Cato Cloud

Software-defined and Cloud-based Secure Enterprise Network

Solution Brief

CATO

NETWORK + SECURITY
IS SIMPLE AGAIN

Legacy WAN and Security Appliances are Incompatible with the Modern Enterprise

The rise of cloud applications and mobile workforces is changing the shape of business and legacy network traffic patterns. The Wide Area Network (WAN) and network security appliances were built to connect and secure static and physical locations, not today's fluid mobile-first and cloud-centric networks.

The network is broken: The fragmentation of the network makes it increasingly difficult to manage, optimize and secure.

Network security can't keep up: Network security must scale, evolve and adapt - fast. The need to upgrade embedded security software creates an exposure given the velocity and sophistication of cyber attacks.

Building and sustaining a secure network is too expensive: The cost of MPLS backhaul, distributed appliances, and the need to securely connect mobile users and cloud infrastructure pressures IT resources and budget.

Cato Networks: Software-defined and Cloud-based Secure Enterprise Network

Cato provides organizations with an integrated network and security platform that is designed for the modern enterprise's needs.

One Network

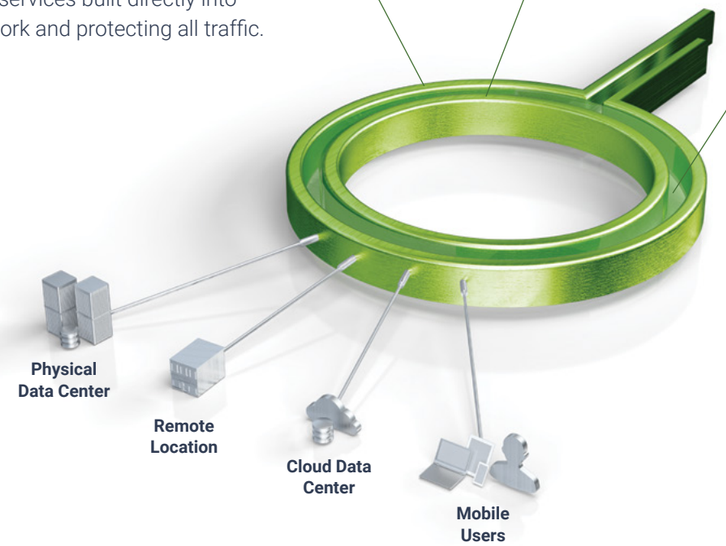
Cato reestablishes the enterprise network perimeter in the cloud, connects all enterprise resources and carries WAN and Internet traffic.

One Security

A full suite of cloud-based network security services built directly into the network and protecting all traffic.

One Policy

Cato enforces a unified policy for all traffic and across all users, locations and applications.



Cato Cloud

The Cato Cloud is the new enterprise network perimeter, implemented as a tightly integrated network and security software stack. It connects all branch offices, mobile users, physical and cloud data centers to provide secure WAN and internet connectivity everywhere.

Integrated Software Stack

Security Services

- Next Generation Firewall VPN
- Secure Web Gateway
- Advanced Threat Prevention
- Secure Cloud and Mobile Access
- Network Forensics

Network Services

- Routing
- Encryption
- Optimization
- Reliability

Agile and Elastic Network Security

Cato has developed a next generation firewall directly built into the network fabric that enforces corporate wide security policy on all traffic. Cato is extending its security capabilities to control access to cloud resources and stop malware infection and data extrusion.

Accelerated, Encrypted and Optimized Network

Traffic routing, DNS, DHCP and encryption is handled by Cato Cloud. Optimal routing between PoPs is ensured by handling traffic end-to-end which minimizes hops and latency. Multiple optimizations including dynamic path selection, forward error correction and transparent proxy are applied to all traffic.

Secure Tunneling Options to the Cato Cloud

- **Existing Firewall:** IPSEC tunnel for WAN and/or internet traffic
- **Cato Socket:** A zero touch tunneling device for a physical location
- **Cato vSocket:** Virtual gateway for Amazon AWS and Microsoft Azure
- **Cato Client:** A software agent for laptops, tablets and mobile devices

A Global, SLA-backed Backbone

Cato runs on top of a global network of physical points-of-presence (PoPs) connected to multiple tier-1, SLA-backed carriers with multi-gigabit links. The PoPs are designed for redundancy and high availability within and across instances.

Management, Scalability and Adaptability

Cato seamlessly scales and rapidly evolves to introduce new features and adapt to emerging threats. Network usage, security events and policy configuration are done through a cloud-based management application.

Cato Security Services

Next Generation Firewall/VPN

- **Secure Internet Access from Anywhere:** Eliminates traffic backhaul with direct internet access from any location
- **Simple Mesh:** Uses simple rules to connect any-to-any location
- **High Performance and Elastic:** Secures traffic at multi-gigabit speeds with no capacity upgrades
- **Application Awareness:** Identifies network access to on-premise and cloud applications regardless of port, protocol, SSL
- **User Awareness:** Identifies users, groups, and locations regardless of IP address
- **Unified, Granular Security Policy:** Controls access to applications, servers and network resources

Secure Web Gateway

- **Dynamic Site Categorization:** Includes a URL database with broad site classification by category including phishing, malware delivery, botnets and other malicious sites
- **Enforce Web Access Policies:** Enforces a corporate policy for web usage
- **Block, Prompt or Track User Access:** Reduces legal or security exposure from risky web usage

Advanced Threat Prevention

- **Anti-malware:** Scans HTTP and HTTPS for malicious files and stop endpoint infections

Secure Cloud and Mobile Access

- **Enforce access control policies** on mobile access to internal and cloud resources
- Seamlessly **extend security policies** to cloud infrastructure

Network Forensics

- **Detailed reporting and monitoring** of real-time and historical network activity
- Collection and delivery of **full network and security events logs** for external analysis

Cato Cloud Network

Routing

- **Optimal Routing:** SLA-backed routing between PoPs
- **Proprietary Protocol:** Better than BGP, considers distance, packet loss, jitter and more

Encryption

- **Secure Last Mile:** SLA-backed global VPN access to the nearest PoP
- **Secure Backbone:** Encrypted last mile and inter-PoP communication

Reliability

- **Active/Active:** Uses 2 ISP links (MPLS, ADSL, Cable, 4G/LTE) for maximum availability
- **Forward Error Correction (FEC):** Minimizes impact of packet loss

Optimization

- **Dynamic Path Selection:** Routes traffic between T-1 carriers based on real-time behavior
- **Fast DNS:** Caching and fast queries
- **Transparent TCP Proxy:** Fast-Ack, window management and fast retransmit
- **Policy-based Routing:** Dynamically allocate application traffic to appropriate link based on link quality

Cato Management Application

Cato NOC/SOC teams, managed service providers and customers' IT staff can:

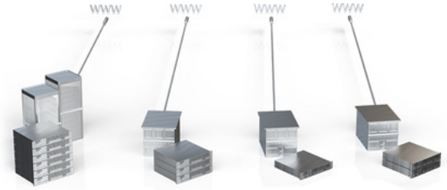
- **Monitor the Network in Real Time:** Including topology, connected devices and network usage statistics
- **Enforce Network Usage and Security Policies:** By business requirements and across all enterprise resources
- **Audit, Monitor and Alert on Events:** Monitor and alert on security events and network usage with full audit of all changes to the system configuration and policies

Use Cases

Appliance Elimination

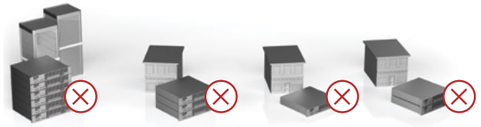
Costly and Complex Appliance Sprawl?

Traditional networks require multiple, dedicated appliances at each location to provide wide area networking (WAN) and security services. Distributed appliances require ongoing management, updates, upgrades and capacity planning to maintain the environment.



Branch Footprint Reduction

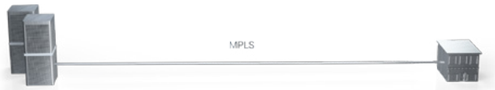
Cato eliminates dedicated branch office network security appliances. Cato protects all connected locations and seamlessly scales to secure all traffic, without the need for unplanned hardware upgrades and resource-intensive software patches. Cato delivers continuous, up-to-date protection without any customer involvement.



Secure and Optimized SD-WAN

Expensive MPLS Links with Limited Capacity?

Enterprises are dependent on high cost and bandwidth-constrained MPLS links. They are looking to augment MPLS-based WAN connectivity with affordable, high-capacity internet links.



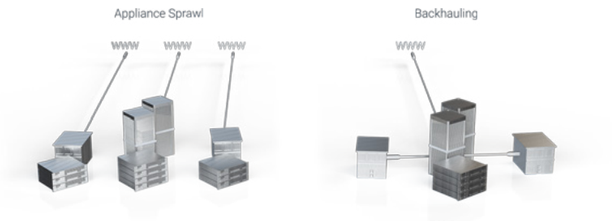
Augment or Replace MPLS Links

Cato enables organizations to offload MPLS traffic, specifically internet-bound traffic to the Cato Cloud. Cato **uniquely** provides built-in network security for direct secure internet access, SLA-backed WAN for MPLS replacement and secure connectivity for cloud infrastructure and mobile users.

Direct Internet Access

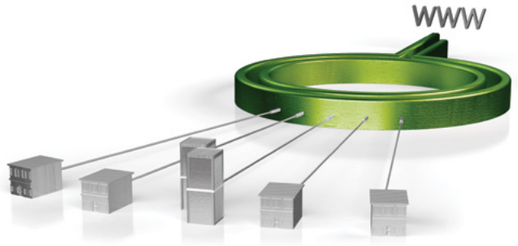
Appliance Sprawl or Traffic Backhaul?

Securing internet access in the branch office is a tough choice between deploying expensive distributed security appliances or backhauling internet traffic that overloads MPLS links and impacts the user experience.



No Appliances and No Backhaul

Cato connects all branch offices and remote locations to the Cato Cloud, providing enterprise-grade network security for any location without the need for dedicated appliances or traffic backhauling.



SLA-backed, Affordable WAN

Bad Response Time from Remote Locations?

High network latency can have a serious impact on productivity and the user experience in remote locations. Enterprises need to make a tough trade-off between an affordable, but high-latency, internet-based network or an expensive SLA-backed MPLS network.

SLA-backed, Affordable, Low-latency WAN

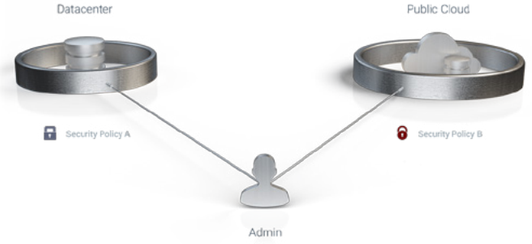
Cato leverages cloud scalability, software-defined networking and smart utilization of a multi-carrier backbone to deliver a high-performance, SLA-backed global WAN, at an affordable price.

Use Cases

Hybrid Cloud Network Integration

Point Solutions for Physical and Cloud Data Centers Connectivity and Security?

Migrating parts of a data center to the cloud can fragment access controls and security policies. This separation complicates policy management and obscures overall visibility.



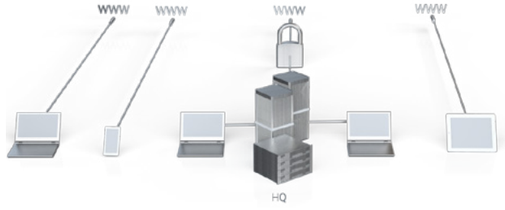
Unified Connectivity and Security Across Physical and Cloud Data Centers

Cato provides simple integration of physical and cloud data center. It seamlessly extends corporate access control and security policies to cloud infrastructures, enabling unified management of both physical and cloud-based resources.

Mobile Workforce, Secure Cloud Access

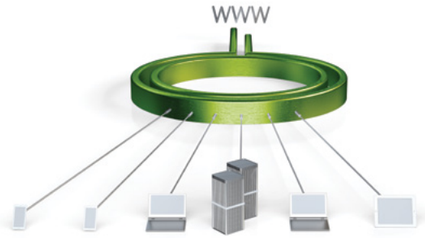
No Visibility and Control for Mobile Access to the Cloud?

Mobile users, especially those using personal devices for work, can connect directly to the web, which bypasses most corporate network security policies. Alternatively, forcing users through a specific network location, such as a data center firewall, impacts performance and the user experience – often leading to non-compliance.

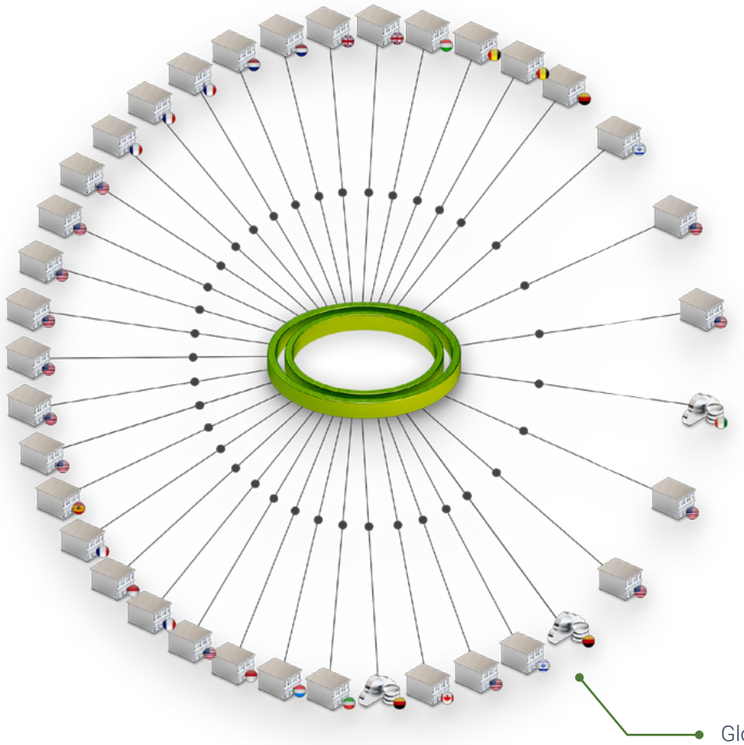


Secure and Optimize Mobile Cloud Access, Everywhere

Cato connects every mobile user to the Cato Cloud and provides secure and optimized access to enterprise resources in physical and cloud data center, cloud applications and internet sites. With compatible cloud applications, it is possible to restrict access to the Cato Cloud IP range, so stolen credentials cannot be used to access enterprise data in the cloud.



36 Sites, Global Manufacturer Network



Global WAN including branch locations and cloud data centers, using the Cato Cloud.

Cato's Capabilities

Capability	Features	Benefit
Affordable, Optimized Global Access to Corporate Data	Global network of Points of Presence (PoPs)	MPLS-like network backbone at a fraction of the cost
	Encrypted, SLA-backed and optimized backbone	Improved user experience and productivity
Flexible and Resilient SD-WAN	• Easily and securely connect branches, users and data centers • Cato Socket supports multiple ISP connections (active/passive, active/active) including MPLS, ADSL, Cable, 4G/LTE • Forward Error Correction: reduce last mile packet loss	Enhanced WAN availability and access
	Multiple Cato Cloud connectivity options through existing equipment, self-service provisioning	Simplify on boarding of new users, offices, M&A assets
Enterprise-grade Security Services	• Next Generation Firewall VPN • Secure Web Gateway • Advanced Threat Prevention • Secure Cloud and Mobile Access • Network Forensics	• Better security posture • No capacity constraints • No more patching
Elastic, Scalable and Agile Network Security	Network security capacity seamlessly scales in the cloud and Cato Security Services are transparently updated with new features and countermeasures against emerging threats	No hardware purchases and upgrades

Capability	Features	Benefit
Enterprise-wide Security Policy	Enforce a unified security policy across all mobile users, branches, physical and cloud data centers and applications (on-premise and in the cloud)	Better control over enterprise access with fewer point solutions policies
Cloud Applications Access Control	Restrict access to cloud apps to Cato Networks' IP Range	Reduce risk of unauthorized access due to credentials theft
Cloud Data center Network Integration	Connect and secure access to cloud data centers and servers	One cloud data centers and servers policy controlling access to both physical and cloud data centers
Cato Central Management Console	• Full visibility of network topology and usage by user, location and application • Easy configure access control and security policy for all assets • Centralized view of network and security events	• Reduces the need to use multiple interfaces • Enhanced ability to troubleshoot network performance problems • Manage a distributed network from a single pane of a glass.
24X7 Cato SOC/NOC	Cato's experts continuously monitor global backbone for optimal service	Augment your IT team's resources and expertise

About Cato Networks

Cato Networks provides organizations with a software-defined and cloud-based secure enterprise network. Cato delivers an integrated networking and security platform that securely connects all enterprise locations, people and data. The Cato Cloud reduces MPLS connectivity costs, eliminates branch appliances, provides direct, secure internet access everywhere, and seamlessly integrates mobile users and cloud infrastructures to the enterprise network.

Based in Tel Aviv, Israel, Cato Networks was founded in 2015 by cybersecurity luminary Shlomo Kramer, who previously cofounded Check Point Software Technologies and Imperva, and Gur Shatz, who previously cofounded Incapsula.

Network+Security is Simple Again

For more information:

www.CatoNetworks.com

@CatoNetworks