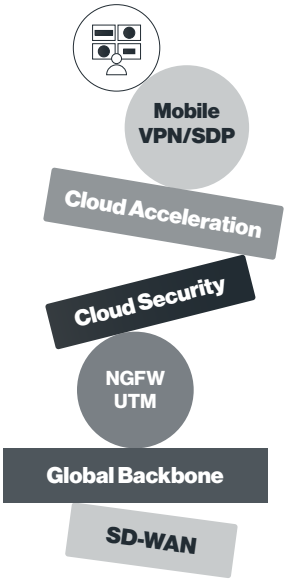
Cato Networks Quick Overview

Legacy Networks and Telcos are Incompatible with the Digital Business

Your business is going digital. It depends on streamlined global access to applications and data on-premises, and in the cloud, alongside supporting users working from anywhere. Legacy networks, comprised of disparate point solutions, are simply incompatible with the modern digital enterprise. There's a clear need for a new type of architecture. Don't take our word for it; Gartner says that "Digitalization, work from anywhere and cloud-based computing have accelerated cloud-delivered SASE offerings to enable anywhere, anytime access from any device." According to Gartner, SASE is the secure network for the future of your business, and a "pragmatic and compelling model that can be partially or fully implemented today."

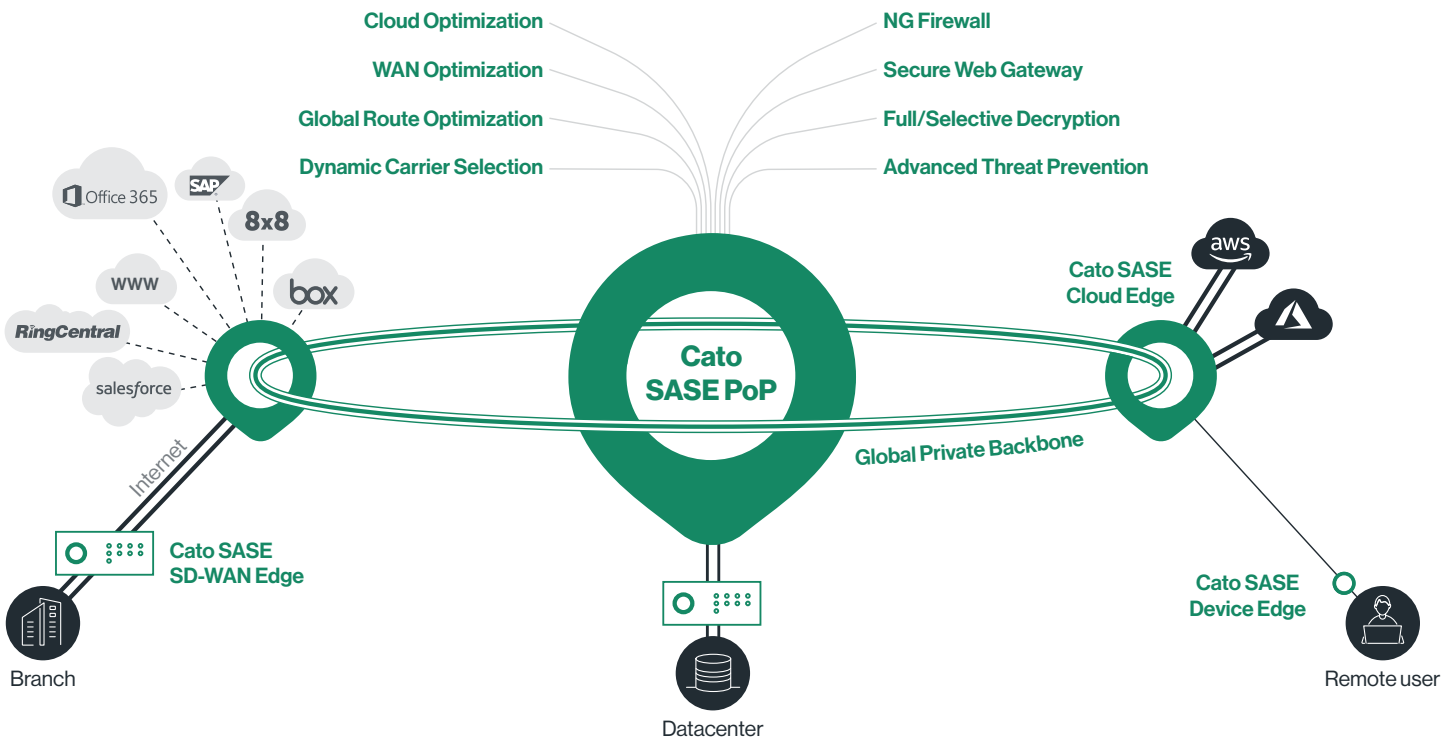


How can IT be Ready for Whatever's Next?

Global, SD-WAN, Security, Cloud , Mobility. **Converged.**

Cato SASE Cloud is a global converged cloud-native service that securely and optimally connects all branches, datacenters, users, and clouds. Cato enables moving away from legacy MPLS, a bundle of security point solutions, and expensive managed services, to a simple, agile, and affordable network. Self-service or a managed service is up to you.

Aligned with the principles set by Gartner, Cato delivers a true SASE service that allows enterprises to optimize user experience, protect against emerging threats, and embrace new business opportunities – everywhere. With Cato, your network, and your business, are ready for whatever's next.



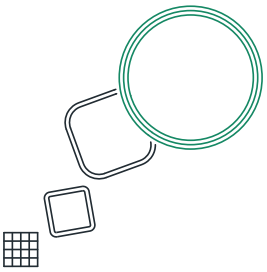
Cato Solutions for Enterprise WAN Challenges:

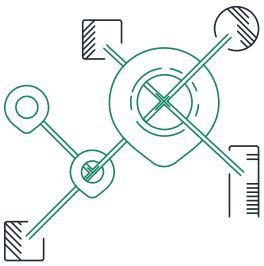
Where do you Want to Start?

Cato enables customers to gradually transform their WAN for the digital business. You can address one or more of the use cases below at your own pace. No matter where you start, Cato will support you throughout your journey.

MPLS Migration to SD-WAN

Cato enables customers to replace or augment MPLS using a combination of high-capacity Internet links and Cato SASE Cloud. Customers boost usable capacity and improve resiliency at a lower cost per megabit. Global enterprises use Cato's global private backbone to reduce costs, meet service levels, improve performance, and deliver security everywhere.





Optimized Global Connectivity

Cato SASE Cloud 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 complete network security stack built into Cato SASE Cloud. By connecting all branch locations to Cato, all traffic, both Internet-bound and WAN, is fully protected by Cato's enterprise-grade, cloud-native security services. There's no need to backhaul Internet traffic to a datacenter or a regional hub, deploy branch network security appliances, or procure stand-alone cloud security solutions.

Cloud Acceleration and Control

Cato provides seamless acceleration of cloud traffic by routing all traffic from all edges to the Cato PoP closest to the cloud datacenter. Because Cato PoPs share the datacenter footprint of major cloud providers, the latency between Cato and these providers is essentially zero. Ther's no need to install cloud appliances or setup hubs to reduce latency to the cloud.

Remote Access Security and Optimization

Cato extends global networking and security capabilities down to a single user's device. Mobile and remote users are no longer treated like second-class citizens of the 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's security-as-a-service stack protects users against threats everywhere and enforces application access control.