Cato Cloud
Global SD-WAN with Built-in Network Security

Solution Brief
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:** Rigid and expensive MPLS connectivity doesn’t fit today’s dynamic enterprise requirements.
- **Legacy SD-WAN falls short:** Addressing network capacity problems and adding inexpensive bandwidth is just a first step. Optimized global connectivity, secure internet access, and integrating cloud resources and mobile users is sorely missing.
- **Complexity creates vulnerability:** The proliferation of point solutions and management silos expands attack surface as threat velocity is increasing and IT skills are scarce.

Cato Cloud: 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** Global SLA-backed backbone that carries Internet and WAN traffic, and can augment or replace MPLS.
- **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 connects all branch locations, the mobile workforce, and physical and cloud datacenters, into a global, encrypted and optimized SD-WAN in the cloud. With all WAN and Internet traffic consolidated in the cloud, Cato applies a set of security services to protect all traffic at all times.

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 regions.

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.

Secure Tunneling Options to the Cato Cloud
- **Existing Firewall**: IPsec tunnel for WAN and/or internet traffic
- **Cato Socket**: A zero touch SD-WAN 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
Cato Cloud Network

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

Encryption
- **Secure Last Mile**: Encrypted tunnel from a location or a mobile device to the nearest PoP
- **Secure Backbone**: Encrypted last mile and inter-PoP communication

Reliability
- **Active/Active**: Uses multiple ISP links (MPLS, ADSL, Cable, 4G/LTE) to maximize availability during provider blackout or brownout
- **Forward Error Correction (FEC)**: Minimizes the impact of packet loss

Optimization
- **Dynamic Path Selection**: Routes traffic between tier-1 carriers based on real-time behavior
- **Transparent TCP Proxy**: Maximize window size via packet-loss mitigation and fast socket-PoP retransmission
- **Policy-based Routing**: Dynamically routes traffic based on application priority and link quality (packet loss, latency, jitter)

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
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

Advanced Threat Prevention
- Anti-malware: Scans HTTP and HTTPS for malicious files and stop endpoint infections
- IPS/IDS: Applies context-aware protection to all traffic based on known vulnerabilities, domain/IP reputation, geo location, DNS, and application and user awareness.

Secure Cloud and Mobile Access
- Enforce access control policies on mobile access to internal and cloud resources
- Seamlessly extend security policies to cloud infrastructure

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

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
Use Cases

Secure Cloud-Based SD-WAN

Expensive and rigid MPLS with wasteful Internet-traffic backhaul?

Enterprises are dependent on costly, bandwidth-constrained MPLS links. Backhauling Internet-traffic across MPLS links wastes precious capacity. The alternative, direct internet access at remote locations, requires dedicated security stacks at each location. IT organizations are looking to augment or replace MPLS-based WAN connectivity, eliminate Internet-traffic backhaul, and avoid costly appliance sprawl.

Augment or replace MPLS and enable secure direct Internet access

Cato SD-WAN enables organizations to augment MPLS with additional last mile services (fiber, cable, xDSL, 4G/LTE) and dynamically direct traffic based on application priority and link quality. Unlike legacy SD-WAN solutions that use the public Internet with MPLS, Cato is uniquely capable to replace MPLS altogether with our global SLA-backed backbone. Cato further extends the benefits of SD-WAN to cloud resources and mobile users and provides a full cloud-based network security stack to support direct secure Internet access everywhere.

Affordable MPLS Alternative

Poor response times at remote locations, and global MPLS charges feel like ransom?

High network latency can undermine user productivity in remote locations. Enterprises are forced to make a tough trade off between an affordable, but high latency, internet-based network or an expensive, low-latency MPLS network.

SLA-backed, affordable global WAN

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

Branch Appliance Elimination

Costly and complex appliance sprawl?
Traditional networks need multiple, dedicated appliances at each branch 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 equipment such as UTMs, firewalls and WAN optimization appliances. The Cato Cloud 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.

Cloud Datacenter Integration

Disjointed and high latency access to hybrid cloud and multi cloud datacenters?
Migrating parts of a datacenter to the cloud can fragment access controls and security policies. This separation complicates policy management and obscures overall visibility. Customers are further challenged to provide optimized, secure access to cloud resources across multiple providers and between global regions.

Converged networking and security across all physical and cloud datacenters
Cato connects physical and cloud datacenters, across all cloud providers and global regions, into a single, flat and secure network. Customers can seamlessly extend corporate access control and security policies to cloud resources, enabling easy and optimized access for mobile users and branch locations to all applications and data anywhere.
Use Cases

Mobile Access Optimization

Slow mobile access to datacenter and cloud applications such as Office 365?
Mobile users struggle to connect globally to datacenter resources and cloud applications, such as single region Office 365 instances, across high-latency public Internet connections. And, direct connections to cloud resources bypass corporate network security leading to the use of “shadow IT” applications.

Secure and optimized mobile access to all applications, globally
Cato connects every mobile user to the Cato Cloud and provides secure and optimized access to enterprise resources in physical and cloud datacenters, cloud applications and Internet sites. Cato uses its global, SLA-backed backbone to optimize routing and reduce latency to key applications, such as Office 365, and enforce application-aware security policies on all access.

Simple Network Automation

Manual and risky network configuration processes can’t keep up with business needs?
Legacy WAN configuration is notoriously complex and risky. Routing over multiple last-mile connections, adjusting to blackouts and brownouts, configuring WAN optimization appliances and policies — all require highly skilled network engineers. A highly manual process that is error prone, network changes take a long time to implement potentially causing an outage.

Simple and safe network automation
Cato cloud-based console and the zero-touch Cato Socket SD-WAN devices, reduce the effort and risk of network changes. Network managers specify application prioritization policies and easily troubleshoot network issues. Cato incorporates multiple services into the SD-WAN, route traffic over the best link, and seamlessly adapt to blackouts and brownouts. Edge devices and cloud services, are fully managed by Cato eliminating the need for maintenance, patches and upgrades.
## Cato’s Capabilities

<table>
<thead>
<tr>
<th>Capability</th>
<th>Features</th>
<th>Benefit</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Affordable, Optimized Global WAN</strong></td>
<td>Encrypted, SLA-backed and optimized global backbone for global connectivity</td>
<td>Affordable MPLS alternative, improves user experience for branch offices and mobile users, globally</td>
</tr>
</tbody>
</table>
| **Secure and Optimized SD-WAN** | • Easily and securely connect branches, users and data centers  
• Policy based routing drives use of multiple links (MPLS, cable, xDSL, 4G/LTE) based on application priority and link quality  
• Forward Error Correction: reduce last mile packet loss | Enhanced WAN performance, availability for all locations and users |
| | Multiple Cato Cloud connectivity option from Cato Socket SD-WAN device, Cato Client, and 3rd party IPSEC devices | 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 | Fully converged, cloud-based security services that are available everywhere and secure all locations and all users |
| **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 capacity constraints  
• No more patching  
• No appliance upgrades or refresh |
| **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 | One policy controlling access to both physical and cloud data centers |
| **Cato Management Application** | • 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 |
Cato Networks provides organizations with a cloud-based and secure global SD-WAN. Cato delivers an integrated networking and security platform that securely connects all enterprise locations, people, and data. Cato Cloud cuts MPLS costs, improves performance between global locations and to cloud applications, eliminates branch appliances, provides secure Internet access everywhere, and seamlessly integrates mobile users and cloud datacenters into the WAN.

Based in Tel Aviv, Israel, Cato Networks was founded in 2015 by cybersecurity luminary Shlomo Kramer, co-founder of Check Point Software Technologies and Imperva, and Gur Shatz, co-founder of Incapsula.

For more information:

www.CatoNetworks.com

@CatoNetworks

Where do you want to start?

- SECURE CLOUD-BASED SD-WAN
- AFFORDABLE MPLS ALTERNATIVE
- BRANCH APPLIANCE ELIMINATION
- CLOUD DATACENTER INTEGRATION
- MOBILE ACCESS OPTIMIZATION
- SIMPLE NETWORK AUTOMATION

Global Backbone. Cloud-Based SD-WAN. Firewall as a Service. All in One