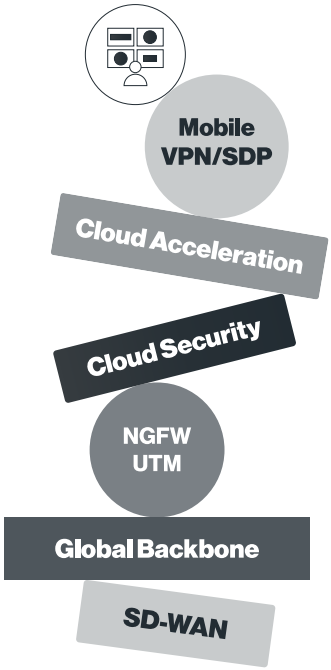
CATO
NETWORKS

Cato Cloud: The World's First SASE Platform

Solution Brief

BCN

The Network and Security Challenges of Digital Transformation



Your business is going digital. It depends on optimized access to applications and data, on-premises and in the cloud, and an increasingly mobile global workforce. The old network of the past, built with MPLS and security appliances, can't adapt to emerging business and technical requirements and the evolving threat landscape.

As a result, the gaps must be patched with even more point solutions. It is difficult and resource intensive to run this complex network yourself. And, outsourcing complexity to a telco is costly and can't deliver the speed and agility that is so essential to a digital business. There has got to 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 the legacy network architecture because:

- MPLS is expensive and rigid built to support WAN access not cloud access.
- Direct secure Internet access at the branch replaces backhauling to a data center over MPLS. At the same time, tighter network security is needed at the branch to protect users from Internet-borne threats.
- The legacy WAN doesn't extend beyond physical locations to accommodate cloud and mobility requirements. More solutions are needed to address emerging requirements and threats.
- Managing all these moving parts is tough - each one has its own console and solution life cycle (size, buy, deploy, configure, scale, upgrade, patch, retire)maintenance.

Telcos are the wrong partners because they are:

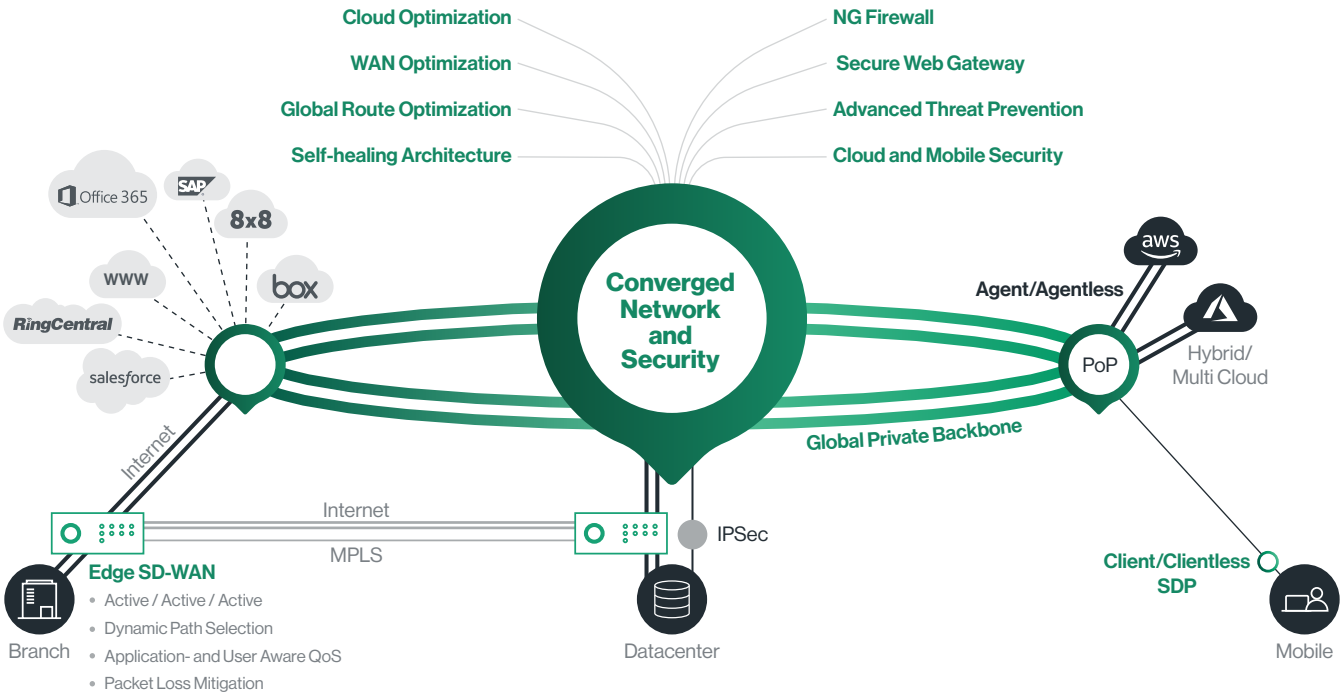
- Expensive, requiring dedicated and custom infrastructure, third-party point products, and complex management.
- Rigid, taking a long time to deploy sites.
- Slow, relying on ticket-based services, depend on third-party support, and have limited expertise.
- Stagnant, failing to own the underlying technology and the product roadmap. Telcos are the last to implement changes.
- Opaque, providing customers limited visibility and control of the network.

The World's First SASE Platform

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

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

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



Global Private Backbone

The Cato private global backbone is comprised of 50+ PoPs worldwide, interconnected by multiple SLA-backed tier-1 providers. All PoPs run Cato's cloud-native software stack. It's fully multitenant, scalable, and ubiquitous, performing all network functions — such as global route optimization, dynamic path selection, traffic optimization, and end-to-end encryption — as well as implementing the inspection and enforcement functions needed by Cato security services.

WAN Optimization

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

Global Route Optimization

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

Encryption

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

Self-healing Architecture

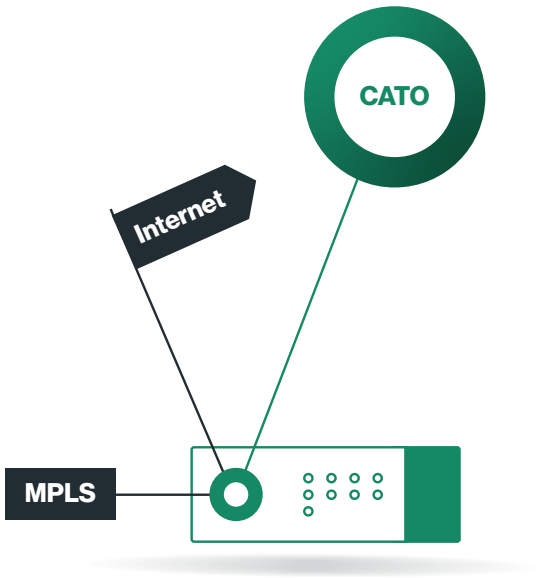
The Cato backbone is continuously monitored and measured. Self-healing capabilities guarantee 99.999% service availability. Elastic, scale-up cloud software design principles assure seamless service infrastructure growth without service downtime or disruptions.

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

Edge SD-WAN

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

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

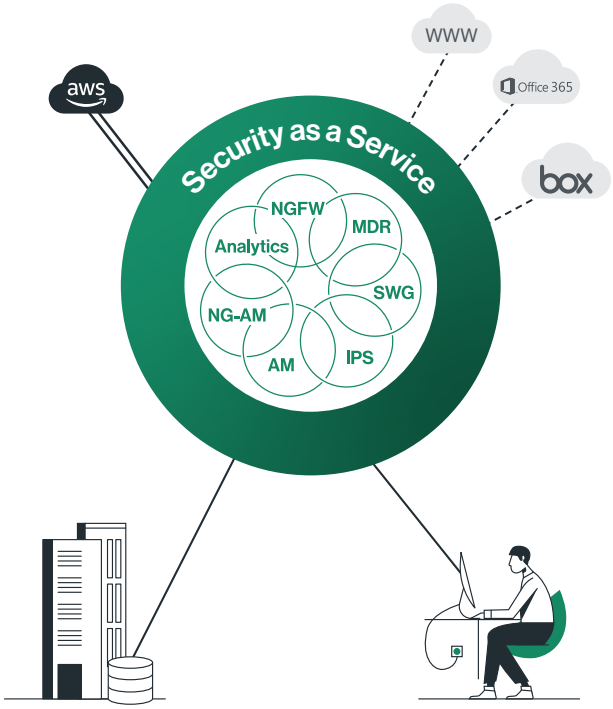


Cato Sockets include:

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

Security as a Service

The Cato security engines are built into the Cato private global backbone and delivered as a service. No additional appliances need to be purchased or deployed. Security engines include an application-aware, next-generation firewall (NGFW); secure web gateway (SWG) with URL filtering; standard and next-generation anti-malware; and IPS managed by the Cato SOC (Security Operation Center). These security engines 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 engines seamlessly scale to process all customer traffic, encrypted and unencrypted, without the need for sizing, patching, or upgrading appliances and point solutions. Cato protects user privacy and fully complies with GDPR. Inspected data is never stored on Cato servers or shared with third-parties. Customers are able to exclude privacy-sensitive applications, such as banking and healthcare, from inspection. In addition, Cato complies with SOC 2 and ISO 27001.



Next-generation Firewall

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

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

Secure Web Gateway

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

Advanced Threat Prevention

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

TLS Inspection

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

Malware Protection

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

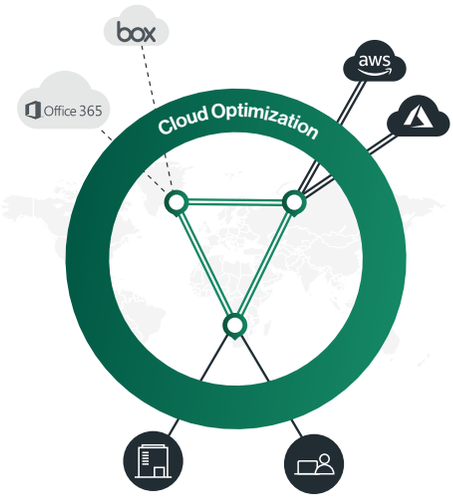
Intrusion Prevention

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

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

Cloud and Mobile Access and Optimization

Cloud Datacenter Integration



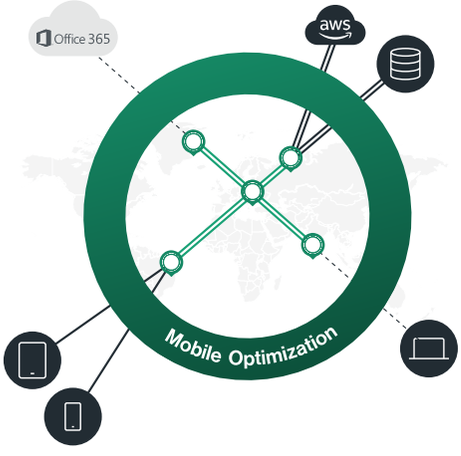
Cato tightly couples cloud datacenters into the SD-WAN, effortlessly. All cloud providers — Amazon AWS, Microsoft Azure, Google Cloud, and others — connect into Cato global backbone by establishing redundant IPsec tunnels, which typically only have to cross the physical datacenter shared with the Cato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

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

Cloud Application Acceleration

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

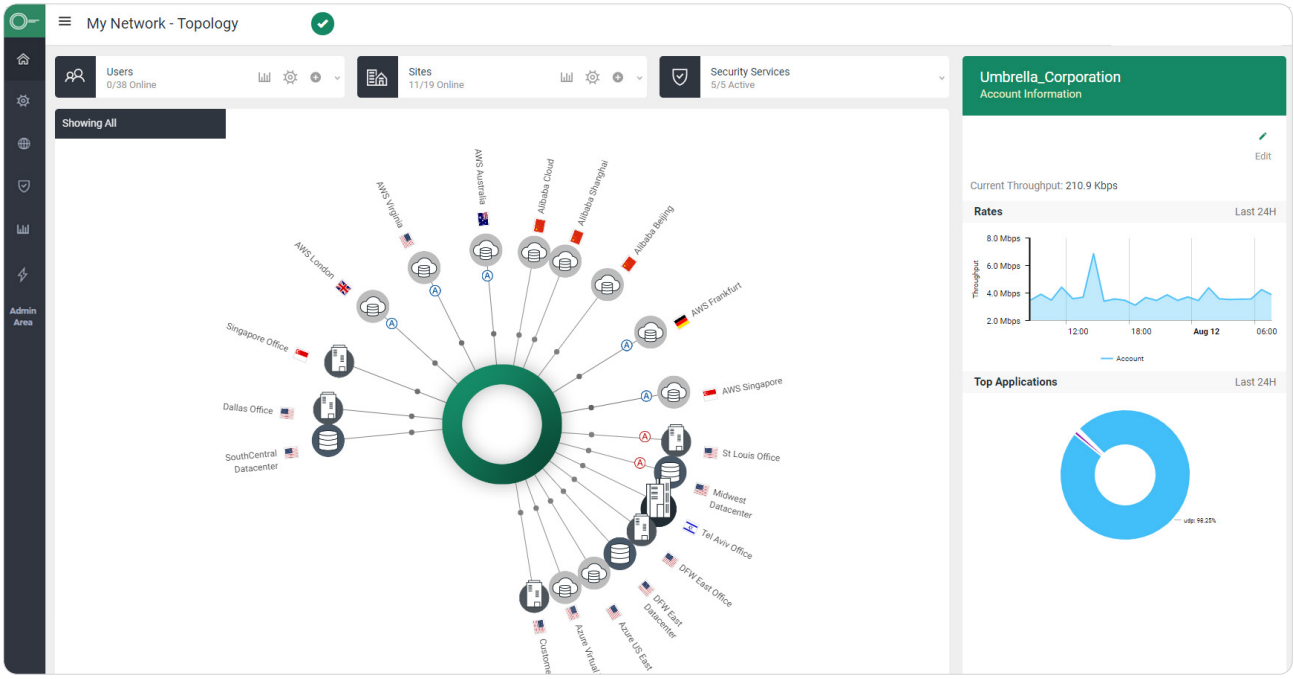
Cato's **zero-trust SDP** (Software Defined Perimeter) mobile access model allows the most granular user access control down to specific applications. By contrast, legacy VPN solution limit access to entire subnets. All user activity is protected by Cato's built-in network security stack, ensuring enterprise-grade protection to all users everywhere.

Cato Management Application

Cato provides a single-pane-of-glass into the complete enterprise network — sites, cloud resources, and mobile users for networking and security — through its cloud-based management application. Through the application, customers and providers can control all parts of the service, including network and security policy configuration, detailed network analytics, and security event reporting.

- **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.



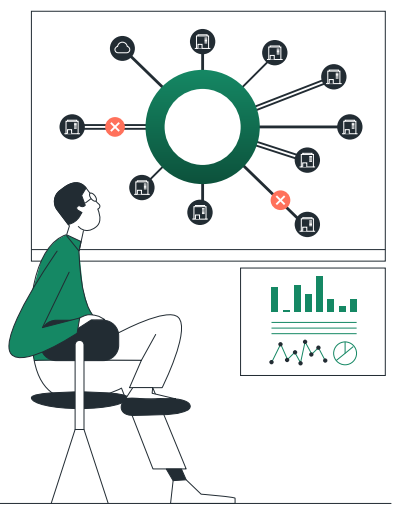
Cato's management console provides a single-pane-of-glass, showing all connected sites, cloud resources, and users.

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.

Multiple management models are a unique advantage of Cato over legacy telcos and managed network services providers which require customers to open tickets for any network change. In addition to site deployment assistance, Cato and its partners offer the following managed services:



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 Threat Detection and Response

As mentioned, Cato provides customers with a premium service to continuously monitor their networks for compromised endpoints. Prevention is no longer sufficient to protect the corporate network. Detection is critical for complete defense against advanced attacks. However, such managed threat detection and response (MDR) services often come at high cost with significant deployment complexity. Cato MDR leverages the deep network visibility of the Cato network to provide a zero-footprint detection of resident threats using a combination of machine learning algorithms that mine network traffic and a human verification of detected anomalies. Cato experts then guide customers on remediating compromised endpoints.

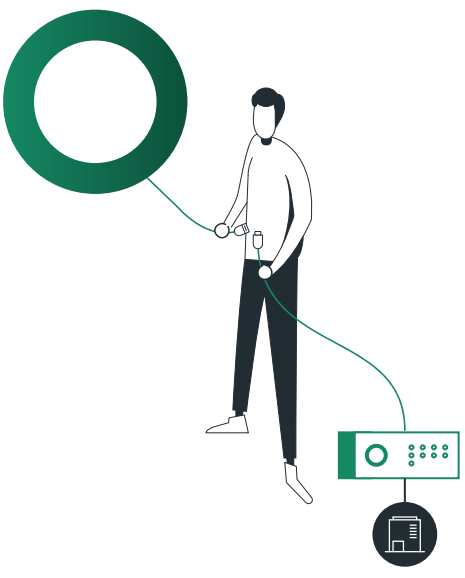
Hands-free Management

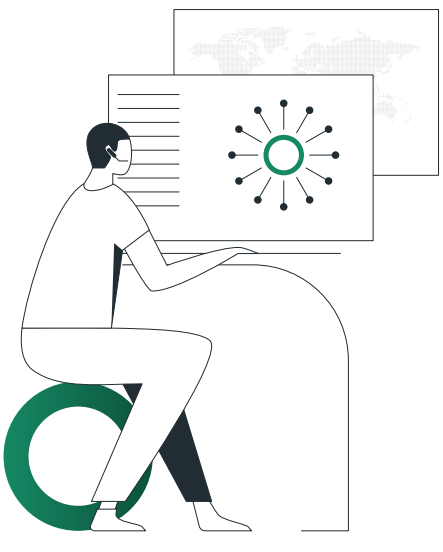
Customers can choose Cato or one of its partners for complete hands-free management of their network. Change requests are submitted and tracked through a ticketing portal and addressed according to Cato's service SLA. Expert staff will perform all changes to networking and security policies as needed to accommodate business and technical requirements.

Site Deployment

With our Site Deployment service, Cato's Professional Services (PS) team handles initial site activations and advanced configurations.

The PS team then fine tunes network and security policies to match the customer's unique requirements. Additional training ensures local resources are equipped to follow through on the remaining site activations. And Cato's PS and Support teams are available to assist during the remainder of the deployment.





Designated Support Engineer (DSE)

For those customers looking for dedicated support, we offer our DSE service that provides a single-point-of contact for support issues. The DSE is a tier-3 support engineer with a deep understanding of customer's environment. This eliminates the need to communicate customer-specific information, helping to speed issue resolution.

Use Cases

MPLS Migration to SD-WAN

Cato enables customers to move away from expensive, rigid, and capacity-constrained MPLS networks to multiple high-capacity Internet links and Cato's last- and middle-mile optimizations. Using Cato Edge SD-WAN, customers boost usable capacity and improve resiliency at a lower cost per megabit. Customers with a global footprint, leverage Cato's affordable global private backbone to replace global MPLS and the unpredictable Internet, optimizing performance and maximizing throughput to resources on-premises and in the cloud.

Optimized Global Connectivity

Cato uses a global private backbone with built-in WAN and cloud optimization to deliver an SLA-backed, predictable, and high-performance network experience — everywhere. Customers who suffer from high latency and network inconsistency across their global locations use Cato to deliver a great user experience when accessing on-premises and cloud applications.

Secure Branch Internet Access

Cato provides a full network security stack built into Cato Cloud. By connecting all locations to the Cato global private backbone through Cato Edge SD-WAN, all traffic, both Internet and WAN, is fully protected by Cato's Security as a Service. There is no need to add the cost and complexity of point-security solutions, appliances, or cloud services.

Cloud Acceleration and Control

Cato accelerates cloud access by routing all cloud traffic to the Cato PoP closest to the cloud destination. Because Cato PoPs share the datacenter footprint of major cloud providers, the latency between Cato and these providers is essentially zero. Cloud access optimization requires just a single application-level rule that determines where cloud application traffic should egress from the Cato Cloud. There is no need to install cloud appliances or setup hubs to reduce latency to the cloud.

Mobile Security and Optimization

Cato's global networking and security capabilities reach down to a single mobile user's laptop, smartphone, or tablet. No more treating mobile users like second-class citizens of your network and security infrastructure. Using a Cato 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 Security as a Service protects mobile users against threats everywhere and enforces application access control.

Work From Home

Cato seamlessly supports work-from-home for all employees, all the time. Customers rapidly connect their on-premises and cloud datacenters to Cato Cloud and enable self-service provisioning of Cato Clients to all users who require work-from-home or remote access. Unlike legacy VPN and SDP products that can't scale to support the entire business, Cato's global and cloud-scale platform is built to optimize traffic to all applications with a global private backbone, and continuously inspect traffic for threats and access control with Cato's converged security stack.

Cato Cloud: Complete WAN Transformation

Replacing MPLS and legacy WANs isn't just an opportunity to connect our offices quickly and affordably. It's an opportunity to transform our entire organization, connecting every user to any resource from anywhere in the world. By transforming, not just upgrading, their networks companies have reduced WAN-related costs while still doubling throughput and adding more locations, decreased deployment times from months to as a little as 30 minutes, and identified threats in their organizations missed by existing security appliances.

Yes, it's a radical vision but one that's a reality. Hundreds of customers are already experiencing the power of Cato. Validate it for yourself by speaking with us today.

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

CATO NETWORKS

BCN