HPE aruba networking

The Definitive Guide to Security Service Edge (SSE)

The modern age of work requires a modern method of application access

HPE GreenLake

The way we connect has changed

"51% of all knowledge workers worldwide are expected to be working remotely by the end of 2021."

- Gartner® 2021

"81% of all enterprises have reported that they have a multi-cloud strategy already laid out or in the works."

- Cloud Computing Statistics 2022

"Remote and hybrid work has increased the number of devices per person, totaling 6.2 billion units in 2021."

- Gartner® 2021

It's undeniable that the world has undergone a mega shift as more and more users, applications, and devices all exist outside the security of the corporate perimeter. After years of trying to cope with traditional network security appliances, IT leaders recognize the ultimate need for evolution in what secure access looks like for the modern business.

Gartner®, too, has identified this shift to cloud and mobility and recognized a specific group of technologies that enables IT leaders to introduce a modern method of connectivity to the business.

This technology group is commonly referred to as the Security Service Edge (SSE).

What is Security Service Edge (SSE)?

A Security Service Edge (SSE) platform provides universal secure access, visibility, and control to all business applications by consolidating security services into a single cloud offering.

An SSE platform fuses together three primary security solutions: ZTNA for private apps, secure web gateway (SWG) for all web access, and CASB for SaaS apps. This is what modern secure connectivity looks like—a single SaaS offering that empowers IT teams to control all user and application access, regardless of location, device or network.

While this document focuses primarily on the value of SSE for user-to-application access, these platforms can also be applied to app-to-Internet, app-to-app across environments, and app-to-app within environments, as well as server-to-server communications.

While it may seem like SSE is just another acronym in the world of IT, it's important to realize the importance it brings to the modern workplace. SSE makes up more than half of Gartner®'s overarching Secure Access Service Edge (SASE) framework, with SD-WAN being the only key component not included within SSE. See the diagram below.

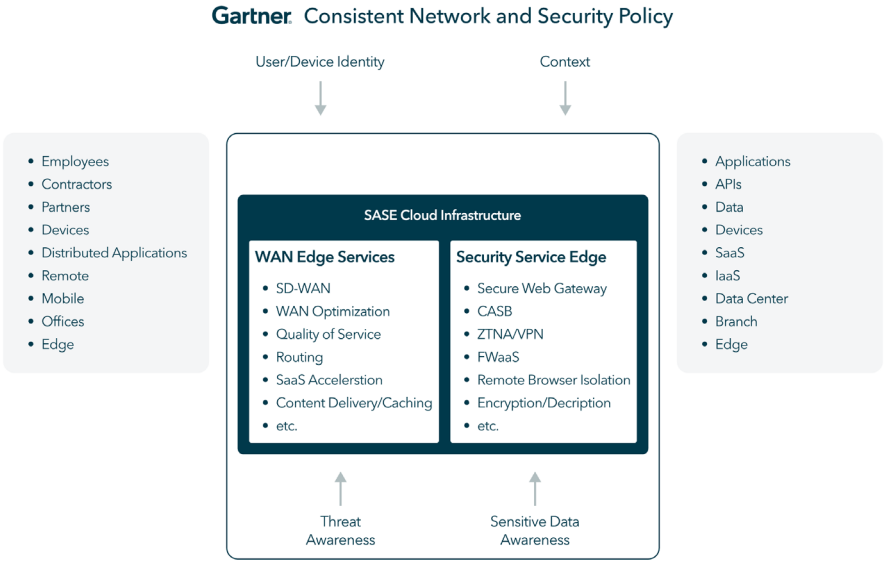

Figure 1. Network and security policy

What does SSE bring to the workplace?

SSE platforms provide the modern alternative to traditional network security technologies (firewalls, VPN gateway appliances, and web gateway appliances) and provides value for multiple teams.

SSE security benefits:

- Provides universal security for all users (employees and third-parties alike), devices, and applications
- Eliminates attack surface and attack vectors
- Minimizes impact of ransomware or malware attack by reducing lateral movement
- Implements least-privileged access with Zero Trust policies
- Protects against data exfiltration with enhanced control of data
- Reduces security blind spots by gaining visibility and control of shadow IT
- Enables SSL encryption at scale with cloud
- Provides a single pane of glass for universal visibility and access of all activity

SSE networking benefits:

- Supports all applications—legacy or cloud—with a single access solution
- Minimizes vendor sprawl and simplifies network services
- Keeps users off the corporate network
- Segments access on a granular one-to-one basis, without network access and with no need for network segmentation
- Optimizes connectivity paths and reduces latency with intelligent routing
- Reduces outages and downtime with precise digital experience troubleshooting
- Speeds deployment and provides effortless scale with a cloud architecture

Enterprise benefits of SSE

- **Secure the distributed enterprise:** Empower your employees to work from anywhere by seamlessly connecting authorized employees to business data regardless of their location, device, or network.
- **Secure third-party access:** Enable your business ecosystem to safely access sensitive data. Make third-party access secure without extending network access or requiring an agent install, all while simplifying identity lifecycle management.
- **Modernize infrastructure:** Transform your network with a modern cloud architecture. Embrace the modern workplace by replacing legacy appliances, simplifying hybrid-cloud adoption, reducing infrastructure costs, and bringing smart automation.

Secure the distributed enterprise

With users and business applications all operating outside the confines of the physical network, the use of network perimeter-based access solutions makes less and less sense. Instead of focusing on securing the network, an SSE platform secures the connections between users and business resources in a way that is versatile, secure, and cost effective—no matter where they work.

- **Universal access to apps:** Provide every user with fast, secure, and reliable access to all business resources—from any device and over any network.
- **Leverage cloud to the fullest:** Make sure your cloud investments are optimized by ensuring a speedy, reliable, and scaled access experience. Cloud-based technologies like SSE are designed for scalable deployments and cost optimization.
- **Optimize experience and enhance productivity:** Gain deeper insights into user access through digital experience monitoring. Make it easier for IT to pinpoint performance issues and speed up troubleshooting.
- **Protect business data:** Secure the business from ransomware and malware attacks. Operate on a Zero Trust basis that enforces least-privilege access to business data, inspection of all traffic, and the reduction of exposed attack surface.

Use cases

- Secure remote access without VPN
- Secure internet and SaaS access
- Monitor end user experience
- Protect against ransomware

Secure third-party access

The success of your business is propelled by your contractors, suppliers, vendors, partners, and B2B customers. Ensuring these users have safe yet seamless access to business resources is critical. An SSE platform implements Zero Trust connectivity to safeguard data while allowing flexible, versatile, and secure access from partners.

- **Employ least-privileged access:** External users should only have access to a limited, approved set of business applications. With SSE, IT can easily define granular application policies that keep access for third-parties separate from employees.
- **Secure access without an agent on the device:** It's often difficult to get third-party users to download a client onto their device. No agent, no problem. SSE supports agentless access for users, eliminating the need to install a client while still enabling secure access.
- **Provide visibility into third-party activity See what third-parties are accessing:** See what your third-parties are accessing through traffic inspection. See what applications are being accessed, what files are being downloaded, and even what the user clicked on.
- **Simplify management of third-party users:** Don't let partner access create security gaps. Simplify the lifetime management of third-party users through multi-tenant support and SCIM 2.0.

Use cases

- Contractor access
- Partner access to OT
- B2B customer access
- Supplier access

Modernize infrastructure

Businesses have adopted cloud, yet connectivity is still anchored in the data center. To support the modern workforce, foster better collaboration, and anticipate future needs, businesses must modernize their infrastructure to get the most out of their cloud investments. An SSE platform provides the underlying technology that optimizes the reliability, availability, and scalability of cloud investments while simplifying overall infrastructure.

- **Support all legacy and modern apps:** Leverage a single solution to support your in-house private applications still running in the data center, or in hybrid cloud, as well as external SaaS apps, with no change to the network.
- **Simplify management and reduce vendor sprawl:** By using a single, integrated SSE platform, IT can significantly reduce network point products. Networking teams can focus on more important projects instead of point-product management.
- **Keep the business running:** Be able to easily measure application, network, and device performance in real time. Gain key insights that help achieve faster troubleshooting and reduce downtime.
- **Automatically scale with cloud:** Instead of having to scale up physical appliances, an SSE platform has a 100% cloud architecture that enables networking teams to scale at the speed of work, and better predict costs than with appliances.

Use cases

- Network transformation
- Cloud-delivered branch
- Accelerate mergers and acquisitions

What to consider in an SSE platform?

When looking for a true SSE platform, it's important to consider solutions with all capabilities built natively into a single cloud platform offering. Many vendors built separate VMs or stitched together isolated infrastructure to create fragmented solutions that weren't designed for today's business needs. A better option is to choose a modern security platform built on a native cloud platform.

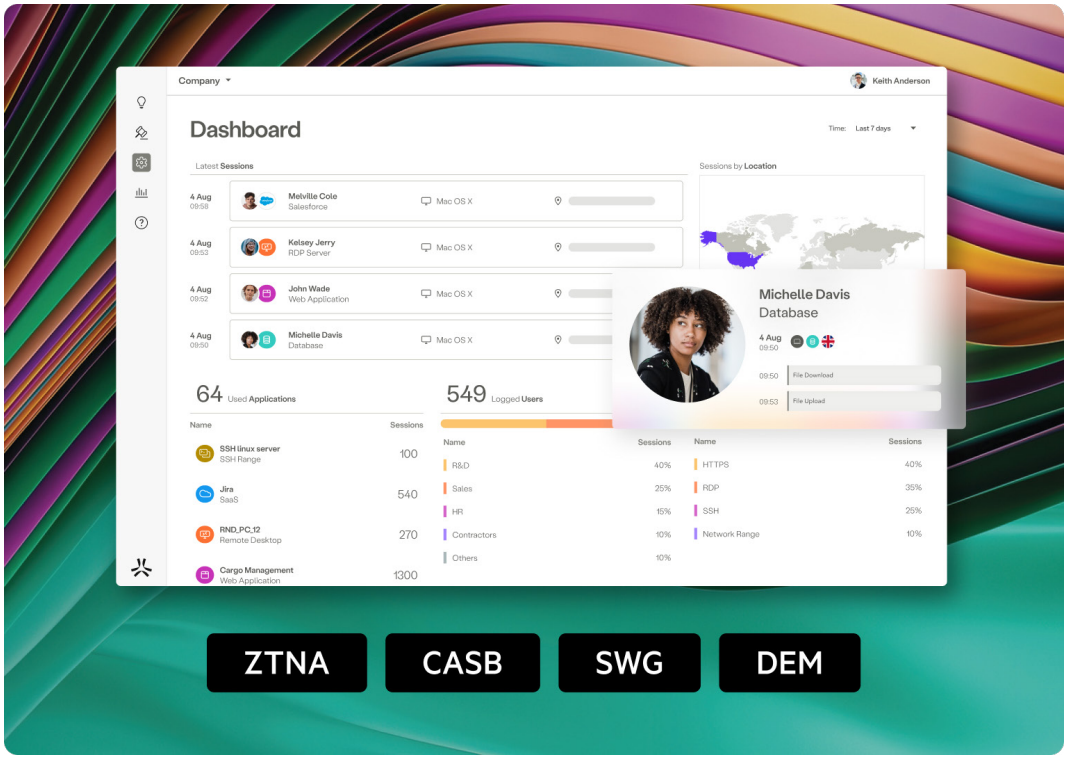

Figure 2. Atmos by Axis

HPE Aruba Networking SSE

Makes securing access to business resources impossibly simple for IT and completely seamless for users.

- **Super simple:** One pane of glass for every app, 100% cloud, and policy tagging for use within minutes
- **Super smart:** Adaptive access using identity, policy, and device posture and automated alerts
- **Super secure:** Zero Trust access with integrated visibility, DLP, and detection and response
- **Enforce zero trust access:** Ensure least-privilege access to resources by using policies and by inspecting traffic. Prevent compromises, reduce lateral movement, and protect against data loss.
- **Go agentless:** Avoid deploying agents on BYOD or third-party devices and the friction that comes with it. Support access to web apps, SSH, RDP, and Git without a client
- **Focus on the user:** Analyze how users interact with your business applications to better detect anomalies, flag potential issues, and ensure networking remains aware of changes in security controls.
- **Stay up-to-date, globally:** Use key tech integrations to automatically verify and adapt access rights based on changes in context to protect data and always ensure least-privilege access.

Getting started with SSE

When starting your journey to SSE, it's important to identify your starting place. Careful planning and prioritization of the most critical applications, data, assets, and user types is key to a successful deployment. A popular method of deployment is to begin using a phased approach.

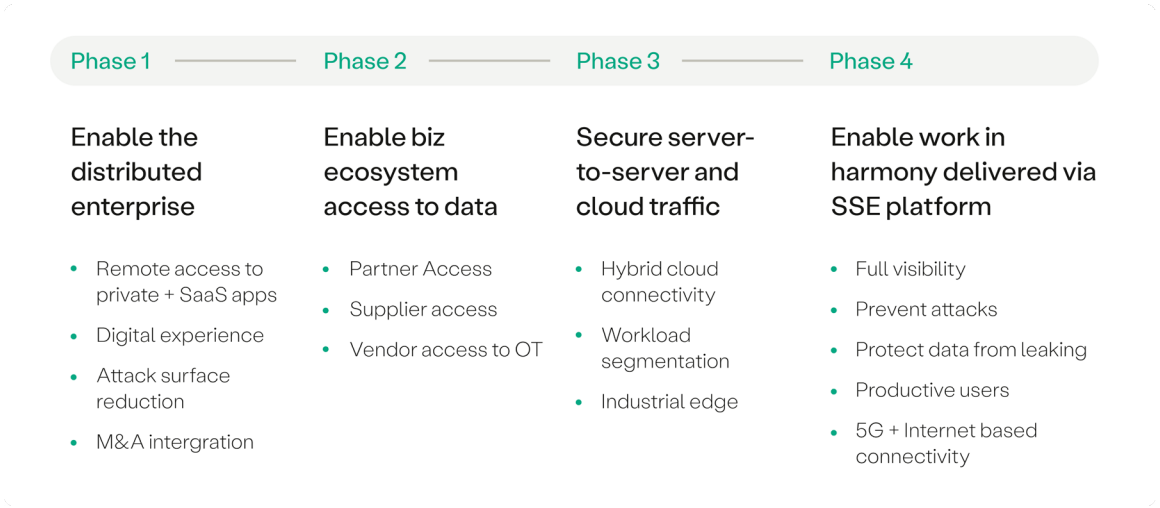

Figure 3. Securing the modern workplace

Taking advantage of these best practices and recommendations will allow you to successfully repeat this process as you extend secure access and protection to your extended business ecosystem, server-to-server traffic, and beyond. Remember, choose an SSE platform that will partner with you and your end users to deliver secure, simple, and seamless access that meets the growing and evolving needs of your business.

Start your SSE journey with HPE Aruba Networking.

Take HPE Aruba Networking Security Service Edge (SSE) Platform for a free test drive.

Get Started

Make the right purchase decision.
Contact our presales specialists.

Contact us

Visit **ArubaNetworks.com**

Hewlett Packard Enterprise

© Copyright 2023 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.

All third-party marks are property of their respective owners.

BWP_SSEGuide_RVK_121523