5 steps to accelerate your SASE adoption and improve your security posture

Introduction: Why are so many of today's organizations embracing SASE?

In the last few years, organizations have had to quickly embrace new technologies and methods of operation as they feel the pressure to accelerate multi-cloud adoption, increase the speed of digital transformation, and accommodate the needs of an expanding hybrid workforce. Legacy security and networking solutions are unable to keep up with these growing trends as they are expensive to scale out, complex to manage, and force traffic backhauling for access to corporate services, straining budgets and hampering performance.

Furthermore, organizations are battling a growing influx of ransomware attacks, as cybercriminals continue to develop new ways to infiltrate networks and data centers, in order to manipulate and even steal data. As many as 75% of the ransomware attacks and breaches examined by Unit 42's incident response team resulted from attack surface exposures, up from just 40% one year before.[2] Effectively mitigating these risks requires a shift in your network security approach and a new plan of action.

IT security leaders are now looking to modernize their network security infrastructure and deploy effective security and networking technologies to protect vital enterprise resources – no matter where they are accessed from – as companies adopt flexible hybrid workplace models.

IT leaders are increasingly viewing Secure Access Service Edge (SASE) as the de-facto integrated networking security framework that addresses their requirements. In fact, the Gartner ® Forecast Analysis: Secure Access Service Edge, Worldwide indicates that over the next four years, the SASE market will grow at a CAGR of 32%, reaching almost $15 billion by 2025.[3]

Where are you on your journey towards SASE?

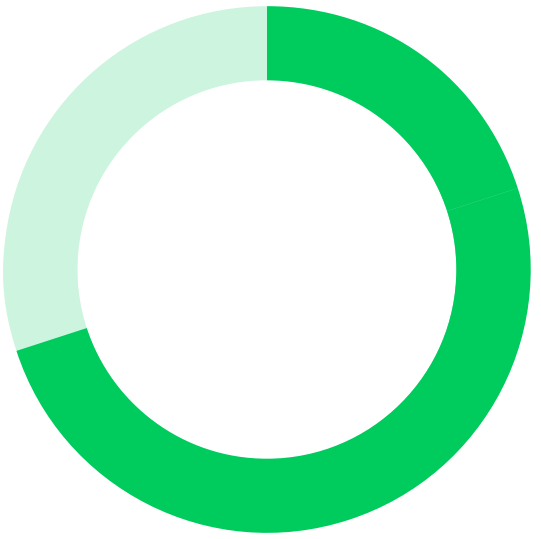
A SASE implementation can't be accomplished overnight. It is a major technology transformation project, and one that requires forethought, advance planning, and the right strategic approach. Organizations that are in the early stages of considering SASE will want to begin by assessing the factors that are driving them towards SASE adoption, then identify their needs and find an experienced, knowledgeable, and trusted partner that can manage the solution for them to help them achieve their goals.

1. Zippia, "30 Essential Hybrid Work Statistics [2023]: Hybrid Work Model, Data, and Productivity." Zippia.com. June 15, 2023
2. Unit 42/Palo Alto Networks, 2024 Incident Response Report.
3. Gartner Research, The Market Guide for Single-Vendor SASE, 2023.

GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.

What is SASE?

SASE uniquely combines a comprehensive set of networking and security capabilities into a single converged platform with a unified console, policies, and data lake. According to Gartner, “Single-vendor SASE offerings deliver multiple converged network and security as-a-service capabilities — such as software-defined WAN (SD-WAN), secure web gateway (SWG), cloud access security broker (CASB), network firewalling, and zero trust network access (ZTNA) — using a cloud-centric architecture.”



63%

of high-growth companies now adhere to a **“productivity anywhere”** model.[1]

[1] Zippia, “30 Essential Hybrid Work Statistics [2023]: Hybrid Work Model, Data, and Productivity.” Zippia.com. June 15, 2023

[2] Unit 42/Palo Alto Networks, 2024 Incident Response Report.

[3] Gartner Research, The Market Guide for Single-Vendor SASE, 2023.

GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.

Step 1:

Assess how your IT objectives and shifting user requirements are impacting your network and security strategy.

There are multiple drivers that typically motivate enterprises to consider a SASE approach to networking and security. Which of the following seven factors are important for your organization? Be sure to involve relevant IT, security, and business stakeholders in this discussion.

#1: Cloud maturity

How far along is your organization on its journey to the cloud?

Because it combines security and networking functions into a single, cloud-delivered service, SASE is an excellent fit for cloud-first companies. SASE eliminates the need to backhaul cloud traffic to the on-premises data center, resulting in reduced latency and improved application performance. SASE builds upon SD-WAN's more agile functionalities. Because it's cloud-hosted and globally available, it can automatically route traffic – including remote users' traffic – according to the organization's policies. This means it's well-suited for connecting users to cloud resources while uniformly and effectively enforcing consistent security. Plus, SASE incorporates cloud-first security capabilities that were purpose-built for safeguarding today's cloud-first computing ecosystems, including ZTNA, SWG, CASB and FWaaS.

#2: Digital transformation

How much progress have you made modernizing your security technology?

SASE makes it possible to deliver cloud-based security services like threat prevention, web filtering, sandboxing, DNS security, credential theft prevention, data loss prevention, and next-generation firewall capabilities – all from a single, centralized platform. These are core capabilities that enterprises need to protect their digital ecosystems from today's advanced threats. The need to update your approach to security will only grow more pressing as your digital strategies advance.

#3: Workplace flexibility

How many of your employees work from home or at other remote locations?

Remote – and especially hybrid – work has become the model of choice for millions of employees and organizations around the globe. Ensuring privacy and security while supporting regionally- or globally-distributed workforces requires a new way of thinking about network security. While the first ZTNA solutions did not provide content inspection and required users to authenticate through a gateway before being granted network access, ZTNA 2.0 capabilities (which are what today's leading SASE solutions incorporate) can accurately identify users, devices, and applications – no matter where they're connecting from. This simplifies policy creation, management, and enforcement, and removes the need to connect to a gateway.

#4: Operational efficiency

Is improving operational efficiency a top priority for your IT and/or security teams?

Because SASE consolidates capabilities into a single, cloud-delivered service that once belonged to two different functions (security and networking), it is inherently more efficient than legacy solutions. In addition, the cloud-delivered service model that SASE makes use of allows you to instantly add capacity – across branches, new locations, or additional remote users – as your business grows.

If you select a SASE solution that includes natively-integrated AIOps, IT teams can leverage AI-based problem detection and predictive analytics to automate complex manual processes, increasing productivity and reducing mean time to resolution (MTTR) for better end-users experiences.

And if you choose a provider that offers managed SASE services alongside a flexible Network as a Service (NaaS) model, you'll enjoy benefits like scalability, automation, performance andcontrol – all of which help keep employees happy and productive.

#5: Reduced complexity

Do you manage a multi-vendor security technology stack? Are your teams challenged to support multiple geographic regions or branch locations?

SASE solutions make centralized policy enforcement and control possible, all from a single dashboard. This way, administrators can manage multiple security and networking controls in one place, adding efficiencies and simplicity.

With a single-vendor SASE approach, deployment is faster, services are more efficient to manage, and integrations are streamlined. Both network and security teams will enjoy better administrative experiences, while end-users will experience less latency.

If you choose an end-to-end managed SASE solution, you'll have visibility across your entire IT environment for improved reliability and performance. Additionally, you won't need to manage different vendors, siloed technology solutions, or varying infrastructures across branch locations.

#6: Multi-cloud strategy

Are your teams struggling to enforce consistent security across multiple cloud environments?

The majority of enterprises now leverage more than one public and/or private cloud to take advantage of the cost efficiencies and service offerings. However, this approach can add complexity, making centralized visibility and consistent policy enforcement more difficult.

Because leading SASE platforms can be flexibly and seamlessly integrated to work with all public cloud providers' infrastructures, they're a natural fit for modern multi-cloud environments.

#7: IT resource scarcity

Are your IT and security teams spread thin? Are your security and technology teams sufficiently resourced to do all that's asked of them?

SASE can simplify several aspects of network and security operations. But implementing a complete SASE approach requires significant transformation, which involves planning, deployment, and management of the new solution. One option is to outsource the management of the SASE solution to a trusted partner. A partner can serve as a one-stop-shop with the technical knowledge to take care of all SASE-related challenges, from planning and design for the initial implementation to the ongoing operation and optimization of the solution.

With managed SASE, organizations will have ongoing access to hands-on expertise. Not only will you have a managed services partner who is with you every step of the way, but you'll also gain access to enhanced monitoring capabilities for faster ticket resolution times when issues do arise – ensuring that your business will run smoothly.

Step 2:

Conduct a gap analysis.

What's the current state of your security infrastructure? Where would you like it to be?

Questions you might ask include the following:

- Which of your security and networking solutions are currently hosted on-premises?
- Which are in the cloud? How many would you like to migrate to the cloud?
- Where do you need more visibility and control over sensitive data?
- Where is your policy enforcement inconsistent?
- Are architectural inefficiencies leading to performance issues? If so, where?
- How far along are you on the journey to Zero Trust adoption?
- What types of issues and frustrations do your end-users routinely encounter?

Step 3:

Compare vendors to identify and select the SASE solution.

As you evaluate different SASE offerings, ensure the following features are incorporated:

1. SD-WAN:

An SD-WAN solution should be application-defined rather than packet-based for better visibility, making it possible to cover applications including Software as a Service (SaaS), cloud and Unified Communications as a Service (UCaaS). An effective SASE solution should also offer integrated SD-WAN with consistent policy enforcement within a cohesive platform, so that you don't need to bolt on disparate products from multiple vendors.

2. ZTNA:

A SASE solution should incorporate continuous threat assessment and trust validation into ZTNA for protecting applications. It should also be able to apply other security services to detect and block anomalous and harmful user behaviors. It should be able to extend the same controls across access to all applications no matter where they reside.

3. CASB:

Your SASE solution should be able to keep up with the explosion in SaaS application adoption by incorporating both inline and API-based SaaS controls for governance, access and data protection, all delivered automatically.

4. FWaaS:

A SASE solution should include FWaaS capabilities equivalent to the protections a next-generation firewall would offer, allowing you to implement comprehensive network security policies in the cloud. It is important to ensure your SASE solution not only provides basic port blocking but also incorporates advanced cloud-based security features such as threat prevention services and DNS security.

5. SWG:

A SASE solution should include the same security services as a traditional SWG, allowing organizations to control access to web and non-web applications and enforce consistent policies to protect all ports, protocols, and applications. The solution should provide a simple onboarding mechanism to give adopters a seamless way to transition from a legacy, stand-alone SWG to a more secure SASE architecture.

6. Platform-driven monitoring:

Your SASE solution should incorporate natively-integrated digital experience monitoring (DEM) that leverages automation and predictive analytics to provide end-to-end visibility and insights for seamless digital user experiences. This allows for speedy incident resolution and gives detailed performance insights into endpoint devices, Wi-Fi networks, network paths and applications.

7. Threat Prevention:

Your SASE solution should incorporate threat prevention to stop zero-day attacks in line in real time. These should be capable of blocking exploits and malware by using the latest threat intelligence as well as machine learning (ML) and artificial intelligence (AI).

8. Internet of Things (IoT) security:

IoT security should be integrated into the SASE platform to secure remote branches, sites, and workers. With ML and AI, the solution should be able to accurately detect devices for full visibility and enforce policies to ensure security across the network, eliminating the need for additional IoT security solutions.

9. Data Loss Prevention (DLP):

DLP enables organizations to accurately and consistently identify, monitor and protect sensitive data everywhere — across networks, clouds, and users, regardless of whether it's at rest, in motion or in use.

10. Platform Extensibility:

A SASE vendor should embrace the integration of third-party services and simplify the process for administrators by providing a platform that makes these integrations easy. This way, organizations can quickly add the services they need with the full support of their SASE provider.

Step 4:

Building out a full-featured SASE implementation can be a complex undertaking. Organizations can make the process more manageable by beginning with a detailed project plan that defines key steps and milestones within the process.

These should include:

- An initial network and security **assessment phase**
- The **design and planning phase**, where special attention should be paid to making migration and implementation smooth
- The **deployment phase**, where you'll begin rolling out cloud services in staged fashion, according to your current environment and security and networking priorities
- The **operationalization phase**, in which your team works to establish rules and policies that ensure your security and networking requirements are met
- The **optimization phase**, in which ongoing service management, including monitoring, analytics and reporting, will allow your deployment to reach its full potential

Step 5:

Evaluate the benefits of a managed SASE solution.

Adopting a managed SASE approach gives all organizations – regardless of their size or level of IT maturity – access to the resources, tools, and technologies they'll need to meet even the most demanding networking and security requirements on a global scale, without all the complexity.

The benefits of Managed SASE include:

- Access to best-of-breed SASE for top-performing services
- Reduced cost and complexity
- Simple and scalable consumption model
- Improved flexibility

When looking for a managed SASE provider, consider the following:

Deep expertise in network and security transformation. Can the provider design, manage, and optimize the implementation? Do they have expertise in state-of-the-art technologies?

End-to-end service offerings. Can the provider act as a one-stop shop that can take care of the entire deployment? The services should improve operational efficiency, not add more work for your in-house teams.

Broad competencies. Security, networking, and IT are becoming increasingly interdependent. The provider should have a wide array of capabilities in all three areas—demonstrated by industry certifications and an established track record.

A global presence. How deep and broad is the provider's geographic coverage and market presence?

Future-proof solutions. How innovative is this provider? They should have extensive R&D capabilities, as well as well-defined product roadmaps.

Best-in-class customer experience. Does this provider offer real-time analytics and advanced automation to support rapid incident resolution? How comprehensive and competitive are their SLAs? What's their track record like for customer support?

Low risk. Choose a firmly-established market leader with financial stability, substantial resources and a large, well-established roster of enterprise clients.

Introducing NTT DATA Managed Network Service with Palo Alto Networks Prisma SASE

NTT DATA has partnered with Palo Alto Networks to deliver NTT DATA's Managed Network Service with Palo Alto Networks Prisma SASE, enabling organizations to make informed decisions while producing better business outcomes. Palo Alto Networks – the only vendor to be recognized as a leader in the 2023 Magic Quadrant™ for SSE and 2022 Magic Quadrant for SD-WAN by Gartner – delivers unified Prisma SASE solutions that improve overall technology infrastructure performance and end users' experiences. Palo Alto Networks and NTT DATA have joined forces to bring customers a best-in-class SASE solution, plus best-in-class managed services.

This new offering marries networking and security capabilities but also incorporates all the technical and management expertise needed to deploy, integrate, and manage them on an ongoing basis. It's powered by the industry's most complete SASE solution, purpose-built to help organizations achieve the best performance — and most value — from their SASE transformation. Adopting Prisma SASE reduces risk, speeds up cloud and digital transformation, and reduces costs overall. A large enterprise can expect a return on investment of up to 270%, according to research from Forrester, and this fact alone provides a strong foundation for business case justification.

To learn more about this new offering, download our Managed SASE white paper, or contact a member of our sales team today.

The Prisma SASE Advantage

As one of the industry's most complete SASE solutions, Prisma SASE from Palo Alto Networks streamlines secure access by connecting all users and locations with all apps from a single product. The superior security of ZTNA 2.0 protects both access and data to dramatically reduce the risk of a data breach, while a cloud-native architecture with integrated Autonomous Digital Experience Management (ADEM) provides exceptional user experiences.

Better Together: Palo Alto Networks + NTT DATA

In summary, this offering brings together the Palo Alto Networks Prisma SASE technology, including its ADEM platform leveraging AIOps functionality, and NTT DATA's extensive network management expertise. Because NTT DATA has long-established experience as an integrated services provider and leader in managed networking, NTT DATA is able to build upon the capabilities of its managed network service platform, including advanced automation and analytics that is layered onto ADEM, and incorporate them within this offering. This means that NTT DATA's Managed Prisma SASE customers will enjoy the improved network performance that the comprehensive monitoring capabilities of this joint offering make possible, while also gaining all the benefits of SASE, including enhanced operational efficiency.

To learn more about this new offering, download our **Managed SASE white paper**, or contact a member of our sales team today.

Learn now

NTT DATA | paloalto® NETWORKS