CATO
NETWORKS

Telco or Cloud-Native Carrier:

# What's the Right Architecture for Your Managed Network Service?

# Telco Services Then and Now

For the past 20 years, enterprises have relied on telcos for their wide area networks. MPLS and the other telco managed network services were designed to address IT's availability, connectivity and reliability requirements.

IT looked to offload the complexity of WAN construction; telcos delivered by packaging the underlying connectivity, network design, third-party appliance integration, and troubleshooting into fully managed services. Enterprises needed to connect their sites, and telcos responded with end-to-end service delivery, sometimes even partnering with other MPLS providers to connect out-of-region sites. IT needed guarantees that services would meet stated requirements with the right "wrapper" to simplify ordering and provider management. Telcos responded by backing claims with Service Level Agreements (SLAs), centralized billing, and a single point of contact.

Yes, there are well-known problems with the telco experience. Telco services come at a premium. Capabilities beyond basic site-to-site connectivity require purchasing yet another telco offering. Opening new offices requires weeks and months. Moves, adds, and changes demand telco intervention. Service tickets often take longer to resolve than enterprise IT might like. Feature introduction is slow. But enterprises, particularly global ones, put up with those pains in large part because the only possible alternative — the Internet — hasn't really been an alternative.

## Business Changes are Incompatible with Telco Services

Increasingly, though, changes in how businesses operate are proving incompatible with telco managed network services (MNSs).
More specifically:


**Application and user bandwidth requirements** have grown significantly in the past decade, yet MPLS bandwidth continues to be at a premium with large capacity connections often unavailable or unaffordable.

**The speed of business has increased.** Business is looking to be more agile, which requires the network to be the same. There's less tolerance for the weeks and months telcos need to connect new locations when users can activate a cell phone in minutes or receive residential Internet in a day.

**The cloud requires low-latency, secure Internet connectivity** for the entire business. Internet performance suffers across MPLS. Too often costs and complexity force MPLS design to backhaul Internet traffic, congesting the network, and adding latency to Internet sessions.

**Users and resources often sit outside company locations.** The cloud, mobile users, contractors, and other remote users — business involves more than just full-time employees in company offices. MPLS services only connect physical locations, requiring additional equipment and services to connect to cloud resources, and mobile or remote users.

Telco attempts to address those dynamics have seen the introduction of managed SD-WAN services. But managed SD-WAN services from telcos continue to wrap all of the problems with the telco experience around SD-WAN (see "The Difference Between Carrier-managed SD-WAN and SD-WAN as-a-Service").

## A New Kind of Carrier is Needed for Today's Digital Business

To address these market dynamics, we need a different kind of provider. One that's as agile as the business, IT is looking to serve. This new carrier needs to be able to deliver a network with the uptime, predictability, reach, and "white glove" service enterprises have come to expect from the best of the telcos experience. At the same time, the carrier must deliver the agility, cost structures and versatility enterprises need in this cloud and mobile era. We call this new kind of carrier the cloud-native carrier (CNaC).

# Where Cloud Software Powers Networking

Like a telco, a Cloud-native Carrier also delivers an MNS, but it is *how* a CNaC delivers an MNS that is so critical. The CNaC architecture differs from that of the telco in three ways: **cloud-native software, affordable SLA-backed network, and management model flexibility.**

## Cloud-Native Software Replaces Proprietary Hardware

Whereas telcos integrate third-party appliances — routers, firewalls, SD-WAN edge devices, and more — to form a service, the CNaC avoids proprietary hardware and converges networking and security functions into a multitenant, cloud-native, software stack.

Shifting intelligence from edge appliances to the cloud, creates a "thin edge architecture" where the compute requirements for connecting devices is reduced to a minimum. As such, CNaCs can connect a diverse range of end-points to the same basic service, avoiding the hidden costs telcos charge for "optional" services. And without hardware appliances, the CNaC avoids costs associated with

- Third-party appliance markups
- Proprietary hardware integrations
- Delivery and stocking of spare equipment
- Monitoring and troubleshooting tools for managing the hardware
- Expert personnel for managing the complex network of hardware
- Specialized tech personnel for supporting customers

that inflate telco costs, impacting service quality or increasing customer pricing (and often both).

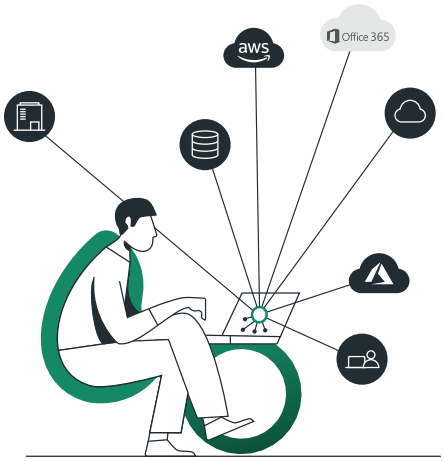
## Global Networks Built By Leveraging SLA-Backed IP Capacity, Not By Pulling Fiber

Telcos built their networks through extensive investment in the physical layer — pulling fiber and cabling, connecting equipment, and terminating with various CPEs. All of which burdens telcos with an expensive, rigid infrastructure that increases the costs and complexity of everything they do.

By contrast, the CNaC leverages the investment already made in IP capacity. The CNaC network is a global, privately managed network of points-of-presence (PoPs), interconnected by SLA-backed capacity leased from

multiple Tier 1 providers. The PoPs monitor their latency and loss and in real-time select the optimum provider for carrying traffic. Sites, mobile users, and cloud resources send all of their traffic — WAN and Internet traffic — to those PoPs by establishing encrypted tunnels across existing last-mile services. Software innovation in network optimizations, monitoring capabilities, and routing intelligence compensate for any underlay issues.

The combination of cloud-native software and inexpensive IP capacity frees CNaCs from the cost structures of telco services. As result, CNaC services can be priced at a fraction of a telco MNS.




## From Self-Service to Fully Managed: Customer Requirements Determine the Right Management Model

Telco architectural constraints make "fully managed" the only management model for anything more than basic connectivity. The underlying telco network is too complex and fragile to be made accessible to customers. Even simple policy changes can impact multiple components. Customers can't be allowed to substantially change the network at the risk of disrupting their own service. As such, even simple network changes require opening support tickets, introducing delay and limiting agility. Full management provides the appearance of simplicity that is so critical to service delivery but complexity never truly disappears. Enterprises fund that complexity in many ways though longer support ticket resolution times and higher service charges.

The CNaC also offers full management as an option but, in addition, the CNaC's multitenant, software-centric architecture allows for self- and co-managed service end-to-end. By using a CNaC's full-featured, self-service portal, IT can provision new users, configure and change firewall and access policies, add static routes and more — without provider involvement. Co-management allows both enterprises and service providers to manage the network. Enterprises can make any pressing changes themselves. The CNaC assumes responsibility for tasks too time-consuming or challenging for many enterprises, such as large-scale edge device monitoring or threat hunting.

In short, the CNaC employs the same model familiar to anyone who's worked with Amazon AWS or Microsoft Azure. Enterprises run their own networking instances and the CNaC maintains the underlying cloud-native software stack and infrastructure. It's an approach made possible because CNaC infrastructure not only appears to be simpler but is in fact simpler.

# Managed Services Evaluation Considerations

The three pillars of any CNaC — affordable **SLA-backed global backbone, cloud-native software, and service management model flexibility** — reduce the costs and improve the agility of the service in many ways:

## Service Management

Service Adoption and Onboarding

Self-Service, Co-Managed, or Fully Managed Models

Problem Resolution Expertise

Last-Mile Management & Delivery

## Cloud-Native Software

Converged Security as a Service

High-Velocity Roadmap

Visibility and Analytics

## SLA-Backed Global Backbone

Optimized Global Connectivity

Cloud and Mobile Coverage

Self-Healing and High Availability

## Affordable SLA-Backed Global Backbone

### Optimized Global Connectivity

Telco networks provide predictable transport critical for enterprise WANs. However, telco networks are never fully global. Invariably some global enterprise sites are outside of the telco network. Enterprise must use a telco partner to connect those location, paying a significant premium in the process. The alternative, connecting across the public Internet, exposes enterprises to the unpredictability of Internet.

The CNaC network is designed for global connectivity. Leveraging multiple Tier 1 global providers allows the CNaC greater reach and better performance than any one of the underlying networks. Using any Internet access service gives enterprises flexibility in selecting their last-mile providers. Built-in optimizations mitigate the effects of latency and reduce packet loss in middle- and last-miles improving data throughput by as high as 40x when compared with MPLS.

### Cloud and Mobile Coverage

A telco MNS is not inherently designed for the cloud. MPLS services connect sites. They do not include affordable, distributed cloud access. Managed SD-WAN also requires enterprises pay for additional SD-WAN appliances near (or in) the appropriate cloud provider datacenter. No MPLS or SD-WAN appliance supports mobile users, requiring the enterprise to pay for yet another telco service, if mobile access is necessary.

By contrast, the thin-edge architecture makes the CNaC inherently mobile- and cloud-friendly. Mobile clients connect to the nearest PoP, allowing one set of policies and traffic rules to govern users in an out of the office. CNaC include cloud datacenter and cloud application connectivity. CNaC PoPs share physical datacenters with cloud datacenter and cloud application entrance points. Application-aware routing directs cloud traffic across the CNaC network to the PoP closest to the destination, in this case, the doorstep of the cloud datacenter or application provider. It's like having a private line right to your IaaS/SaaS provider.

Affordable SLA-Backed Global Backbone

## Self-Healing and High Availability

The digital business relies on an operational network and not just for in-region locations, but network tenants worldwide. Telcos ensure in-region uptime by hardcoding high availability into their networks. They design in multiple layers of expensive and rigid hardware-based redundancy, detecting and resolving blackouts across their last-mile services. Failures in equipment components, last-mile access, and more require manual intervention, often necessitating an engineer to go on-site. Core redundancy is difficult to ascertain, and out-of-region, telcos rely on the last-mile management of their partners. Mobile and cloud resources are ignored entirely or require additional service costs.

The CNaC network includes self-healing for all resources. CNaC PoPs connect across multiple carrier networks, guaranteeing core redundancy. Should there be a blackout or even a brownout on any one carrier network, the PoP software detects the event and automatically routes traffic across around the problem. Within the last mile, should a CNaC PoP become unavailable, all connected sites, cloud resources, or mobile users automatically reconnect to another PoP. Should a local line experience a brownout or blackout, traffic is automatically switched over to another line. And should a customer's CPE fail, affordable high-availability allows even small branch offices to keep working through a redundant device. Finally, fewer physical components means less opportunity for lengthy downtime from device failures.

Cloud-Native Software

## Converged Security as a Service

Essential to leveraging the Internet is protecting against intrusions, data exfiltration, and other Internet-based attacks. Those protections are not built into a telco MNS, requiring integrations with external security appliances, virtual network functions (VNFs), or cloud services. Adding those components impacts enterprises in many ways, namely:

- Visibility is obscured and service delivery made complicated by the disparate solutions.
- Security involves customer-dedicated appliances. Sizing CPEs is not a trivial matter and forced upgrades will become routine.
- Telcos remain burdened with additional costs of patching, scaling, and maintaining appliances.

Telcos must assume these costs and pass them onto their customers to be competitive, ultimately increasing price or lowering the quality of the service.

The CNaC builds security services into the network including next-generation firewall (NGFW), advanced threat prevention, and secure web gateway (SWG). There are no distinct appliances or VNFs. The multitenant cloud software provides security and networking capabilities for all users. The CNaC cloud software is elastic, automatically provisioning and de-provisioning resources as necessary. Security and networking specialists maintain the infrastructure and support integrated managed threat detection (MDR) services. As such, the CNaC faces none of the scaling challenges or additional costs confronting a telco when offering security capabilities with a MNS.

## High-Velocity Roadmap

Businesses evolve and so do IT requirements for the MNS. With the telco, new feature introductions depend on the cooperation of component suppliers. Those suppliers have their own development schedules and priorities, preventing telcos from immediatly addressing customer feature requests. The telcos have influence but little control over the supplier roadmaps. All of which makes innovation and new feature introduction a significant challenge for telcos.

But with a CNaC running its own software stack, new feature introduction is part of the company's DNA. There are no delays from third-party cooperation or dependencies on third-party development timelines. No third-party components or appliances means no integration challenges in delivering new features. Urgent customer requests can be met quickly.

Cloud-Native Software

## Visibility and Analytics

Providers have a unique opportunity to deliver a superior level of management by leveraging their cross-customer view. But to achieve that vision, they need unobstructed visibility into the full network context (metadata) of all customer traffic.

With the telco, traffic flow visibility remains fragmented by the numerous components comprising the telco network. Often the telco lacks access to the SD-WAN device, NGFW, and other appliances comprising the enterprise's MNS instance. Where the telco does have access, numerous hurdles prevent them gaining a complete view of the underlying traffic patterns.

Appliances will often only store traffic summaries, maximizing their storage resources by eliminating the raw traffic captures. But it's the metadata from those raw traffic flows that are critical for network analysis. Accessing appliance data is also challenging, requiring the mastery of vendor APIs, if they're available at all. Data must be ingested into a data warehouse for analysis, normalized, and only then can it be processed. In short, it's very difficult for telcos to derive detailed, cross-customers, insights.

With a single, converged network and security stack the CNaC sees all WAN and Internet traffic. The metadata of all traffic flows is stored in a massive data warehouse for further processing by machine learning algorithms and human researchers. The resulting insights allow the CNaC to deliver detailed security and networking insights, such as those necessary for threat hunting. Such insights are unavailable with traditional telco services.

Service Management

## Service Adoption and Onboarding

To keep pace with the digital business, IT needs to become more agile. A major part of that effort is a network where site additions can be done quickly and easily. A telco MNS brings the complexity typical of adopting a telco service. There are no free service trials to test the service. Site deployments take weeks in part due to the requisite telco line installations.

By contrast, a CNaC is designed for rapid adoption and expansion. Deployment is fast. Sites use over any available Internet transport; mobile and cloud deployment is a matter of downloading a piece of software or configuring a few parameters in the management console. There are no underlay dependencies other than any Internet connection. Adding a new site is simply a matter of connecting to the network. With most intelligence residing in the cloud, zero-touch provisioning is, well, truly zero-touch.

## Self-Service, Co-Managed, or Fully Managed Models

Agility, of course, is more than just minimizing the time for site installations. It's also about shortening network configuration times. With telco MNS, the underlying complexity of the telco network requires the telco to make all changes. Even something as simple as updating a routing table requires opening a support ticket, which may take hours and days to resolve. In an era where we as consumers are used to self service models, telcos continue to require IT to use old-fashioned ticketing systems.

The CNaC bring the "cloud" mentality to configuration management. The underlying simplicity of a CNaC network — cloud-inherent software running on COTS servers in the cloud — allows the CNaC to expose configuration of the customer's instance to the enterprise. With the CNaC's full-featured self-service portal, enterprises can provision new users, configure and change firewall and access policies, add static routes and more without any provider involvement. The CNaC also offers full management — with 24x7x365 last mile management, single-ticket submission, and a central point of contact — it's just not required.

Service Management

## Problem Resolution Expertise

When problems emerge, enterprises need a partner to respond quickly and effectively. Telco support is highly dependent on third-party organizations. Constructing the network out of various appliances puts the most in-depth technical expertise outside of the telco. Enterprises often find they need tier-2 or even tier-3 support before reaching someone with sufficient technical knowledge to resolve a problem. Should there be a software bug or integration problem relating to a component, support times grow as telcos must wait on third-party vendors. The same is true with out-of-region offices. Telcos again are dependent on their partnering providers to resolve the issue.

With a CNaC running its own software stack, product knowledge is internal to the organization. Fast, expert support is immediately available on the first call. Patches or feature requests are serviced directly by the CNaC's engineering team. In practice, the direct access a CNaC's support team has to the engineering team dramatically reduces time to resolution.

## Last-Mile Management and Delivery

Telco MNS bundles the last mile, simplifying deployment. At the same time, though, enterprises are locked into the last-mile providers approved by the telco. Even telco managed SD-WAN, which allow some flexibility in selecting the last-mile provider, requires at least one connection to the telco's network.

CNaCs utilize the customer's existing last mile. As such, enterprises have more flexibility in picking their ISP. The additional freedom leaves enterprises responsible for negotiating those relationships while offloading the management of those last miles onto the CNaC — if that's what the customer wants. Centralized ordering, invoicing, and billing can be provided by last-mile aggregators, who maintain relationships with local ISPs and other last-mile providers around the globe.

By combining cloud-native software, an affordable SLA-backed global backbone, and management model flexibility, CNaCs can address and adapt to the needs of the modern business. They bring the advancements of the cloud to infrastructure, offering enterprise a new kind of telco experience — the CnaC experience.

# Cato Networks is the Cloud-Native Carrier

Your business is going digital. It depends on optimized access to applications, data on-premises and in the cloud, and an increasingly mobile global workforce.

Enterprise networks of old can't keep pace with the digital business. Stitching together point solutions is difficult and resource intensive; telco services are too expensive and rigid. There has to be a better way.

Cato is the global CNaC of today. Cato connects all datacenters, branches, mobile users, and cloud resources into a global, optimized secure, managed SD-WAN service. All WAN and Internet traffic is protected by a comprehensive suite of security service, updated and managed by dedicated security experts.

Replacing MPLS and multiple networking and security point solutions with Cato Cloud forms a network so agile and efficient it can meet today's -- and tomorrow's business requirements.

Your business must leap forward to the digital age to stay competitive, and the IT infrastructure can't fall behind. Cato provides the secure and global network that is the new foundation of your digital business.

**Contact us**

# Cato. Network at the Speed of Now.

- Global Private Backbone
- Edge SD-WAN
- Security as a Service
- Cloud Datacenter Integration
- Intelligent Last-mile Management
- Cloud Application Acceleration
- Mobile Access Optimization

### Managed Services

- Managed Threat Detection & Response
- Intelligent Last-Mile Management
- Hands-Off Management
- Sites Deployment

# Cato Networks is the Cloud-Native Carrier

Your business is going digital. It depends on optimized access to applications, data on-premises and in the cloud, and an increasingly mobile global workforce.

Enterprise networks of old can't keep pace with the digital business. Stitching together point solutions is difficult and resource intensive; telco services are too expensive and rigid. There has to be a better way.

Cato is the global CNaC of today. Cato connects all datacenters, branches, mobile users, and cloud resources into a global, optimized secure, managed SD-WAN service. All WAN and Internet traffic is protected by a comprehensive suite of security service, updated and managed by dedicated security experts.

Replacing MPLS and multiple networking and security point solutions with Cato Cloud forms a network so agile and efficient it can meet today's -- and tomorrow's business requirements.

Your business must leap forward to the digital age to stay competitive, and the IT infrastructure can't fall behind. Cato provides the secure and global network that is the new foundation of your digital business.

**Contact us**

# Cato. Network at the Speed of Now.

### Cato Cloud

- Global Private Backbone
- Edge SD-WAN
- Security as a Service
- Cloud Datacenter Integration
- Intelligent Last-mile Management
- Cloud Application Acceleration
- Mobile Access Optimization

### Managed Services

- Managed Threat Detection & Response
- Intelligent Last-Mile Management
- Hands-Off Management
- Sites Deployment

# Appendix

| | Cato | Telco | Cato Impact |
|---|---|---|---|
| | | OVERALL | |
| **Cost** | Affordable: Own software stack (no third-party software license); virtual multiprovider backbone (no underlay infrastructure to own or maintain) | Expensive: Multiple third-party software licenses; custom-built, underlay network | Lower cost per Mbits/s at the same or better performance |
| **Agility** | High: Use any provider's underlay (MPLS or Internet - DIA or 3G/4G); Configuration and policy changes (network or security) made in minutes; expert tier-1 support | Low: Wait for MPLS line installation; underlay lock-in; wait for telco to make configuration and policy changes; expert support only available at tier-2 or tier-3 | Faster time to deploy, faster network configuration; faster problem resolution |
| | | AFFORDABLE SLA-BACKED BACKBONE | |
| **Optimized Global Connectivity** | Optimized: Global, SLA-backed backbone with built-in WAN optimization | Not optimized: Physical backbone limited in coverage; no bult-in WAN optimization | Better throughput for a lower cost per Mbits/s |
| **Self-Healing and High Availability** | Global: Multiple levels of redundancy with automated self-healing software | On-net: Hard-coded HA design in provider's network with manual intervention; partner-dependent off-net availability | Better availability through automated resilience |
| **Cloud and Mobile Coverage** | Built-in: Cloud and mobile are equal tenants on the wide area network | Add-on: Cloud and mobile available at additional cost, if at all | Seamless connectivity across all resources — cloud, mobile users and sites. |
| | | CLOUD-NATIVE SOFTWARE | |
| **Network Security** | Built-in: Cato Security Services include NGFW, SWG, Advanced Threat Prevention, Cloud and Mobile Access Protection and Network Forensics. | Add-on: Network security must be engineered into the network at additional cost | Lower cost; easier configuration and management |
| **Service Roadmap Velocity** | Fast: Cato controls pace of innovation, and the incorporation of customer requirements, features and feedback. | Slow: Highly dependent on third-party component roadmap and integration into the telco service offering. Very hard for the telco to impact these roadmaps | Future-proof, service innovation |
| **Provider Visibility and Analytics** | Complete: Cato collects and analyzes metadata for all WAN and Internet traffic from all customers | Limited: Telco visibility obstructed by various appliances | Cross-enterprise insights; new kinds of affordable, easy-to-deploy analytic-driven services, such as threat-hunting |
| | | SERVICE MANAGEMENT | |
| **Service Adoption and Onboarding** | Fast: Deploy sites with any available Internet transport (DIA; 3G/4G), if necessary, switch to MPLS when available; no underlay dependencies | Slow: Requires telco underlay, must wait for MPLS installation, no free service trials | Faster time to deploy |
| **Self-Service, Co-Managed, or Fully Managed Models** | Rapid: Visibility and control, seamless platform maintenance | Slow: Ticket-based network change management: slow and rigid, heavy infrastructure to maintain that must be factored into the cost of service | Fast network configuration; less grunt work; lower costs |
| **Problem Resolution Expertise** | Fast: Expert support directly linked to Cato cloud engineering | Slow: Out of region, lack of expertise, disconnected from third-party product engineering | Faster time to resolve |
| **Last-Mile Management and Delivery** | Global: Wherever Internet or MPLS connectivity exist | Partial: Strong regional coverage but must partner with other MPLS providers for out-of-region connectivity | Faster time to deploy new locations |