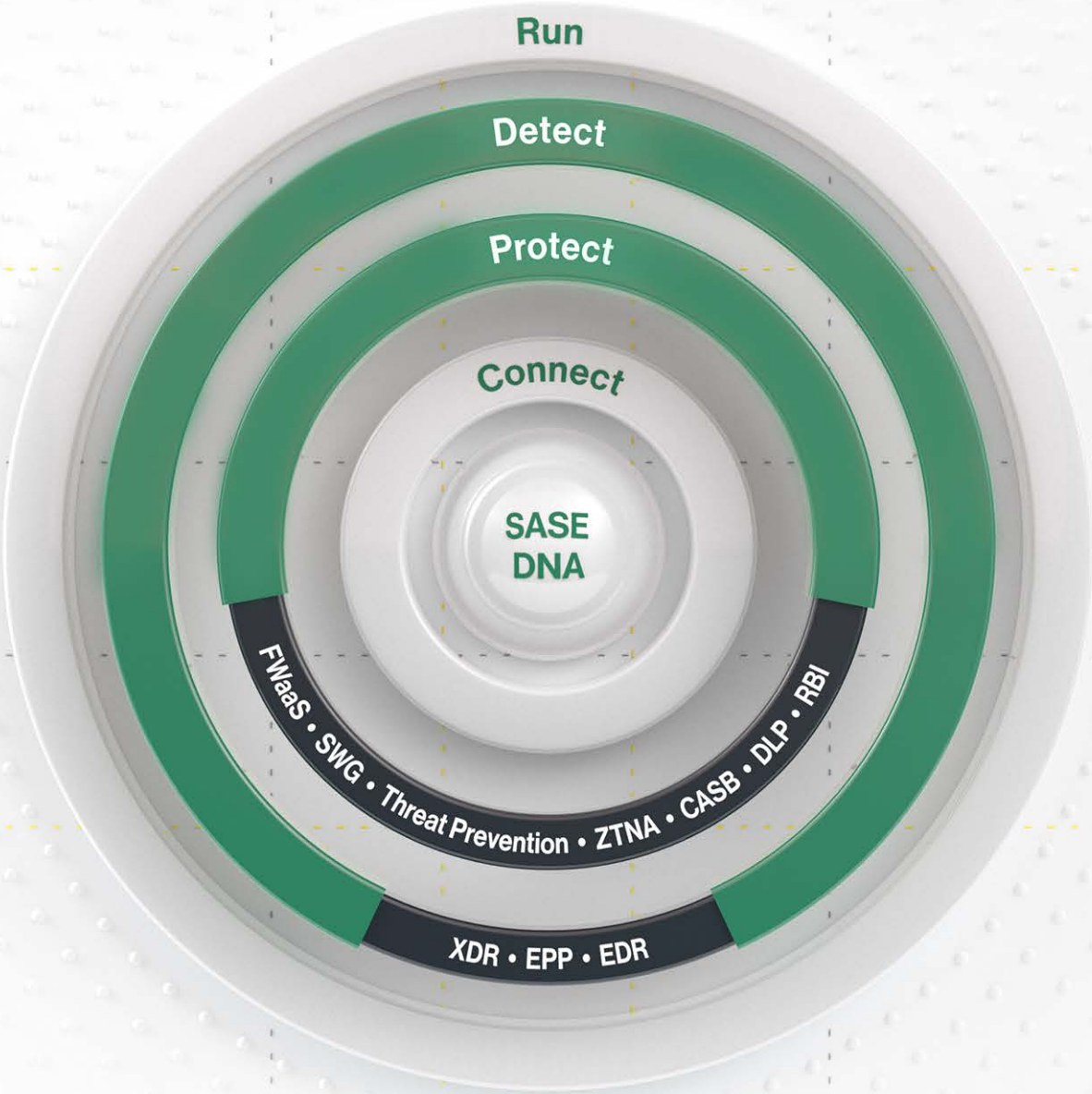
CATO
NETWORKS

Cato Networks Security as a Service

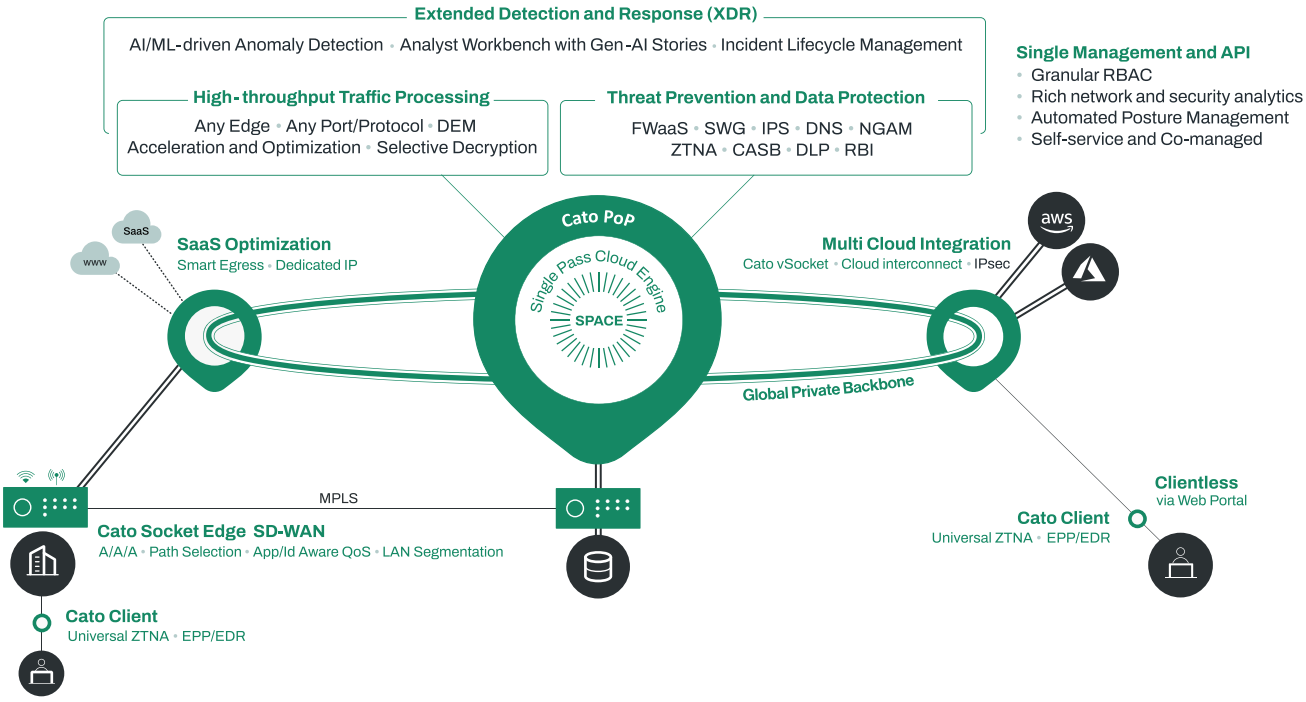


Contents

Overview

The Cato Cloud was built from the ground up to enable networking and security teams to effectively protect the corporate network from today's rapidly changing threat landscape. The Cato Security Service Edge pillar of the Cato Cloud, Cato SSE 360, converges multiple security capabilities including Firewall as a Service (FWaaS), Secure Web gateway (SWG), Cloud Access Security Broker (CASB), Data Loss Prevention (DLP), Zero Trust Network Access (ZTNA) and advanced threat prevention including IPS and Next-generation Anti Malware.

Cato provides seamless expansion from SSE to a full Secure Access Service Edge (SASE) solution by converging the networking (SD-WAN) and security (SSE 360) pillars into a global, cloud-native SASE service. With Cato, customers can enforce a unified security policy across all users, locations, and data.



Because Cato is delivered as a cloud service, customers are relieved of the burden of upgrades and updates - a big resource hog. Customers also don't need to size or scale network security. All traffic will be secured by Cato according to the customer-specific security policy while Cato is taking care of the underlying infrastructure.

As part of the service, Cato employs a dedicated research team of security experts, Cato Research Labs, who continuously monitor, analyze and tune all the security engines, risk data feeds, and databases to optimize customer protection. Enterprises of all sizes are now able to leverage the security and threat detection expertise of Cato Research Labs and a hardened cloud platform to improve their security posture.

Cato's Cloud-native Security Architecture

Cato PoP Instances: Traffic Processing Engine

PoP Structure

At the core of the Cato Cloud is a cloud network, comprised of geographically distributed Points of Presence (PoPs) each running multiple compute nodes. Each PoP runs a purpose-built software stack, the Cato Single Pass Cloud Engine (SPACE), that applies routing, encryption, optimization, and advanced security services to all traffic.

PoP Scalability and Resiliency

Cato PoPs are designed to handle massive loads of traffic. Cato can scale processing capacity by adding compute nodes to the same PoP (vertical scaling) or adding PoPs in new locations (horizontal scaling). Since Cato maintains the infrastructure, customers don't have to size their network security environment. All licensed capacity, even if encrypted, is guaranteed to be processed by the Cato PoPs for all licensed security services.

If a PoP compute node fails, the impacted edges automatically reconnect to an available node within the same PoP. In case of a full PoP failure, the impacted users and locations will automatically connect to the nearest available PoP. Regardless of which PoPs enterprise resources connect to, the Cato Cloud always maintains a consistent logical enterprise network, continously enforcing corproate security policies.

Built-in PoP DDoS Protection*

Elastic capacity enables Cato Cloud to accommodate customer growth and withstand various types of flood attacks. To reduce the attack surface, only authorized sites and mobile users can connect and send traffic to the backbone. The external IP addresses of the PoPs are protected with specific anti-DDoS measures, such as SYN cookies mechanisms and rate control mechanisms. Cato owns a block of IPs in part for automatically reassigning targeted sites and mobile users to unaffected addresses.

* Does not extend to Applicative or Volumetric DDoS protection to servers accessible via a Cato PoP

Encrypted PoP Full Mesh

All PoPs are interconnected using fully-meshed, encrypted tunnels.The encryption algorithm is AES-256 and uses restricted symmetric keys (per PoP instance). Keys are rotated every 60 minutes to reduce key exposure.

Deep Packet Inspection

The Cato SPACE includes a Deep Packet Inspection (DPI) engine built to process multi-gig traffic at wire speed, including packet header and payload.

Cato SPACE automatically identifies thousands of applications and millions of domains on the first packet. This robust library is continuously enriched by third-party URL categorization engines and machine learning algorithms that mine a massive data warehouse built from the metadata of all traffic flows traversing Cato Cloud. Customers can also configure policies to identify custom applications or have that done for them by Cato engineers.

TLS Inspection

The Cato SPACE can perform DPI on TLS-encrypted traffic for threat prevention and data protection. TLS inspection is essential as a larger share of all Internet traffic is now encrypted, and malware uses encryption to evade detection. With TLS Inspection enabled, Cato decrypts and inspects encrypted traffic. Everything is done at the PoP so there are no performance constraints. To decrypt, the customer must install Cato certificates across its network. Customers can create rules to selectively apply TLS inspection to a subset of the traffic, such as filtering packets by application, service, domain, or category, or excluding packets from trusted applications or for reasons of regulatory compliance. Even if decryption is not applied or configured, all traffic is subject to FWaaS, SWG, and IPS rules involving packet metadata, such as IP addresses and URLs.

Cato SASE Cloud

Global Private Backbone of 80 + PoPs

Cato Cloud: Full Security Protection Everywhere

North America
27 PoPs

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

Europe
18 PoPs

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

Asia
20 PoPs

Australia, Melbourne
Australia, Perth
Australia, Sydney
China, Beijing
China, Shanghai
China, Shenzhen
Hong Kong
India, Chennai
India, Mumbai
Indonesia, Jakarta
Japan, Osaka
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
8 PoPs

Brazil, Sao Paulo
Chile, Santiago
Colombia, Bogota
Costa Rica, San Jose
Ecuador, Quito
Mexico, Mexico City
Mexico, Monterrey
Peru, Lima

Middle East & Africa
6 PoPs

Israel, Tel Aviv
Kenya, Nairobi
Morocco, Casablanca
Saudi Arabia, Jeddah
South Africa, Johannesburg
United Arab Emirates, Dubai

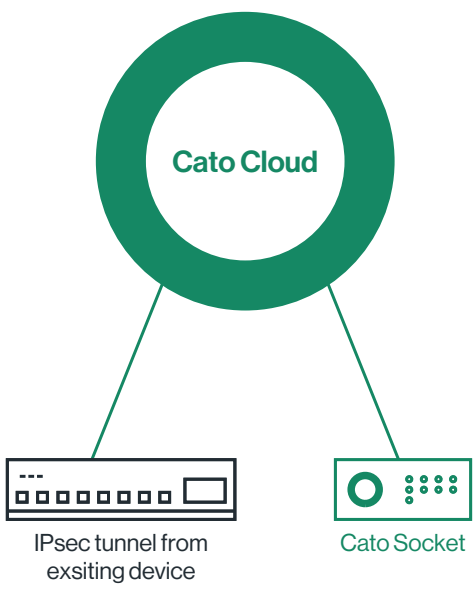
Cato Edges

Cato Socket Security

Customer edges connect to Cato through encrypted tunnels. A tunnel can be established in multiple ways. The Cato Socket is a zero-touch appliance deployed at physical locations and dynamically connects to the nearest PoP across a DTLS tunnel for optimum security and efficiency. If a tunnel disconnects due to a PoP failure, the Cato Socket reestablishes the tunnel to nearest available PoP. Alternatively, customers can use IPSec-enabled devices, such as UTMs or firewalls, to connect to the nearest PoP.

Sockets are secured by:

- Blocking all external traffic, only responding to authenticated traffic
- Restricting administrative access from internal interface via HTTPS or SSH
- Forcing administrators to set new passwords upon first-time login
- Storing no data from processed packets
- Encrypting all communications
- Securely distributing updates over an encrypted communication, cryptographically authenticated (digitally signed software packages)



Cato Client for Laptops and Mobile Devices

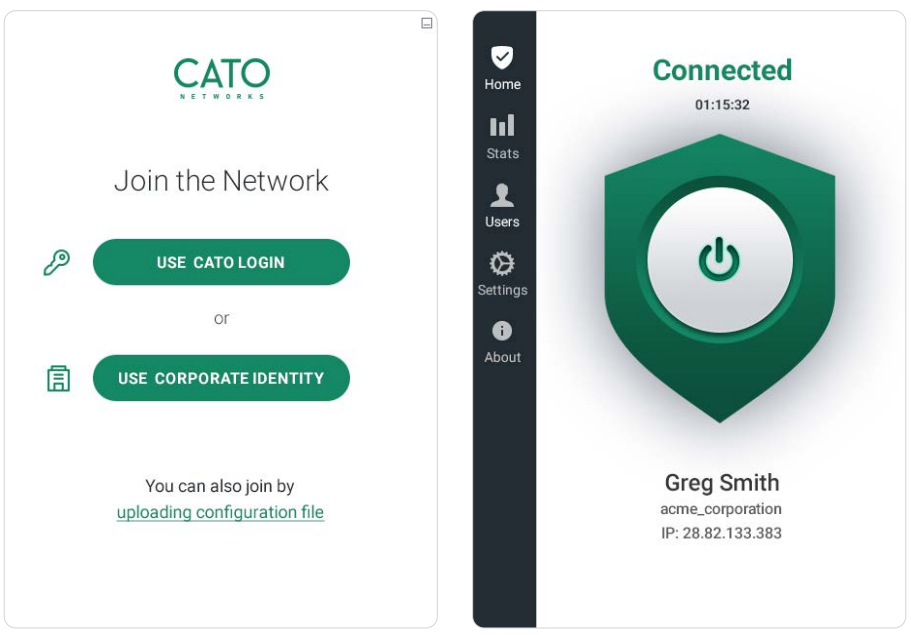
The Cato Client runs on mobile devices, including personal computers, tablets and smartphones covering Windows, Mac, iOS and Android. Cato Client uses device VPN capabilities to create an encrypted tunnel to the nearest PoP of the Cato Cloud.

Onboarding of mobile Users is initiated via integration with Active Directory, or through user configuration in the management application. Users are invited to register to Cato via email. Users provision themselves in several steps through a dedicated portal. User authentication can be done in several ways:

Username and Password: As part of the onboarding process and depending on the selected authentication method, users can set their authentication password. Cato ensures password confidentiality at all times, whether at rest or in transit.

Multi-factor Authentication (MFA): Cato provides several methods of MFA, including SMS and Google Authenticator.

Single Sign-on (SSO): Cato supports integration with the corporate identity management system, authenticating users with their corporate credentials.



Cato Security Service Edge (SSE 360)

Cato SSE 360 is a set of enterprise-grade and agile network security capabilities, delivered through the Cato Single Pass Cloud Engine (SPACE). Current capabilities include Firewall as a Service (FWaaS), Secure Web gateway (SWG), Cloud Access Security Broker (CASB), Data Loss Prevention (DLP), Zero Trust Network Access (ZTNA) and advanced threat prevention including IPS and Next-generation Anti Malware. Because Cato built the platform, new capabilities can be added quickly without impact to the customer environment. All capabilities are configured and managed through Cato's management application providing a single pane of glass.

Firewall-as-a-Service (FWaaS)

Cato FWaaS inspects both WAN and Internet traffic. It can enforce granular rules based on device, network, application, identity, risk and many other access context attributes.

Application Awareness

Cato FWaaS provides full application awareness, regardless of port, protocol, evasive techniques, or SSL encryption. Cato SPACE extracts the relevant context, such as application or services, as early as the first packet and without SSL inspection. Cato Research Labs continuously enriches the application database to expand coverage.

Cato provides a full list of signatures and parsers to identify common applications. In addition, custom application definitions identify account-specific applications by port, IP address or domain. Both types of application definitions are available for use by the security rules enforced by Cato.

User Awareness

Cato enables admins to create contextual security policies based on individual users, groups, or roles. In addition, Cato's built-in analytics can be viewed by site, user, group or application, to analyze user activity, security incidents and network usage.

Today at 11:18 AM | a few seconds | 1 | URL Filtering | Dev Socket | Compromised | Block

Time	FRQ	Src Host	Src Country	Dest IP	Dest Country	Dest Port	Service	App Category	HTTP host	DNS
Oct 30, 2017 11:18 AM	1	Natis-MBP	Israel	5.10.78.77	Netherlands	443		Compromised	www.fqtag.com	www.

Today at 1:07 PM | a few seconds | 2 | URL Filtering | GT Industries | Compromised | Block

Time	FRQ	Src User	Src Host	Src Country	Dest IP	Dest Country	Dest Port	Service	App Category	HTTP host	DNS	O
Oct 30, 2017 1:07 PM	2	sjones	172.16.101.23	United States	144.217.180.2	Canada	80		Compromised	img0.joyreactor.com	img0.joyreactor.com	W

LAN Segmentation

Cato FWaaS supports the definition of LAN segments as part of the site context. Cato supports several types of LAN segments:

- **VLANs -** VLAN tags are stripped as packet enter the Cato Cloud, then upon re-entering the LA N the VLAN tag is re-applied
- **Routed Range -** LAN segments that are connected through a router into a Socket
- **Direct Range -** LAN segments that are directly connected to the Socket, not via a router, and are different than the site's native range

By definition, no traffic is allowed between different segments. Allowing such connections requires the creation of local segmentation rules, enforced by the Cato Socket, or the creation of WAN firewall rules that are enforced by the Cato Cloud with full inspection of the traffic.

Networks

LAN1

Range Type	IP Ranges		Characteristics			
Native Range	Range:	10.10.2.0/24		Gateway: 10.10.2.1 ID(VLAN):	DHCP Range:	10.10.2.100-10.10.2
VLAN	Range:	192.168.2.0/24	Name: Guest Wifi	Gateway: 192.168.2.1 ID(VLAN): 302	DHCP Range:	192.168.2.10-192.1

LAN Segmentation Specifications

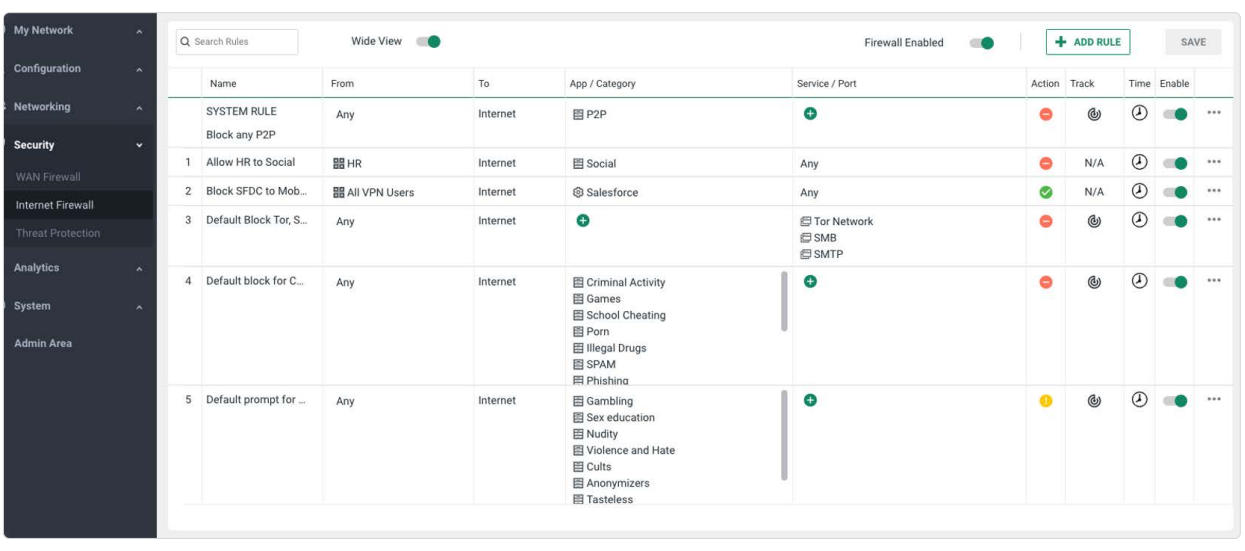
WAN Traffic Protection

Using the WAN firewall, security admins can allow or block traffic between organizational entities such as sites, users, hosts, subnets, and more. By default, Cato's WAN firewall follows a whitelisting approach, having an implicit any-any block rule. Administrators can either follow this approach or switch to blacklisting.

WAN Sites Access Rules

Internet Traffic Protection

Using the Internet firewall, security admins can set allow or block rules between network entities such as sites, individual users, subnets, and more to various applications, services, and websites. By default, Cato's Internet firewall follows a blacklisting approach. Thus, to block access, you must define rules that explicitly block connections from one or more network entities to applications. Admins can switch to whitelisting if necessary.



	Name	From	To	App / Category
	SYSTEM RULE Block any P2P	Any	Internet	P2P
1	Allow HR to Social	HR	Internet	Social
2	Block SFDC to Mob...	All VPN Users	Internet	Salesforce
3	Default Block Tor, S...	Any	Internet	

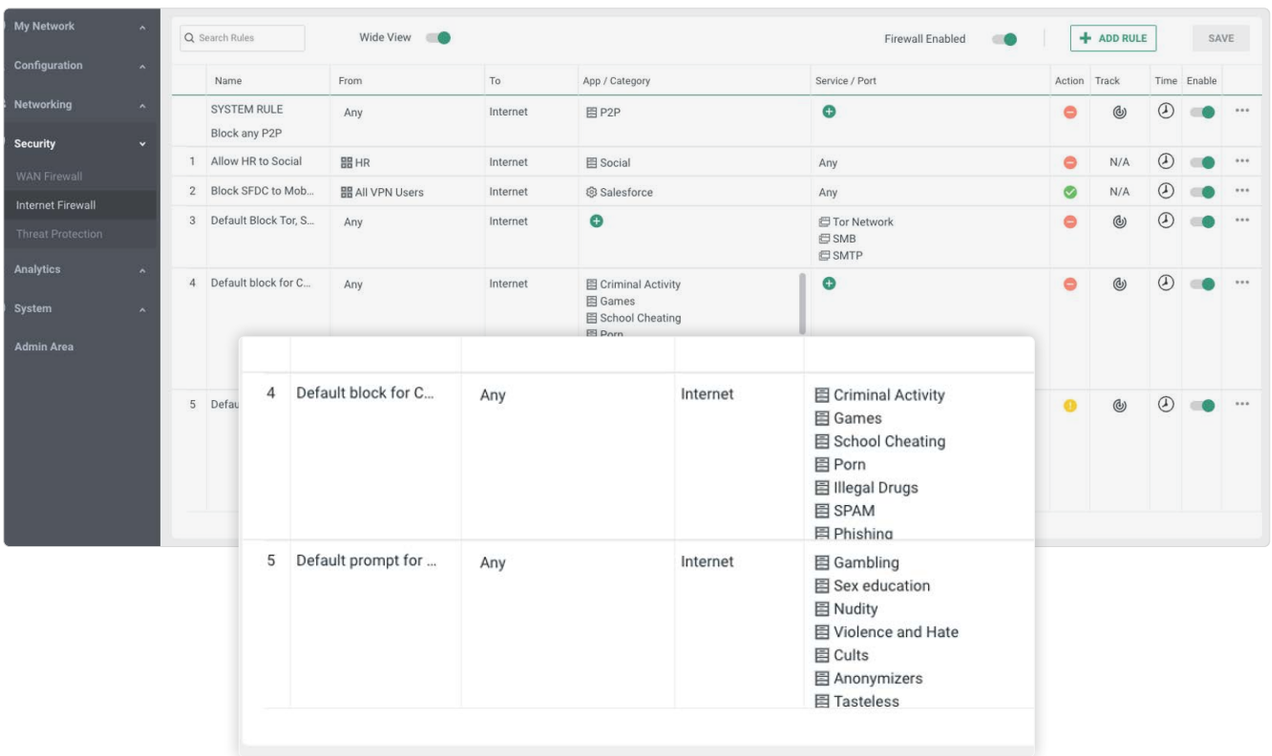
Internet Applications Access Rules

Secure Web Gateway (SWG)

Cato SWG allows customers to monitor, control and block access to websites based on predefined and/or custom categories. Cato creates an audit trail of security events on each access to specific configurable categories. Admins can configure access rules based on URL categories.

URL Categorization and Filtering Rules

Out of the box, Cato provides a predefined policy of dozens of different URL categories including security-oriented categories such as Suspected Spam and Suspected Malware. As part of the default policy, each category is set with a customizable default action, Cato enables admins to create their own categories and use them in custom rules, enhancing the granularity of web access control.



URL Categories and Default Action

URL Filtering Actions

Each category of URL filtering rule has the following actions:

- **Allow:** lets the user access the target URL.
- **Block:** prevents the user from accessing the target URL, redirecting to dedicated blocking page.
- **Monitor:** lets the user access the target URL and records the access event in the event log.
- **Prompt:** redirects the user to a dedicated warning page about the URL. The user can decide whether or not to proceed. This event is recorded in the event log.

Malware Prevention

As part of Cato's Advanced Threat Protection, Cato offers several premium services. One of these is anti-malware protection. Customers can use this service to inspect both WAN and Internet traffic for malware. Anti-malware processing includes:

Deep Packet: Inspection of traffic payload for clear and encrypted traffic (if enabled). File objects are extracted from the traffic stream, inspected, and blocked, where appropriate.

True Filetype Detection: Is used to identify the actual type of a file going over the network regardless of its file extension or the content-type header (in case of HTTP/S transfer). Cato uses this capability to detect all potential high-risk file types, defeating evasion techniques that are used by either attackers or misconfigured web-applications. This engine is also used by Cato IPS providing more context during flow analysis and acts as a key factor in detection of malicious network behavior.

Malware Detection and Prevention: Leverages multi-layered and tightly-integrated anti-malware engines. First, a signature and heuristics-based inspection engine, which is kept up-to-date at all times based on global threat intelligence databases, scans files in transit to ensure effective protection against known malware.

Second, we've partnered with SentinelOne, an industry leader, to leverage machine learning and artificial intelligence to identify and block unknown malware. Unknown malware can come as either zero-day attacks or, more frequently, as polymorphic variants of known threats that are designed to evade signature-based inspection engines. With both signature and machine learning-based protections, customer data remains private and confidential, as Cato does not share anything with cloud-based repositories.

Processing happens at line speed, without imapct to the end user experience. When a malicious file is detected, user access will be blocked, and the user will be redirected to a block page. Customers have the ability to configure Cato's anti-malware service to either monitor or block. It is possible to apply exceptions for specific files for a set duration.

Intrusion Prevention System (IPS)

Cato's IPS inspects inbound and outbound, WAN and Internet traffic, including TLS-encrypted traffic. IPS can operate in monitor mode (IDS) with no blocking action taking place. In IDS mode, all traffic is evaluated and security events are generated.

IPS Protection Engines

The Cato IPS is comprised of several layers of protection:

Behavioral Signatures: Cato IPS looks for deviation from normal or expected behavior of the system or the user. Normal behavior is identified by using Cato's big data analytics and our deep traffic visibility across many networks. For example, an outgoing HTTP connection to an unknown URL containing a suspicious TLD. Following research that was conducted by Cato Research Labs, such traffic is likely to be malicious.

Reputation Feeds: Leveraging both in-house and external intelligence feeds, the Cato IPS can detect or prevent inbound or outbound communication with compromised or malicious resources. Cato analyzes many different feeds, validates them against traffic in the Cato Cloud, and sanitizes them to reduce false positives before applying them to production customer traffic. Feeds are updated on an hourly basis without any involvement of the customer.

Protocol Validation: Cato IPS validates packet conformance to the protocol, reducing attack surface from exploits using anomalous traffic.

Known Vulnerabilities: Cato IPS protects against known CVEs, and rapidly adapts to incorporate new vulnerabilities into the IPS. An example of this capability is how Cato IPS blocks the Eternal-Blue exploit used extensively to spread ransomware within organizations. (For more information, see here and here.)

Malware Communication: Cato IPS can stop outbound traffic to C&C servers based on reputation feeds, and network behavioral analysis.

Geolocation: Cato IPS enforces a customer-specific geo-protection policy, optionally stopping traffic based on the source and/or destination country.

Network Behavioral Analysis: Cato IPS can detect and prevent inbound/outbound network scans.

IPS as a Service

One of the unique characteristics of the Cato IPS is that it is provided as a service with zero involvement required from the customer. Cato updates, tunes and maintains IPS signatures, both those developed in house (based on big-data collection and analysis of customers' traffic), and those originating from external security feeds. Cato Cloud scales to support signature processing so customers don't have to balance protection and performance to avoid unplanned upgrades as processing load exceeds available capacity.

Cloud Access Security Broker (CASB)

Cato CASB enables enterprises to gain better visibility and control over their cloud-hosted applications. It provides in-depth visibility into SaaS usage and enables enterprises to better cope with shadow IT.

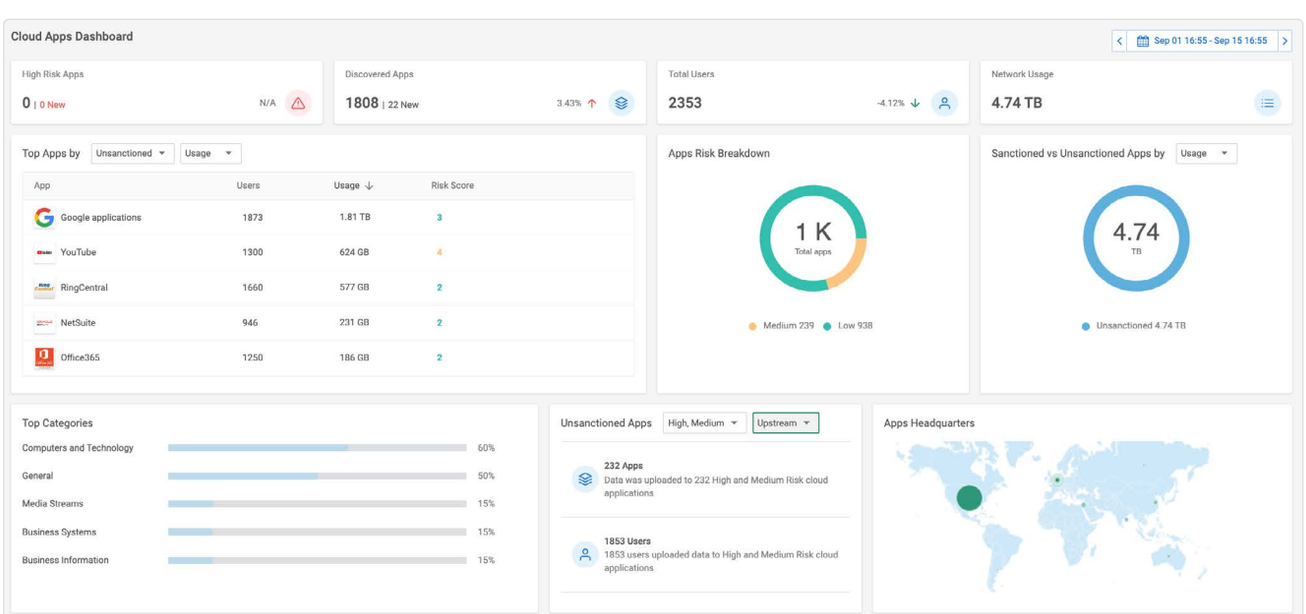
Cato CASB is comprised of four stages:

Visibility: The first challenge of cloud-based SaaS usage is understanding its full extent. While some applications have been procured and provided by the IT team itself, also referred to as sanctioned applications, many SaaS applications are being adopted and used by employees without the IT department's approval and knowledge. These are unsanctioned applications, and their usage constitutes what is known as Shadow IT.

Assessment: The second stage is understanding the business need as well as the risk each unsanctioned application poses. This enables making decisions regarding its permitted usage.

Enforcement: Once the analysis phase is done and the required access policy is determined for each app, the rules which will enforce this policy can be defined via the Cato SASE Cloud Management Application.

Protection: The last stage is ensuring the protection of SaaS usage. Cato's SASE achieves this through the convergence of its security tools. All SaaS traffic is processed by multiple security tools including FWaaS, SWG, IPS, NGAM and Datal Loss Prevention (DLP).



CASB: Cloud Apps Dashboard

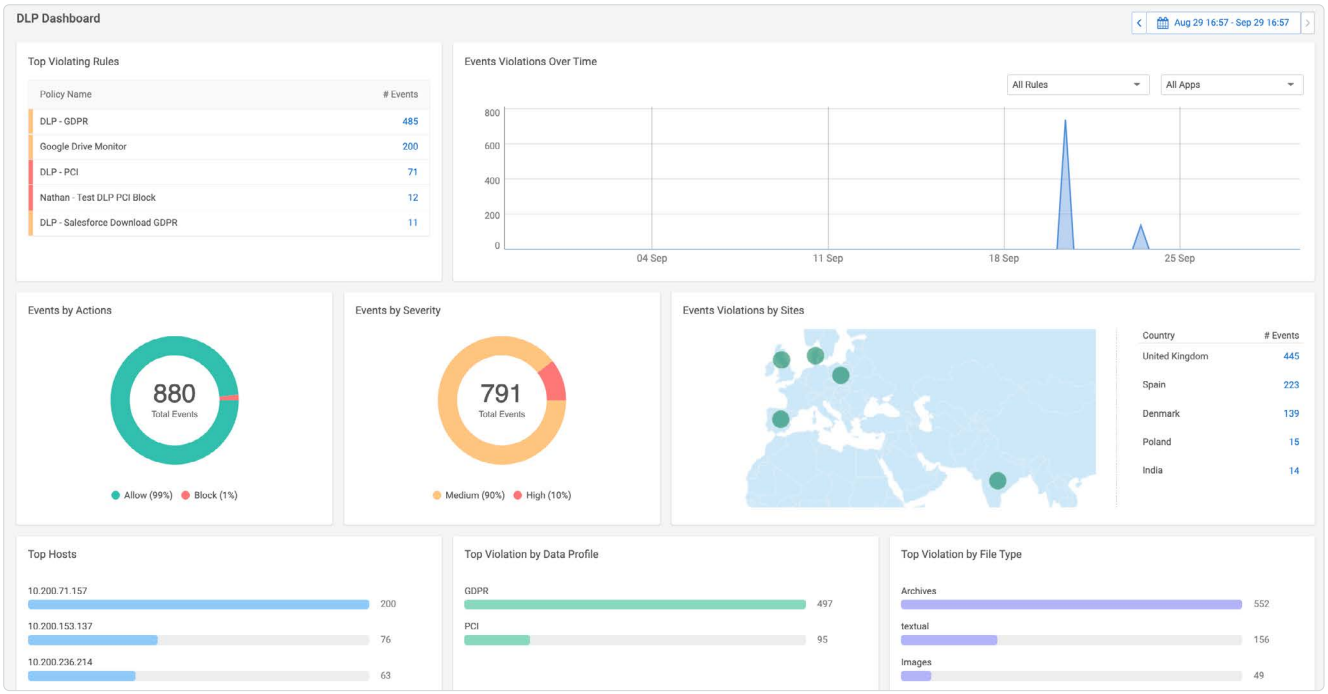
Data Loss Prevention (DLP)

Cato DLP allows enterprises to protect sensitive data against unintentional loss or a data breach. Natively built into Cato SASE Cloud, Cato DLP has full visibility to all traffic from all sources and to all destinations.

Comprehensive Sensitive Data Visibility and Control: Cato DLP enables comprehensive sensitive data visibility and control inline to any web site or cloud application. Data protection via APIs is available for leading cloud app providers.

Extensive Out-of-the Box Detection: Rich, preconfigured library of over 350 data types and file types enables detection of a wide range of sensitive global and national data formats such as social security numbers and credit card numbers, as well as files storing intellectual property.

Streamlined DLP Policy Configuration and Analytics: Easy to configure policies allows granular access control according to types of sensitive data, required action, and dynamic access risk assessment to meet compliance mandates. A dedicated dashboard and efficient event log filtering provide immediate visibility for monitoring, investigation and remediation of potential data loss events.



Remote Browser Isolation (RBI)

Browsing is a serious security risk since browsers run website code on the local device. Malicious code can let cybercriminals onto the device, and from there, onto the network. Admins typically block bad sites using a Secure Web Gateway (SWG), but it can be frustrating and unproductive for users if the SWG blocks every new, uncategorized site. Cato's Remote Browser Isolation (RBI) service provides secure browsing through a virtualization service that streams web pages safely to the user's device. In-browser code is executed remotely, keeping users safe from threats such as ransomware and phishing. For uncategorized websites, Cato RBI gives Admins a new option, to 'Isolate', that allows end users to browse safely, without disrupting their productivity. Cato RBI adds another layer of protection against web- and browser-based threats, protecting against new attacks not yet documented, new sites not yet categorized, and user error.

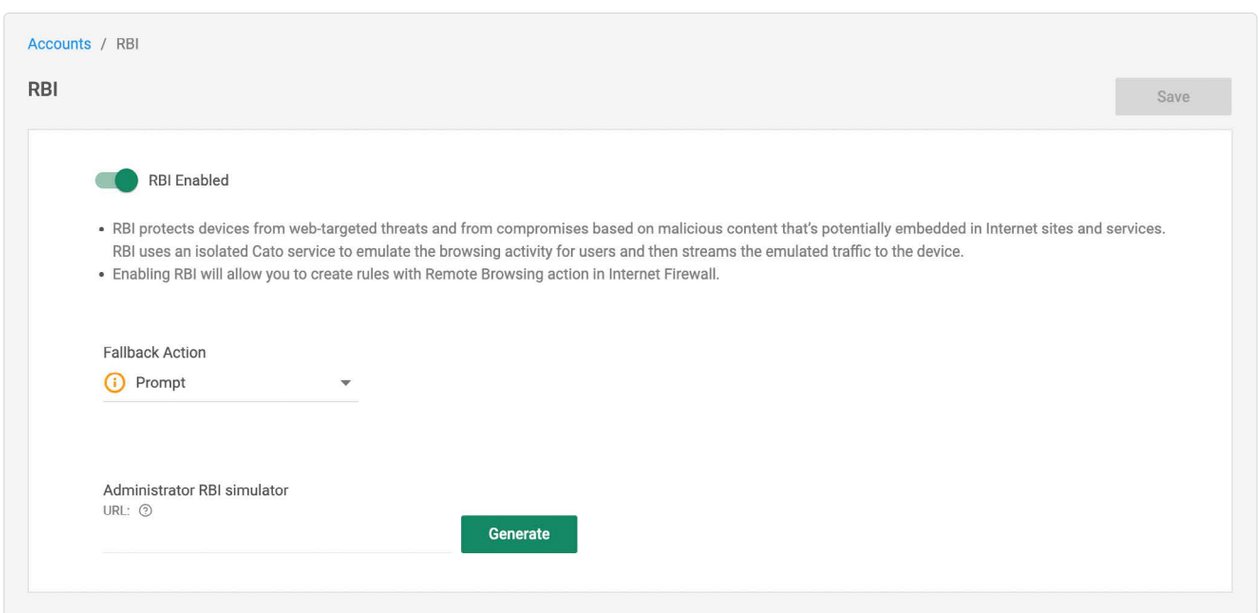
Fast : Cato's RBI is accessible in minutes with just a few clicks. It does not require configuration and works out of the box. Alongside "Allow", "Block" and "Prompt", admins simply have a new option to "Isolate" uncategorized pages.

Simple: Cato's RBI requires zero maintenance. There is nothing to install and nothing to patch. It is a seamless part of the Cato service.

Secure: Cato's RBI renders web pages safely to the user's device as a stream of pixels. In-browser code is executed remotely, and downloads are blocked, keeping users safe.

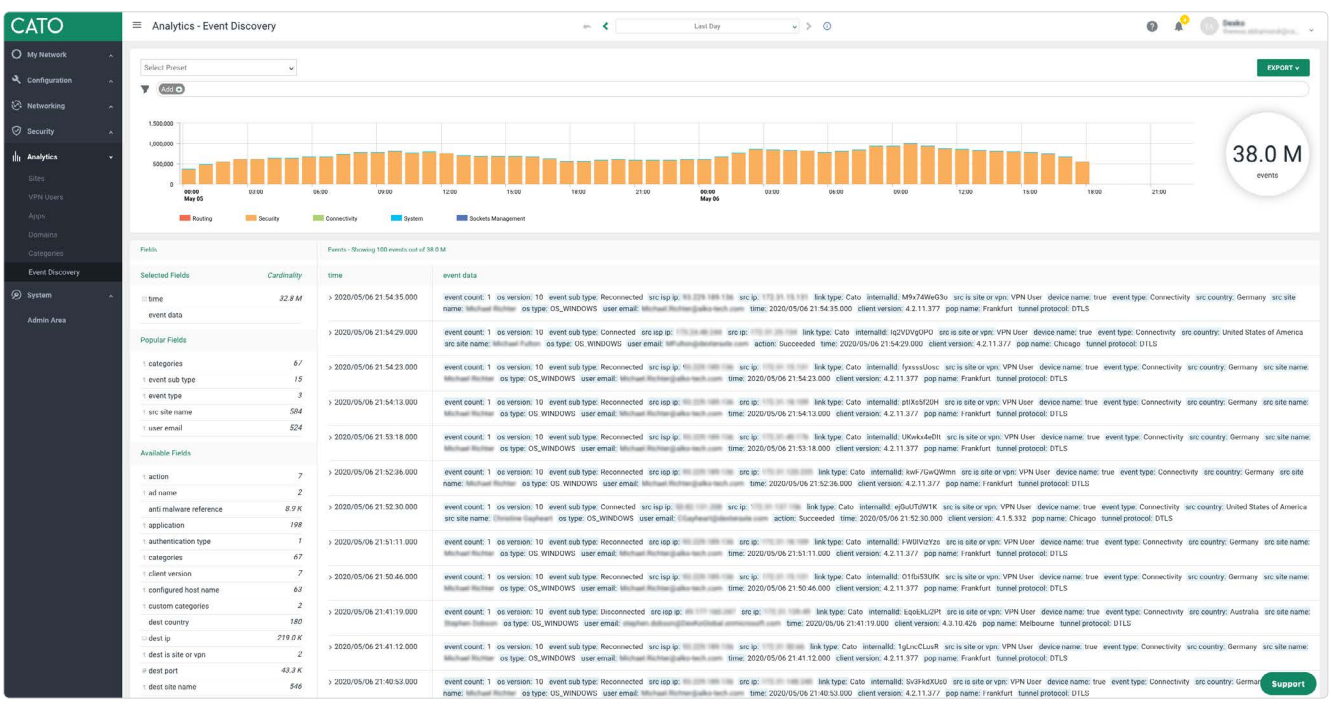
All edges: Cato RBI applies to all web traffic from all edges. There is no need to configure in multiple locations or for different edges.

Flexible: Cato's robust multi-layered protection (including IPS, Anti-malware, Next-Gen Anti-malware, CASB, and DLP) allows admins to choose which traffic to route through RBI, keeping users both productive and safe.



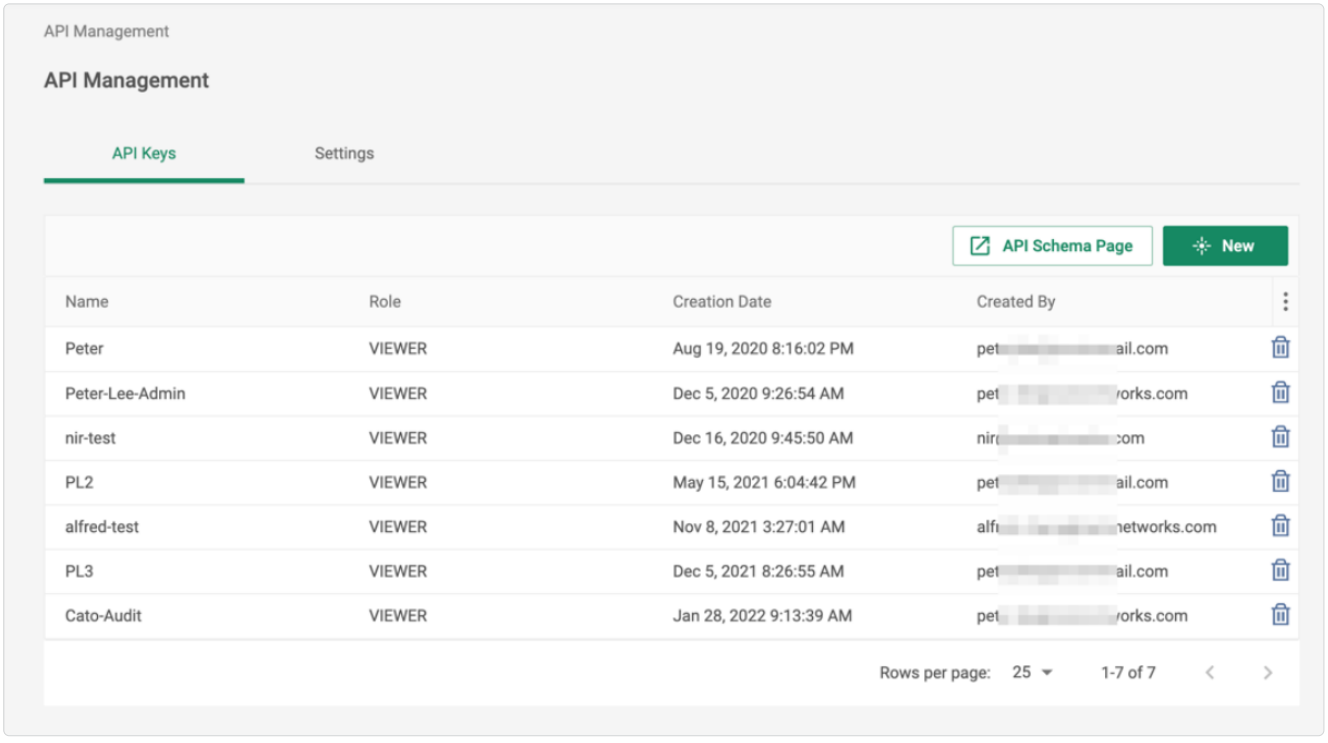
Event Discovery

Event Discovery provides the IT team with the advanced hunting and research capabilities of a high-end operations center. Event Discovery organizes more than 100 network and security events into a single, queryable timeline. Complex queries can be easily built by selecting from the types and sub-types of events presented on the screen. The data warehouse is stored and maintained by Cato.



Security Event API

Cato continuously collects networking and security event data for troubleshooting and incident analysis. 6 months of data is kept by default. Customers can programmatically download configuration, status and event data via Cato's GraphQL API for integration with a SIEM system or storage in a remote location. All access to the Cato API requires an API key generated in the Cato Management Application (CMA) by account administrators.



Cato 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.

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

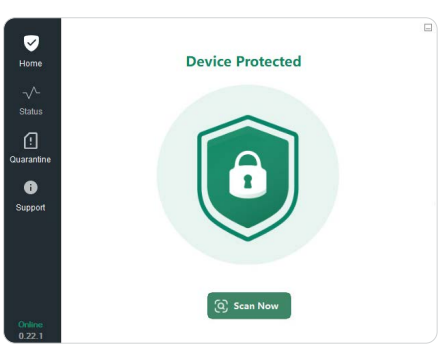
Admins see Endpoint events alongside network, security and user events, giving them a single context and allowing them to correlate events. This gives them better understanding than with a separate EPP.

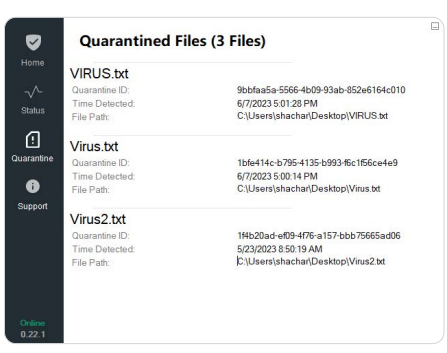
Faster Remediation

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.





Extended Detection and Response (XDR)

Cato XDR

Cato XDR helps security teams detect and respond to incidents, helping them be 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 interesting phenomena while reducing noise. It reduces alert fatigue by correlating Block alerts from prevention engines. It finds threats that real-time engines cannot see, correlating signals with heuristics and machine learning, to detect elusive threats. It detects suspicious behavior using advanced statistical models and UEBA to find anomalies.

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 the Cato Single Pass Processing Engine (SPACE). 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 17,000 of confirmed incidents.

Our native data is enriched with more than 250+ proprietary and 3rd party sources and more than 5M records of valid Indicators of compromise (IoCs).

Investigate faster with guided information

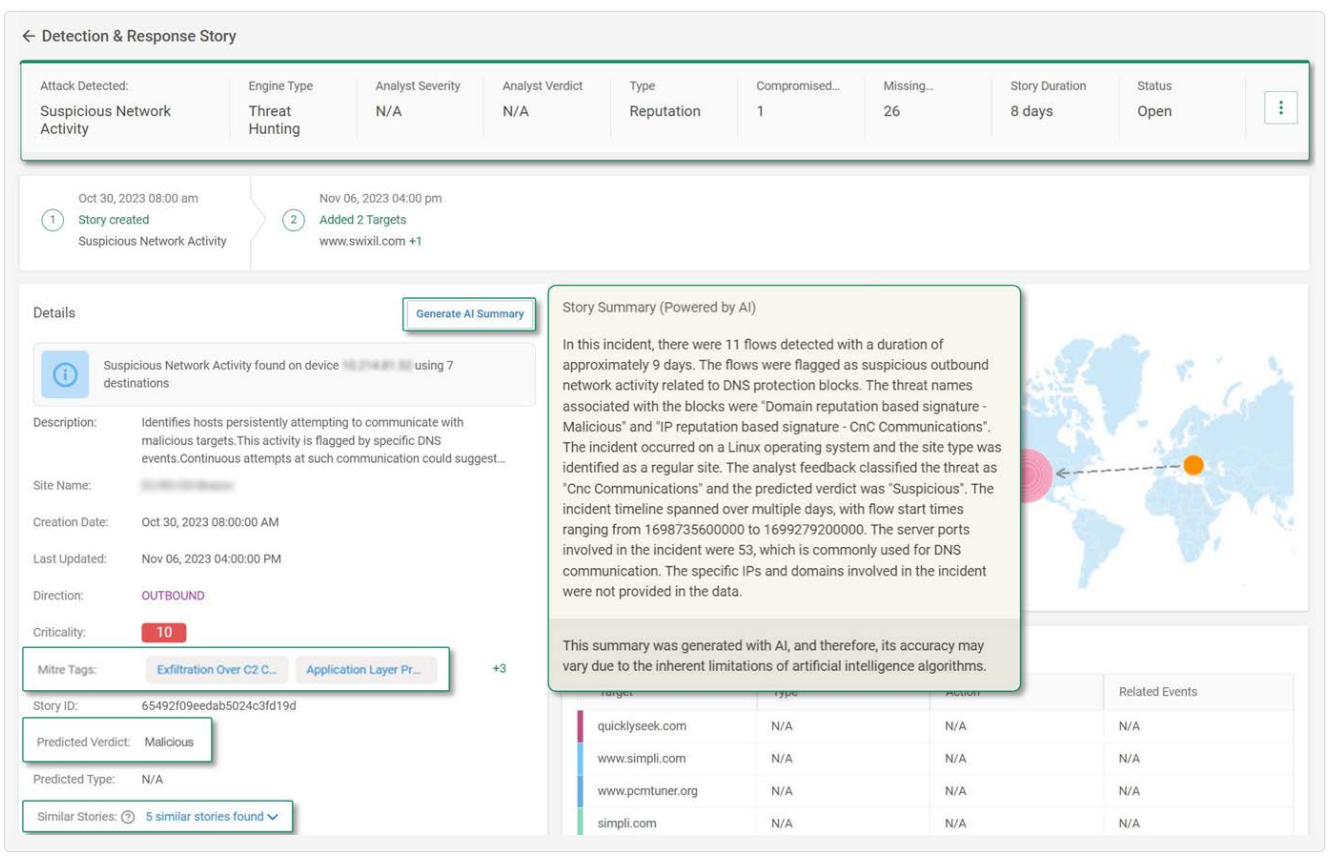
Detected incidents contain all the information required for an in-depth investigation. The information is rich, accurate, easy to analyze, all in one place and presented in a guided order, reducing the time investigate and thus increasing analyst capacity.

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.



Cato Managed XDR

Customers who wish to have Cato XDR managed for them can choose a managed service from their Cato Partner, or from Cato, whose management service is called Managed XDR.

Cato Managed XDR enables enterprises to offload the resource-intensive and skill-dependent process of detecting, investigating and remediating threats to the Cato SOC team.

Cato collects and analyzes all network flows, verifies suspicious activity, and notifies customers of important threats. This is the power of networking and security convergence to simplify network protection for enterprises of all sizes.

Cato Managed XDR Service Capabilities

Expert Threat Verification: Cato security researchers review flagged threats over time and assess the risk. The Cato SOC will only alert on actual threats.

Threat Containment: Verified live threats can be contained automatically by configuring customer network policies to block C&C domains and IP addresses or disconnect a compromised machine or user from the network.

Remediation Assistance: The Cato SOC will advise on the threat level of risk, recommended remediation, and a follow up until the threat is eliminated.

Reporting and Tracking: Every month, the Cato SOC will issue a custom report summarizing all threats detected, their descriptions and risk levels, as well as impacted endpoints.

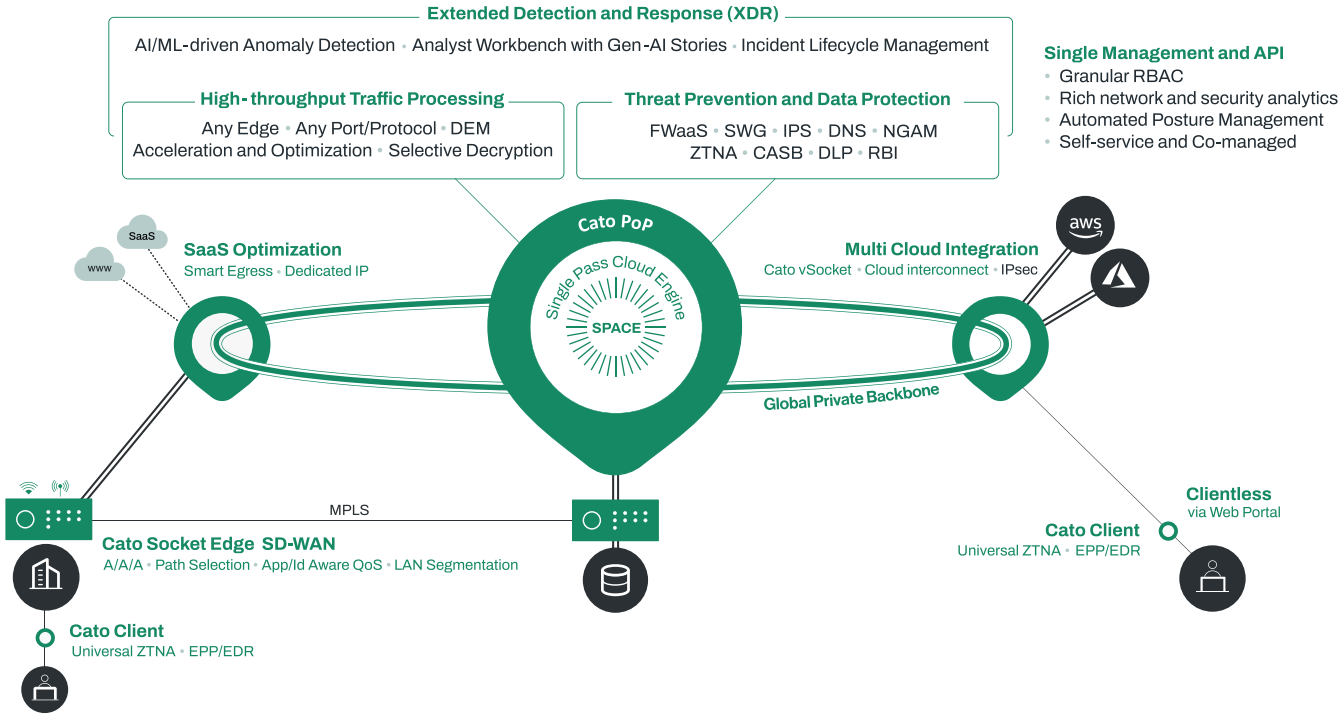
Summary

Cato SSE 360 enables organizations of all sizes to apply enterprise-grade protection everywhere. Datacenters, branches, mobile users, and cloud resources can be protected under a unified policy and with the same set of defenses. As a cloud service, Cato seamlessly optimizes and adapts security controls for emerging threats without any customer involvement. Traditional chores associated with appliance-based security, such as capacity planning, sizing, upgrades, and patches, are no longer needed, offloading that responsibility from security teams. With Cato, customers maintain an optimal security posture at all times and minimize the risk of breach and data loss. They can keep security teams focused on the business and budgets under control.

About Cato Networks

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

Cato SASE Cloud Platform



Cato. WE ARE SASE.

Cato SASE Cloud Platform

Connect

Cloud Network

Cloud On-Ramps

Protect

Network Security

Endpoint Security

Detect

Incident Life Cycle Management

Run

Unified Management and API

Use Cases

Network Transformation

MPLS to SD-WAN Migration

Global Access Optimization

Hybrid Cloud and Multi-Cloud Integration

Business Transformation

Vendor Consolidation

Spend Optimization

M&A and Geo Expansion

Security Transformation

Secure Hybrid Work

Secure Direct Internet Access

Secure Application and Data Access

Incident Detection and Response