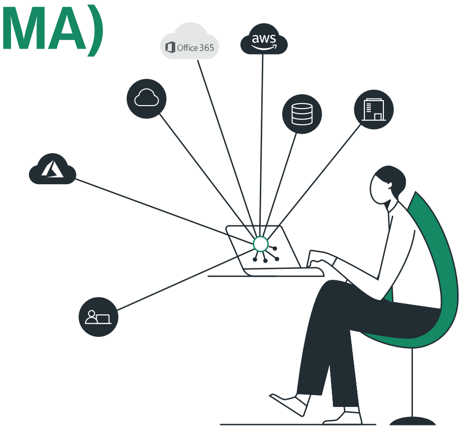
Cato IoT/OT Security benefits from the prevention capabilities of the Cato SASE Cloud platform. Beyond policy enforcement, Cato's advanced threat prevention fully protects IoT/OT assets, providing consistent protection against known and emerging threats.



●	Hewlett Packard Enterprise	209	6.41%
●	Brother	152	4.66%
●	Epson	150	4.60%
●	Samsung	149	4.57%
●	Canon	145	4.45%
●	Huawei	139	4.26%
●	HP	135	4.14%
●	Xiaomi	133	4.08%
●	Apple	131	4.02%
●	Fitbit	117	3.59%
●	Philips	115	3.53%
●	IBM	114	3.50%

Device Name	Site	Category	Device Type	Manufacturer	OS	MAC Address	Last Seen IP
Abigail	Kyiv Site	Mobile	iPhone 14 Pro	Apple	iOS	AA:2D:16:BC:2E:7D	65.154.241.92
Abigail	Prague Site	Mobile	Samsung Galaxy S23	Samsung	Android	64:56:E8:2D:70:3E	178.239.39.170
Abigail	US Site	Mobile	Samsung Galaxy S23	Samsung	Android KitKat	50:29:D4:A3:03:06	13.247.20.131

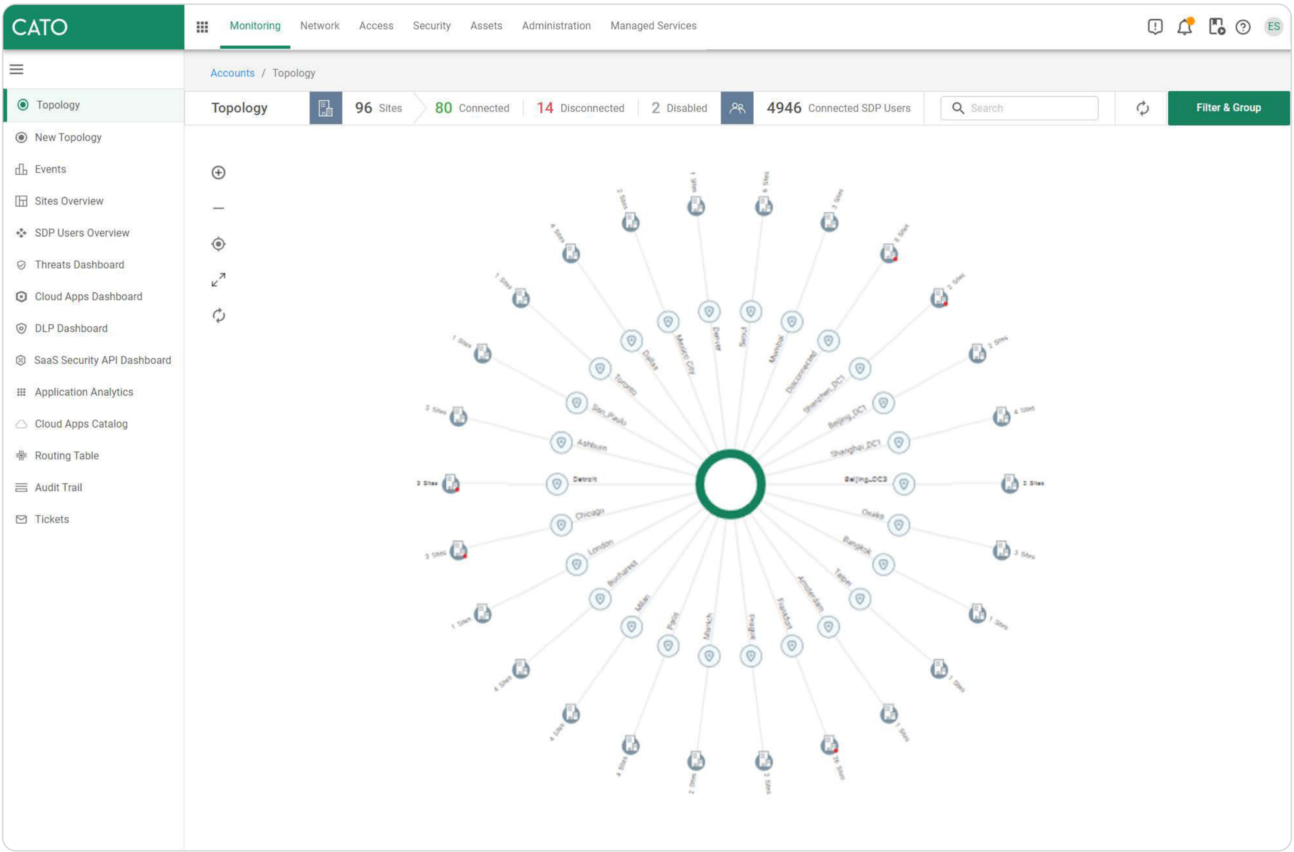
Cato Management Application (CMA)



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 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.

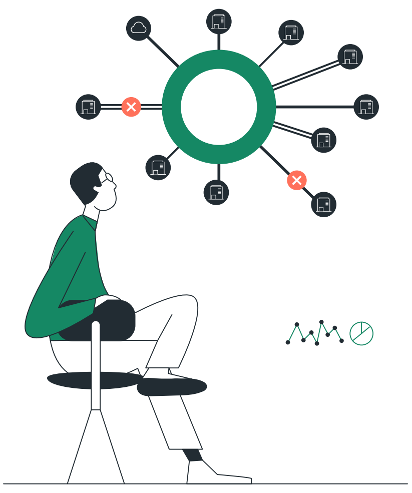


Cato's management console provides a single-pane-of-glass, showing all connected sites, cloud resources, and users.

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 their multiple, global ISPs without expending precious internal IT resources.

Managed XDR

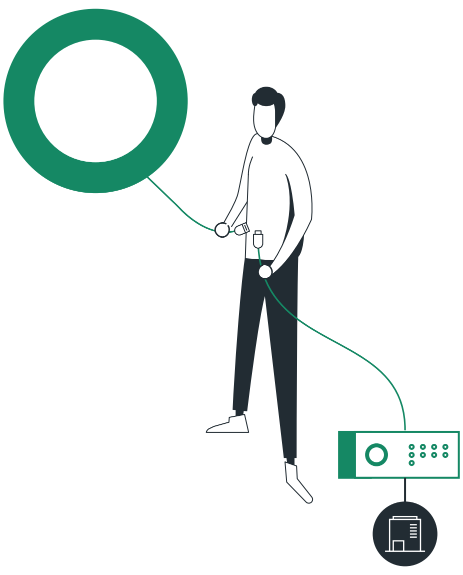
Cato XDR can be managed by the customer, by a Cato Partner, or by the Cato Managed XDR service. With Cato Managed XDR, customers offload the responsibility to detect, investigate and remediate threats to the Cato SOC team. The Cato SOC reviews flagged threats and assesses risks, alerting only on actual 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, risks 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 Success Engineer 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 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 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 Platform: Complete Network and Security 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 80+ 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.

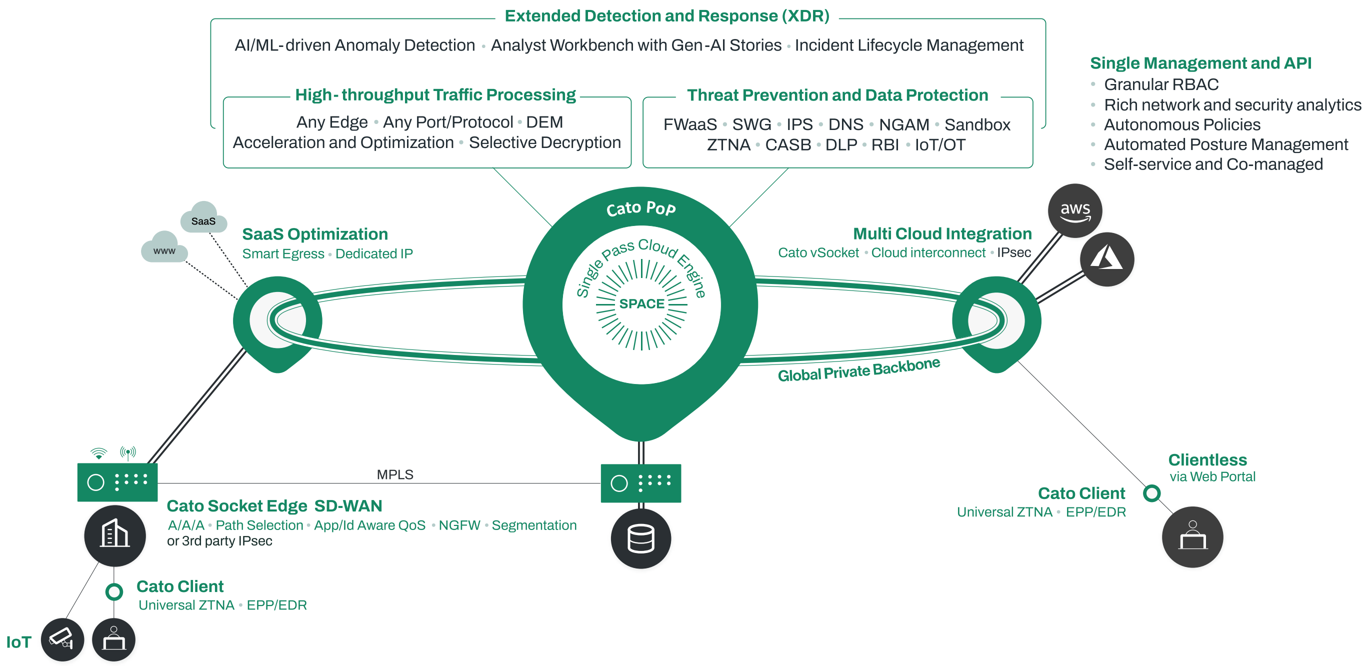
With Cato, customers can easily migrate from MPLS to SD-WAN, optimize global connectivity to on-premises and cloud applications, enable secure branch office Internet access everywhere, and seamlessly integrate cloud datacenters and mobile users into a high-speed network with a zero trust architecture.

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.

About Cato Networks

Cato provides a world-leading single-vendor SASE platform. Cato creates a seamless and elegant customer experience that effortlessly enables threat prevention, data protection, and timely incident detection and response. Using Cato, businesses easily 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



Extended Detection and Response (XDR)
AI/ML-driven Anomaly Detection • Analyst Workbench with Gen-AI Stories • Incident Lifecycle Management
High-throughput Traffic Processing
Any Edge • Any Port/Protocol • DEM
Acceleration and Optimization • Selective Decryption
Threat Prevention and Data Protection
FWaaS • SWG • IPS • DNS • NGAM • Sandbox
ZTNA • CASB • DLP • RBI • IoT/OT
Single Management and API
Granular RBAC
Rich network and security analytics
Autonomous Policies
Automated Posture Management
Self-service and Co-managed
SaaS
www
SaaS Optimization
Smart Egress • Dedicated IP
Cato PoP
Single Pass Cloud Engine
SPACE
Multi Cloud Integration
Cato vSocket • Cloud interconnect • IPsec
aws
Global Private Backbone
MPLS
Cato Socket Edge SD-WAN
A/A/A • Path Selection • App/Id Aware QoS • NGFW • Segmentation
or 3rd party IPsec
Cato Client
Universal ZTNA • EPP/EDR
IoT
Clientless
via Web Portal
Cato Client
Universal ZTNA • EPP/EDR

For more details, please contact us:

https://www.konelynk.tech/secureedge-service#h.qb2dd1c

info@konelynk.tech

+675 71865999