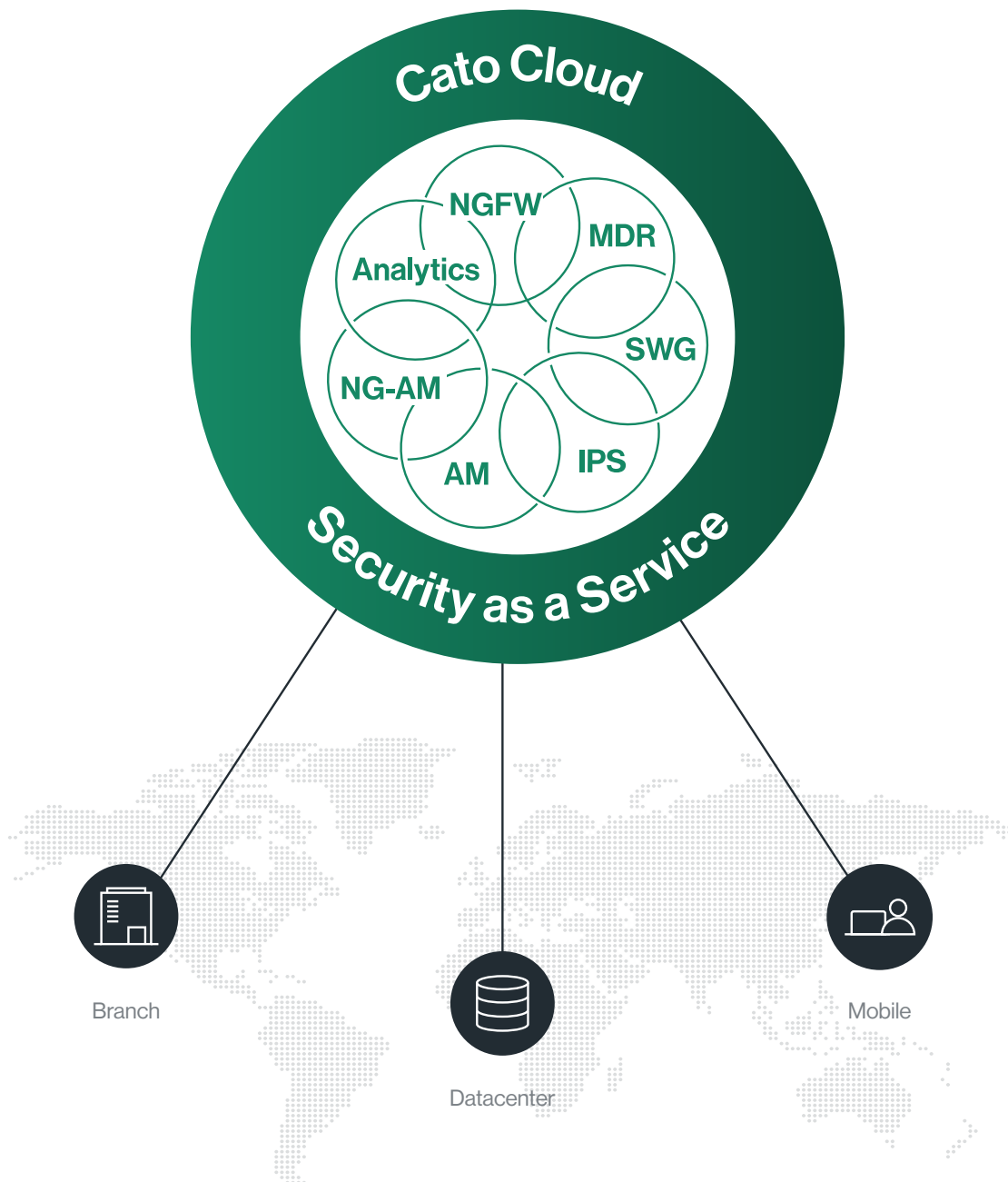


Cato Networks Security as a Service



Contents

Overview	3
-----------------	---

Last- and Middle-mile Cato Security Architecture	4
---	---

Cato PoP Instances: Traffic Processing Engine	4
---	---

Cato Socket and Appliance Connectivity	5
--	---

Cato Client for Laptops and Mobile Devices	5
--	---

Cato Edges	5
-------------------	---

Cato Security as a Service	6
-----------------------------------	---

Next-generation Firewall	6
--------------------------	---

Secure Web Gateway	7
--------------------	---

Anti-malware	8
--------------	---

IPS	9
-----	---

Security Events API	9
---------------------	---

Managed Threat Detection and Response	10
--	----

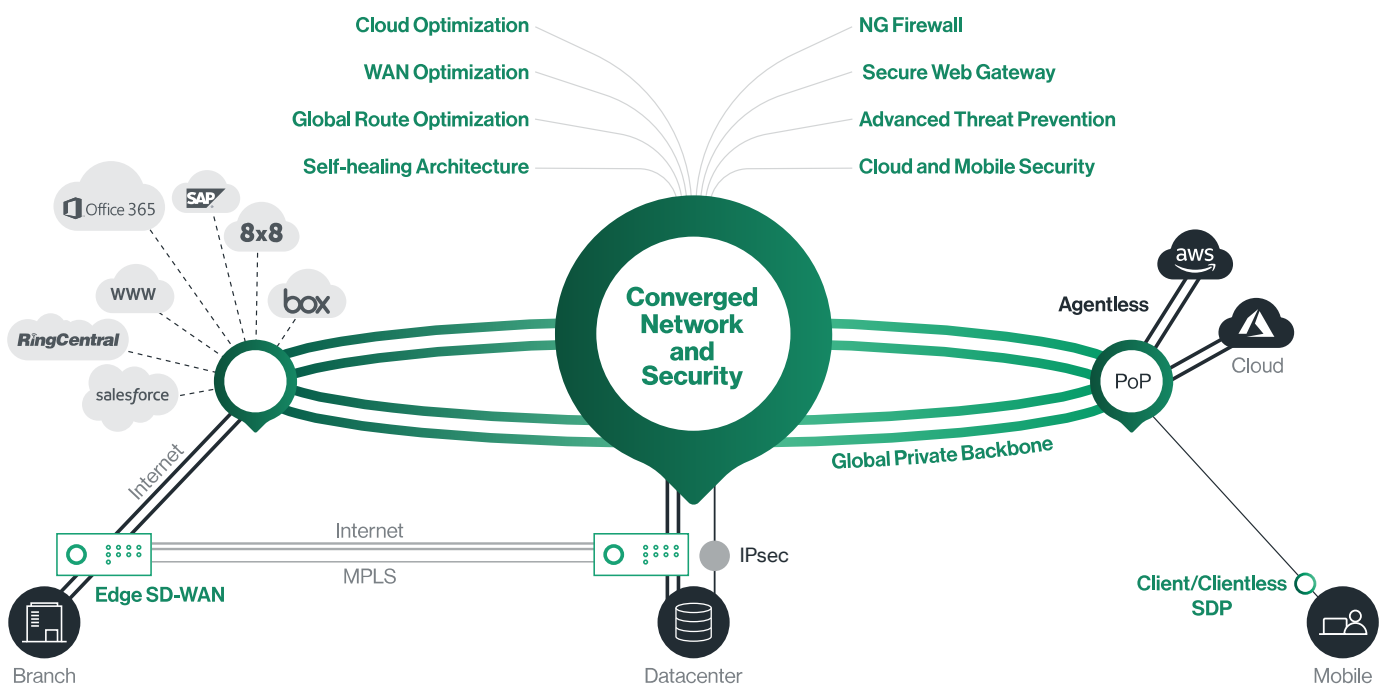
Summary	10
----------------	----

Cato MDR Service Capabilities	10
-------------------------------	----

About Cato Networks	11
----------------------------	----

Overview

Cato Networks provides a global and secure managed SD-WAN Service — the Cato Cloud. 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. Cato's unique characteristic is the convergence of the networking and security pillars into a single platform. Convergence enables Cato to collapse multiple security solutions such as a next generation firewall, secure web gateway, anti-malware, and IPS into a cloud service that enforces a unified policy across all corporate locations, users 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 passing to Cato's licensed security services will be handled 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.

Last- and Middle-mile Cato 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 processing servers. Each PoP runs a purpose-built software stack that applies routing, encryption, optimization, and advanced security services on all traffic. The PoP is comprised of multiple, powerful commodity off the shelf servers (COTS) running the same software stack.



PoP Scalability and Resiliency

Cato PoPs are designed to handle massive loads of traffic. Cato can scale processing capacity by adding server instances to the same PoP (vertical scaling) or adding PoPs in new locations (horizontal scaling). Since Cato maintains the infrastructure, customers are freed from sizing 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 server instance fails, the impacted edges automatically reconnect to an available server within the same PoP. In case of a full PoP failure, the impacted edges will connect to the nearest available PoP. Regardless of which PoPs enterprise resources connect to, the Cato Cloud always maintains a consistent logical enterprise network, creating a substantial degree of availability and resiliency.



Built-in PoP DDoS Protection

Cato PoPs are built to process large amount of traffic simultaneously. 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.



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 PoP software includes a Deep Packet Inspection (DPI) engine built to process massive amounts of traffic at wire speed, including packet header or payload. The DPI engine is used by multiple Cato security services including NGFW anti-malware, IDS/IPS and network control (SD-WAN).

Our DPI engine 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 PoP can perform DPI on TLS-encrypted traffic for advanced threat protection service's such as anti-malware and IDS/IPS. 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 NGFW, URL filtering, and IPS rules involving packet metadata, such as IP addresses and URLs.



Cato PoPs - Advanced Security Everywhere

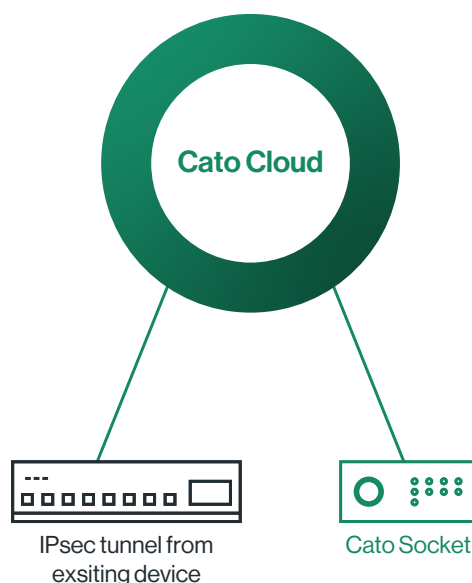
Cato Edges

Cato Socket and Appliance Connectivity

Customers 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. The Cato Socket 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- or GRE-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

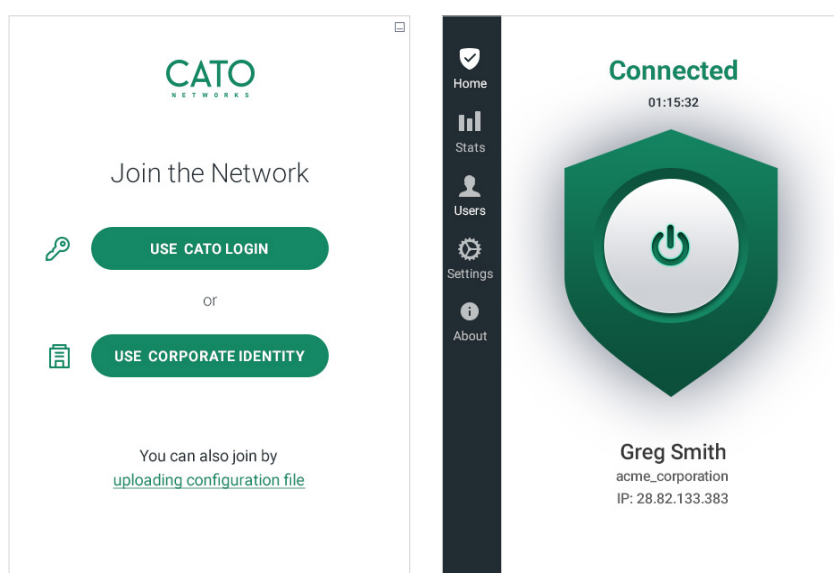
The Cato Client runs on mobile devices, including personal computers, tablets and smartphones covering Windows, Mac, iOS and Android. Cato Client uses device VPN capabilities to tunnel to Cato. Support is also available for additional VPN clients.

Onboarding of mobile Users can be 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 as a Service

Cato Security as a Service is a set of enterprise-grade and agile network security capabilities, built directly into the cloud network as part of a tightly integrated software stack. Current services include a next-generation firewall (NGFW), secure web gateway (SWG), advanced threat prevention, security analytics, and a Managed Threat Detection and Response (MDR) service. Because Cato controls the code, new services can be rapidly introduced without impact on the customer environment. Customers can selectively enable the services, configuring them to enforce corporate policies.

Next-generation Firewall

The Cato NGFW inspects both WAN and outbound Internet traffic. It can enforce granular rules based on network entities, time restrictions, type of traffic.



Application Awareness

Cato NGFW provides full application awareness, regardless of port, protocol, evasive techniques, or SSL encryption. The DPI engine classifies the relevant context, such as application or services, as early as the first packet and without SSL inspection. The relevant information is extracted from network metadata. Cato Research Labs continuously enriches the application database to expand coverage.

The DPI-classified context is available throughout Cato whether for network and security monitoring; network visibility for identifying “Shadow IT” and other trends; or for enforcement, such as enforcing block/allow/monitor/prompt rules.

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 running in Cato.



User Awareness

Cato enables admins to create contextual security policies by defining and enabling access control to resources 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.

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

Time	FRQ	Src User	Src Host	Src Country	Dest IP	Dest Country	Dest Port	Service	App Category	HTTP host	DNS
Today at 1:07 PM					URL Filtering		GT Industries	Compromised		Block	
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



LAN Segmentation

Cato NGFW 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 LAN 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.

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.

Name	From	To	App / Category	Service / Port	Action	Track	Time	Enable
1 Sites to Cloud	London Headquarters	→ AWS-US East Azure - Europe	Any	Any	Green	N/A	🕒	🟢
2 Users to Cloud	All VPN Users	→ AWS-US East Azure - Europe	Any	Any	Green	N/A	🕒	🟢

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, having an implicit . 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. 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.

Name	From	To	App / Category
SYSTEM RULE	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	Tor Network

Internet Applications Access Rules

Secure Web Gateway

Secure Web Gateway allows customers to monitor, control and block access to websites based on predefined and/or customized 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 actions. Cato enables admins to create their own categories and use them in custom rules, enhancing the granularity of web access control.

Name	From	To	App / Category	Service / Port	Action	Track	Time	Enable
SYSTEM RULE Block any P2P	Any	Internet	P2P		Block	Track	Time	Enable
1 Allow HR to Social	HR	Internet	Social	Any	Allow	N/A	Time	Enable
2 Block SFDC to Mob...	All VPN Users	Internet	Salesforce	Any	Block	N/A	Time	Enable
3 Default Block Tor, S...	Any	Internet	Tor Network, SMB, SMTP		Block	Track	Time	Enable
4 Default block for C...	Any	Internet	Criminal Activity, Games, School Cheating, Porn, Illegal Drugs, SPAM, Phishing		Block	Track	Time	Enable
5 Default prompt for ...	Any	Internet	Gambling, Sex education, Nudity, Violence and Hate, Cults, Anonymizers, Tasteless		Prompt	Track	Time	Enable

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.

Anti-malware

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 impact 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.

IPS

Cato's Intrusion Prevention System (IPS) inspects inbound and outbound, WAN and Internet traffic, including SSL 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 Research Labs 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 DPI engine. 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.



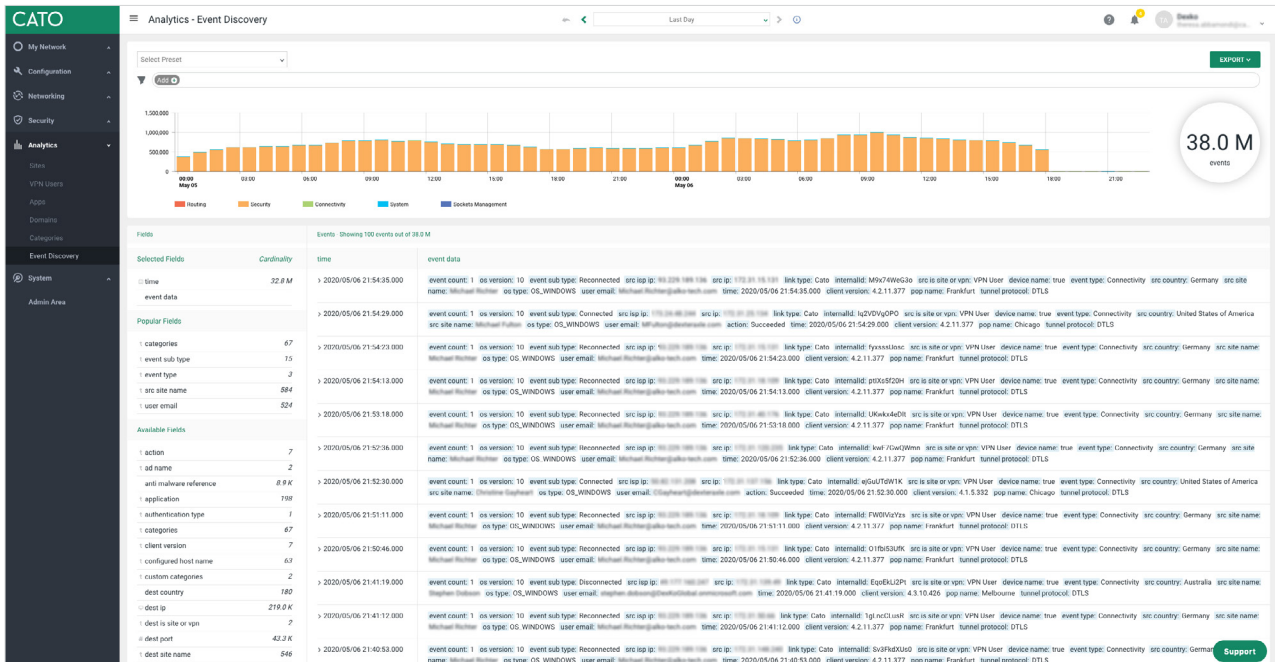
Network Behavioral Analysis: Cato IPS can detect and prevent inbound/outbound network scans.

IPS Managed 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 Research Labs 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.

Event Discovery

Event Discovery (called Instant*Insight) provides any 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. A year of data is kept by default. Admins can access and view this data through the Cato Management Application. Cato allows customers to export event log files (in either JSON or CEF format) for integration with a SIEM system or storage in a remote location. The log files are stored in a secure location, and each account is privately separated from other accounts.

Logs Exporter

Logs Exporter Settings

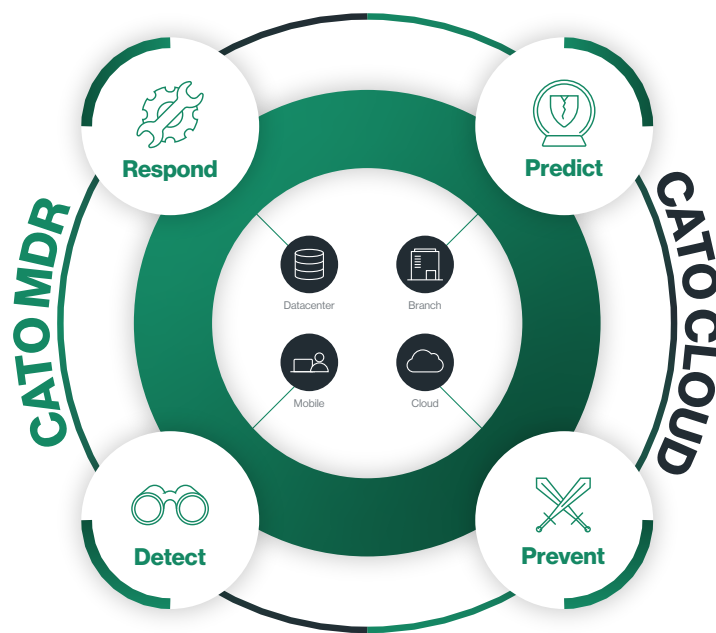
Format:

Event types to be sent

AuditTrail
 Health
 Security
 System

Managed Threat Detection and Response

Cato MDR enables enterprises to offload the resource-intensive and skill-dependent process of detecting compromised endpoints to the Cato SOC team. Cato seamlessly applies a full MDR service to customer networks. Cato automatically collects and analyzes all network flows, verifies suspicious activity, and notifies customers of compromised endpoints. This is the power of networking and security convergence to simplify network protection for enterprises of all sizes.



The MDR service adds means of detection and response to the prediction and prevention means delivered by Cato Cloud

Cato MDR Service Capabilities



Zero-footprint Network Visibility

Cato gathers complete metadata for every Internet and WAN flow initiation, including originating client, timeline, and destinations. All without deploying any network probes..



Automated Threat Hunting

Advanced algorithms look for anomalies in Cato's flow data warehouse and correlate them with threat intelligence sources. This machine learning driven process produces a small number of suspicious events for further analysis.



Expert Threat Verification

Cato security researchers review flagged endpoints and traffic 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's Security as a Service enables organizations of all size 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.

About Cato Networks

Cato is the world's first SASE platform, converging SD-WAN and network security into a global, cloud-native service. Cato optimizes and secures application access for all users and locations. Using Cato, customers easily migrate from MPLS to SD-WAN, optimize global connectivity to on-premises and cloud applications, enable secure branch Internet access everywhere, and seamlessly integrate cloud datacenters and mobile users into the network with a zero trust architecture. Using Cato, customers easily migrate from MPLS to SD-WAN, optimize connectivity to on-premises and cloud applications, enable secure branch Internet access everywhere, and seamlessly integrate cloud datacenters and mobile users into the network with a zero-trust architecture. With Cato, the network, and your business, are ready for whatever's next.

Cato. The Network for Whatever's Next.

Cato Cloud

[Global Private Backbone](#)

[Edge SD-WAN](#)

[Security as a Service](#)

[Cloud Datacenter Integration](#)

[Cloud Application Acceleration](#)

[Secure Remote Access](#)

[Cato Management Application](#)

Managed Services

[Managed Threat Detection and Response \(MDR\)](#)

[Intelligent Last-Mile Management](#)

[Hands-Free Management](#)

[Site Deployment](#)



ISO 27001 Certified



SOC2 Approved



GDPR Compliant