CATO
NETWORKS

Cato SASE Cloud

The Future SASE – Today and Tomorrow

Gartner recently published its
“2021 strategic roadmap for SASE convergence.”

In it, Gartner outlines the current state of SASE solutions, a roadmap for customers to adopt SASE, and the desired future of SASE solutions to support that roadmap. Gartner indicates that “SASE is a pragmatic and compelling model that can be partially and fully implemented today.”

This document is Cato’s perspective on the Gartner document.

SASE Customer Roadmap: 2021 and Beyond

SASE Market Is Driven By an Architectural Transformation

SASE was created as a framework for secure and optimal access to applications. The agile nature of the access context including the identity, device, network, application, and data requires an equally agile platform to deliver secure and optimal access available to everyone and everywhere. Simply put, a move from a product-based to service-based architecture.

Gartner sees a need for customers to change their network security architecture. Gartner states that "Perimeter-based approaches to securing anywhere, anytime access has resulted in a patchwork of vendors, policies, and consoles creating complexity for security administrators and users." Therefore, "To protect anywhere, anytime access to digital capabilities, security must become software-defined and cloud-delivered, forcing changes in security architecture and vendor selection."

SASE Has Both Security and Networking Catalysts

Gartner recognizes that the path to SASE is not trivial. They identify several catalysts to a SASE project. Gartner states that "Enterprises that consider existing skill sets, vendors, and products and timing of hardware refresh cycles as migration factors will reduce their secure access service edge (SASE) adoption time frame by half." Additional catalysts include "Branch office transformation projects (including software-defined WAN [SD-WAN], MPLS offload, internet-only branch and associated cost savings) are increasingly part of the SASE project scope."

SASE Projects Should Be Deployed Gradually

Initially, Gartner sees gradual deployment of SASE across use cases (ZTNA first), limited vendor consolidation (VPN, SWG, CASB), and leveraging network transformation (MPLS offload). Longer term, customers should reduce their vendor footprint to one or two, deploy full ZTNA for all users everywhere, gain total control of traffic and data storage for compliance, and create a unified networking and security IT team around the SASE platform.

The Current and Future State of SASE Platforms

Gartner looks at the state of SASE offerings as a whole. It identifies a current state where vendor architectures and capabilities are either inadequate or incomplete in delivering SASE, and a future state that will deliver on the SASE promise. We will look into the gaps Gartner sees between current SASE and future SASE in more details, but we want to first introduce a key observation we have on their analysis overall.

SASE Architecture vs. SASE Capabilities

SASE has two core parts: the architecture and the capabilities. To get the benefits of SASE you must have the right architecture and then you can choose the capabilities that fir your particular situation. Having the right architecture allows vendors to add capabilities while maintaining the "SASE way" of delivering these capabilities. Many vendors have built a large portfolio from acquisitions of non-integrated products. They can "check all the boxes," and they could have done it a long time ago, but this will not amount to a true SASE architecture and will likely miss the goal of doing SASE in the first place.

As the only SASE platform built from the ground up according to the SASE architectural principles, Cato has the right platform to deliver SASE – today and tomorrow. We run an aggressive roadmap, based on customer feedback, to add the capabilities we are missing. Because we have the right architecture, customers can be assured that all capabilities will have the same converged, global, elastic, and resilient attributes of the Cato SASE Cloud coupled with a single pane of glass management. Cato will never allow fragmentation of its SASE platform.

In summary, it is much easier to add capabilities to the right architecture, than it is to retrofit an architecture to consistently deliver these capabilities.

Current vs Future of SASE Architecture and Capabilities

Current SASE	Future SASE	Cato SASE Cloud: The Future SASE – Today and Tomorrow
Inconsistent policy enforcement that is location dependent.	Consistent policy enforcement, regardless of location, with support for local decision making.	Location independent, single policy that is enforced across all edges (branches, users, clouds). All of Cato's policy enforcement is in the cloud, with local segmentation support.
Complex administration using disparate management consoles and policies.	Ease of administration via a consolidated policy control plane.	One Console for all policies and analytics across all networking and security capabilities.
Rudimentary or nonexistent sensitive-data visibility and control. Basic threat detection capabilities.	Sensitive-data visibility and control as well as threat detection.	Full threat prevention and detection, sensitive data visibility and control (coming 2021) without compromising on any architectural requirement.
Immature or nonexistent capabilities in the security parts of the SASE portfolio. Not all vendors currently address the full set of required and recommended SASE capabilities .	Consistent policy enforcement covering all types of access Consistent coverage for all types of entities, including users and devices at branch office, campus and edge locations.	Cato SASE Cloud consistently covers all types of access using a cloud-heavy/thin edge architecture. Cato has dedicated solution to connect all edged to the cloud. Cato SD-WAN for physical locations, Cato SDP client-based and clientless access for user devices (PC, MAC, iOS, Android, Linux), Cato vSocket and IPSec tunnels for any cloud (AWS, Azure, GCP, etc). Cato's global private backbone optimally and securely interconnects all these edges between themselves and the Internet. Cato continuously rolls out new SASE capabilities into the Cato SASE Cloud, within the same architecture and policy management model, to address customer current and emerging requirements.
Monolithic architectures with multiple inspection points that ignore encrypted traffic or incur a significant performance hit.	Single pass inspection of encrypted traffic and content at line speed.	Cato SASE Cloud implements a single-pass engine that is globally distributed across 65 PoPs. Cato's single-pass engine leverages a single shared context for every packet (device, identity, network, application, data) to enforce granular policies without adding latency and overhead. All traffic and content, in all directions (WAN, Cloud, Internet), from all sources (users, branches, clouds) is fully decrypted and inspected at line speed by the Cato SASE Cloud. Because Cato is built as a cloud-native architecture capacity is dynamically distributed across the cloud with built-in high availability and redundancy (any SASE compute node in any PoP can serve any endpoint).
Basic SLAs, rarely with contractual penalties.	Highly available, low-latency services with contractually enforced SLAs.	Cato SASE Cloud provides 99.999% availability SLA with contractual penalties.
Basic or no ZTNA capabilities lacking inspection and limited integration into endpoint security and management tools.	Delivers a zero-trust networking security posture.	Cato SASE Cloud delivers ZTNA to endpoints including risk-based access polices, strong authentication and continuous risk assessment.
Fragmented and frustrating end-user experience.	Transparent and simplified end-user experience.	Cato Client and Clientless Access provides simple end user experience.
Separate and siloed teams responsible for security versus network engineering.	Unified IT responsibility for access engineering.	Cato SASE Cloud offers single pane of glass for both networking and security teams as a foundation of organizational IT convergence.

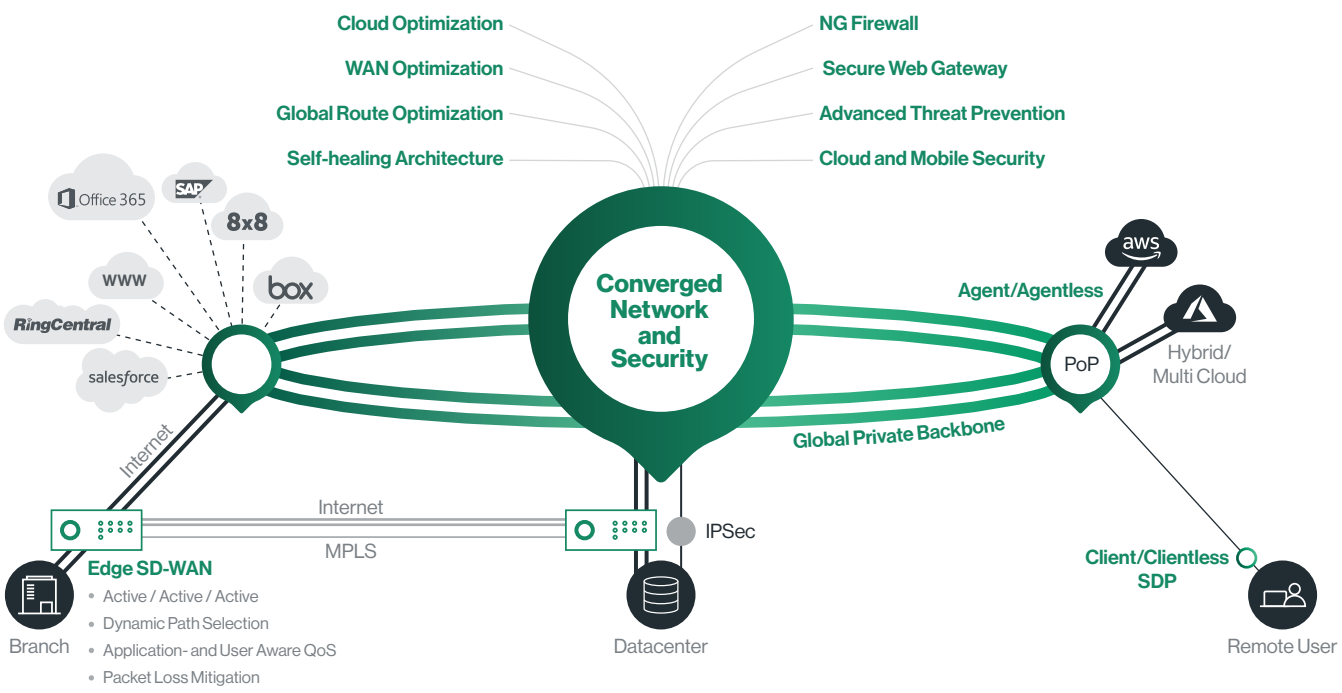
About Cato Networks

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, including branch offices, mobile users, and cloud datacenters, and allows enterprises to manage all of them with a single management console with comprehensive network visibility. Cato's SASE platform has all the advantages of cloud-native architectures, including infinite scalability, elasticity, global reach and low total cost of ownership.

Connecting locations to the Cato cloud is as simple as plugging in a preconfigured Cato socket appliance, which connects to the nearest of Cato's more than 60 globally dispersed points of presence (PoPs). Mobile users connect to the same PoPs from any mobile device via a simple piece of software that is easy to install and use. With Cato, new locations or users can be up and running in hours or even minutes, rather than days or weeks.

At the local PoP, Cato provides an onramp to its high-performance global private backbone and security services. Cato monitors traffic and selects the optimum path for each packet across the backbone for performance that is as good or better than legacy MPLS. Since mobile users run across the same backbone as all other resources, the remote access experience is no different from working at the office.

With Cato, customers can easily migrate from MPLS to SD-WAN, optimize global connectivity to on-premises and cloud applications, enable secure branch office Internet access everywhere, and seamlessly integrate cloud datacenters and mobile users into a high-speed network with a zero trust architecture. Whether its mergers and acquisitions, global expansion, rapid deployments, or cloud migration, with Cato, the network and your business are ready for whatever is next in your digital transformation journey.



Cato SASE. Ready for Whatever's Next.

Cato Cloud

Global Private Backbone

Edge SD-WAN

Security as a Service

Cloud Datacenter Integration

Cloud Application Acceleration

Secure Remote Access

Cato Management Application

Managed Services

Managed Threat Detection and Response (MDR)

Intelligent Last-Mile Management

Hands-Free Management

Site Deployment

ISO 27001 Certified

SOC2 Approved

GDPR Compliant