Unified SASE: Cohesive connectivity and security

Reduce security risks while improving network performance and management

HPE GreenLake

Security experts have shined a much-deserved spotlight on Secure Access Service Edge (SASE). They know that there's a new normal in today's enterprise where security practices that used to be effective aren't anymore. Networks that were manageable, aren't. Solutions that once worked, don't work as well as they once did.

In the face of these hard truths, it's time for a new secure access paradigm that can balance security and connectivity. SASE combines SD-WAN and Security Services Edge (SSE) to bring security and connectivity together — providing secure, anywhere access that can span everyone and everything — under a singular cloud-managed console.

Unified SASE delivers on the promises of SASE and more. By tightly integrating SSE and SD-WAN, network architectures are simplified without sacrificing security or performance. Businesses can accelerate deployments and streamline operations while reducing cybersecurity risk.

Deliver high performance and uninterrupted access while reducing risk

Implementing SASE is a journey that requires strategic decisions.

You can start your journey by deploying all elements at once or you can start smaller. For example, you can start by deploying Zero Trust Network Access (ZTNA) to ensure secure access from anywhere, which replaces legacy, insecure, remote-access VPNs. Another good option is to begin by connecting all your locations with secure SD-WAN.

No matter which option you choose, integrating security and connectivity into the same solution can make operations simpler. With unified SASE, organizations can more efficiently and confidently implement global digital innovation that relies on secure networking at its core.

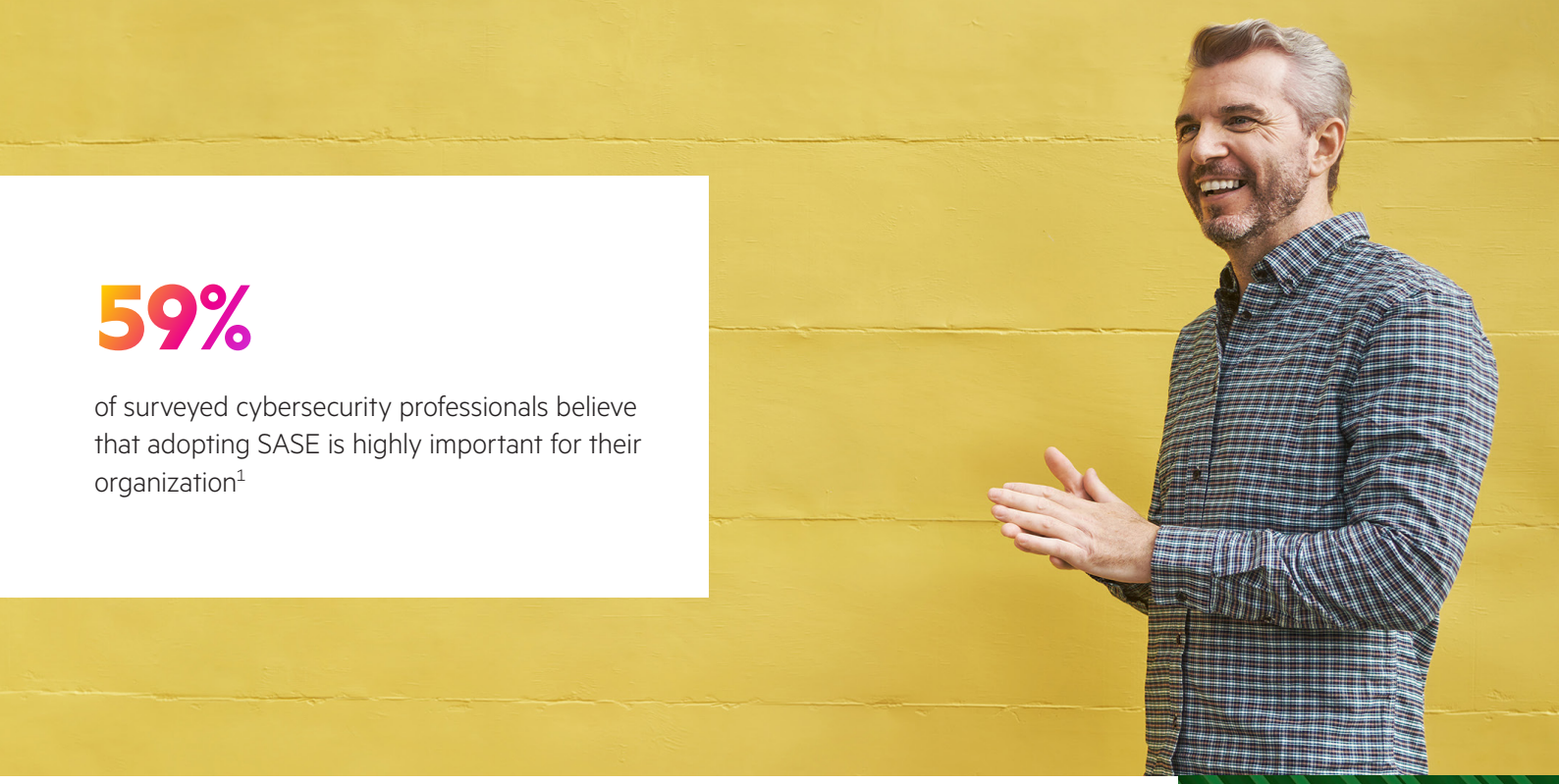
Combined with this secure connectivity, unified SASE supports must-have network performance. A centralized platform provides network and security operations teams with network-wide visibility into events, security incidents, and performance.

The benefits of bringing security and connectivity together

Without unified SASE, realizing both security and connectivity goals can be challenging. The forces of hybrid work, digital acceleration, and IoT growth can create a tough balancing act between connectivity and security objectives. But you can move from pain to gain.

Often, you'll see signals that the time is now to make unified SASE a reality so that you can deliver high performance, robust security, and uninterrupted access to your business demands. Signs to watch for are:

- Even with a full assortment of security tools and appliances, it's a struggle to support secure apps across the web, hybrid cloud, and software as a service (SaaS).
- To help stay ahead of evolving threats, there is a need to adopt Zero Trust principles throughout the organization.
- Remote users are unhappy due to performance issues, and their VPN connections are a security risk.
- User experience is inconsistent for cloud and data center apps.
- Connectivity and security are so complex that it's difficult to accelerate deployments and realize results.
- Both security and network teams are spending too much of their time on troubleshooting.
- App performance in the cloud is so inconsistent that it frustrates users.
- Limited resources and skillsets are preventing or slowing SASE adoption.



59%

of surveyed cybersecurity professionals believe that adopting SASE is highly important for their organization[1]

Realizing unified SASE that brings connectivity and security together

As your organization grows and embraces new innovation, unified SASE can help you deliver consistent connectivity and security everywhere — without compromising performance or managing multiple platforms, tools, and controls. When getting started, consider this SASE checklist:

- **A foundation for your SASE journey** — Can you unify SASE and connect your entire enterprise using policies and management from the same console? Does the solution avoid vendor lock-in and allow you to set your own pace toward unified SASE?
- **Accelerated deployments** — Does the SASE solution consolidate your footprint from edge to data center to cloud?
- **Network and security collaboration** — Can both networking and security teams use the same tools to meet objectives and reduce complexity?
- **Exceptional user experience** — Are users connected, protected, and productive?
- **Top-tier IT experience** — Does IT have intuitive controls that help them configure, manage, and operate at scale for secure anywhere and everywhere network connections?

[1] "Security Service Edge Adoption Report," Cybersecurity Insiders, March 2024

Unify connectivity and security with unified SASE from HPE Aruba Networking

To gain unified SASE and bring security and connectivity together from edge to cloud, take these steps:

Step 1

Connect securely across every user, device, and app

HPE Aruba Networking EdgeConnect SD-WAN delivers simplified, secure, anywhere access while delivering consistent experiences for apps in private or public clouds or SaaS. Both users and IT gain advantages with faster deployments and proactive insights for support. Edge-to-cloud security through Dynamic Segmentation enables you to define and enforce policies for users and devices, so you can protect your organization from IoT-based threats, going beyond what is defined in typical SASE architectures.

Step 2

Enable secure access from anywhere with SSE

HPE Aruba Networking SSE gives users secure access to any business resource — whether private, SaaS, or internet-based — without multiple UIs or complex policies. Highly scalable, with more than 500 point-of-presence locations, the HPE Aruba Networking solution unifies ZTNA, SWG, CASB, and DEM to provide and support secure connections wherever they are needed.

Step 3

Automate network configuration and security at scale

With HPE Aruba Networking Central, IT can manage and secure any size network — branch, remote, campus, data center, or colocation — using AI-powered, cloud-based tools. Network and security ops teams gain built-in support for Zero Trust Security; automated, self-healing workflows; and AI-based device discovery and profiling, intent-based policies, and orchestration for faster resolutions and better user experiences.

Step 4

Build a future-ready network

High-performance Wi-Fi 6/6E and Wi-Fi 7 wireless access points boost IT, user, and IoT experiences with intelligent, fast, and secure enterprise wireless connectivity that helps ensure you're ready for the future.

Why HPE Aruba Networking at the edge?

Work smarter — not harder — on your digital transformation journey. A security-first, AI-powered modern network can lay a solid foundation for your future. The modern network can accelerate technology adoption, improve end-user experience, and reduce cyber risk.

A common network and security foundation from HPE Aruba Networking, built on Zero Trust principles and available for flexible, aaS consumption, can help you optimize user experiences, unlock higher performance, and keep up with evolving threats.

Learn more at

HPE connected edge

Visit **HPE GreenLake**

Chat now (sales)

Hewlett Packard Enterprise

© Copyright 2024 Hewlett Packard Enterprise Development LP. The information contained herein is subject to change without notice. The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

a50010478ENW