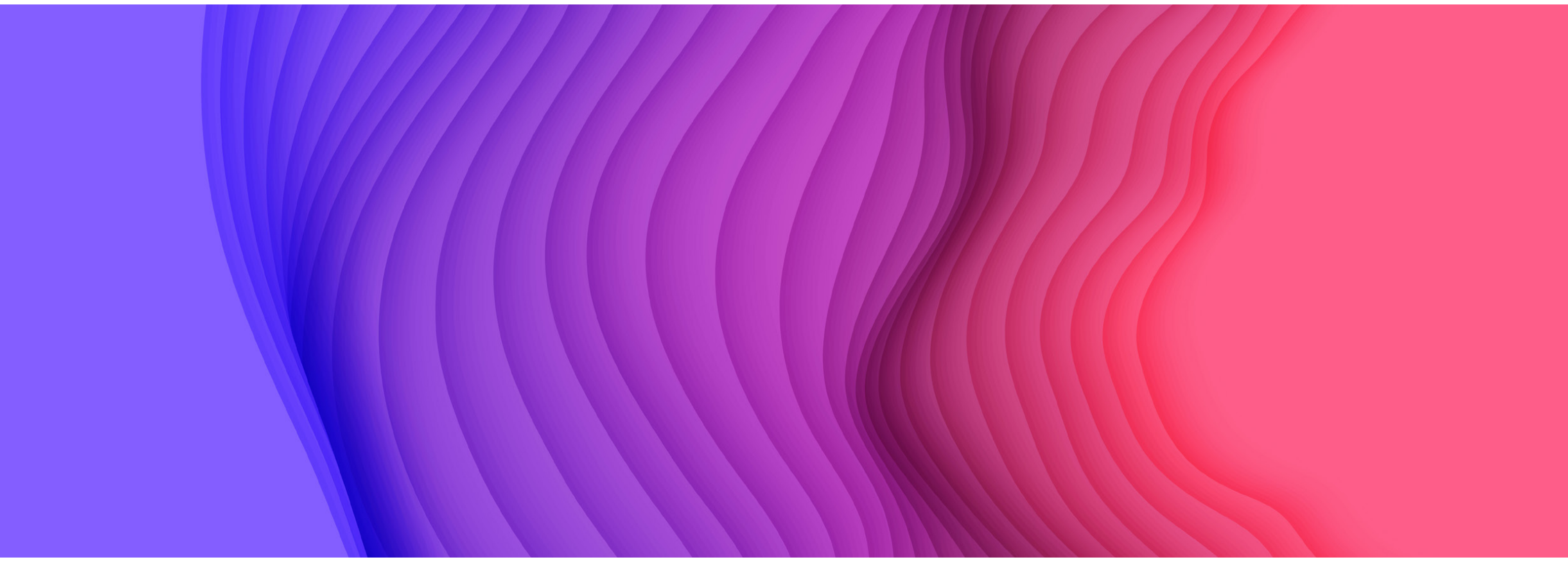
An introductory guide to unified SASE

For a simpler, more cost-effective journey to SASE



51%

of global knowledge workers will be full-time remote by the end of 2021," increasing the demand for SASE solutions.[1]

In the next 12 months,

46%

of organizations will have deployed a SASE architecture.[2]

65%

of enterprises will have consolidated individual SASE components into one or two explicitly partnered SASE vendors by 2025.[3]

The rise of unified SASE: A simpler, more cost-effective journey to SASE

Over the last year, many IT leaders have embraced a Secure Access Service Edge (SASE) framework to enable faster and more secure connectivity across their global organizations. SASE converges the functions of network and security solutions into a single, cloud-native service that delivers consistent connectivity and security from everywhere.

SASE is not just a technology trend; it is a strategic imperative for modern businesses looking to thrive in the digital era.

However, not all SASE solutions are created equal. Some SASE providers offer multiple point solutions that are loosely integrated or require routing between different vendors' PoPs, which can introduce latency, performance issues, and management overhead.

Then there are SASE solutions that deliver all the core capabilities of SASE from a single, tightly integrated platform—improving security posture, staff efficacy, user and admin experiences, and cost efficiency.

This is what we call unified SASE. And for a simpler, more cost-effective journey to SASE, it's the way to go.

In this guide, you will learn everything you need to know about unified SASE, including:

- What is unified SASE?
- The benefits of single-vendor SASE for the modern business
- A powerful unified SASE with HPE Aruba Networking
- Starting your SASE journey

By the end of this guide, you will have a clear understanding of how unified SASE can help you achieve your security goals faster and more effectively.

[1] Gartner Press Room, June 2021

[2] 2023 Ponemon Institute report

[3] Gartner Blog, December 2022

The driving forces behind SASE adoption

First things first, why adopt SASE at all? The answer can be summarized in 3 simple statements:

1. **Security** that was once effective, now isn't.

2. **Networks** that were once manageable, now aren't.

3. **Solutions** that once worked well, now don't.

The traditional network and security architectures that relied primarily on perimeter-based secure connectivity no longer meet the needs of the modern business environment. The rapid adoption of cloud services, mobile devices, IoT, OT, and remote/hybrid work has created a distributed and dynamic workforce that needs secure and reliable access to applications and data anywhere, anytime, and on any device.

However, while business needs have evolved, leveraging traditional network security solutions exposes organizations to new connectivity challenges and risks, such as:

- **Increased attack surface and complexity:** With more users, devices, locations, and cloud services to protect, the organization must deal with more potential entry points for attackers and more security tools to manage and update. Not to mention each entry point (i.e., user or device) has direct access to the corporate network, further increasing risk.

- **Poor user experience and decreased productivity:** With more traffic being backhauled through the VPN and the corporate network, users experience increased latency, jitter, packet loss, and bandwidth limitations that affect their performance and productivity, not to mention satisfaction.

- **High operational costs and inefficiencies:** With the proliferation of both network and security solutions to deploy, maintain, update, and troubleshoot, the organization must spend more resources and time on managing the infrastructure and resolving issues.

Addressing these challenges and risks may feel overwhelming. However, by working together, networking and security leaders can banish these issues by utilizing a SASE framework.

What is SASE?

Secure Access Service Edge, or SASE, is a cybersecurity concept that was first introduced by Gartner® in 2019. According to Gartner, SASE is an IT framework that combines networking and security functions into a single platform that securely connects all users, devices, and applications across the globally distributed workforce.

SASE is made up of two "technology sets" including WAN Edge Services (SD-WAN) and Security Service Edge (ZTNA, SWG, CASB, and DEM) which together enable network and security teams alike to enable any user, device, or server to securely connect from anywhere over any transport method. Leveraging a vast SD-WAN fabric and cloud-delivered SSE with a global network of PoPs allows fast edge-to-cloud access, which reduces latency and improves performance.

The elements of SASE

There are two core technology sets that make up a unified, single-vendor SASE offering:

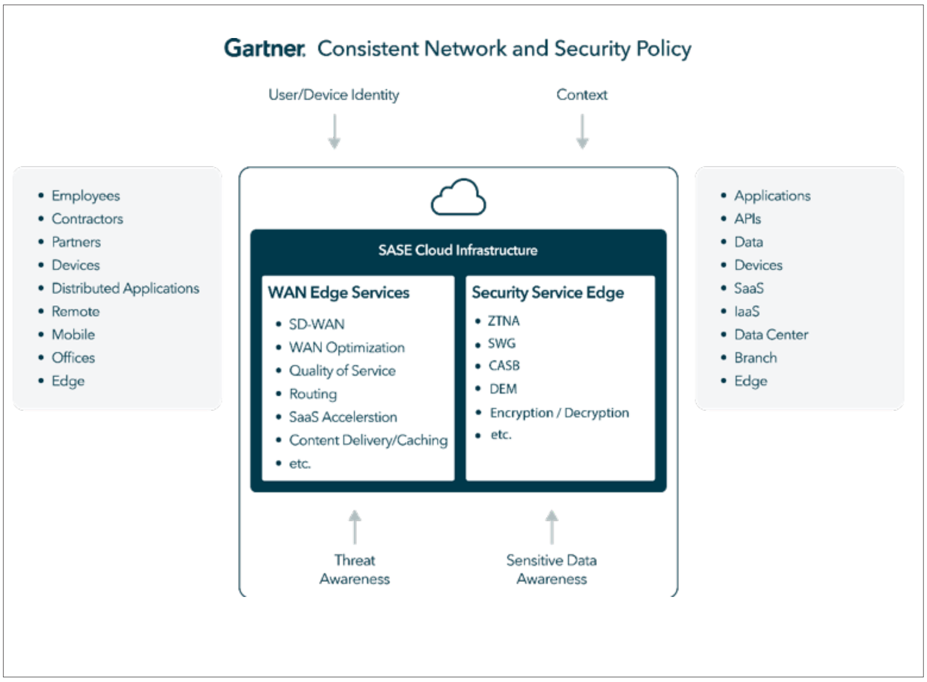


Figure 1. Components of a unified, single-vendor SASE offering

WAN Edge services (Secure SD-WAN)

- **Security:** Secure SD-WANs include next-generation firewall capabilities, including IDS/IPS and granular segmentation—enabling organizations to replace branch firewalls and secure IoT devices. Additionally, all connections are encrypted over the SD-WAN fabric.
- **Multicloud networking:** Virtual instances of SD-WAN solutions can be deployed in cloud service providers such as AWS, MS Azure, and Google Cloud—establishing a resilient connection from the branch office to the cloud. SD-WAN also intelligently steers application traffic to the cloud to avoid backhauling traffic to the data center, and dynamically adapts to changes in traffic patterns.
- **Dynamic path control:** SD-WAN combines multiple transport links including MPLS, broadband internet, 4G/5G, or satellite links. It dynamically selects the best links based on network conditions and business intent.
- **Path conditioning:** SD-WAN solutions also use techniques such as Path Conditioning to overcome the adverse effects of dropped and out-of-order packets that are common with broadband internet and MPLS connections. This provides a private-line-like performance over internet links, enabling organizations to reduce MPLS dependency and quickly spin up new branches.
- **Dynamic path control:** This feature accelerates the transmission of data over the WAN by applying TCP protocol acceleration as well as data deduplication and compression algorithms.
- **Centralized orchestration:** Business and security policies are centrally managed from a single interface. This simplifies network operations and troubleshooting, as administrators can make changes and apply policies from a central location.

Security service edge (SSE)

Zero Trust network access (ZTNA) | Secure access to private applications

- ZTNA technology provides granular, identity-based Zero Trust access to private applications and resources, regardless of where they are hosted or where the users are located. Modern ZTNA solutions allow teams to fully eliminate remote access VPNs for employees and third-party users, significantly reducing the attack surface by allowing access to specific authorized private applications without extending access to the underlying network.

Secure web gateway (SWG) | Secure access to the Internet

- SWG protects the distributed business against advanced attacks with capabilities like web filtering, SSL inspection, and malware detection and prevention. SWG ensures that authorized users get fast, secure access to Internet resources while protecting the business from harm.

Cloud access security broker (CASB) | Secure access to SaaS applications

- CASB allows IT to identify, manage, and control the use of cloud services. A CASB service mediates connections between users and cloud-based SaaS applications and helps regulate data flow, prevents data loss, and uncovers shadow IT to ensure sensitive data remains protected.

Digital experience monitoring (DEM) | Enhanced digital experience & productivity

- DEM gives enhanced, in-line visibility and analysis into the interactions, experience, and performance of devices, applications, and networks. DEM helps IT teams better utilize their time by accelerating troubleshooting, allowing for pinpoint diagnostics of experience issues.

What is unified SASE?

Unified SASE combines the two technology sets—SD-WAN and SSE—into a single-vendor solution that allows businesses to achieve even greater simplicity, operational efficiencies, and cost savings. A unified approach also allows greater agility and faster deployment, increasing your time-to-value. Gartner predicts that by 2025, 50% of SD-WAN purchases will be part of a single-vendor SASE offering, up from less than 10% in 2021.

The benefits of single-vendor SASE for the modern business

Unified SASE offers organizations the many benefits of SASE, while making adoption simpler and more cost-effective. It does this by:

- **Unifying and improving security posture:** Unified SASE reduces the attack surface and improves threat detection and response times by applying universal security policies and centralized access controls across all traffic and locations.
- **Improving efficiency in networking and security teams:** Having a single-vendor SASE not only brings consolidation, but it also unifies networking and security functions. This alleviates roadblocks between teams and minimizes complexities and cost, while optimizing cross-functional collaboration and implementation. Network and security operations are streamlined by providing a centralized management system for visibility, configuration, monitoring and troubleshooting.
- **Offering a better user and admin experience:** Unified SASE allows teams to guarantee high-performance, low-latency connectivity for users to apps by auto-routing traffic via the fastest access paths and avoiding backhauling traffic to the data center. End-users receive an optimized access experience while admins gain simple yet granular access controls applied through universal Zero Trust policies.
- **Reducing costs and increasing flexibility:** SASE lowers capital expenditure (CapEx) and operational expenditure (OpEx) by eliminating the need for multiple point solutions and hardware appliances. Unified SASE is also highly scalable, quickly adapting to changing business needs, and provides multiple points of presence for geographically distributed organizations.

How to start deploying unified SASE

Deploying a single-vendor SASE solution may seem daunting, but it does not have to be. With the right partner and a clear roadmap, organizations can transition to SASE smoothly and securely, without disrupting their existing operations or compromising their performance.

There are five basic steps that most successful SASE deployments follow:

- **Step 1: Define your SASE goals and requirements.** Identify your business goals, use cases, and SASE requirements. Assess your current network and security architecture. Find the gaps, challenges, and existing resources.
- **Step 2: Choose a single-vendor SASE provider.** Compare different providers based on their capabilities, coverage, performance, scalability, reliability, support, and pricing. Look for a well-architected single-vendor SASE solution that is integrated, unified, flexible, and easy to use.
- **Step 3: Design and develop your SASE game plan.** Work with your provider to define your network topology, security policies, user groups, application profiles, and connectivity options based on best practices. This should be a collaborative process with your SASE provider to ensure the greatest success for your business.
- **Step 4: Begin SASE deployment with a phased approach.** Deploy the necessary components such as agents, connectors, SD-WAN devices or private PoPs through a centralized management console. Migrate your users, devices, locations, and applications to your SASE solution in a phased or batched approach. SASE can work in tandem with existing solutions, allowing deployment to be as quick or slow as your team needs.
- **Step 5: Leverage SASE to the fullest.** As deployment continues, use the tools and dashboards from your provider to gain visibility, insights, and feedback to further optimize your SASE solution. Get the most out of your investment and discover new use cases and functionality where SASE can further benefit your business.

A powerful unified SASE with HPE Aruba Networking

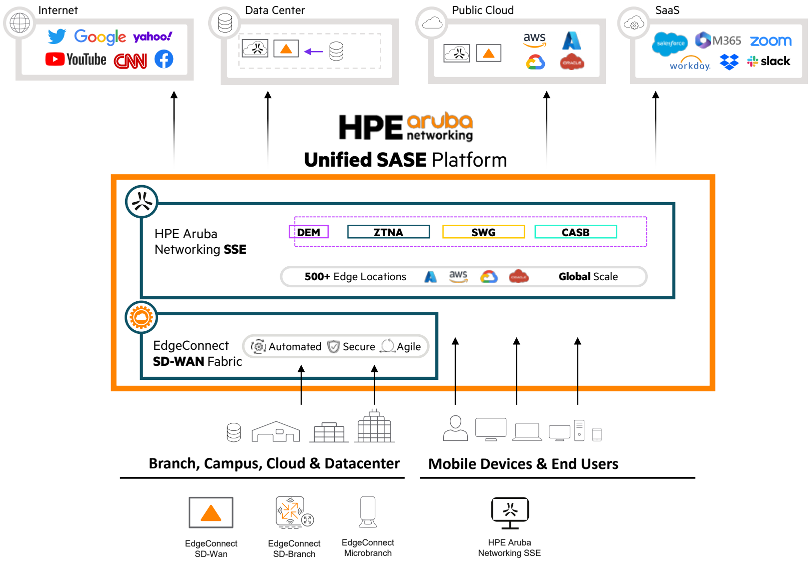


Figure 3. HPE Aruba Networking unified SASE platform

If you are looking for a powerful single-vendor SASE solution that delivers secure and reliable business access from anywhere, HPE Aruba Networking SASE may be your answer. With its industry-leading SD-WAN and award-winning SSE, HPE Aruba Networking offers a comprehensive, unified approach to SASE designed for today's distributed and dynamic enterprise.

With the increasing demands for integration between networking and security solutions, HPE Aruba Networking helps IT teams consolidate, simplify, and secure their business connectivity. With HPE Aruba Networking, IT teams can deliver WAN and cloud security controls directly to the application at the network edge with HPE Aruba Networking EdgeConnect SD-WAN—rather than routing data through the data center—while SSE ensures that Zero Trust security controls can be applied to all people and devices, no matter where they connect—on campus, in branch, at home, or on the road.

Starting your SASE journey

"In the next 12 months, 46% of organizations will have deployed a SASE architecture."

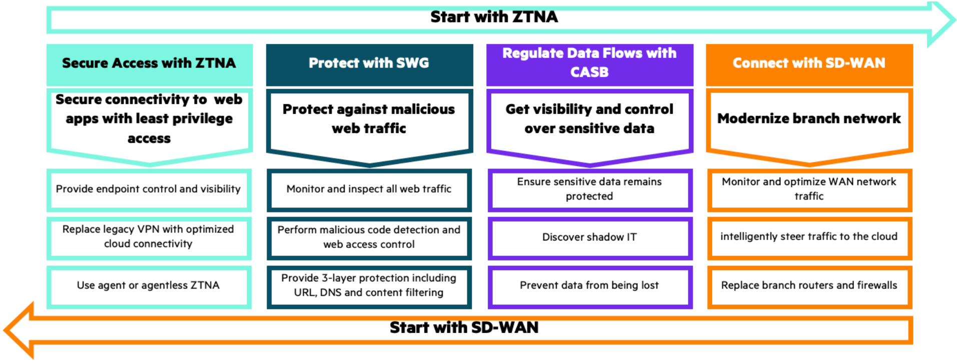
- 2023 Ponemon Institute Report[4]

SASE is not just a passing technology trend; it is a strategic imperative for modern businesses looking to thrive in the digital era. SASE can help organizations overcome the challenges and risks of network and security architectures focused primarily on network control, and achieve better security posture, user experience, operational efficiency, and cost savings.

And with unified SASE, delivered by a single-vendor SASE provider that meets your goals and requirements, you can get there even faster.

If unified SASE sounds like a good fit for your organization, there is one question remaining: Where do you want to start your implementation? Here are the two most common paths organizations take.

[4] 2023 Ponemon Institute report



Start with ZTNA

Secure Access with ZTNA	Protect with SWG	Regulate Data Flows with CASB	Connect with SD-WAN
Secure connectivity to web apps with least privilege access	Protect against malicious web traffic	Get visibility and control over sensitive data	Modernize branch network
Provide endpoint control and visibility	Monitor and inspect all web traffic	Ensure sensitive data remains protected	Monitor and optimize WAN network traffic
Replace legacy VPN with optimized cloud connectivity	Perform malicious code detection and web access control	Discover shadow IT	intelligently steer traffic to the cloud
Use agent or agentless ZTNA	Provide 3-layer protection including URL, DNS and content filtering	Prevent data from being lost	Replace branch routers and firewalls

Start with SD-WAN

Path 1: Start with SSE (specifically ZTNA)

The 2023 SSE Adoption report found that 67% of businesses plan to begin their SASE journey with SSE technology. If this sounds like you, consider replacing VPN with HPE Aruba Networking ZTNA to provide Zero Trust access to your private applications, whether that be in the data center, cloud, or anywhere in between.

Learn more about HPE Aruba Networking SSE

Path 2: Start with SD-WAN

Begin your SASE journey by embarking on SD-WAN. Complete your secure edge portfolio—small office/home office, branch, campus, or WAN—with a single SD-WAN fabric powered by HPE Aruba Networking EdgeConnect.

Learn more about HPE Aruba Networking EdgeConnect

Chat with an expert at arubanetworks.com/company/contact-us/contact-us-form

Make the right purchase decision.
Contact our presales specialists.

✉ **Contact us**

DICKER DATA

HPE aruba networking