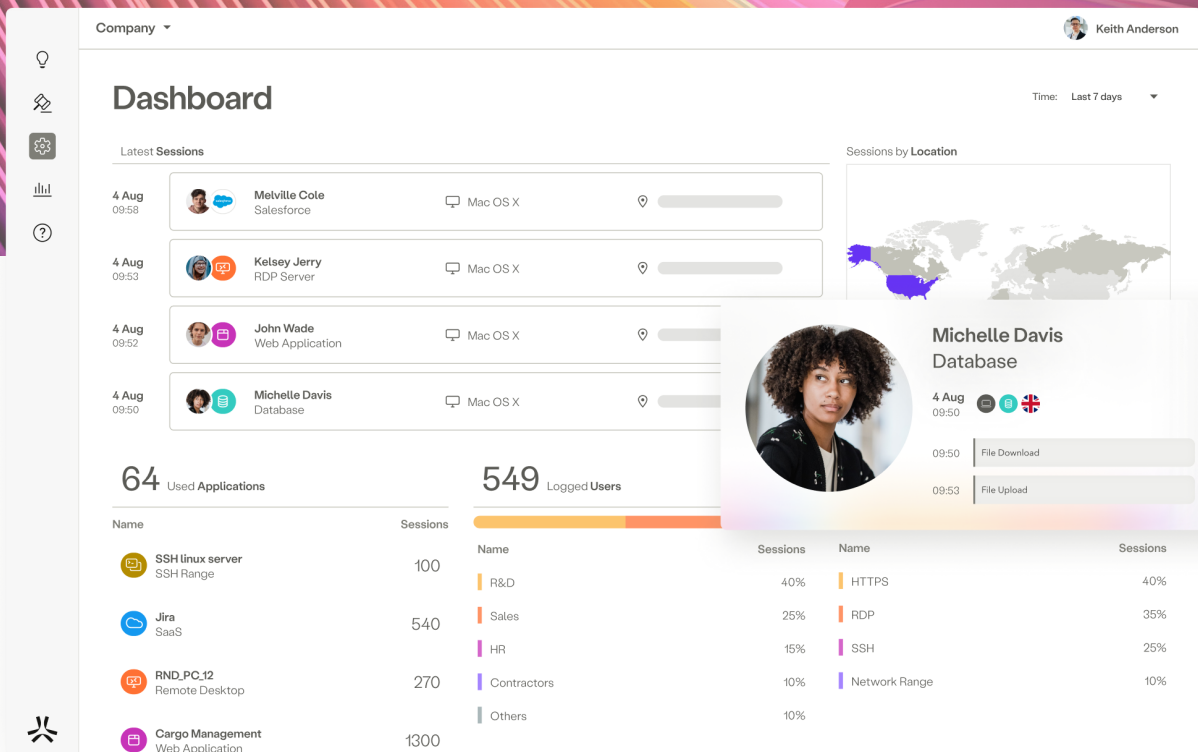# HPE Aruba Networking SSE

Enable seamless and secure access for every user, device, and application, from anywhere with HPE Aruba Networking SSE

When connectivity is in sync with the workplace you can:

Enable the distributed enterprise	**Secure third-party access**	**Modernize infrastructure**
94%	**1/3**	**Transform**
of organizations state their workforce is primarily hybrid or fully remote.[1]	**users are partners, suppliers, vendors, or customers**. Enable the business ecosystem to securely access sensitive data—without extending network access or installing an agent.	**the network to a modern cloud architecture**. Replace legacy appliances, simplify hybrid-cloud adoption, reduce infrastructure costs, and introduce automation.

[1] SSE Adoption Report, Cybersecurity Insiders, 2024

To outpace competition, IT has been asked to invest in services designed to ensure the productivity of the workforce and its supply chain. This has created an opportunity for IT to define the new technologies that will connect their users to key business resources like Microsoft 365, Salesforce, and SAP®. Ninety percent of IT leaders have plans to adopt SaaS and hybrid cloud services that extend connectivity out to their workforce. In this modern workplace, every user, application, and their device are connected to the internet.

Unlike the traditional network, the internet cannot be controlled by IT. Because of this, the network solutions that worked for the past 30 years are not only obsolete, but they place users on the network and expose infrastructure to the internet. A new approach is needed in order to securely and seamlessly control access over the internet.

HPE Aruba Networking aims to accelerate the transition to the modern workplace, through security connectivity with its Security Service Edge (SSE) platform. HPE Aruba Networking SSE is a platform that uses more than 500 edge locations to elegantly connect users, devices, and servers, to the business resources needed for work. The platform artfully integrates Zero Trust Network Access (ZTNA), Secure Web Gateway (SWG), Cloud Access Security Broker (CASB), and Digital Experience Monitoring (DEM) into one, cloud-delivered platform that feels weightless, and is controlled by a single pane of glass.
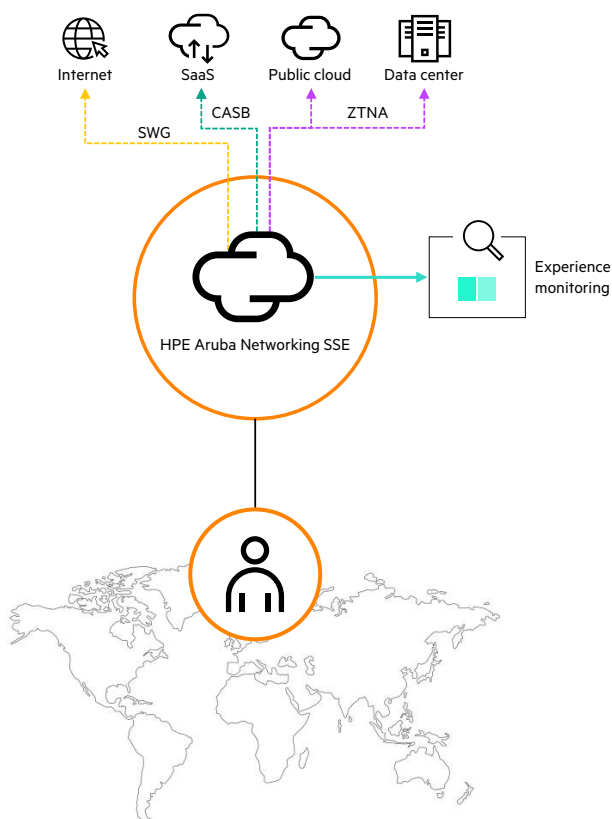
Super simple

SSE helps minimize complexity

Direct the orchestra of users and apps from one pane of glass. Its cloud design lightens the management burden for IT and is equipped with an elegant policy-tagging system for simplicity.

Super smart

SSE proves being smarter, cooler

Auto-sync with the environment with a cybersecurity mesh of IDP and endpoint services to auto-tune policies, and fluently adapt access rights. SSE proves to be smarter, cooler, and even reacts faster to user experience issues.

Super secure

SSE makes security omnipresent

Inspect traffic to elevate visibility and prevent ransomware. Protect against data leakage. Detect and respond faster to protect against threats.

HPE Aruba Networking SSE capabilities

ZTNA

HPE Aruba Networking ZTNA is a highly advanced service within the industry. It uses identity, policy, and context to broker secure, one-to-one, connections to private apps (even VoIP, AS400, and Internet Control Message Protocol [ICMP]). It fully replaces VPN and avoids the need for network access or exposure.

SWG

HPE Aruba Networking SWG uses advanced SSL inspection, URL filtering, and DNS filtering to help ensure that authorized users get fast, secure access to the internet—while protecting the business from internet-based threats that aim to harm it.

CASB

HPE Aruba Networking CASB mediates the connections between users and cloud applications and helps discover Shadow IT to apps. CASB helps ensure sensitive business data in motion remains protected while helping prevent cyber threats.

DEM

HPE Aruba Networking DEM helps ensure user productivity by measuring hop-by-hop metrics and monitoring app, device, and network performance. IT can easily pinpoint connectivity issues and reduce mean time to innocence.

Single pane of glass

With the unified SSE dashboard, IT can manage access to private apps, internet, SaaS apps, and DEM from one console. Easily define policies, track user activity, manage tenants, and oversee a cybersecurity mesh of SSE, IDP, and endpoint security.

Inspection of all traffic

View user activity, files downloaded, commands used and block malicious actions by inspecting all private and public traffic with HPE Aruba Networking ZTNA and SWG.

Application discovery

Shine light on unsanctioned applications and domains, easily define policies for each, and reduce the organization's overall attack surface.

Automated alerts and data classification

HPE Aruba Networking SSE uses AI to generate alerts, automatically detect potential security events, and improves the classification of data.

Agent and agent-less

The SSE agent forwards traffic to the HPE Aruba Networking SSE platform, performs device posture assessment, and integrates with existing endpoint solutions. The agent supports iOS, Android™, Mac, and Windows. HPE Aruba Networking SSE also has robust agentless capabilities, allowing secure access to web-based apps—even browser-based RDP, SSH, Git, and database.

Server-to-server access

HPE Aruba Networking SSE helps ensure servers safely communicate with other servers, applying Zero Trust to nonuser entities.

Data leakage prevention

Protect sensitive data from leaking out to the internet by sitting in-line and enforcing policies that block file downloads, copy and paste, and help meet compliance standards. Support agentless and agent-based deployments.

Detection and response

Prevent malware-based attacks before they even begin with advanced malware scanning and detection. Increased insights allow teams to respond to security events faster than ever.

Make the right purchase decision. Contact our presales specialists.

Contact us

Learn more at

ArubaNetworks.com/products/sse/

Visit **ArubaNetworks.com**

Hewlett Packard Enterprise