Network Security is Simple Again

Cloud-based and Enterprise-grade Secure Network for Your Business

CATO NETWORKS

Table of content

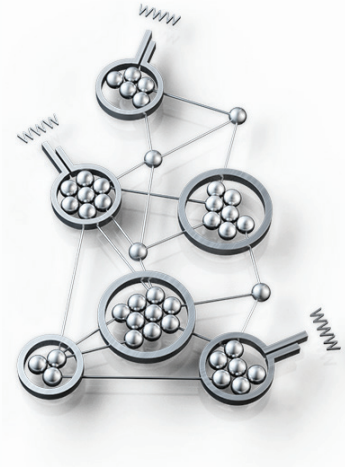
Executive Summary

It wasn't so long ago that managing and securing enterprise networks was simple.
We had one network connecting fixed locations with on-premise enterprise applications. Security was a simple matter of placing a firewall at the network perimeter and anti-virus software on the endpoints.

This reality has changed.

The increasingly distributed enterprise made global networking very costly and network security more complex as it stretched to cover multiple locations. Then came Cloud, mobility and IoT. Data and applications migrated to the Cloud. Anywhere mobile access and BYOD became a standard. **The perimeter dissolved and the network's simple form was broken.**

This transformation has occurred as Cyber attacks intensified and their sophistication increased.

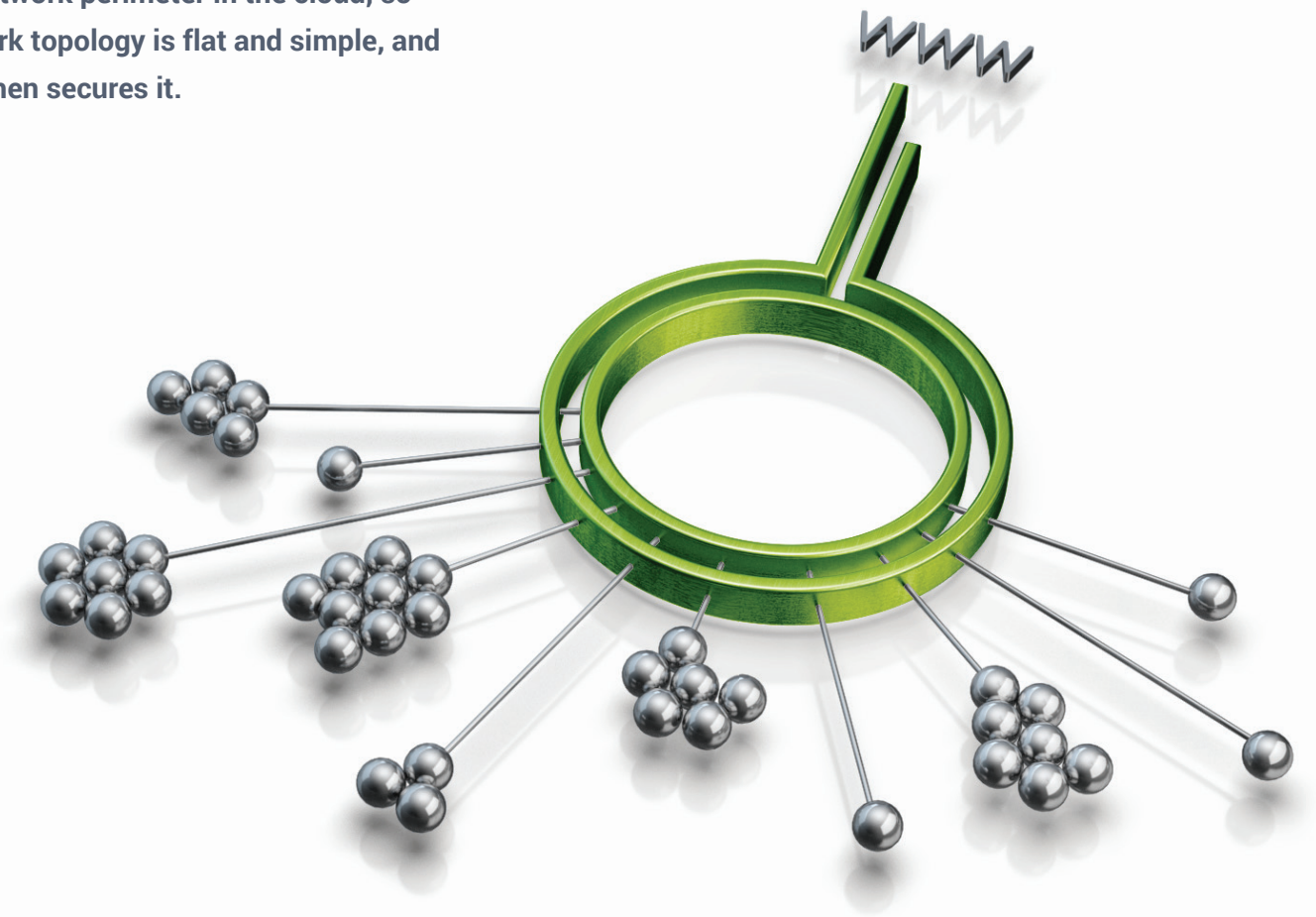


Securing the perimeter-less network is a complex task.
Security appliances are spreading throughout the enterprise with new point solutions emerging to address key requirements not covered by existing solutions. Security teams are pressured to maintain multiple policies across products, manage unnatural topologies, such as complex site-to-site mesh and traffic backhauling; integrate and secure new public Cloud infrastructure; and cope with mobile users directly accessing the Internet and bypassing network security altogether.

The increasingly distributed enterprise made global networking very costly and network security more complex

The underlying global network presented a significant challenge as well, especially at time where bandwidth-intensive video and voice communication became a standard business practice. Organizations that couldn't afford a managed MPLS network resorted to unmanaged Internet connections, with unpredictable latency and performance. Larger, distributed enterprises had seen networking cost skyrocket as their global footprint expanded. And, Cloud infrastructure and mobile users that are now a critical part of the business were left completely outside the realm of legacy WAN security and acceleration solutions.

With the fundamental understanding that managing and securing a network that is so complex will forever be complex, Cato Networks is rethinking network security from the ground up and bringing it into the Cloud. Cato first re-establishes the network perimeter in the cloud, so network topology is flat and simple, and only then secures it.



All locations, office-based and mobile users, on-premise and Cloud applications connect to the Cato Cloud Network: a global, encrypted and optimized network that maximizes end user experience and productivity across the enterprise. With the flip of a switch, customers selectively enable the full range of Cato's enterprise-grade security services, such as a Next Generation Firewall, VPN, URL Filter and more - securing both Wide Area Network (WAN) and Internet traffic. A unified policy can now be enforced across all network activity regardless of source or destination.

With Cato, network security is simple again.

The Challenge of the Dissolving Network Perimeter

Globalization, Cloud and Mobility are Changing the Business

Network security used to be a simple exercise. We had a clear network perimeter, encapsulating our offices, users and on-premise applications. Securing the network was also simple: put a firewall at the perimeter, separate the “inside” (the enterprise resources) from the “outside” (the Internet), and your network was secured.

This is no longer the case. Three major forces had dissolved the network perimeter, making the current network security paradigm obsolete: Globalization, Cloud and Mobility.

Globalization is making network topology more complex. We now need to connect various locations into a single global network. To secure it, we have to deploy multiple security solutions, often packaged into appliances, at each location.

The increase use of the **Cloud** is loosening our grip on enterprise applications and data. Public Cloud applications such as Office 365, Salesforce.com and Box.com are replacing on-premise applications. Cloud infrastructure is using virtual servers and storage to replace physical datacenters. We now have to deal with data spread in multiple locations, some outside our control.

Mobility is providing new ways for our users to access enterprise resources, mixing and matching personal and work activities using “Bring Your Own” devices (BYOD). Our ability to control the devices, and the way they are used is severely restricted.

Three major forces had dissolved the network perimeter, making the current network security paradigm obsolete: Globalization, Cloud and Mobility.

Traditional Network Security is Incompatible with the New Enterprise

Networking and security teams had to respond to the new business reality with the toolbox provided by their vendors. This has led to the following challenges.

Appliance sprawl: each distributed location had to be covered by a full security stack including a firewall, URL filter and anti-malware to enable secure Internet access. This is a costly proposition from capital expenditure and IT resources perspective that many organizations, and especially midsize ones, can't afford. UTM security appliances, which were touted as a solution to this problem, are reducing the branch office footprint but sacrifice capacity and security capabilities.

Traffic backhaul: to avoid appliance sprawl, many organizations had chosen to backhaul traffic to a central location that had a full security stack and secure Internet access. The need for internet traffic to go through a secure location had created the so-called "Trombone effect": the increase in packet latency that causes slow application response times and impacts remote employees productivity.

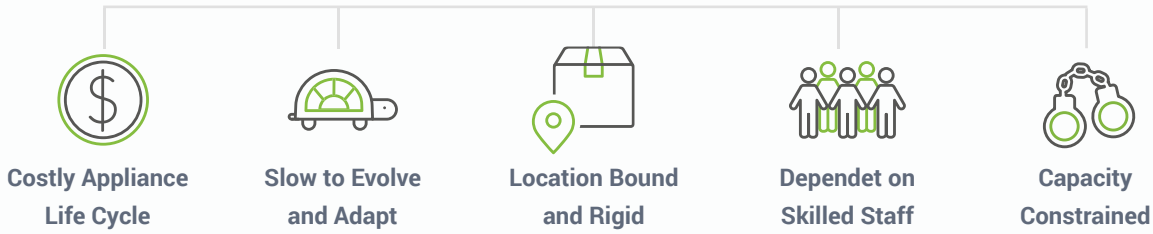
Complex site-to-site and site-to-Cloud configuration: to connect all network resources into the enterprise network, IT security configures VPN tunnels between office firewalls. In addition, there is a need to use a separate solution and process to connect Cloud resources to the network (Amazon AWS or Microsoft Azure segments) and enable IT staff to manage it. This is a sensitive configuration that has to take into account multiple access paths and network redundancy.
A mistake can cause a serious network disruption, making IT averse to changes causing accumulation of obsolete rules that could create a security exposure.

Complex protection of Cloud access, point solutions explosion: as new business requirements emerged, so did point solutions. For example, the increase use of Cloud applications created a new category of Cloud Access Security Brokers (CASB) solutions. Naturally, they are deployed between the user and the Cloud applications. However, since there are so many ways, both inside and outside the network to access the Cloud, deployment got very complex. IT teams had to use a combination of proxies and APIs to secure all the different paths to the data.

Mobile users evade security controls: the expansion of the mobile workforce and the use of personal devices to access business data (BYOD) had further challenged legacy network security. Mobile users could directly access the Internet and bypass network-enforced security policies. Forcing mobile users through VPN to ensure secure access to the Internet created performance and user experience problem, especially for global travelers. In turn, leading to security policy violations. Indeed, getting into the “line of sight” between users and data, to enforce access control on mobile, Internet and Cloud access, is the hallmark challenge of the Dissolving Perimeter.

Network Security Appliances are Costly to Own and Complex to Manage

The new business requirements of globalization, Cloud and mobility has exacerbated an already challenging environment for IT teams. The appliance form factor has serious constraints that make it costly to own and complex to manage.



The appliance lifecycle impacts IT budget and resources: appliances had to be purchased, deployed, configured and maintained. Power, cooling and rackspace requires detailed capacity planning, especially for remote locations and data centers. If they fail, they have to be repaired or replaced. As they age, end of life policies force customers to upgrade appliances just to keep up with the latest software from their vendors. Finally, software subscription is a substantial recurring cost.

Capacity constraints create resource waste or unplanned expenses: customers are over-purchasing appliance capacity to plan for growth. As capacity drives licenses and maintenance cost, unused capacity is simply a waste of money. On the flip side, buying smaller capacity can cause out-of-budget forced upgrades as the business grows.

Location bound appliances means multiple instances for full coverage and redundancy: since appliances are placed in specific locations in the network, they often cover specific parts of the traffic depending on the source and the destination. This means multiple instances have to be purchased to provide full coverage and meet redundancy requirements.

Skilled IT staff is needed to sustain an appliance-based infrastructure: IT security and networking experts are a scarce and expensive resource. They are often assigned to larger locations, where they are needed the most, leaving remote locations exposed. Ultimately, if you need an expert to deploy an appliance, you have to pay to get it done.

Appliance software is slow to evolve and adapt: Network security is there to protect our networks against attacks. Vendors upgrade their software to stop the attacks they are seeing. However, attack visibility with on-premise appliances is limited - because data isn't accessible by the vendors. And, upgrading appliance software requires down time and technical supervision to ensure business continuity. The result is that appliances are falling behind in their ability to detect and prevent security attacks.

Cato Networks: Cloud-based Secure Network for the Enterprise

Cato Networks was founded by network security veterans to provide enterprises of all sizes with a secure network that supports a global, distributed, Cloud-and-mobile centric business.

Cato has identified 3 core challenges that must be addressed by a future secure network:

The network is broken: the fragmentation of the network across locations, data centers, Cloud environments and a mobile workforce makes it increasingly difficult to manage, optimize and secure.

Network security can't keep up: network security must scale, evolve and adapt - fast. This is essential for any organization that want to stand a chance against the increased velocity and sophistication of cyber attacks.

Building and sustaining a secure network is too expensive: As security budgets are subject to extensive scrutiny, a radical shift from capital and resource intensive security model is a business necessity.

Cato takes a three-step approach to delivering a secure network:

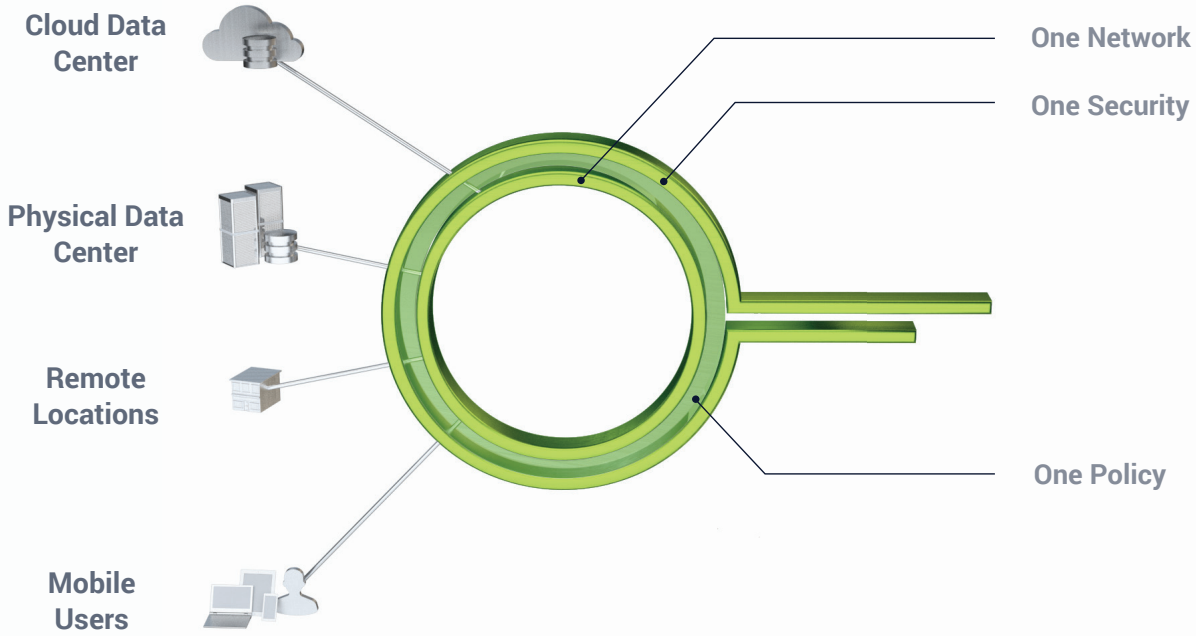
Simplify the network: Cato first reestablishes the enterprise network perimeter in the Cloud and connects all network resources to it. This solves the network fragmentation problem.

Secure the network: Cato then applies a tightly integrated set of agile and elastic security services to protect the network. This addresses the need to quickly evolve security capabilities while cutting the cost of on-premise security infrastructure.

Enforce a unified policy: by integrating the networking and security layers, it is possible to enforce corporate security policy on all traffic, regardless of source (user, system, location) and destination (on premise, Cloud or Internet).

Cato Networks has created a new platform, built from the ground up to address the new world's challanges. It is comprised of 2 tightly integrated pillars: the Cato Cloud Network and Cato Security Services.

Let's look at these pillars more closely.



Cato Networks has created a new platform, built from the ground up to address the new world's challanges. It is comprised of 2 tightly integrated pillars: the Cato Cloud Network and Cato Security Services.

Cato Cloud Network: global, encrypted and optimized enterprise network backbone

The Cato Cloud Network is the home of the new enterprise network perimeter, binding together all network resources (branch offices, data centers, Cloud assets and mobile users). The Cato Cloud Network carries all WAN and Internet traffic, excluding LAN traffic within a given location.

Global Network Backbone of Cato PoPs

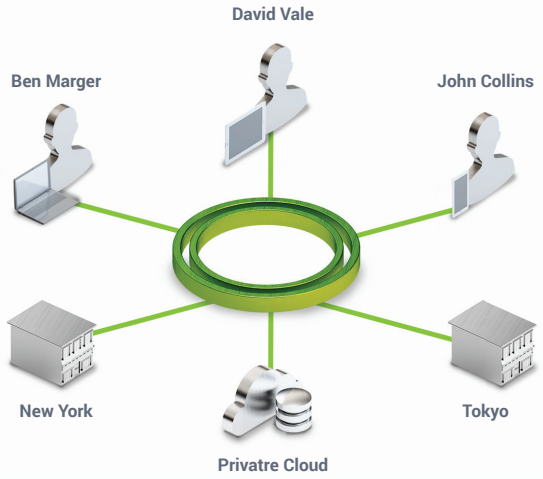
The Cato Cloud Network is a global network of physical points-of-presence (PoPs) connected to a backbone comprised of multiple tier-1 carriers with multi-gigabit links. The traffic in the backbone is encrypted and Cato ensures optimal routing and minimal latency that is superior to an unmanaged internet connection. The PoPs are designed for redundancy and high availability and seamlessly scale to accommodate capacity growth.

Customers connect their network resources to the Cato Cloud Network using **secure tunnels.** Each office, datacenter, cloud segment or mobile user dynamically connect to the nearest PoP and enjoys an optimized access across the Cato Cloud Network to on-premise, Internet and Cloud resources.

The Cato Cloud Network is a global network of physical points-of-presence (PoPs) connected to a backbone comprised of multiple tier-1 carriers with multi-gigabit links.

One Logical Enterprise Network

Regardless of the physical PoP a network resource is connected to, Cato creates one logical enterprise network. Connectivity rules between resources are managed in the Cato Cloud without the need to maintain a hub-and-spoke configuration. This approach makes it extremely easy to plug a new resource (a new office, a new user or a new Cloud asset) to the network and instantly enable secure access to it.



Plugging into the Cato Cloud Network

There are several ways to establish a secure tunnel to the Cato Cloud Network over an existing Internet connection. Customers can use:

- **Existing firewalls** that create a VPN tunnel to the Cato Cloud
- **Cato Socket:** a tunneling device for a physical location that ensure continuous access to the nearest active PoP, and supports multiple Internet connections for maximum redundancy. Simply plug the socket to power and to an Internet connection and use the Cloud-based console to activate it.
- **Cato vSocket:** a virtual instance of Cato Socket that can connect a Cloud-based segment of virtual servers in Amazon AWS or Microsoft Azure.
- **Cato Client:** a software agent for laptops, tablets and mobile devices. Admins generate email invitations that take mobile users through a self-service provisioning process to deploy the Cato client on their devices. Once active, access to corporate resources is tunneled through Cato Cloud and governed by corporate policies.

Overall, the Cato Cloud Network simplifies the enterprise network topology. It solves the challenge of connecting all network resources (physical, Cloud and users) into a simple unified network, that can be effectively secured.

Cato creates one logical enterprise network.

Cato Security Services: Enterprise grade, Elastic and Agile Network Security

Once all WAN and Internet traffic is consolidated in the Cato Cloud Network, network security becomes simpler because the distribution of network resources no longer complicates the enforcement of security. Cato applies a set of tightly integrated Cato Security Services to secure all network traffic.

Agile, Tightly-integrated Networking and Security Stack Built for the Cloud

Cato has built the networking and security stack from the ground up. Each Cato PoP is running the full stack so all traffic is encrypted, optimized and secured. The PoPs are centrally managed, and the Cato Security Services are seamlessly updated with new features and capabilities.

Cato leverages its unparalleled visibility to the traffic of multiple networks to detect emerging and active threats to transparently and quickly develop and deploy countermeasures with the Cato Security Services

Each Cato PoP is running the full stack so all traffic is encrypted, optimized and secured.

Enterprise-grade security services

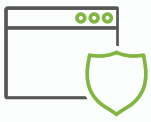
Cato Security Services includes the following capabilities:

Cloud Firewall

- **Secure Internet Access for Any Location**: Eliminate traffic backhaul with direct Internet access to the nearest Cato PoP that provides a secure exit point to the Internet
- **Simple Mesh**: Enable and control access between remote offices, headquarters and data centers eliminating hub and spoke topology
- **High performance and elastic**: designed to secure traffic at Multi-gigabit speeds with no capacity upgrades
- **Enhanced Network visibility**: Monitor and analyze access to/from the network from any user and device

Cloud VPN

- **Always Local VPN**: Optimized VPN access to the network via dynamic session assignment to the nearest Cato PoP. Eliminating hub and spoke VPN is particularly valuable to global travelers that are typically forced to connect to HQ, sometimes at the other side of the world.
- **Integrated On-Premise and Cloud (VPC) Access**: unified access control for enterprise on-premise and Cloud resources without managing two security configurations (on-premise network security and Cloud provider network security).
- **Flexible secure VPN configuration**: Centrally managed DHCP and IP address reducing configuration complexity. Connectivity to the Cato Cloud supports a wide range of link security mechanisms (L2TP, IPSec, DTLS).



Application Control

- **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**: control application, data and resource usage for all access regardless of source and destination
- **Application Traffic Shaping**: restrict application bandwidth usage by location, user, group, time of day and other attributes

URL Filtering

- Dynamic URL databases, seamlessly updated in the Cloud
- Restrict access to categorized and reputable sites to reduce exposure to drive-by-downloads and malware infections
- Self-service approval for web site access and submission for admin approval

Cato Management Application

Cato empowers Cato NOC/SOC teams, managed service providers and customers' IT staff to use a Cloud-based management application to:

- Gain in depth visibility into overall network activity by location, application groups or users
- Enforce network usage policies by business requirements
- Enforce security policies and resources access controls across the entire enterprise
- Monitor security events and network usage alerts

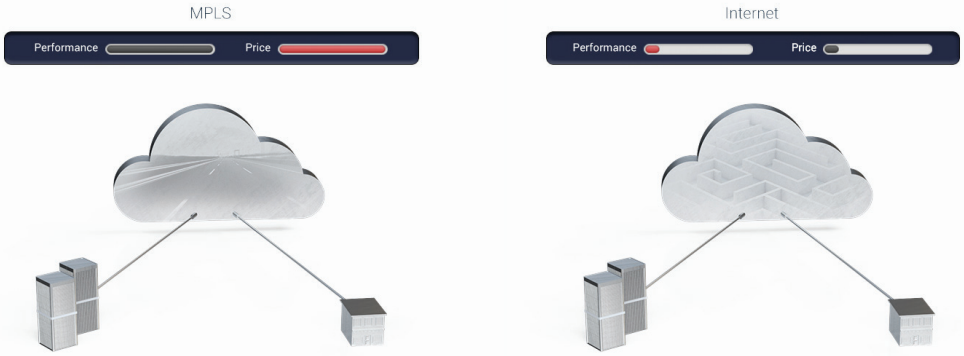
Cato Networks Use Cases: Making network security simpler, better and more affordable

Cato's Network Security as a Service architecture, dramatically impacts the cost and complexity of delivering a secure network for the business.

We see 4 use cases that deliver the value: High performance Wide Area Network (WAN), Branch office Appliance Elimination and Traffic Backhaul Reduction, secure Web and Cloud access for the Mobile Workforce, and Public Cloud network integration. We will discuss them below.

High performance and Low Latency Enterprise WAN

Before Cato



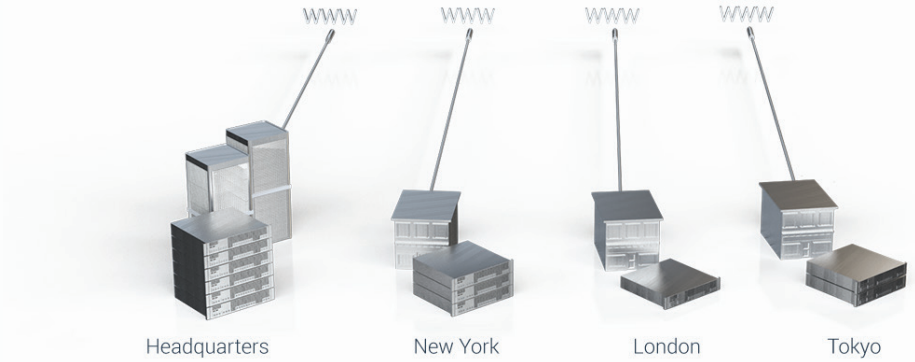
Connecting all enterprise resources into a high performance WAN is a key business enabler. Yet, until today, organizations had to either use very expensive MPLS connections with guaranteed SLA and low-latency OR rely on a cheap unmanaged Internet connection with unpredictable uptime and latency. Essential a trade off between price and performance.

After Cato

Cato Networks offers organizations a third option: **a high performance, low latency network at an affordable price.** Cato Networks has created an optimized global network, the "middle mile" that ensure traffic goes through a minimal number of hops and carriers to minimize latency. And, that optimization works not only for intra-enterprise traffic but also for enterprise-to-Cloud traffic.

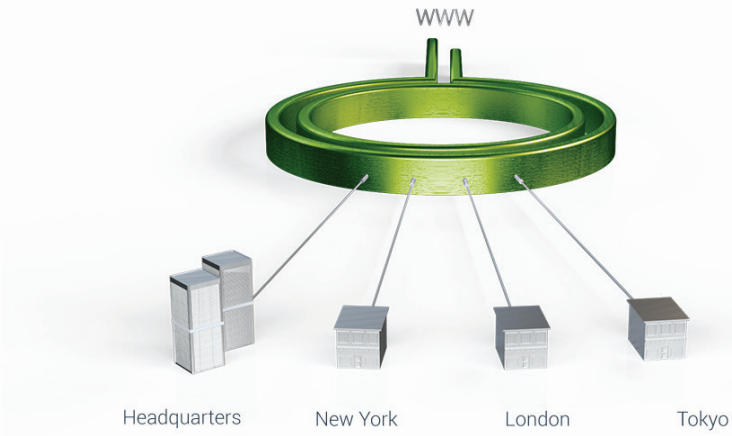
Branch Office Appliance Elimination and Traffic Backhaul Reduction

Before Cato



Deploying security appliances at every location is costly and complex to manage. The tough choice IT managers faced, until today, was to take on that cost or backhaul traffic to a central location with secure Internet access.

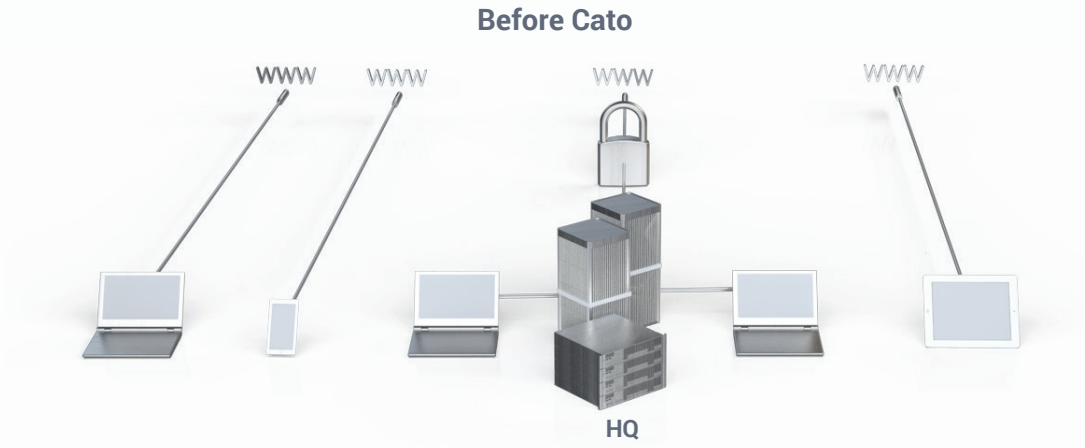
After Cato



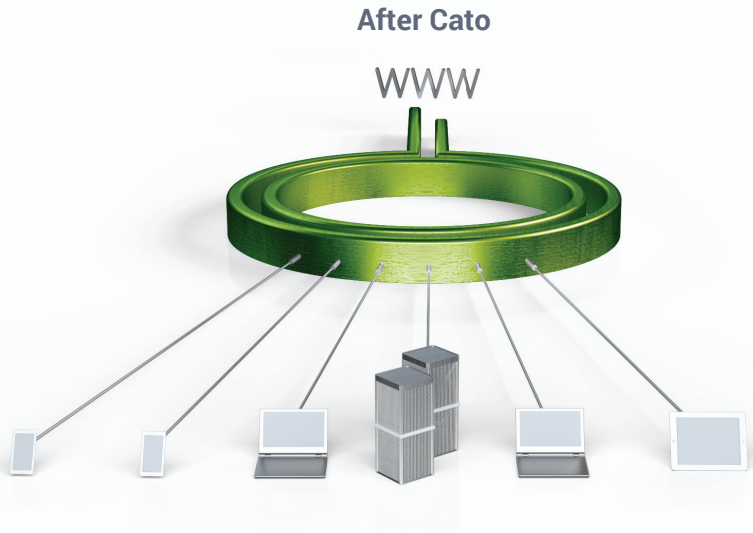
Cato Networks enables IT organization to have their cake and eat it too. All branch offices connect to the nearest Cato Cloud Network PoP. Each Cato PoPs fully enforces all of the customer Internet access security policies regardless of location. **No appliances and no backhaul** are needed. As an added benefit, Cato carries and optimizes the traffic between the branch office and the Internet and Cloud destinations instead of just dropping it into the unmanaged internet. This improves latency and response time for applications such as Office 365.

Each Cato PoPs fully enforces all of the customer Internet access security policies regardless of location. No appliances and no backhaul

Branch Office Appliance Elimination and Traffic Backhaul Reduction



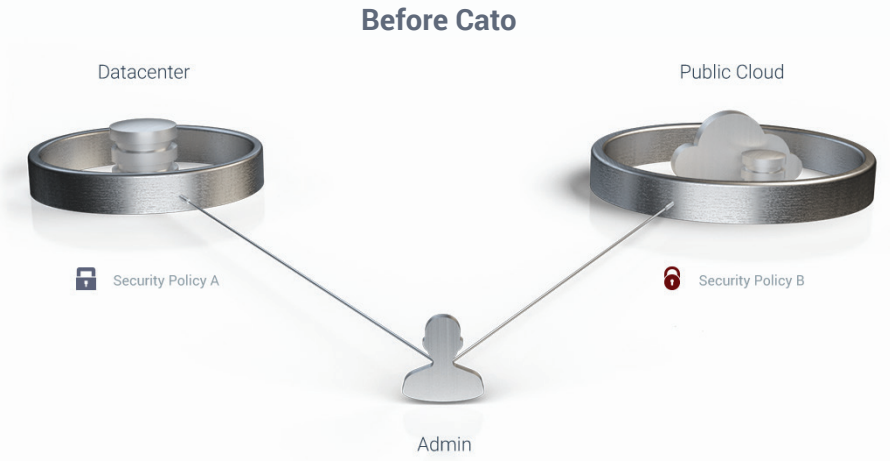
Mobile workforce security is the “stepchild” of network security. The ease of accessing Internet and Cloud resources from laptops, tablets and smartphones, is at odd with cumbersome experience of using VPN clients to access internal, on-premise, resources. As a result, IT security is often challenged with enforcing security controls on mobile users.



Cato Networks easily **extends corporate security policy to the mobile workforce** by connecting them to the Cato Cloud Network through the Cato Client. Access to public enterprise Cloud applications (Office 365, Salesforce and other SaaS services) and Cloud infrastructure (Amazon AWS (VPC) and Microsoft Azure) can be restricted to Cato Cloud Network IP and additional access control policies enforced. Internet access is secured by Cato NGFW and URL Filter. As an added benefit, travelling mobile users dynamically connect to the nearest PoP and enjoy an optimized access over the Cato Cloud Network to Internet, Cloud and on-premise destinations.

Cato Networks easily extends corporate security policy to the mobile workforce

Public Cloud Network Integration



The migration of datacenter resources to the Cloud is used by many IT organizations. The integration of Cloud-based segments, including application servers and databases requires management of a new set of access control policies, native to the Cloud platform, effectively splitting the security policy between physical and Cloud resources.

Cato Networks treats Cloud-based datacenters as yet another element of the enterprise network. Cato vSocket creates a secure tunnel to the Cato Cloud enabling all access control, to both physical and Cloud-based datacenters to be governed by Cato policies.

Cato Networks treats Cloud-based datacenters as yet another element of the enterprise network.

Summary

This is the state of business today: it is expanding globally, relies on data and applications in the Cloud and is driven by a mobile workforce. This transformative change can't be supported by a rigid and constrained appliance-based security solutions. We need a new approach, a revolution rather than an evolution, to provide a secure network to the enterprise.
Cato Networks was founded to revolutionize the way network security is delivered, managed and evolved. Cloud, software, commodity hardware and low-cost global connectivity enable us to provide businesses with an enterprise-grade secure network - at the fraction of the total cost of ownership they experienced with legacy security and networking solutions.

This should hardly come as a surprise. These forces have reshaped whole industries and multiple IT domains. Networking and security, delivered as a service, are next.

About Cato Networks

Your business has a new shape. It is expanding globally, relying on data and applications in the Cloud, and driven by a mobile workforce. It was easier to protect the business when it had one simple network perimeter - but that perimeter is now gone.
We need a new approach, a revolution rather than an evolution, to provide a secure network for the way we are now doing business. Cato Networks is rebuilding a new network perimeter, in the Cloud, protected by a tightly integrated set of security services. We provide businesses with a simple, affordable and enterprise-grade secure network - at the fraction of the cost of legacy approaches. No more costly hardware deployments, management complexities, capacity constraints, outdated software, or restricted visibility.
By rethinking network security from the ground up, and bringing it onto the Cloud, securely connecting your business is simple again.

Cato. Network security is simple again