HPE GreenLake

Implementing edge-to-cloud networking security

In most enterprises today, users, devices, and the applications they need to run are spread across numerous locations. Users are accessing the network from virtually everywhere to reach business resources that are hosted in the cloud, on-site, and by third parties. While the ability to work from anywhere has many benefits, it also creates new security challenges for IT and security teams:

- **Hybrid environments:** The rise of hybrid workforces and distributed teams is dissolving the traditional security perimeter
- **Cloud vulnerabilities:** As more sensitive data is hosted in the cloud, enterprises are facing cyber threats that exploit previously trusted users and devices for malicious purposes
- **Increased attack surface:** With more users, locations, and the adoption of connected devices (IoT), enterprises have more entry points to defend against attackers

To better protect users, devices, and applications, traditional security architectures need to evolve. The goal is to ensure fast, reliable, and consistent access that supports user productivity—without compromising security. To achieve this goal, organizations are increasingly adopting more innovative security strategies built on the principles of Secure Access Service Edge (SASE) and Zero Trust.

Why security needs to evolve

Legacy VPNs have often provided poor user experience

Additionally, the use of VPNs without granular controls can overextend network privilege, granting users more access to resources than necessary and increasing security risks.

Traditional network architectures route application traffic to the data center for security inspection

This is no longer practical, and because applications now reside mostly in the cloud, backhauling creates latency and impacts application performance.

Data is increasingly hosted in SaaS applications, requiring extra steps to secure

Sensitive data can be stored in both sanctioned and unsanctioned cloud applications and may travel over unsecured links, leading to a potential risk of data loss.

The explosion of IoT devices has significantly increased the attack surface

IoT devices are not inherently secure, often built on a simple design with a lack of sophisticated security mechanisms.

New compliance and regulatory mandates

From Health Insurance Portability and Accountability Act (HIPAA) to General Data Protection Regulation (GDPR), organizations need to ensure compliance, but often lack the essential tools and comprehensive reports needed to demonstrate compliance.

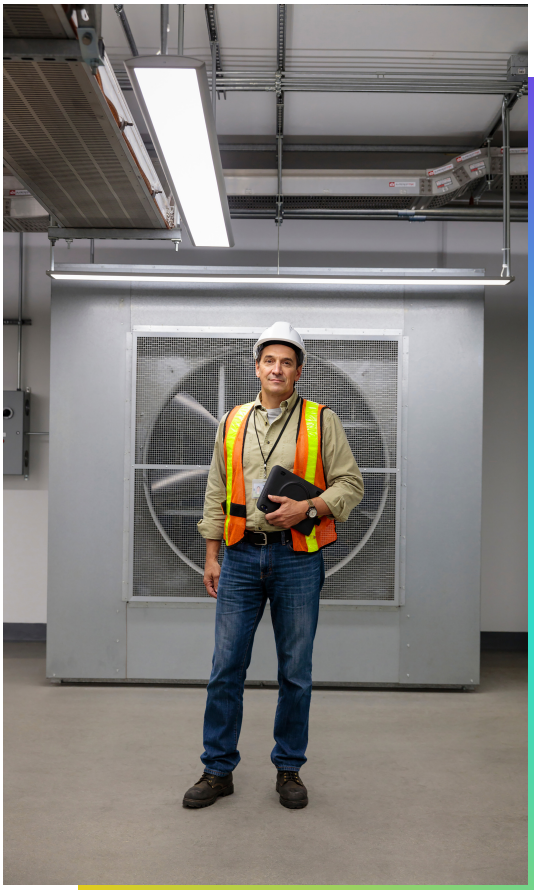
Best practices for more advanced network security

1. Build a robust SASE framework

SASE, a term coined in 2019, is the convergence of networking and security. It combines SD-WAN with Security Service Edge (SSE) to provide a more secure network architecture—and has become a strategic imperative for modern businesses looking to thrive in the digital era.

- **SD-WAN** is a virtual WAN architecture that allows organizations to leverage any combination of transport services—including Multiprotocol Label Switching (MPLS), Long Term Evolution (LTE), and broadband internet services—to more securely connect users to applications. It uses intelligent steering across the WAN to eliminate the need to backhaul SaaS traffic to the data center.
- The security component of SASE, **SSE** is a combination of advanced cloud-delivered security services including Zero Trust Network Access (ZTNA), Secure Web Gateway (SWG), and Cloud Access Security Broker (CASB). ZTNA assumes that no user can be trusted by default and supports least privilege access, which provides more secure access to remote users.

To implement SASE, organizations commonly take one of two paths. They can start by securing remote workers with ZTNA, or they can begin by addressing application performance issues in branches with SD-WAN. Organizations can also choose between a single vendor or a multivendor approach.

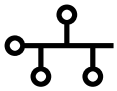


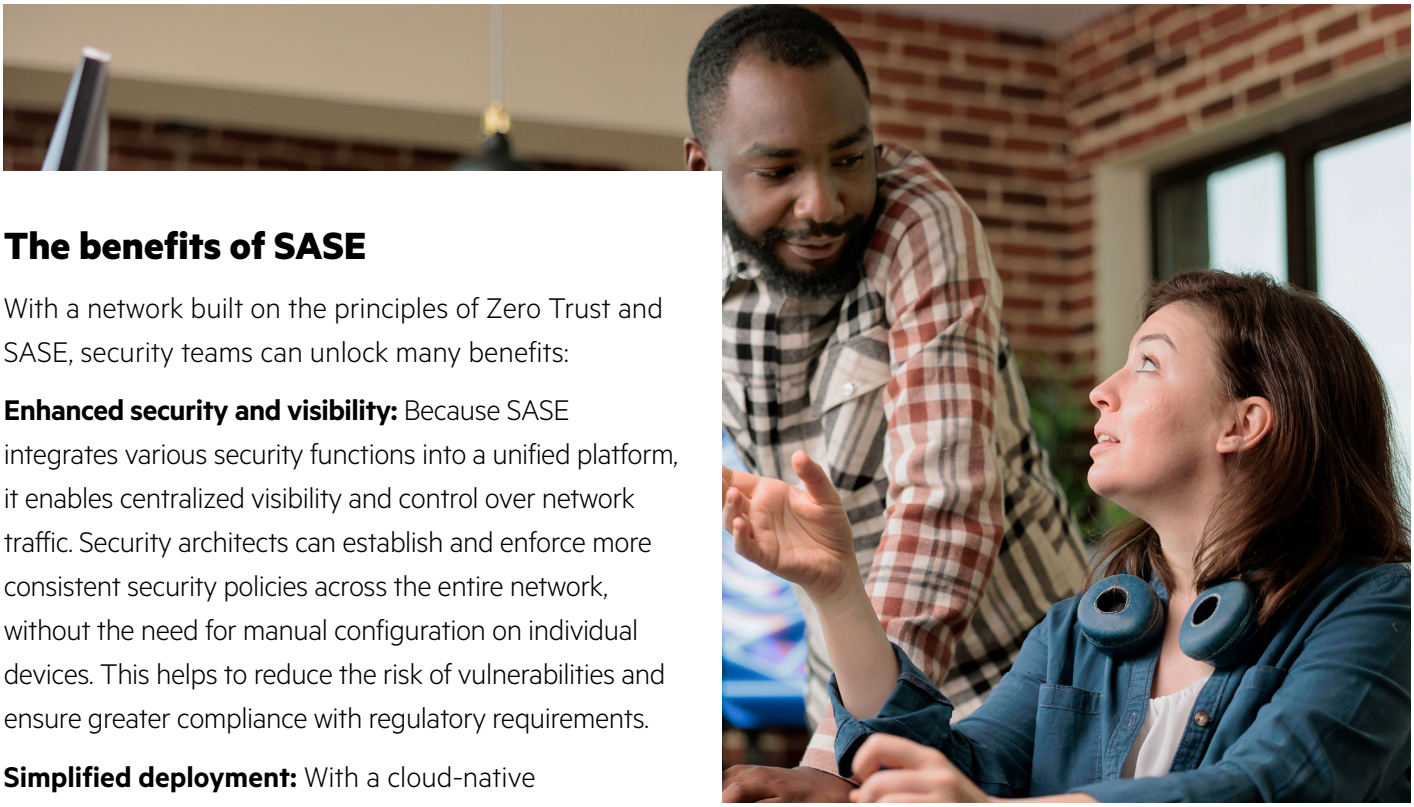
Single vendor SASE	Multivendor SASE
Offers simplicity, ease of deployment, a single point of contact for support, and simpler licensing	Allows for selecting best-of-breed solutions based on network requirements

2. Implement a Zero Trust model to enhance security within SASE

Implementing a Zero Trust model is critical for enhancing security within the SASE framework.

Zero Trust security is based on the principle of assuming that no user or device can be trusted by default—no matter their location or network connection. It requires verifying and validating every user's identity and device before granting them access to resources.

How Zero Trust aligns with SASE	
Microsegmentation 	A core principle of Zero Trust, microsegmentation divides the network into smaller segments and applies granular access controls. In the SASE framework, microsegmentation ensures that access to resources is restricted based on identity, device, and other contextual factors. This helps prevent lateral movement within the network and limits the potential impact of a security breach.
Identity-based access controls 	Zero Trust security emphasizes the use of identity-based access controls to grant or deny access. All users must authenticate and prove their identity before receiving access to resources. In SASE, identity-based access controls are enforced through technologies such as ZTNA, which authenticate users and devices before granting them access to specific applications or data.
Continuous monitoring 	This plays a vital role in enforcing the Zero Trust approach within the SASE framework. It involves monitoring user behavior, network traffic, and security events in real time to identify any anomalies or suspicious activities. With continuous monitoring, teams can more quickly detect and respond to potential threats, ensuring ongoing security of the network.



The benefits of SASE

With a network built on the principles of Zero Trust and SASE, security teams can unlock many benefits:

Enhanced security and visibility: Because SASE integrates various security functions into a unified platform, it enables centralized visibility and control over network traffic. Security architects can establish and enforce more consistent security policies across the entire network, without the need for manual configuration on individual devices. This helps to reduce the risk of vulnerabilities and ensure greater compliance with regulatory requirements.

Simplified deployment: With a cloud-native architecture, SASE allows for quick and easy deployment across various locations and environments.

Advanced threat detection and response: SASE leverages technologies like AI and machine learning to identify and analyze network traffic patterns, detect potential threats, and respond to them in real time, empowering security architects to stay one step ahead.

Automated updates: SASE incorporates automated updates to ensure security measures and capabilities are always up to date—reducing the need for manual updates and patching, and the risk of security gaps due to outdated software or configurations.

For organizations as a whole, SASE enables more secure connectivity from anywhere, protects web browsing, ensures control over cloud-hosted data, and enhances application performance and security at branch offices.

Build a resilient network for the future

Hewlett Packard Enterprise is unlocking the power of the cloud with advanced network security. When you implement security-first solutions, you can rapidly work and scale to get more value from your data across your hybrid cloud. HPE can transform your network into a security solution that enables you to support users and devices located anywhere. Let's explore the networking solutions that can help you succeed.

Learn more at
HPE.com/edge

Visit **HPE GreenLake**

Chat now

Hewlett Packard Enterprise

a50010537ENW