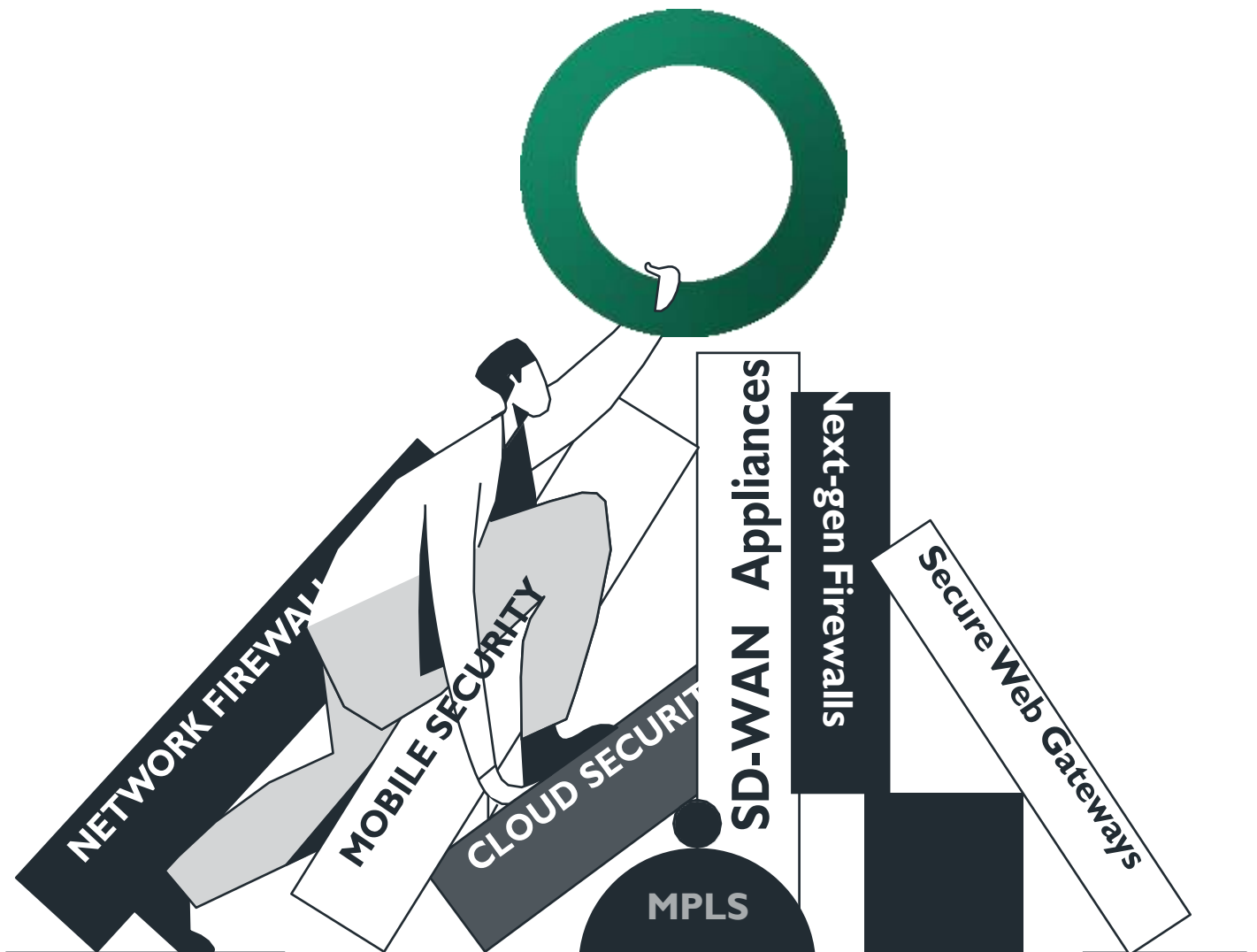


The Network for the Digital Business Starts with the **Secure Access Service Edge (SASE)**



The Need for Speed: How IT Must Support the Digital Business

The digital business is all about speed. Time to develop new products, deliver them to the market, and respond to a change in business conditions or the competitive landscape. Technology is how speed happens, and IT must enable the business to get things done. Automation, agility, elasticity, and flexibility are some of the traits of the modern IT infrastructure, which is already demonstrated via the increased usage of cloud computing.

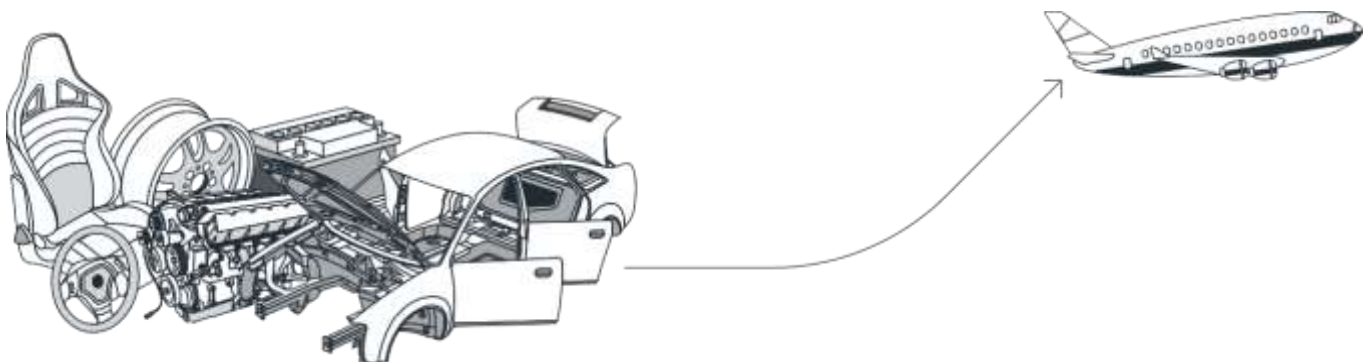
Unlike cloud computing, networking and security are painfully incompatible with the cloud-centric and mobile-first business. The network is rigid and static. Security is heavily fragmented across multiple domains of physical locations, cloud resources, and mobile users. Together, networking and security are slowing down the business as silos erected decades ago are stretched and patched to accommodate emerging business requirements.

Networking and security need to become part of the IT platform for the digital business. Don't take our word for it: Gartner has recently defined a new category that converges network and security into a single cloud-based service: Secure Access Service Edge (SASE). Simply put, SASE is the secure network for the future of your business.

The Challenge: You Can't Build a Jet from Car Parts

Historically, IT teams solved emerging business needs with point solutions. For example, adding SD-WAN boxes to offload capacity constrained and expensive MPLS connections to Internet links; or adding firewalls in branches to enable secure Direct Internet Access (DIA). The result of this approach was technological silos, built upon point solutions that are loosely integrated and separately managed. Ultimately, IT needs to provide consistent performance and strong security, in a cost-effective way, to all business resources, globally. This is an architectural challenge, not a functional problem, that requires the elimination of IT silos, and the use of "point solution patches" to address new business requirements.

It's the realization that IT architecture must evolve beyond the silos and the use of point solutions that is driving SASE



SASE: A New Networking and Security Architecture for the Business

SASE is a new category defined by Gartner analysts Neil McDonald (security analyst) and Joe Skorupa (networking analyst). SASE details an architectural transformation of enterprise networking and security that will enable IT to provide a holistic, agile and adaptable service to the digital business. The SASE Cloud service has 4 main characteristics: it's identity-driven, cloud native, globally distributed, and supports all edges (WAN, cloud, mobile, edge computing).



Identity-driven: The basis for SASE Networking and Security Policies

At the core of SASE is the identity. An identity is attached to every enterprise resource: a person, an application, a service, or a device. It's the identity that determines the true essence of the resource - not its physical location. Identity, as part of a broad and dynamic context awareness drives the risk and network service profile of every flow, and the resulting mix of authentication methods, threat inspection, and data access authorization. Identity "blindness" is a trait of pure networking vendors, however it's "table stakes" with security vendors. The benefit of security and networking convergence is the infusion of identity throughout the access life cycle from ensuring quality of service to applying risk-driven security controls.



Cloud-native: Built-for and delivered-from the cloud

A core characteristic of SASE is a cloud-native, as-a-service model. A cloud-native architecture leverages key cloud capabilities including elasticity, adaptability, self-healing, and self-maintenance.

SASE calls for the creation of a network of cloud points of presence (PoPs) which comprise the SASE Cloud. The PoPs run the provider software that delivers a wide range of networking and network security capabilities as a service. The PoPs should seamlessly scale to adapt to changes in traffic load via the addition of compute nodes. The PoPs can be upgraded to deliver new features or bug fixes seamlessly and without IT involvement. The cloud architecture must include self-healing capabilities to automatically move processing away from failing compute nodes and PoPs and into healthy ones.

These capabilities can't be achieved by spinning up virtual appliances in the cloud. As appliances are designed to serve a single customer (single tenant) and lack the overall cloud orchestration layer to ensure elasticity and self-healing. The approach of service chaining legacy point products, appliances or cloud services, will likely affect service quality and performance.

Globally Distributed: Available Near All Edges

SASE Cloud is implemented as a globally distributed cloud platform. The SASE Cloud design guarantees that wherever your edges are, the full range of networking and security capabilities will be available to support them. SASE providers will have to strategically deploy PoPs to support business locations, cloud applications and mobile users. As Gartner notes, SASE PoPs must extend beyond public cloud providers' footprints (like AWS and Azure), to deliver a low-latency service to enterprise edges.



Building a global cloud platform requires providers to hone their ability to rapidly deploy PoPs into cloud and physical datacenters, ensure high capacity and redundant connectivity to support both WAN and cloud access, and apply security and optimization end-to-end across all edges.

All Edges: Physical Locations, Clouds, Users and Edge Computing

SASE uniquely supports all enterprise edges equally. By adopting a cloud-first approach to networking and security, SASE decouples many common capabilities, such as network optimization and threat prevention, from physical location edges, and places them in the cloud. For example, legacy network security appliances are tied to a specific physical location, which is not suitable for serving the cloud or mobile edges.

SASE includes a thin-edge component to connect different edges to the available SASE PoP. The edges work in tandem with the SASE cloud service to overcome PoP failures or access issues to ensure continuous service. As noted earlier, the SASE Cloud is designed to deliver the same set of capabilities from every PoP, and without dependency on customer specific components simplifying, the shift of traffic across the SASE Cloud.

Edge implementations vary. Physical locations use SD-WAN devices and multiple Internet links to maximize throughput, enforce QoS, and overcome link failure or degradation. Mobile workers use a client or clientless web access for enterprise-grade protection and optimized access to datacenter and cloud applications. Cloud datacenters will connect to the SASE Cloud over multiple tunnels, with all traffic secured and optimized regardless of the source edge.



The Core Capabilities of SASE: Plug-and-Play Visibility, Optimization, and Control

The SASE architecture is made of two core components. SASE Cloud acts as an aggregator of networking and security capabilities. SASE edge connectors drive traffic from physical, cloud, and device edges for SASE cloud processing. SASE uses a single-pass, traffic processing engine to efficiently apply optimization and security inspection with rich context for all traffic. Contrast the SASE model with stacking point products where each product analyzes traffic for a specific requirement, adds overhead for actions like decryption, and lacks the context generated in other network and security point products.

Selected SASE capabilities include:



Authentication: Upon connection of an edge, dynamic risk assessment drives activation of multi-factor authentication.



Access: Access to key applications and service is controlled by application- and user-aware next generation firewall policies. In addition, a zero-trust network access model can ensure users only access authorized applications without gaining general network access.



Prioritization: Application identification assigns priority to the traffic to optimize loss-sensitive applications like Voice over IP (VOIP) and virtual desktop access (VDI) over other traffic such as general Internet browsing.



Decryption: To enable deep packet inspection, encrypted traffic can be decrypted once to allow multiple threat prevention engines to process the traffic.



Threat prevention: Multiple security engines parse the traffic to detect risky access. These include Secure Web Gateways (SWG) that look for malicious websites, anti-malware to prevent download of malicious files, IPS to stop inbound and outbound anomalous connections that are indicative of bot activity, and more.



Data loss prevention: SASE applies specific data loss prevention rules to detect sensitive data in the network flows and stop it from leaving the network. Similarly, a Cloud Access Service Broker (CASB) can enforce granular access control to cloud applications.

While this is a subset of the SASE capabilities, the SASE architecture is designed to rapidly extend the “single pass traffic processing engine” with new ones. This unique benefit of SASE is future proofing the network, extending the SASE cloud and the new capabilities to anyone and everywhere. Similarly, adapting the SASE cloud service to new threats or attack vectors can be done centrally and immediately affects all enterprises and all edges without the need for IT to deploy or activate these added capabilities.

The Right IT Foundation for the Digital Business

The Benefits of SASE

SASE creates a holistic platform that connects all edges to the networking and security capabilities they need. This lowers the cost, complexity and risks of supporting the business in a dynamic environment. Here are some of the key benefits of the SASE platform:



Agility: Supported by the SASE architecture, IT can deliver optimized networking and strong security to all locations, applications, and users regardless of where they are. Provisioning of new resources and capabilities is fast and simple. Just deploy the right edge client and plug into the SASE platform and corporate policies drive your network and security experience.



Collaboration: IT teams can leverage the convergence of network and security to manage all features and policies in a single interface, using a common terminology, and gain deep visibility into network and security events. Cross team collaboration improves the overall service delivery to the business that often involves a combination of availability, performance, and security requirements.



Efficiency: With SASE, IT teams are relieved of the grunt work to maintain on premises infrastructure. Physical topology, redundancy, scaling, sizing, and upgrading is dramatically reduced. IT can now achieve better service to the business, while focusing precious resources and skills on business-specific problems rather than the grunt work of generic infrastructure maintenance.



Cost reduction: The simplification of the network and security stack, and the consolidation of multiple point products enables both vendors and customers to reduce the overall costs of keeping the infrastructure running.

What is Not a SASE?

SASE carries such a big promise that a marketing war is likely to erupt between SASE wannabees. Gartner warns that some traditional vendors will try to deliver a SASE-like solution based on wrapping their existing products in a SASE package. Such attempts will create a risk to service quality and delivery, as these technologies weren't designed for cloud-native delivery. In a nutshell, look carefully at the underlying SASE architecture to determine the fit with the expected outcomes.

Telco Bundles are the Exact Opposite of SASE

For over a decade, telcos have offered to take away the complexity of managing your network and security stack, through a bundle of point solutions they procure, install and manage. Complexity didn't go away, and your spend increased to pay for both the products and the people to manage them. Also, you were dependent on the telco to do everything for you, often slowing the IT organization to a crawl. This is the exact opposite of SASE: legacy appliances and fragmented management with limited or no visibility. SASE is built with the scalability, self-service, and agility of the cloud. Your telco isn't.

Virtual Machines in the Cloud are Still a Stack of Appliances

Instantiating virtual machines in an IaaS like AWS, Azure and alike is great, but not for SASE. While it does move on-premises appliances to be 'in the cloud', they are still disparate point solutions that lack the cloud-native integration, single pass processing, global reach, and elasticity of a SASE. And, depending on the vendor mix, you'd still need to use multiple management consoles.

Service Chaining Sounds Close, But not Really

Facing the reality of a multi-vendor environment, service chaining is a technique to link together multiple point solutions such as SD-WAN, routers, firewalls, WAN optimizers and more. Regardless of the use of multiple physical appliances or Universal Customer Premises Equipment (uCPE) that host multiple virtual machines, these are still discrete solutions that need to be sized, scaled and managed separately. Ultimately, SASE offers convergence as the key defining attribute and service chaining isn't convergence but loosely coupled linking of point solutions.

The Incomplete SASE: Cloud and Edge Vendors Must Plug Big Holes in their Offerings

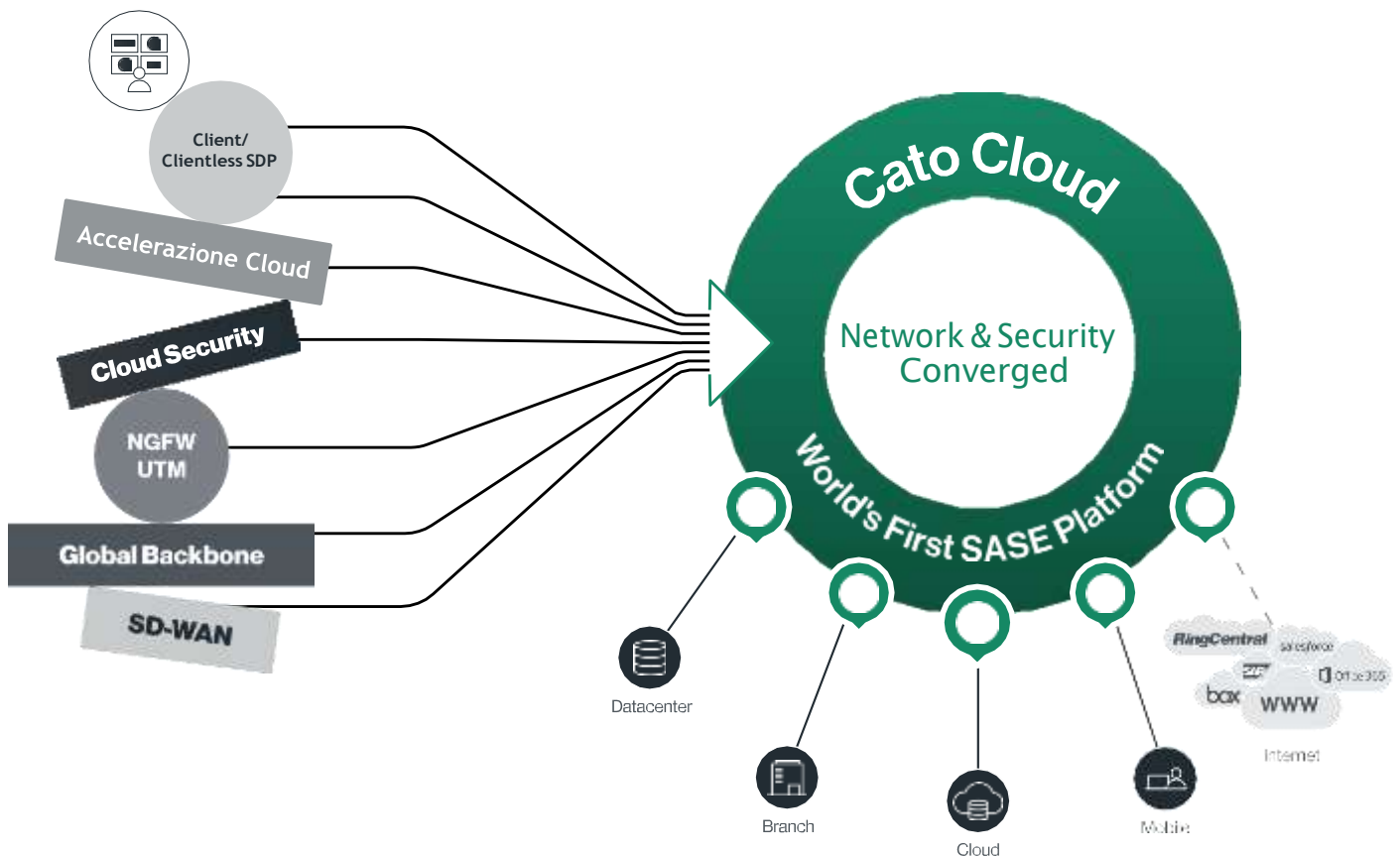
Security-as-a-Service vendors have been working to deliver multiple security capabilities via their cloud services including SWGs and CASBs. These vendors still lack the key SASE elements of controlling network flows and natively supporting the WAN edge. Without a natively integrated and mature technology to reliably and securely connect all edges (offices, cloud datacenters, users and devices) to the SASE Cloud, SWGs and CASBs remain a silo that needs integration with other products. Similarly, edge appliance vendors now face the task of building the breadth of SASE Cloud capabilities as globally distributed, cloud-native services.

Cato Networks: A Full SASE Platform You Can Deploy Today

Your SASE journey can start today with WAN transformation or appliance refresh. How do you pay for SASE?

The good news is, that the budget for SASE is already here. Your next security appliance refresh, your upcoming MPLS contract renewal, or your M&A integration project - all represent great catalysts to launch the SASE project. The migration doesn't have to happen all at once, and most SASE platforms support a gradual migration process, during which a SASE can co-exist with legacy network and security solutions until they are fully retired.

While the SASE category defined by Gartner is new (published first in [Gartner's Hype Cycle for Enterprise Networking 2019](#), its implementation is not. The Cato Cloud is a market-proven SASE platform you can deploy today. Cato converges enterprise network and security capabilities into a single pass software stack delivered as a cloud service.



Cato is the convergence of networking and security in the cloud

Cato Cloud Meets the Key Attributes of the SASE Architecture



Identity-driven everything: Cato automatically determines the identity or the resource connecting to the Cato Cloud regardless of location. The identity is attached to the flow, and is used, together with other context elements to trigger multi-factor authentication, drive application-level access control policies, determine network quality of service, and continuously assess the data risk associated with the flow.



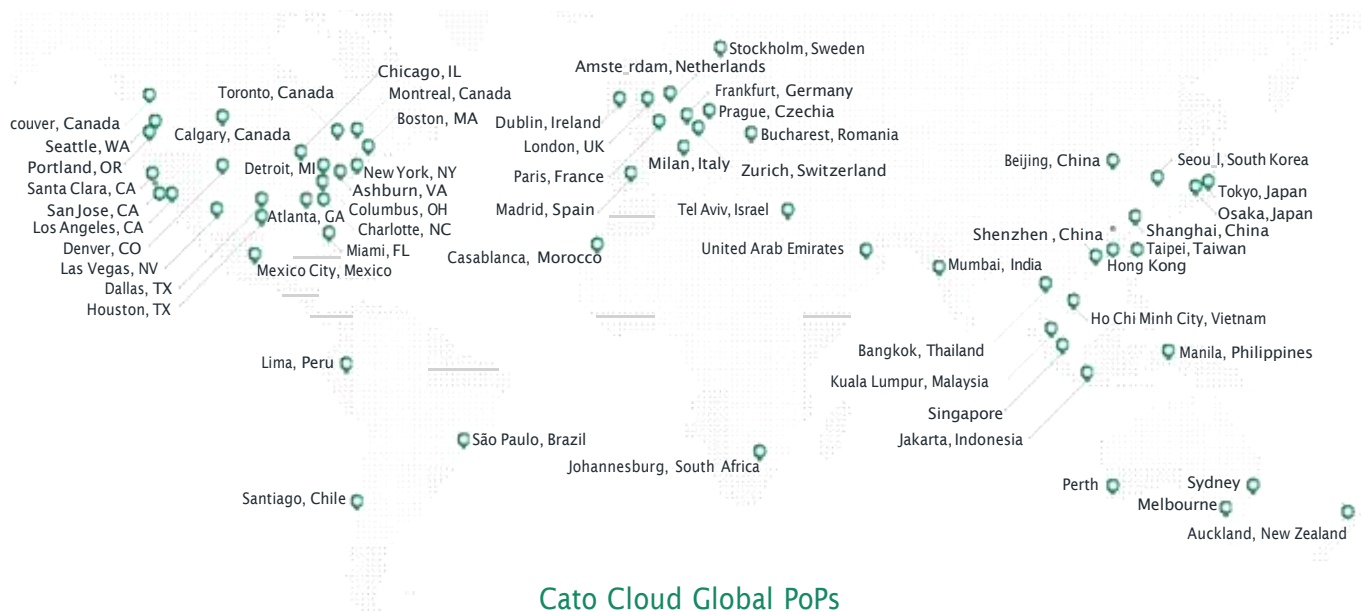
Cloud-native traffic processing: Cato developed the Cato Cloud from scratch as a cloud-native service. It uses a “single pass engine” to process all traffic from the packet up and provide optimization and security. Cato doesn't use purpose-built appliances or virtual machines and is therefore able to provide Cato customers the scalability, self-service, and agility of cloud providers.



Support for all edges: Physical locations, mobile users on any device, cloud datacenters and applications, use Cato edge solutions to plug into the Cato Cloud. Physical locations use an edge SD-WAN device (Cato Socket), a Software-Defined Perimeter (SDP) client or clientless web browser is offered for mobile devices, and IPsec tunnels connect cloud resources to the Cato Cloud. Regardless of edge, Cato's full set of networking and security capabilities is readily available from the nearest Cato PoP.

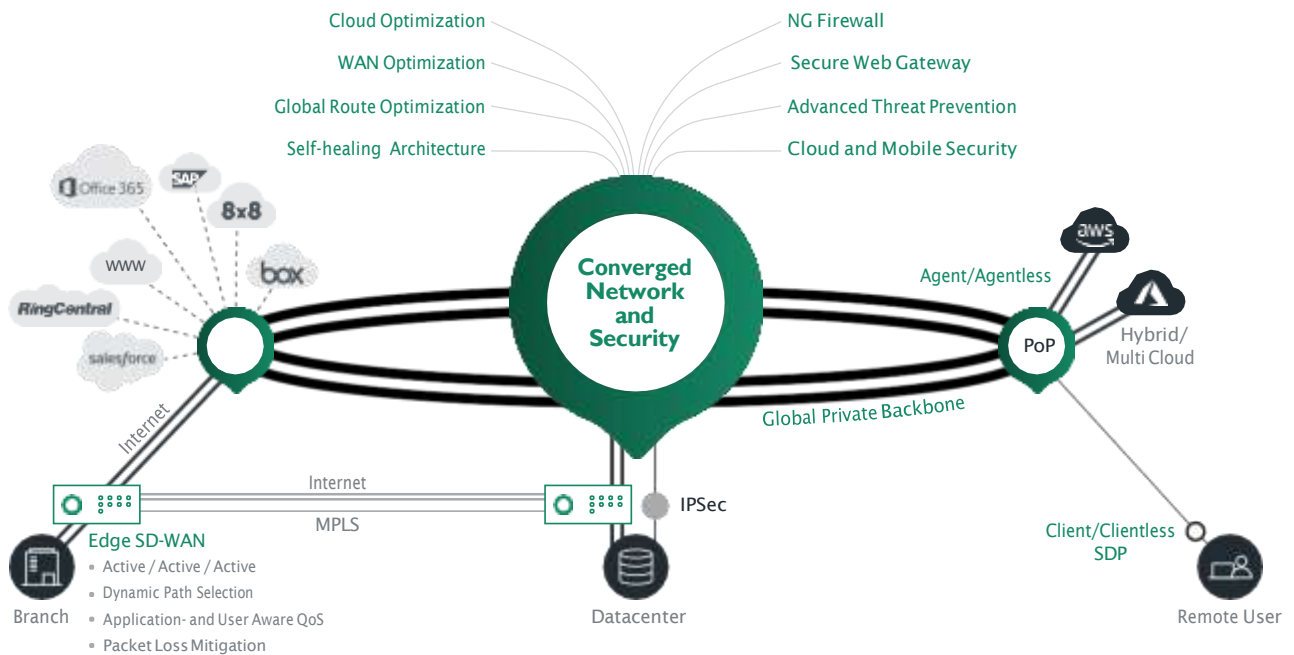


Globally distributed network of PoPs: Cato Cloud spans over 50 PoPs from which the full capabilities of the service are delivered. All of Cato's PoPs are interconnected by multiple tier-1 carriers, forming a global private backbone that optimizes WAN and cloud traffic. The PoP software applies deep packet inspection to secure the traffic against multiple threats as it flows through the Cato Cloud.



About Cato Networks

Cato is the world's first SASE platform, converging SD-WAN and network security into a global, cloud-native service. Cato optimizes and secures application access for all users and locations. Using Cato, customers easily migrate from MPLS to SD-WAN, optimize global connectivity to on-premises and cloud applications, enable secure branch Internet access everywhere, and seamlessly integrate cloud datacenters and mobile users into the network with a zero trust architecture. Using Cato, customers easily migrate from MPLS to SD-WAN, optimize connectivity to on-premises and cloud applications, enable secure branch Internet access everywhere, and seamlessly integrate cloud datacenters and mobile users into the network with a zero-trust architecture. With Cato, the network, and your business, are ready for whatever's next.



For more details, please contact us

Cloudtivity Consulting Services, LLC
 (770) 833-6371
info@cloudtivityconsulting.com
<https://cloudtivityconsulting.com/>



Cato. The Network for Whatever's Next.

Cato Cloud

- [Global Private Backbone](#)
- [Edge SD-WAN](#)
- [Security as a Service](#)
- [Cloud Datacenter Integration](#)
- [Cloud Application Acceleration](#)
- [Mobile Access Optimization](#)
- [Cato Management Application](#)

Managed Services

- [Managed Threat Detection and Response \(MDR\)](#)
- [Intelligent Last-Mile Management](#)
- [Hands-Free Management](#)
- [Site Deployment](#)