Single-vendor SASE
vs other SASE Alternatives

CATO NETWORKS

The primary goal of SASE is to set design guidelines for how networking and security capabilities, currently offered as stand-alone point solutions, should be built and consumed as a converged cloud service to achieve operational simplicity, reliability and flexibility.

Since Gartner first defined SASE in 2019, several networking and security vendors repositioned their existing offerings as SASE. **In this e-book we compare the Single-vendor SASE recommended by Gartner, with other SASE Alternatives.**

Digital transformation calls for a new IT architecture approach

We live in a digital world where users, applications and data are spread across multiple network environments such as physical locations and clouds. The traditional network boundaries have disappeared, leaving a myriad of smaller network perimeters, as small as a single user working from home. The traditional approach of deploying point solutions to connect and secure those networks has major limitations: increasing complexity and operational costs, lack of control and visibility, and growing risks associated with security inconsistencies and gaps.

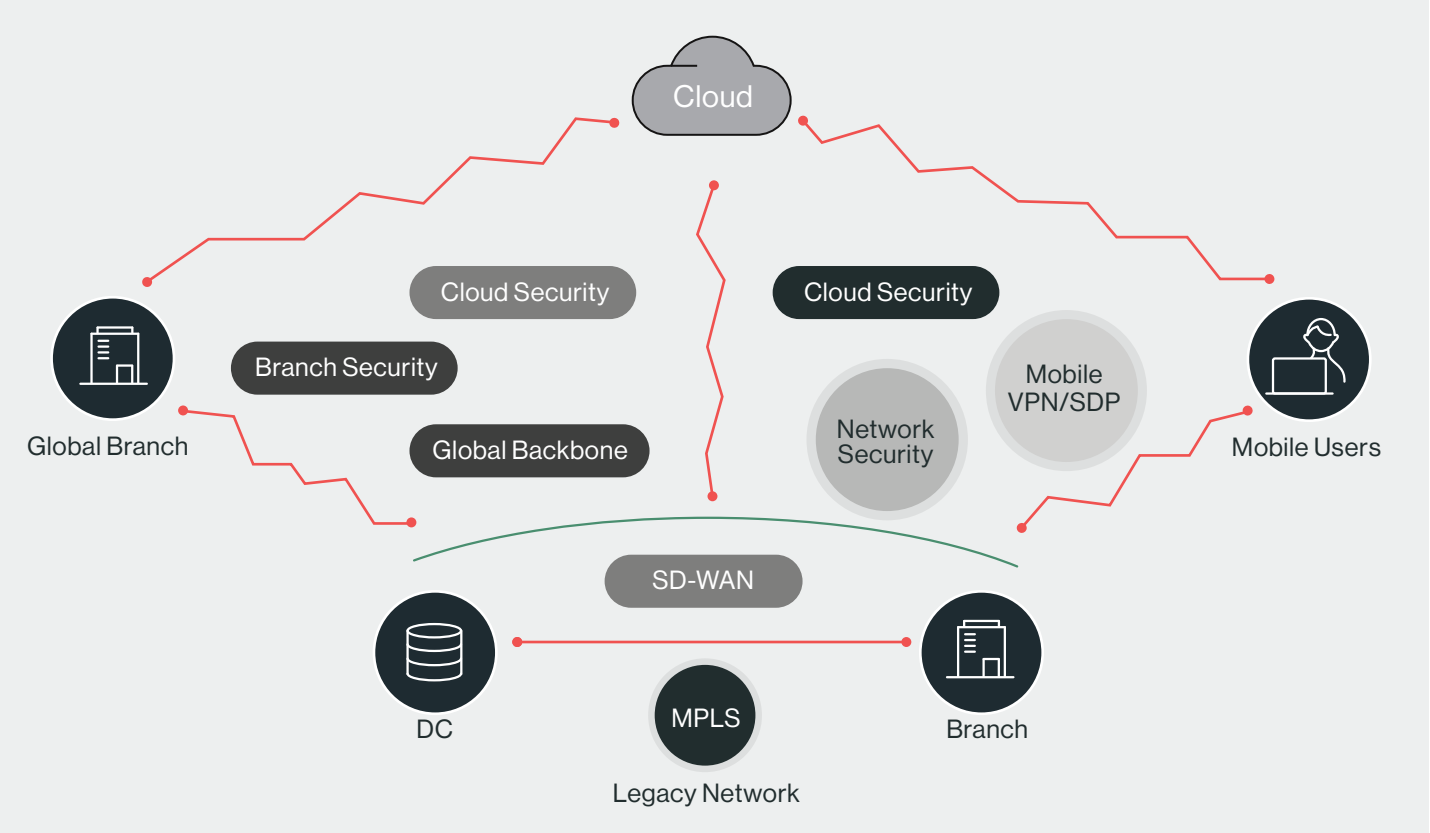


Figure 1. Multiple point solutions architecture to address the new multi-edge ecosystem

What's the solution? **SASE**

Back in 2019, Gartner defined the guidelines for a future-proof IT infrastructures in a report called "The future of Network Security is in the Cloud". These guidelines form the foundation of the Secure Access Service Edge or SASE framework. This is a new architectural approach that is built to address current and future requirements for optimal and secure application access, for all users and at any location.

The SASE definition is based on the following architectural requirements:

Converged
Networking and security capabilities must be converged into a single software that performs core operations like routing, inspection and enforcement in parallel. Context sharing amongst networking and security functions improves control and visibility.

Cloud-native
Delivered from the cloud, a SASE solution must be multi-tenant, and able to scale elastically to accommodate dynamic capacity requirements. This implies the use of a microservices software architecture and rules out solutions based on legacy appliances hosted as virtual machines in the cloud.

Identity-driven
Zero trust network access (ZTNA) must be enforced based on user identities, allowing granular access control to applications and data, and attack surface reduction.

Global
To support users, data and applications wherever they may be and without performance degradation, a SASE solution must be available all over the world through PoPs (Points of Presence) that are as close as possible to the enterprise users and applications.

Support all Edges
Branches, datacentres, clouds and remote users must all be equally served by the exact same software. This ensures a uniform security policy and optimal application performance. Chances for security gaps or misconfigurations are dramatically reduced.

Additionally, a well-architected SASE solution must be manageable via a single management application, simplifying administration, monitoring and troubleshooting.

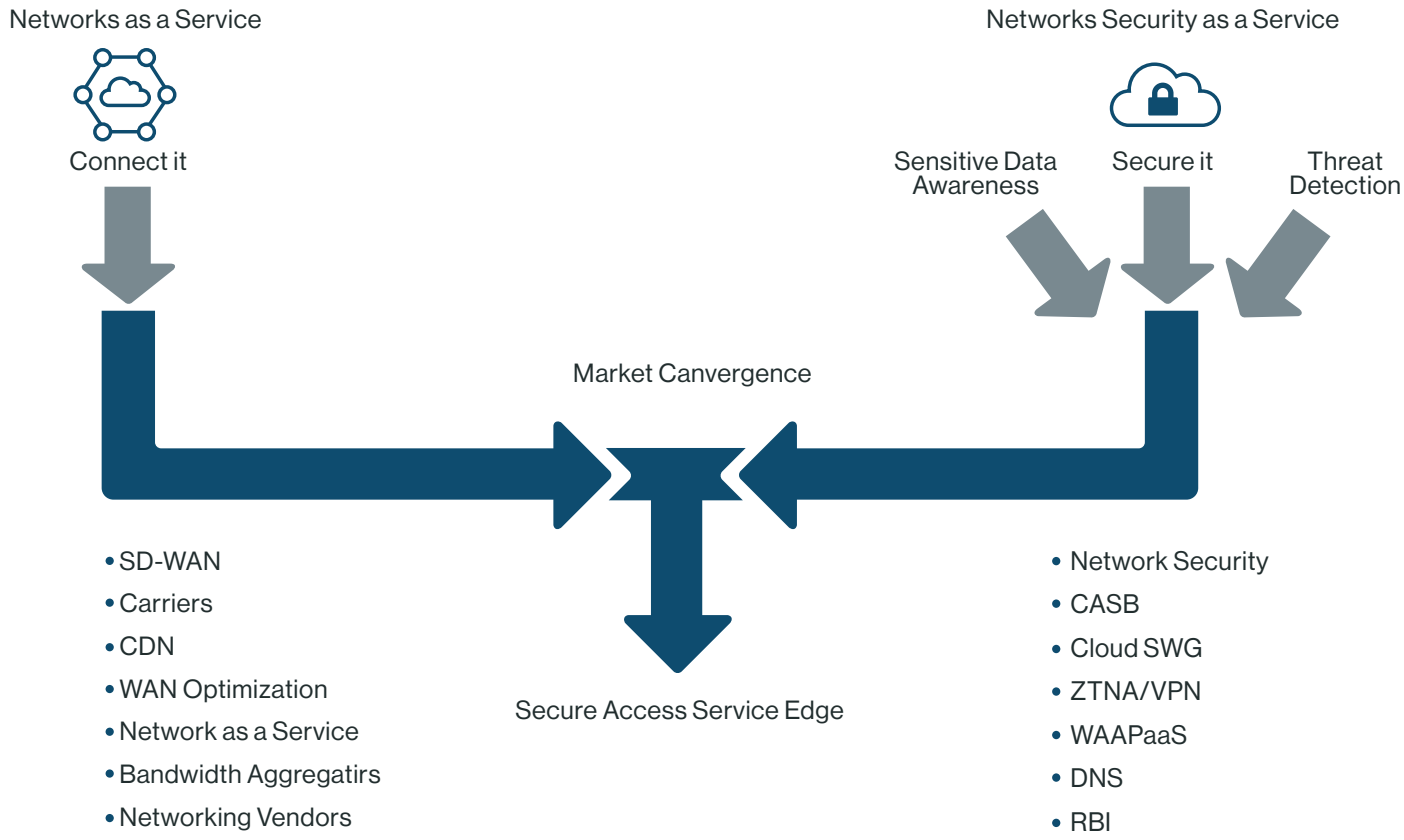


Figure 2- Gartner's SASE diagram showing the convergence of networking and security
CDN. content delivery network, RBI. remote browser isolation, WAAPaaS: web application and API protection as a service.
Source: Gaetner
ID: 441737

Common SASE architectures

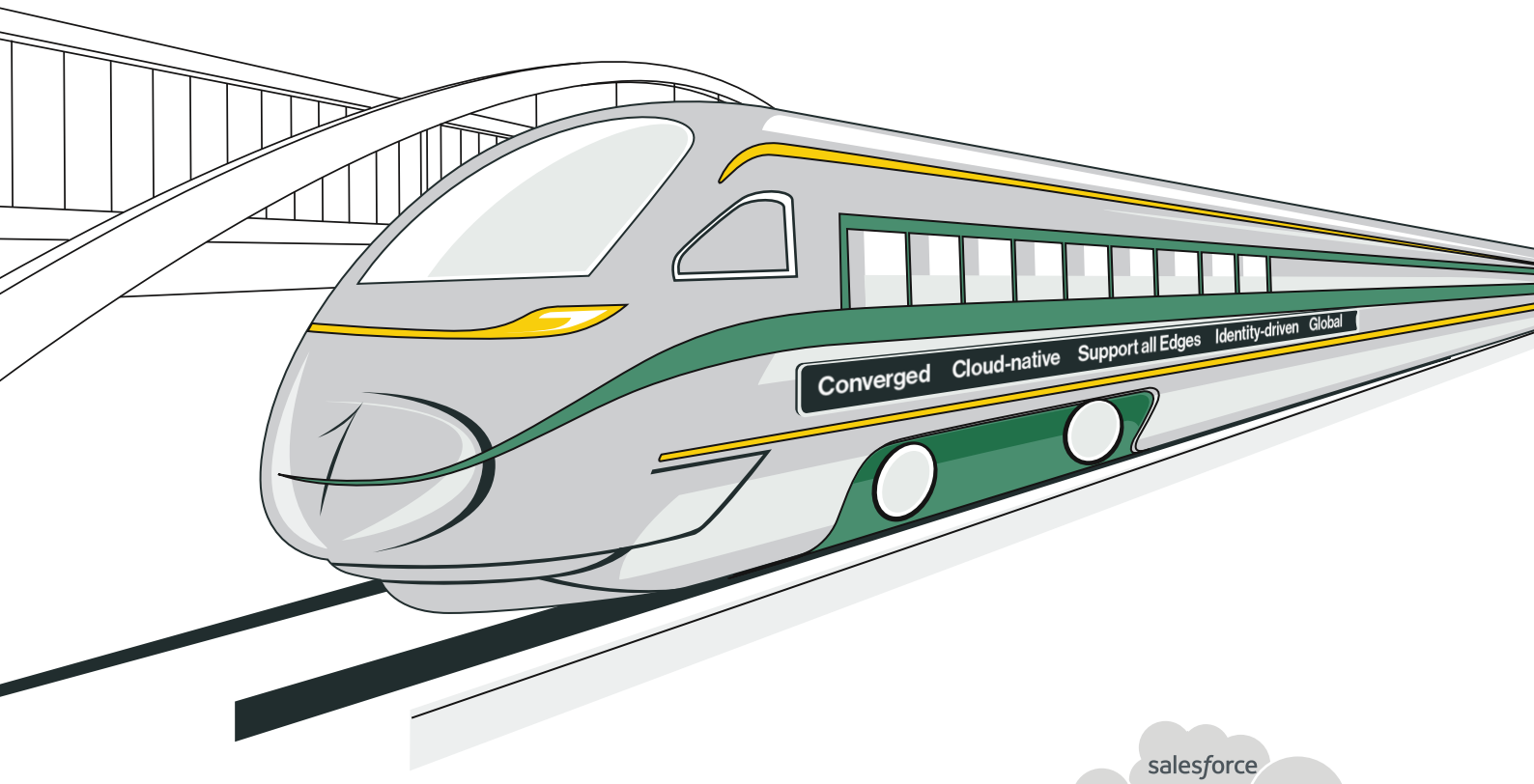
Since Gartner first defined SASE 4 years ago, there has been considerable momentum around SASE, with several networking and security vendors repositioning their existing offerings as SASE. Gartner's Market Guide for Single-Vendor SASE is attempting to clear some of the confusion. Beyond the recommendation to go for a "Single-vendor SASE" as much as possible, and tick all the 5 architectural requirements of SASE described above, Gartner mentions 2 other alternatives in the market that some vendors coin as SASE, but have a limited scope and capabilities:

- Multi -vendor SASE
- Portfolio-vendor SASE (or managed SASE)

Even though not mentioned by Gartner, we should also discuss an additional option, as we are seeing some legacy equipment vendors promoting their offerings to the market as "SASE". For lack of a better term, we will call it

- Appliance-based SASE

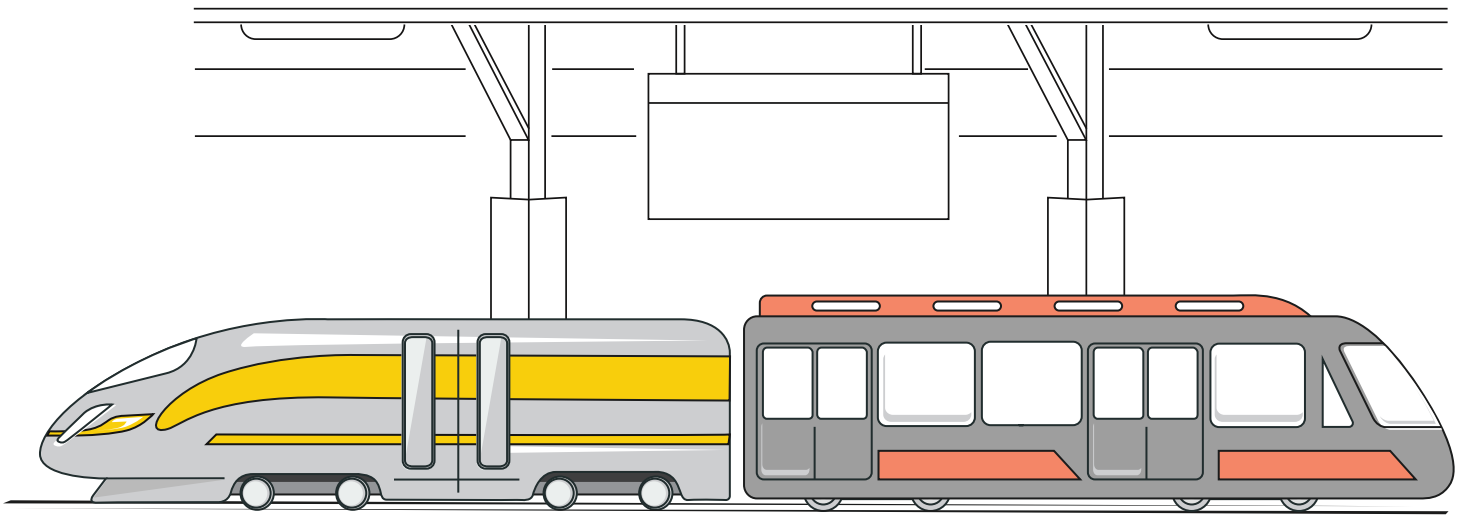
Let's look in more detail at the characteristics and architecture of each SASE architecture.



01 Single-vendor SASE

A single-vendor SASE provider converges network and security capabilities such as SD-WAN, SWG, CASB, FWaaS, ZTNA and more into one cloud-native offering. The solution is delivered as-a-Service and enables consolidation of point products, elimination of multiple appliances at the branch and consistent zero-trust security enforcement. Event data from all functions is stored in a single data lake, providing shared context which leads to better visibility and security efficacy. Administration, monitoring and troubleshooting are all done from a single management application for improved efficiency and compliance.

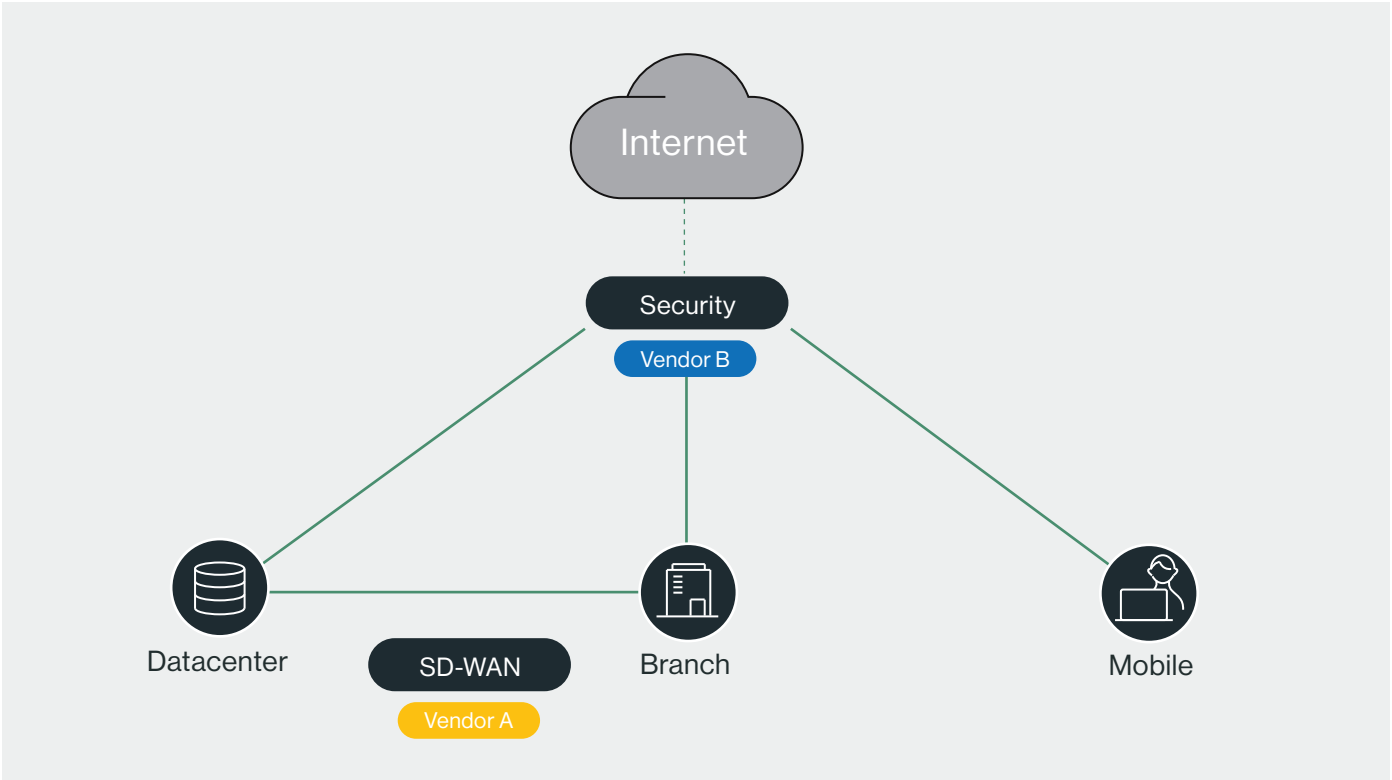
Figure 3. Single Vendor SASE architecture

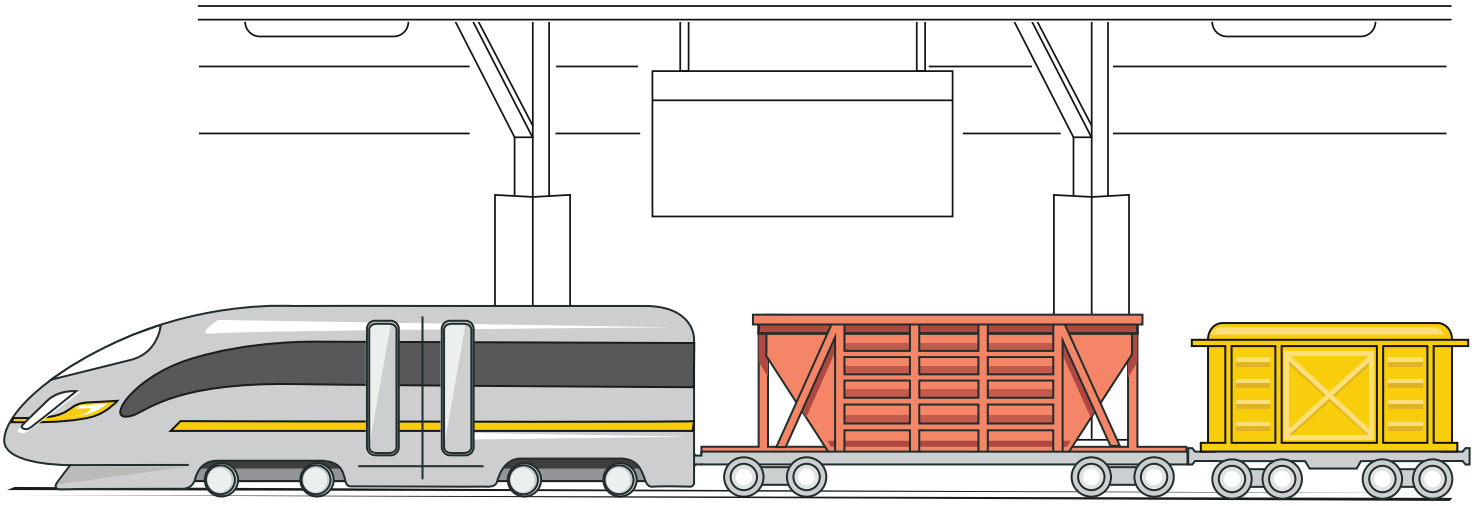


02 Multi-vendor SASE

A multi-vendor SASE is a where two distinct vendors are required to deliver all the functionalities of SASE. This approach, often built on a combination of a network-focused vendor and a security-focused vendor, has several implications for the enterprise. Integration work is required to make sure the vendors' solutions operate in harmony.

Log collection and correlation is required for full visibility. Importantly, multiple management applications are required for administration. Multi-vendor SASE can achieve similar functionality to single-vendor, but the increased complexity leads to degraded visibility, agility and flexibility.





03 Portfolio-vendor SASE (or managed SASE)

A portfolio-vendor SASE is a scenario where a vendor, typically a service provider, system integrator, or MSP is chosen to deliver the SASE functionality by integrating multiple point solutions. In some cases, the offering can include central management application that uses APIs to monitor and configure the underlying point products.

Even though this model offloads the end customer from the burden of integrating and managing multiple point products, it still presents the challenge of managing a complex and etherogenous SASE infrastructure.

MSPs opting to offer this architecture approach will have to deal with long lead times for change requests and support tickets, impacting agility and flexibility.

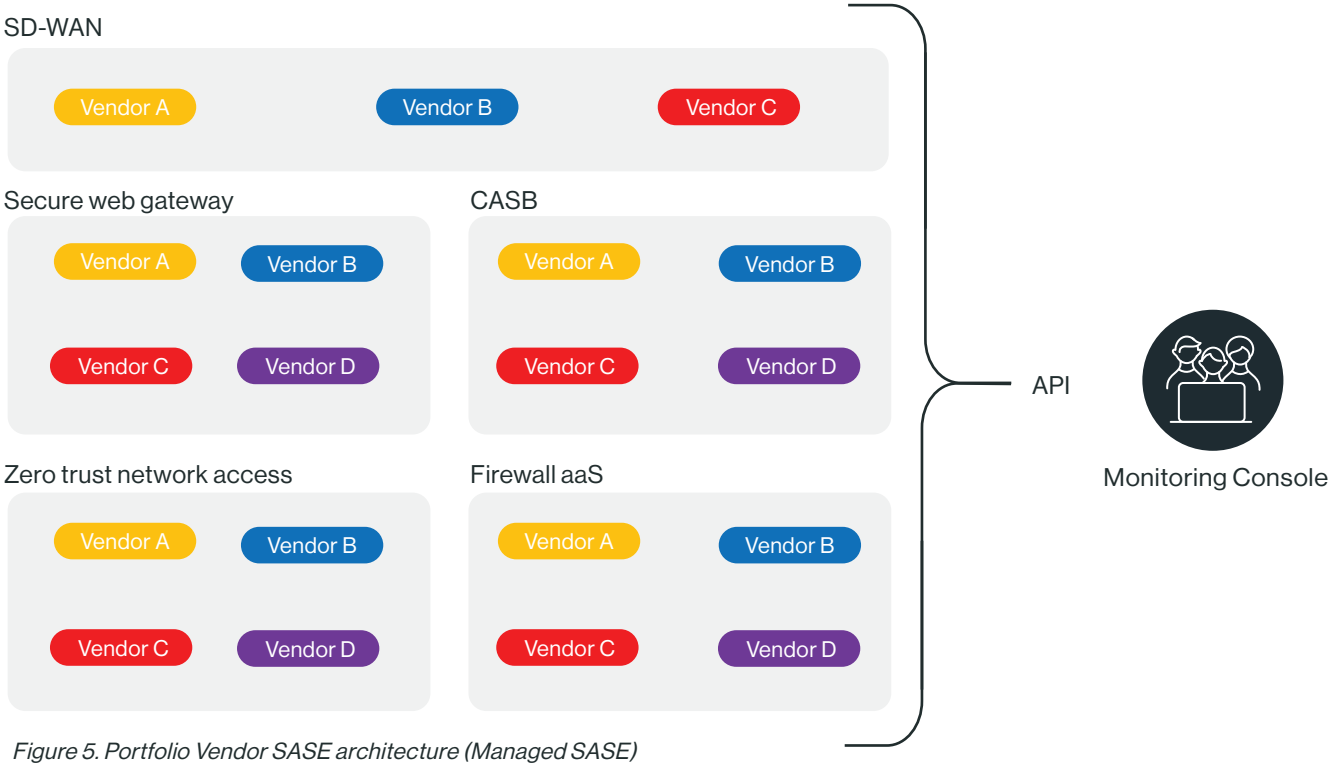
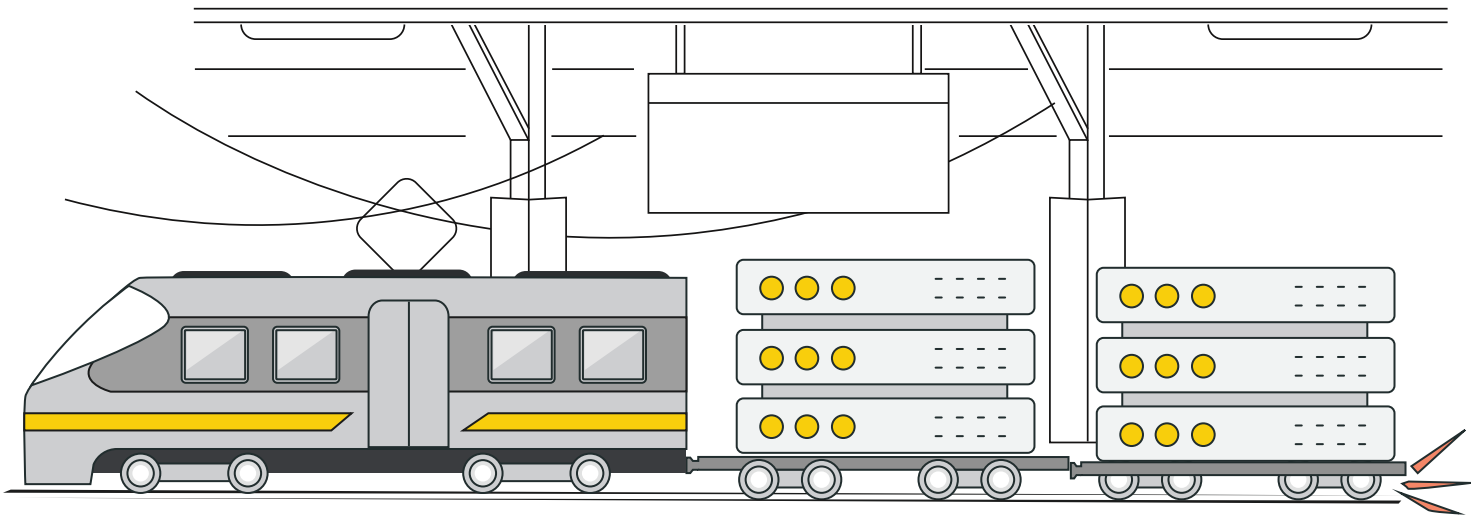
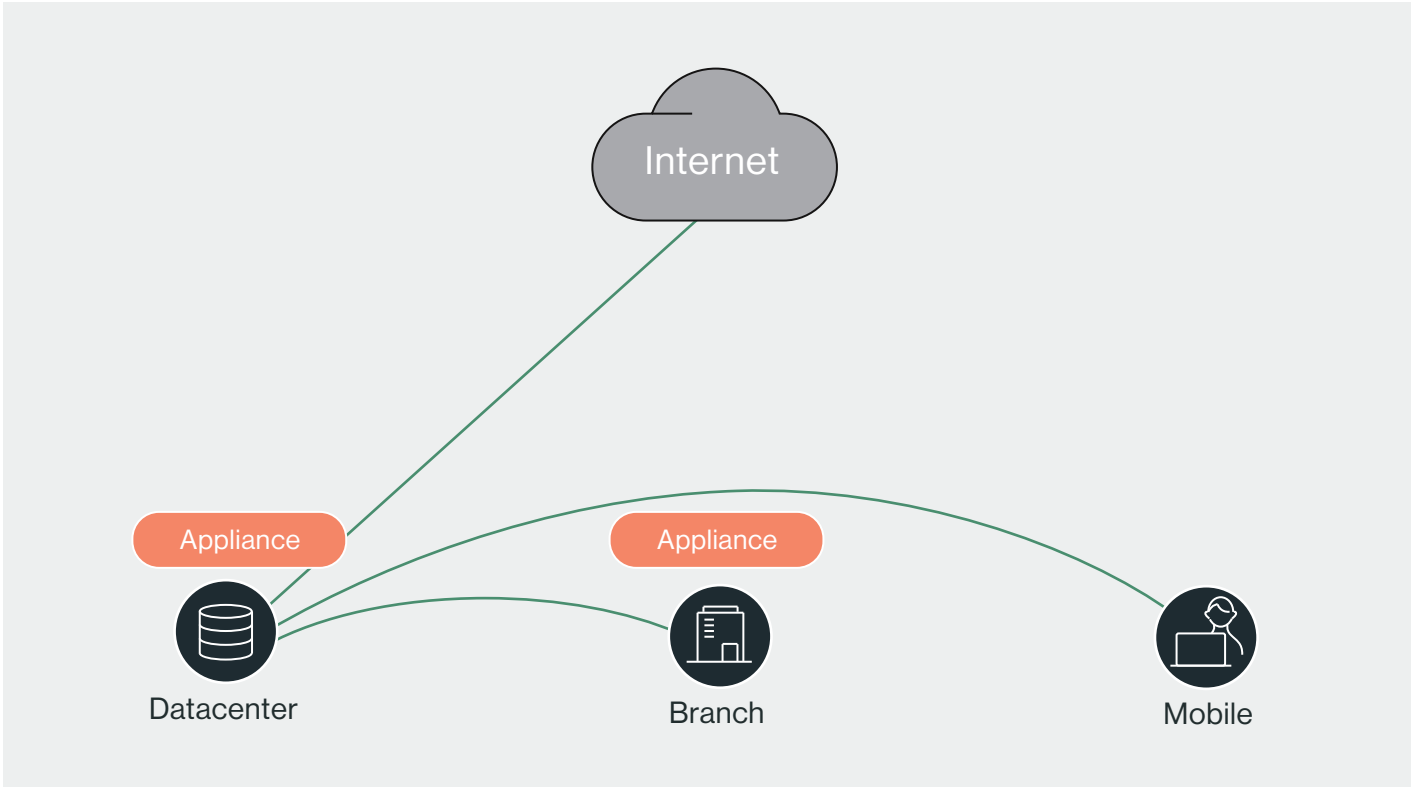


Figure 5. Portfolio Vendor SASE architecture (Managed SASE)



04 Appliance-based SASE

Appliance-based SASE is a misleading proposition, offered by vendors who cannot or haven't yet transitioned their legacy on-premise offering to be cloud-native. In such an architecture, remote users and remote branch traffic is typically backhauled to a central inspection and enforcement appliance, located on-premises or in a cloud data centre, before it is sent to its destination. While an appliance-based SASE solution may offer convergence of network and security capabilities, its physical nature and the need to detour network traffic, reduces flexibility, performance, operational efficiency and productivity.



CATO NETWORKS

Which SASE Option Is Best for My Enterprise?

In a fragmented market, choosing a SASE architecture that best fits the organization's digital transformation needs can be challenging. Mapping the various SASE options against Gartner's original requirements will help.

Requirement	Single-vendor	Multi-vendor	Portfolio-vendor	Appliance-based
Converged	+	-	-	+
Identity-driven	+	Partial	Partial	+
Cloud-native	+	Partial	Partial	-
Global	+	Partial	-	-
All-edges	+	+	+	+

For example

In multi-vendor SASE, identity awareness, global availability and cloud-native architecture are applicable to the cloud security capabilities only. They are absent from the networking components. This leads to reduced control, visibility and availability. A portfolio vendor will suffer from the same limitations, but often also lacks global capabilities.

Multi-vendor, portfolio-vendor and appliance-based options have existed for many years, in various forms. Digital transformation, the rise of remote working and the dissolving network perimeter have made them unfit for the modern enterprise.

Organizations of all sizes are looking to simplify their infrastructure and operations to become more agile and react quickly to new IT requirements and sophisticated cyber threats.
A Single-vendor SASE provides the most reliable path to building this infrastructure:

- **Convergence** eliminates complex integration and troubleshooting work.
- **An identity-driven** approach increases security and compliance
- **A cloud-native** architecture ensures support for future growth
- and **global availability** enhances productivity and supports worldwide operations and expansion.
- Lastly, **support for all edges** enhances both security and efficiency by using one platform and one policy engine for all parts of the enterprise.

This demand, and the rising adoption of single-vendor SASE, is clearly echoed in Gartner's recent research:

By 2025, one-third of new SASE deployments will be based on a single-vendor SASE offering, up from 10% in 2022.

By 2025, 80%

of enterprises will have adopted a strategy to unify web, cloud services and private application access using a SASE/SSE architecture, up from 20% in 2021.

By 2025, 65%

of enterprises will have consolidated individual SASE components into one or two explicitly partnered SASE vendors, up from 15% in 2021.

By 2025, 50%

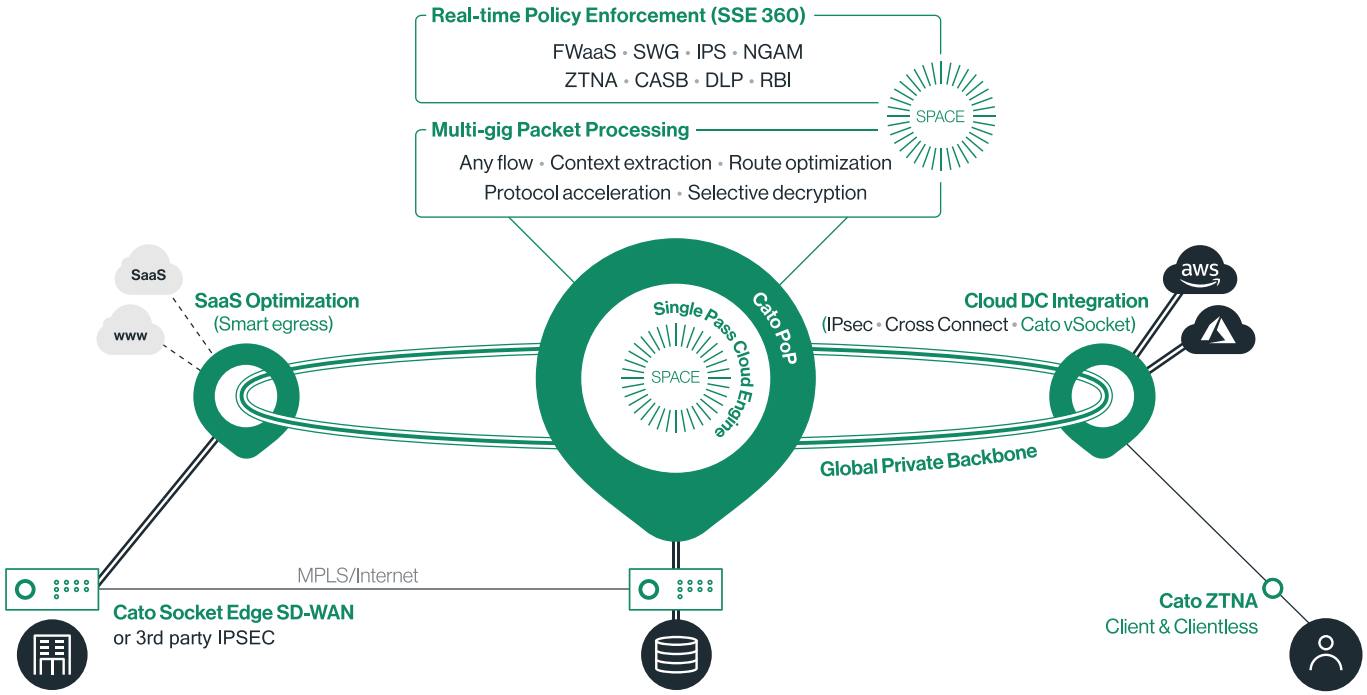
of new SD-WAN purchases will be part of a single-vendor SASE offering, up from 10% in 2022.

Almost all enterprises worldwide face similar challenges. They are all looking to improve network security, increase agility and flexibility and enhance efficiency and productivity. A single-vendor SASE is perfectly suited to deliver those objectives.

Ready for Whatever's Next.

SASE, SSE, ZTNA, SD-WAN: Your journey, your way.

Cato pioneered the convergence of networking and security into the cloud. Aligned with Gartner's Secure Access Service Edge (SASE) and Security Service Edge (SSE) frameworks, Cato's vision is to deliver a next generation secure network architecture that eliminates the complexity, costs, and risks associated with legacy IT approaches based on disjointed point solutions. With Cato, organizations securely and optimally connect any user to any application anywhere on the globe. Our cloud-native architecture enables Cato to rapidly deploy new capabilities and maintain optimum security posture, without any effort from the IT teams. With Cato, your IT organization and your business are ready for whatever comes next.



For more details please contact us