



HPE aruba
networking

10 reasons CxOs are adopting SASE to enable hybrid work

HPE 
GreenLake



1. Securing the business apps that employees rely on most for work

CxOs can use SASE to provide secure access to business applications based on the identity and context of the users and devices. Secure Access Service Edge (SASE) combines software-defined wide area networking (SD-WAN) and Security Service Edge (SSE) solutions into a unified cloud-delivered solution that protects users, endpoints, applications, systems, and remote networks from threats and data breaches while allowing access to the resources needed for work.

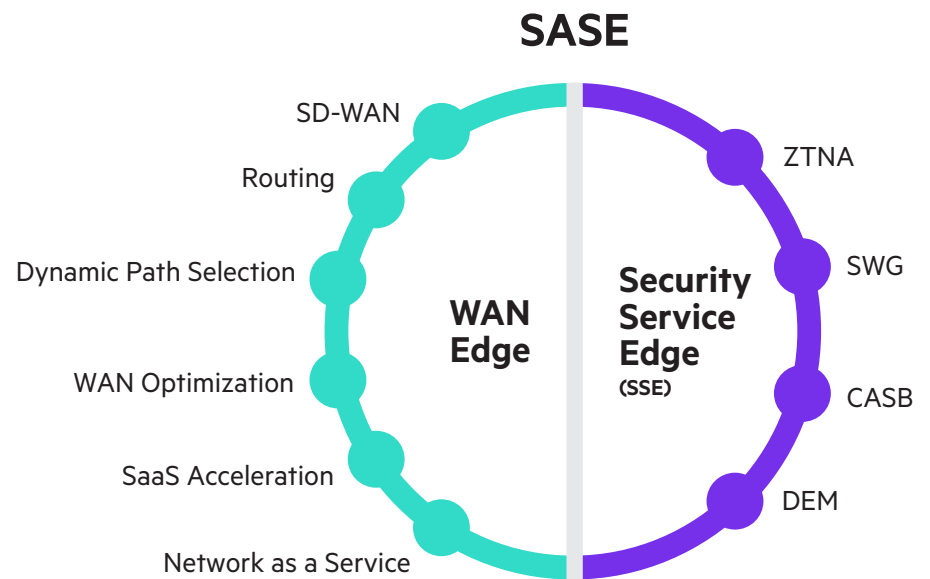


Figure 1. Secure Access Service Edge

2. Optimizing the user experience across all edges

Digital experience monitoring (DEM) capabilities ensure a high-quality user experience across remote and campus environments and provide the ability to pinpoint experience-impacting issues, such as device CPU spikes, Wi-Fi outages, local ISP outages, application outages, etc.

Built-in DEM functionality with SASE allows performance visibility into both managed and unmanaged (BYOD) devices, enabling teams to better serve their distributed workforce by optimizing experience.

3. Educating employees to be good digital citizens

SASE solutions provide helpful alerts and warnings to employees to help them make informed decisions that protect the business from breaches. The result is less accidental data leakage, fewer successful social engineering attacks, and a higher security IQ for all employees.





63%

of organizations have 3+ security solutions

4. Simplifying access services into one solution

Rather than relying on multiple point products to provide secure access, CxOs can leverage SASE to consolidate disparate products into a single, unified access SASE architecture.

This combines the power and functionality of SD-WAN and SSE—Zero Trust Network Access (ZTNA), Secure Web Gateway (SWG), Cloud Access Security Broker (CASB), and Digital Experience Monitoring (DEM)—into one solution, instead of a handful.

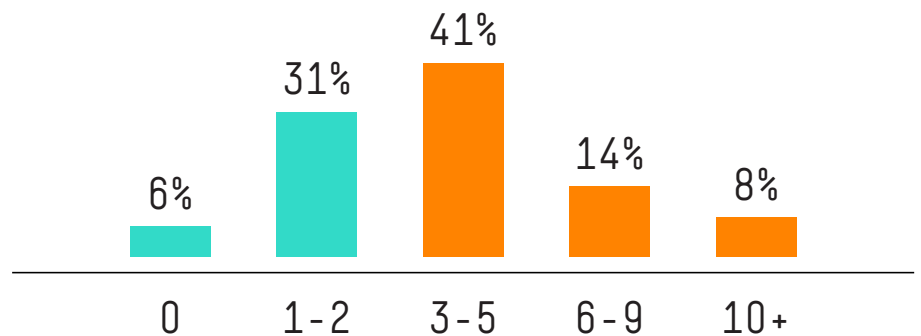


Figure 2. Number of security solutions per organization polled. 2023 SSE adoption report, Cybersecurity Insiders

5. Enabling and managing connectivity from anywhere

Employees have frictionless, secure access to apps while working from home, on the go, and at the office. Leaders can view user access logs in granular detail for audit logging and forensic analysis. SASE solutions include smart capabilities like captive-portal recognition and smart-routing that make hybrid work easier to manage both for the end-user and the IT admin.





6. Scaling and disaster recovery

In 2022, 61% of companies stated they managed more than 3+ VPN gateways globally (2022 VPN Risk Report, Cybersecurity Insiders). While more gateways increase resilience and redundancy, it also exponentially increases management overhead and attack surface.

Unlike gateway-based VPN approaches, SASE dramatically increases the number of points of presence (PoP) for access services, which significantly increases performance and scale without the management overhead requirements or risk potential.

SASE services provide an exponential increase in availability of key access services for private apps, SaaS apps, and the Internet. More PoPs equate to more scale—especially when the SASE service runs on a public cloud backbone. Disaster recovery improves dramatically because failure of one PoP triggers automatic traffic routing to the next closest PoP—reducing downtime for the business.

7. Transforming to the cloud

IT leaders can adopt hybrid multi-cloud architectures easily because SASE services support access to any environment—whether data center, public cloud, or SaaS. No application is left behind; the best SASE services not only support modern web applications, they even support legacy applications like IBM AS400, VoIP, and initiated protocols as well. There is no need for new infrastructure or to re-architect the network environment. Combining advanced SD-WAN with built-in application-aware next-gen firewall capabilities allows IT to implement Zero Trust network segmentation to secure IoT devices and even go beyond what is defined by SASE.

8. Seeing immediate value, with simple implementation

It is easy to get started with SASE technologies. The most popular starting point for many organizations is using the SASE's ZTNA capability to replace VPN. 95% of companies use VPN¹ and 63% of companies say they expect SASE to eliminate their need for VPN².

With SASE, existing infrastructure can still be used, and then transitioned out over time as the IT leader adopts SASE for additional use cases like third-party access, accelerating IT integrations during mergers and acquisitions, Internet access, SaaS protection, SD-WAN, and more.

9. Managing budget relationships is easier

Because SASE projects are typically driven 50% by security and 50% by the infrastructure team, these projects bring these two groups together to make decisions jointly.

SASE reduces total cost for teams by eliminating the need for multiple point products, hardware appliances, maintenance contracts, and operational overheads. CxOs can ask the SSE vendor for business value reports that map out the expected cost savings based on customized criteria from the customer's existing environment.

¹ 2022 VPN Risk Report, Cybersecurity Insiders

² 2023 SSE Adoption Report, Cybersecurity Insiders





10. Enforcing compliance universally

SASE ensures compliance with various regulations and standards by applying consistent security policies across all edges—users, devices, applications, locations, etc.

IT leaders can use SASE to store access logs and broker connections in the country of origin to comply with regulations like GDPR. Sensitive data can be protected from being viewed or accessed from unauthorized personnel—key for regulations like PCI DSS, HIPAA, FIPS-140, etc. SASE can separate work traffic from personal user traffic to make sure that only work data is inspected, and employee privacy remains intact.

SASE also provides visibility and reporting capabilities that help demonstrate compliance to auditors and stakeholders.

SASE is the future of hybrid work. It enables CxOs to provide secure, reliable, and seamless access to business applications from anywhere, on any device. It can simplify the IT infrastructure, reduce operational costs, and ensure compliance with various regulations and standards. It can also enhance user experience, educate employees, and scale with organizational needs. SASE is not just a technology; it is a strategic advantage for CxOs who want to lead their organizations in the digital era.

For more information visit

arubanetworks.com/sase.

Visit ArubaNetworks.com



To learn more about how SASE can help you enable hybrid work, contact us today.



Contact us