HPE aruba networking

Solution overview

Introduction to HPE Aruba Networking SSE

Secure access to all users, devices, and applications from anywhere with a single SSE platform

HPE GreenLake

The challenge with today's security solutions

It's a fact that cannot be overlooked: the global business landscape has experienced a huge transformation. An ever-increasing number of users, applications, and devices are now operating beyond the protective boundaries of traditional network security. After enduring years of challenges with conventional network security solutions, IT executives are coming to terms with the pressing need for security transformation. They are reimagining the DNA of secure access in light of the demands of modern business.

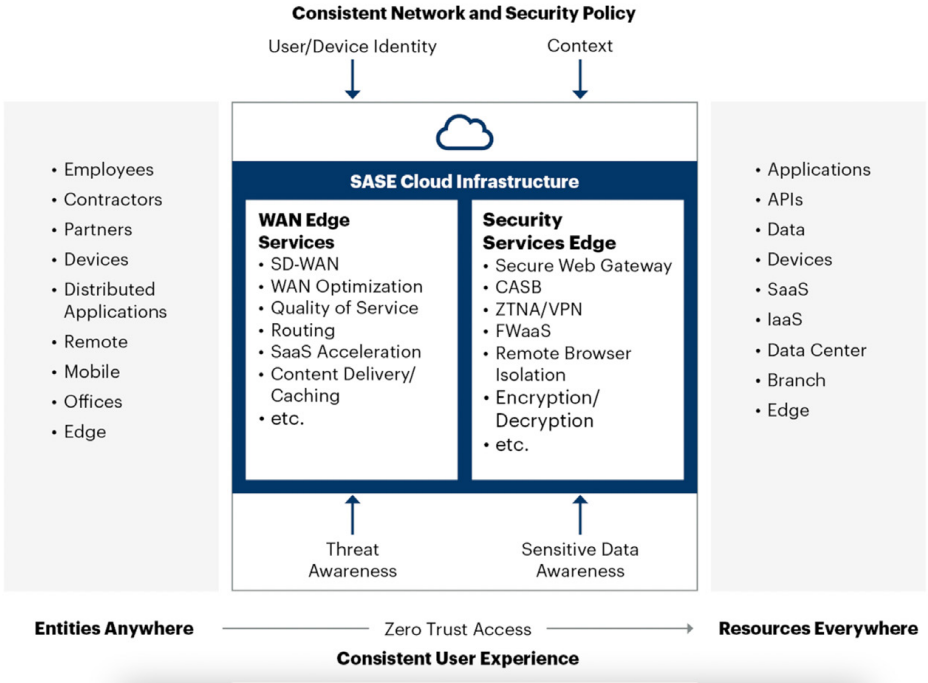
In parallel, industry analysts have acknowledged this pivotal move towards cloud-based security solutions due to increased mobility and cloud adoption. They have pinpointed a new suite of technologies, known as Security Service Edge (SSE), that empowers teams to modernize their secure access strategies for all users, devices, and applications in a simple, consolidated way. The HPE Aruba Networking SSE solution is a great fit for this evolution, offering universal secure access tailored to the needs of today's ever-changing business.

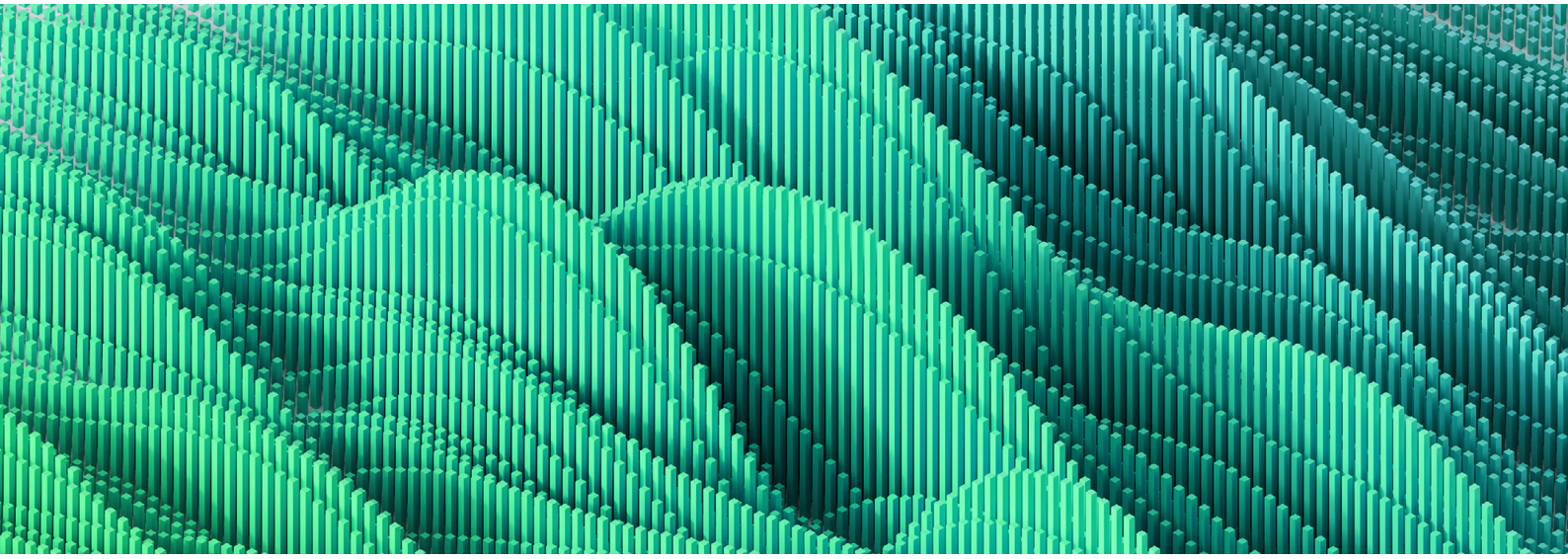
What is SSE?

Security Service Edge (SSE) is a comprehensive cloud-based solution that ensures secure access, visibility, and governance across all business applications. It represents a unified security model that integrates core security components such as: Zero Trust Network Access (ZTNA) for safeguarding private applications, Secure Web Gateway (SWG) for managing web access, Cloud Access Security Broker (CASB) for securing SaaS applications, and Digital Experience Monitoring (DEM) for ensuring an optimized digital experience across all access needs. This convergence of services epitomizes the future of secure connectivity — a singular, cloud-centric service that equips IT departments with the authority to regulate access to users and applications, irrespective of their physical location, the devices they use, or the networks they connect to.

While HPE Aruba Networking SSE might appear to be just one more acronym in the expansive IT lexicon, it is significant for any contemporary workplace, making up half of SSE, with the other half composed of WAN Edge Services.

SASE detailed view





Key technologies within HPE Aruba Networking SSE

- **Zero Trust Network Access (ZTNA)**
  A vast improvement over traditional VPN access to private applications, ZTNA extends application access to remote and hybrid users and allows access to only authorized resources after authentication. ZTNA essentially ensures that no user or device is trusted by default when accessing applications. Instead, all users and devices must pass robust identity verification processes to gain access to appropriate resources. Furthermore, least-privilege access is applied as users can access only the specified apps and data that admins permit.
- **Secure Web Gateway (SWG)**
  SWG is a core SSE service that manages internet access by applying company policies and preventing unwanted and unknown internet traffic from entering an organization's internal network. SWG protects users from accessing malicious websites, internet-spawned viruses, and malware, while still enabling users to access resources needed to get work done.
- **Cloud Access Security Broker (CASB)**
  CASB enhances the SSE security function. It enforces access and data loss prevention security policies as users and services access various corporate resources (whether cloud-based, private apps, etc.) and helps comply with company and industry security policies.
- **Digital Experience Monitoring (DEM)**
  DEM enables organizations to deliver a user experience that makes employees productive and safe. DEM monitors users' digital experience to ensure the system can handle spikes in CPU usage, network outages, and application performance challenges while giving IT visibility and metrics into each internet and network step.

The advantages of SSE

HPE Aruba Networking SSE provides a modern alternative to traditional network-based security technologies (firewalls, VPN gateway appliances, and web gateway appliances) and value for multiple teams.

The security advantages of SSE include:

- Provides universal secure access 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-privilege 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

The networking benefits of SSE are equally compelling:

- Supports all applications — legacy or cloud — with a single access solution
- Minimizes vendor sprawl and simplifies network services
- Never extends access to 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

SSE is revolutionizing the way businesses approach network security and connectivity, offering a more agile, secure, and efficient model that is well-suited to the demands of modern business.

Elements of HPE Aruba Networking SSE

HPE Aruba Networking **SSE cloud**

With over 500 global edge locations running on the backbone of AWS, Microsoft, Azure, and Google Cloud Platform™ the SSE cloud securely connects any authorized users to any business application, based on intuitive zero trust policies.

HPE Aruba Networking **user portal**

The end user's interface which, based on their identity and defined access policy, allows each user to see all their permitted agent or agentless applications — and easily connect to them with a click of a button.

HPE Aruba Networking **policy tags**

The HPE Aruba Networking SSE logical tagging system helps IT admins define granular, zero trust policies in minutes. Policies can be defined by groups of apps, individual apps, groups of users, individual users, location, device posture, and much more — making policy setting simple.

HPE Aruba Networking **SSE agent**

The HPE Aruba Networking SSE agent is a lightweight agent that runs on the end user's machine. The SSE Agent performs device posture analysis, encrypts traffic, and then automatically forwards traffic to the HPE Aruba Networking SSE cloud. The SSE Agent continuously adapts access rights based on changes in context and supports applications that require thick client access. The SSE agent can even support VoIP (peer-to-peer) and server-initiated (ICMP) flows. For web-based applications, no agent is required; instead, users can leverage agentless access with a simple browser.

HPE Aruba Networking SSE connector

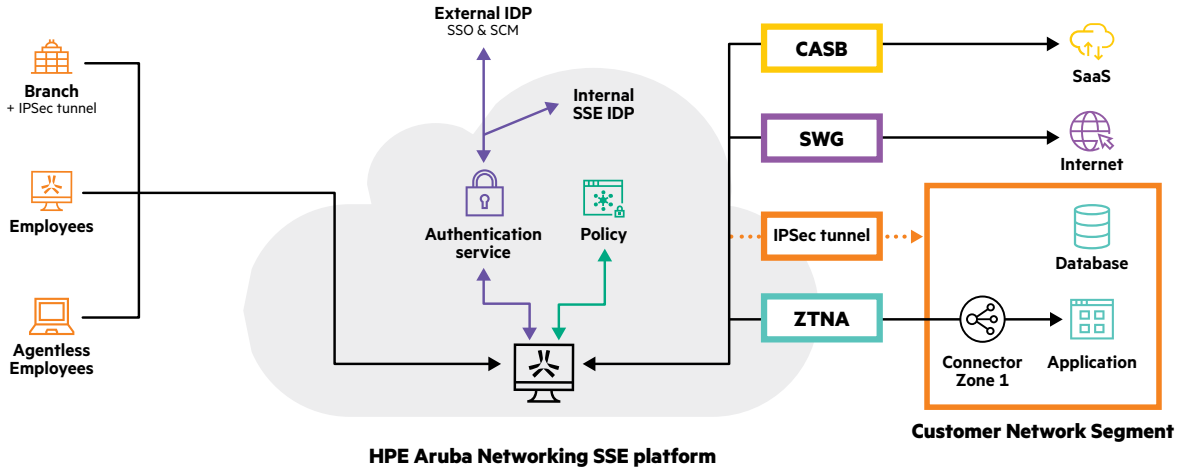
Often deployed in pairs, the HPE Aruba Networking SSE connector is a lightweight VM that frontends your private applications when specifically leveraging the ZTNA service. The SSE connector provides a secure, outbound-only, authenticated connection between the application and only the HPE Aruba Networking SSE Cloud. The SSE connector cloaks the location of your network and apps and never exposes IPs, minimizing attack surface and risk of internet-based attacks. Additionally, the SSE connector is the key to granting users applications without network access and eliminating risk of lateral movement by establishing one-to-one connections.

How does HPE Aruba Networking SSE work?

HPE Aruba Networking SSE is designed to provide comprehensive security for organizations within a single solution as they access various applications, whether on the web, in the cloud, or privately hosted. Here's how:

1. **User attempts to access application:** A user tries to access a business application from any location around the globe.
2. **HPE Aruba Networking SSE mediates request:** The request is received by the closest of our 500 edge locations which allows teams to avoid pass-through connections that can lead to risk. SSE becomes the first stop and mediates all access requests at scale.
3. **User is identified and authenticated:** The SSE platform leverages SAML and SCIM attributes from either an internal or external IdP provider to identify the user or entity trying to access a resource. This could be an employee, third party, or partner.
4. **Zero trust policies are enforced:** The SSE platform enforces access policies based on context, such as the user's identity, device posture, user location, etc. SSE policy enforcement is built on zero trust principles, which means users are granted access only to the specific resources the user is permitted to use. Zero trust access is enforced across all application types including private applications, SaaS applications, and internet browsing.
5. **Data is checked for threats:** The HPE Aruba Networking SSE platform scans all traffic for threats with universal SSL inspection, data loss prevention, URL filtering, malware and anti-virus scanning, and sandboxing. The SSE platform also includes Firewall-as-a-Service (FWaaS) capabilities that protects against external threats and data exfiltration.
6. **The fastest access path is identified:** The SSE service leverages smart routing across the multi-cloud architecture (AWS, Azure, GCP™) which automatically identifies the most optimized access path across our 500 global edge locations across the globe.
7. **Access is granted to the user:** Once identified, verified, and deemed secure, access to the specific resource is granted to the user via the fast access path.
8. **Access is continually monitored and controlled:** The SSE platform doesn't stop once the secure connection is established, but continuously monitors the user activity and transactions ensures that any suspicious behavior is detected and controlled.
9. **Access is adapted based on changes to context:** The HPE Aruba Networking SSE platform adapts to ongoing threats and changes in user behavior, device posture, etc., to minimize risk and maintain a robust security posture.

Throughout this process, the SSE solution provides visibility and control over all interactions between users and applications, maintaining security without compromising the user experience



What makes HPE Aruba Networking SSE unique?

Not all SSE solutions are created equal, and the HPE Aruba Networking SSE solution was built from the ground up to serve customers in ways that other vendors do not.

Universal security: a new standard of safety

With HPE Aruba Networking SSE, you get complete security. It's a one-stop secure connectivity platform that secures access across every user, device, and app. Enjoy the ease of having everything in one place: one cloud, one interface, and one set of rules for full protection.

Simplified management: your command center

HPE Aruba Networking SSE makes managing security simple. With our intuitive single-pane-of-glass interface, you can improve operational efficiency and minimize administrative overhead. Our platform offers easy, yet granular, policy and access management, providing a streamlined yet detailed control over your entire business network.

Resilient multi-cloud architecture: the backbone of your business

Built to scale and for the cloud, HPE Aruba Networking SSE was designed to meet the growing and evolving performance needs of your business. Our multi-cloud SSE architecture is scalable and flexible, built on the most reliable cloud platforms (AWS, Azure, and GCP), and boasts more than 500+ global edge locations, bringing secure access as close to the end-user as possible.

Smart Routing: the fast track to connectivity

Intelligence is woven into the nature of the HPE Aruba Networking SSE platform. Connectivity is automatically optimized by finding and connecting global users to the least latent route across all global edge locations, improving performance and reducing downtime. This smart platform shows its strengths in a few key ways:

- **Accelerated multi-region access:** HPE Aruba Networking SSE connects users to apps quickly by finding the shortest path to the closest app version, making things more reliable and improving the experience.
- **TCP optimizations:** The HPE Aruba Networking SSE solution keeps connections stable and consistent by adjusting how data packets are sent. This is crucial for keeping apps running smoothly and making sure users have a great experience.

These key aspects of HPE Aruba Networking SSE deliver benefits like better security, performance, and management, all leading to a great experience for users and IT admins and more efficient operations.

HPE Aruba Networking's ZTNA is designed to meet the demands of the modern, hybrid workforce, providing fast, secure access to business resources while maintaining visibility and control for IT departments.

Solution overview

Zero Trust Network Access (ZTNA)

As more organizations are supporting increasingly mobile workforces and furthering their cloud adoption, a corresponding number of teams are struggling to achieve the same level of security and control that they once had as they face this new frontier. HPE Aruba Networking's ZTNA is a modern solution designed to provide secure access to private applications. As part of the broader SSE framework, our ZTNA ensures that only authorized users can access authorized private applications, thereby reducing the attack surface and enhancing security. ZTNA operates on the principle of "least privilege access," meaning users are granted the minimum level of access necessary to perform their tasks.

The ZTNA service supports a wide variety of applications with or without an agent, including both modern web apps and legacy thick client apps. Users benefit from fast access to both on-premises and cloud-based apps without having to undergo repetitive logins or know the location of the app, creating a seamless access experience. Additionally, ZTNA offers adaptive access controls that continuously evaluate the context of access requests, adjusting permissions dynamically based on user behavior and other factors.

By moving away from traditional VPN solutions, ZTNA provides granular, policy-based access control aligned with Zero Trust Security. HPE Aruba Networking's ZTNA is designed to meet the demands of the modern, hybrid workforce, providing fast, secure access to business resources while maintaining visibility and control for IT departments. This approach not only enhances security but also improves the overall user experience by ensuring quick and reliable access to necessary applications.

Key ZTNA features and functions

Secure access to all private apps

Secure access to all private applications, including modern web apps (SSH, RDP, Git, DB, etc.) or legacy thick-client apps (VoIP, ICMP, AS400, etc.).

Agent or agentless access

Access private apps with or without an agent. Integrations with any SSO solution create a frictionless user experience.

Minimized attack surface

Minimize attack surface by eliminating any exposed network and app IPs. Make your network invisible to the open-internet and threat actors alike, while granting users access to specific access to private apps, never full network access.

Least-privilege access

Easy zero trust policies based on identity and adaptive context allow organizations to simply enforce least-privilege access down to an application level. No complex micro segmentation needed, just zero trust enforcement.

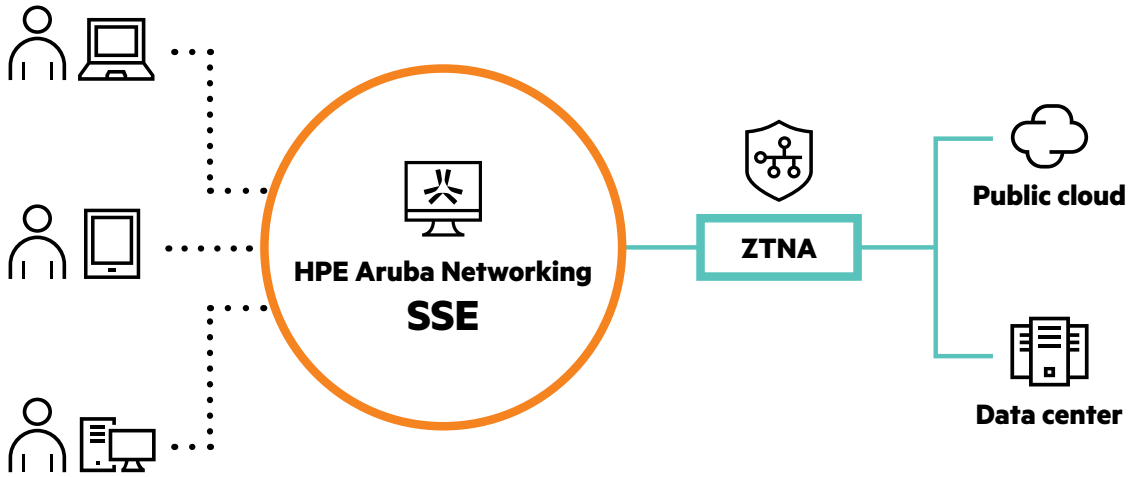
SSL inspection for private apps

Leverage SSL inspection at scale to determine who accessed what URLs, view downloaded files, see commands used, and receive alerts.

Supports all ports and protocols

Unlike other ZTNA solutions, our ZTNA fully replaces VPN as it supports all ports and protocols, enabling organizations to invest in technologies and platforms that truly help consolidate and eliminate the need for legacy technologies.

How does ZTNA work?



1. **A user attempts to access a private app**
   Secure access to all ports and protocols — even VoIP and ICMP — and support agent and agentless access.
2. **ZTNA service mediates the request**
   Instead of pinging the VPN concentrator on the corporate network, the request comes straight to the HPE Aruba Networking SSE platform for evaluation.
3. **ZTNA service validates identity and policy**
   Verify user identity and enforce zero trust policy. Permissions will automatically adapt access rights based on real-time changes in context (device posture, location, etc.).
4. **ZTNA identifies nearest SSE connector**
   Once access is granted, the SSE cloud signals the nearest SSE connector — which exclusively communicates with the SSE cloud — to establish a secure, outbound connection to the private application.
5. **ZTNA securely connects to resource**
   The ZTNA service stitches connectivity between user and application with an outbound connection. This makes private apps invisible to the internet, keeps users off the network, and delivers a safer connection to valuable applications.
6. **ZTNA inspects traffic and monitors user experience**
   The ZTNA service continues to inspect private app traffic and user behavior to detect and alert on potential threats, all while enhancing the overall user experience.

Benefits of ZTNA

- **Universal access made simple:** ZTNA simplifies access to business resources by providing a consistent and seamless connection experience, regardless of the user's location. Whether employees are working from home or the office, ZTNA ensures they have fast and reliable access to all necessary business resources.
- **Faster access speeds:** ZTNA enhances productivity by optimizing the routing of traffic to ensure the quickest and most efficient path to the required resource is used. This is achieved without the need for manual intervention from users or IT staff, reducing traffic latency and improving overall performance.
- **Reduced attack surface with zero trust:** By adhering to the principle of "never trust, always verify," ZTNA minimizes the attack surface. It conceals private resources from the internet and enforces least-privilege access, ensuring that only authorized users can access the network and its resources. This approach significantly reduces the risk of unauthorized access and potential breaches.
- **Reduce management overhead:** ZTNA can streamline the management of remote access. It eliminates the need for traditional VPN solutions and much of the associated inbound security stack. Organizations can manage all aspects of remote access — policies, applications, devices, users, and data — through a single interface, simplifying administration and scaling as needed.

Secure Web Gateway (SWG)

HPE Aruba Networking's SWG is a next-generation Secure Web Gateway service designed to make securing access to the internet effortless and safe for all work locations. The cloud service acts as a security broker between an organization's mobile users, offices, branches, and the open internet. HPE Aruba Networking SSE inspects internet traffic and brokers the fastest connection possible via cloud, allowing companies to replace various network-centric outbound gateway appliances as part of a larger SSE platform.

Our SWG solution offers fluent SSL traffic inspection with a proxy architecture that auto-mediates connections to the internet. The SWG service provides tunable access controls, applying zero trust to internet and SaaS access while protecting users from threats. Additionally, it includes data protection features, giving visibility into user activity and applying inline DLP controls to prevent data leakage. The SWG service also facilitates easy detection and prevention of sophisticated attacks with threat intelligence protection, malware and anti-virus scanning, cloud firewall functionality, and real-time sandboxing.

Key SWG features and functions

DNS/URL filtering: Proactively blocks access to malicious sites and content, safeguarding your network's integrity and user data. It works by intercepting DNS queries and analyzing the URLs against a continuously updated database of known malicious sites. If a match is found, access to the site is blocked, preventing potential security breaches.

Threat intelligence protection: Utilizing advanced algorithms and real-time threat data, this protection layer blocks access to risky URLs and domains. It assesses the content, domain details, and reputation score of each site. Sites with suspicious or malicious characteristics are restricted, thereby reducing the risk of cyber threats.

DLP for internet access: DLP prevents sensitive data from leaving the confines of the business, even for internet traffic. DLP for internet access uses Data Security Profiles, which define what constitutes sensitive data, and employs Regex Pattern Matching to scan and detect any data that matches these profiles. When a match is found, predefined actions are enforced to control the data flow and mitigate the risk of data leaks.

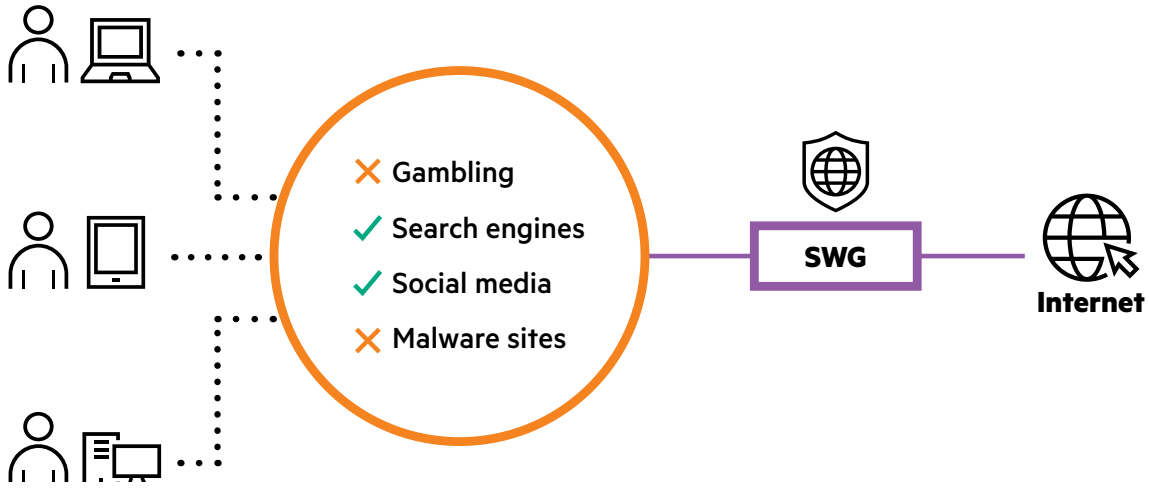
Malware and anti-virus scanning: Protect against known viruses and malware by using hash matching and antivirus (AV) scanning techniques. Files and data packets are scanned

against a database of signature hashes known to be associated with malware. If a hash match is found, the file is flagged as malicious and appropriate actions are taken to neutralize the threat.

Cloud firewall (FWaaS): The cloud firewall, or Firewall-as-a-Service, filters network traffic within the SSE cloud. It supports all ports and protocols, providing granular control over network access. Policies can be configured to allow or deny traffic based on various criteria, ensuring that only legitimate traffic is permitted, and potential threats are blocked.

Real-time sandbox: The sandbox feature offers real-time scanning of files in a secure, isolated environment with both fast and deep analysis options, ensuring comprehensive threat detection. It boasts a high-speed analysis with 99% of files examined in under a minute, maintaining operational continuity with no access downtime. This allows organizations to proactively defend against advanced cyber threats without disrupting user productivity.

How does SWG work?

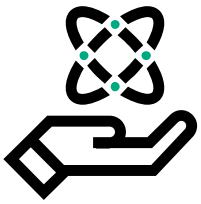


1. **Office or mobile employee attempts to access the internet**
   Traffic is automatically routed to the nearest edge location via the SSE agent.
2. **The SWG service proxies and inspects traffic**
   Traffic is identified as internet-bound and directed to the SWG service within the HPE Aruba Networking SSE cloud.
3. **SWG validates identity and applies policy**
   Apply security controls — like URL/DNS filtering, Threat Protection, Malware Scanning, Sandboxing, and cloud firewall — and block access to known malicious and risky sites.
4. **SWG fluently connects user to internet resource**
   After access controls are applied and internet resource has met security requirements, the user is delivered a safe, encrypted, connection to the internet.
5. **SWG remains in line and monitors user experience**
   If security posture changes, access will be severed automatically. Admins can view activity and ensure strong access performance.

Benefits of SWG

- **Visibility and control:** HPE Aruba Networking's SWG provides comprehensive visibility into internet traffic and user activity across the organization. This allows for detailed monitoring and control of web access, ensuring that only safe and compliant traffic is allowed. SWG helps in enforcing acceptable use policies and prevents access to malicious or inappropriate websites.
- **Data protection:** One of the primary functions of our SWG service is to protect sensitive data from being leaked or accessed by unauthorized entities. It does so by inspecting outgoing traffic for sensitive information and blocking such transmissions if they violate data protection policies. This is crucial for maintaining compliance with regulatory requirements and protecting intellectual property.
- **Detection and prevention:** Our SWG is equipped with advanced threat detection capabilities that can identify and block a wide range of cyber threats, including malware, phishing attacks, and other internet-based attacks. By analyzing web traffic, SWG can prevent these threats from reaching the users or compromising the network.
- **Security at scale:** As organizations grow and their operations expand, SWG scales to provide consistent security across all users and locations. Whether employees are working from the office, remotely, or using cloud services, SWG ensures that the same level of security is applied, protecting against threats regardless of where the traffic originates or where the users are located.

Cloud Access Security Broker (CASB)



Shadow IT refers to the use of applications and services without IT's explicit approval

HPE Aruba Networking's CASB is a modern Cloud Access Security Broker (CASB) solution designed to enhance cloud security and secure access to SaaS applications for organizations. Our CASB serves as the security mediator between users and SaaS applications, providing inline CASB protection for data in motion, effectively regulating data flows, uncovering shadow IT, and preventing data loss.

HPE Aruba Networking's CASB provides end-to-end visibility, allowing centralized management of user access, downloads, and sharing permissions. CASB's operation is straightforward: it proxies traffic to avoid risky pass-through connections, validates identities, applies policies, and securely connects users to resources while inspecting traffic and monitoring user experience.

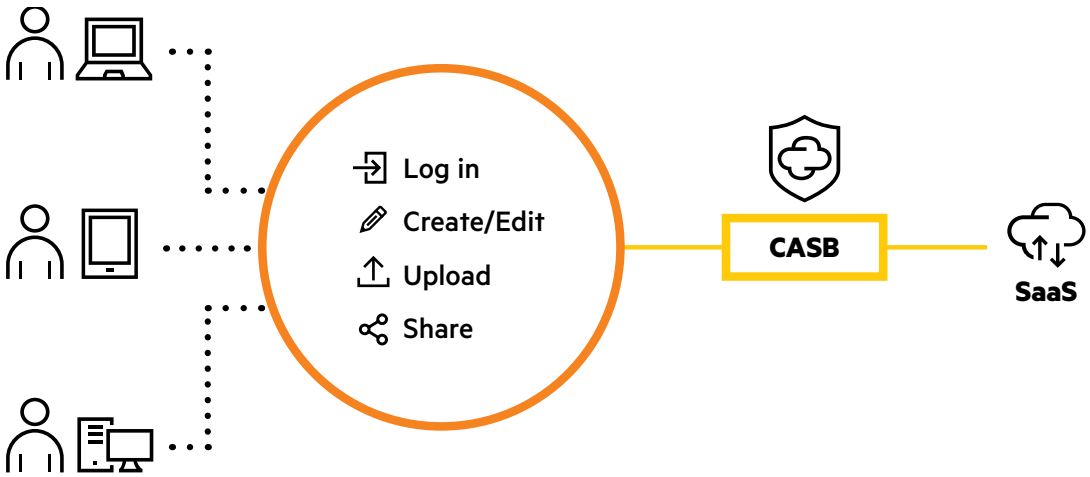
Emphasizing ease of use and scalability, our CASB delivers secure access to modern cloud services and applications. In our cloud-centric world, CASB as part of the broader HPE Aruba Networking SSE platform aims to deliver value with increased visibility, compliance, and data security from the outset.

Key CASB features and functions

- **In-line CASB:** HPE Aruba Networking's In-line CASB acts as a gatekeeper between your organization's users and SaaS apps/cloud services. Enforce security policies in real-time with in-line CASB as data moves to and from the cloud. This can include authentication, encryption, and other security controls.
- **SSL inspection for CASB control:** With SSL inspection for SaaS, teams can inspect encrypted SSL/TLS traffic to stop potential threats or data leakage before it happens. By decrypting the traffic, the CASB can apply security policies to protect sensitive data.
- **Unlimited SaaS apps for SSL inspection:** Our CASB offers unlimited capacity to inspect SSL/TLS traffic across any number of SaaS applications, ensuring comprehensive coverage without performance concerns.
- **Visibility into apps and shadow IT:** Gain visibility into SaaS apps and shadow IT to better understand and manage the risks associated with sanctioned and unsanctioned app usage.

- **Granular control of restricted actions:** With CASB, admins can set granular policies that restrict certain actions like uploading, downloading, sharing data, etc., from any SaaS application. This is an important requirement to protect against data loss and ensure compliance with various regulations.
- **DLP for SaaS-based apps:** DLP tools help protect sensitive data within SaaS applications by monitoring, detecting, and blocking potential data breaches or unauthorized access.
  - **DLP regex/dictionary matching:** DLP solutions can now use regular expressions (regex) and dictionary matching to identify and protect sensitive data. This allows for more granular and flexible data security policies that can match specific patterns or terms within files.
  - **OCR (Optical Character Recognition):** OCR technology converts images of text, such as scanned documents or photos, into editable and searchable data. This is particularly useful for processing documents that contain sensitive information like social security numbers.
- **Compliance with predefined and custom dictionaries:** Predefined and custom dictionaries can be created to ensure compliance with specific regulations like HIPAA, PCI DSS, GDPR, and NIST. These dictionaries contain terms and patterns that are unique to each regulation, helping organizations meet their compliance obligations.

How does CASB work?



1. **A user attempts to access a cloud service**
   User attempts to access a SaaS app or IaaS platform. Traffic is automatically routed to the nearest edge location via the SSE agent.
2. **The CASB service proxies and inspects traffic**
   Traffic comes straight to the HPE Aruba Networking SSE cloud and SSL inspection is performed.
3. **CASB validates identity and applies policy**
   In-line CASB and data protection controls — i.e., Upload, downloads, and share activities, Object Character Recognition, Compliance — are applied and access privilege automatically adapts based on real-time context changes.
4. **CASB securely connects to SaaS resource**
   With restricted actions in place, secure SaaS access is extended to the user while restricting unauthorized behaviors to prevent data loss and enforce compliance.
5. **CASB remains in line and monitors user experience**
   Admins gain visibility into all user activity while accessing the SaaS app. If security posture changes, or the user attempts unauthorized activity, access is reassessed, and admins alerted.

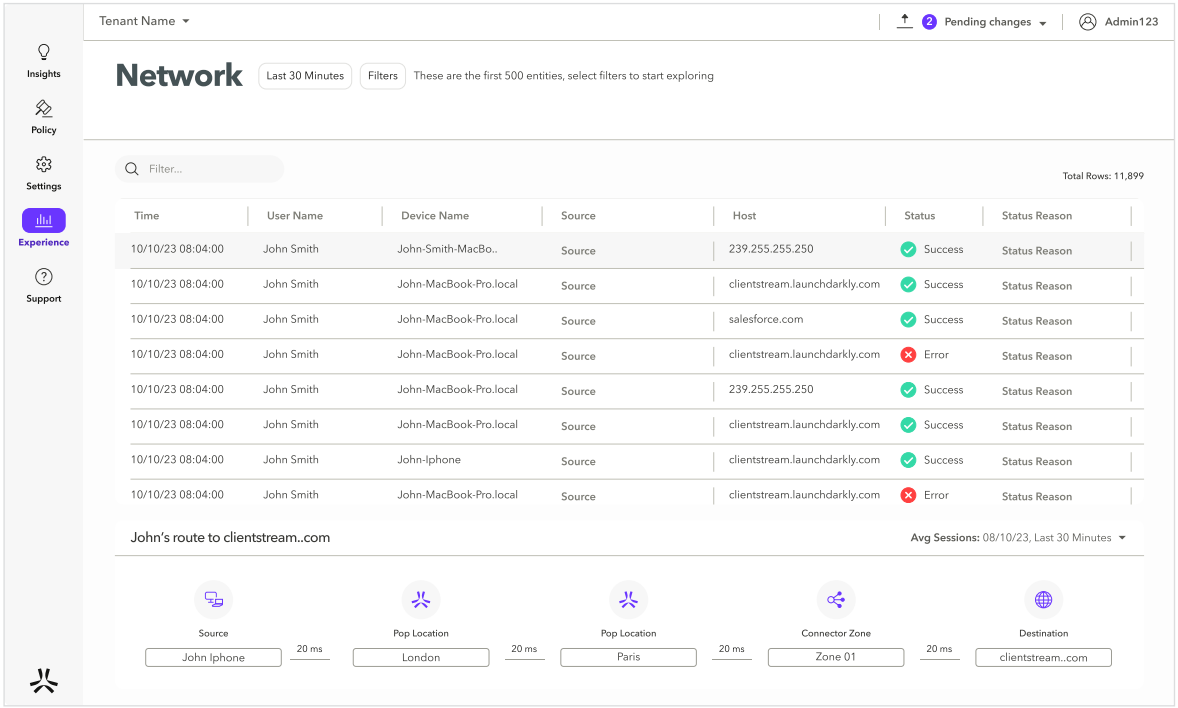
The benefits of CASB

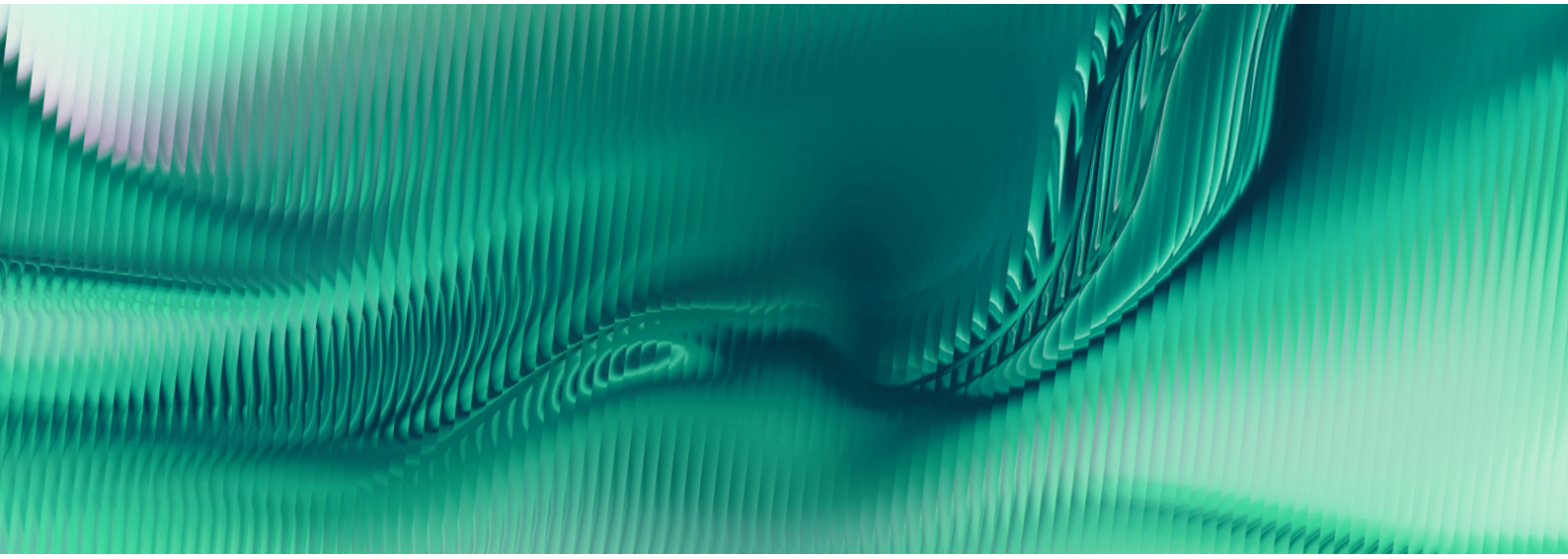
- **Enhanced data security:** HPE Aruba Networking's CASB provides real-time scanning and monitoring of data usage and flow to and from the SaaS provider. This includes DLP capabilities that protect sensitive data by preventing unauthorized sharing and ensuring that data security policies are enforced.
- **Visibility and control:** Organizations gain detailed visibility and control over their cloud environment with CASB. Teams can see all user traffic, identify which cloud applications people are using, and apply granular controls to manage how data is accessed and used.
- **Compliance:** Our CASB helps organizations comply with data privacy regulations by enforcing corporate cybersecurity policies across multiple cloud environments. They provide risk assessments and scores for users and applications, aiding in the management of compliance requirements.
- **Threat mitigation:** Our CASB offers protection against both known and unknown threats, including anti-malware and antivirus. CASB detects unusual behavior across cloud applications, identifying risks like ransomware, compromised users, and rogue applications, and can automatically remediate threats to limit organizational risk.
- **Operational efficiency:** By consolidating multiple types of security policy enforcement into a single point, CASB allows organizations to streamline their security operations. This integration simplifies the management of security policies and reduces the complexity of securing multiple cloud services.

Digital Experience Monitoring (DEM)

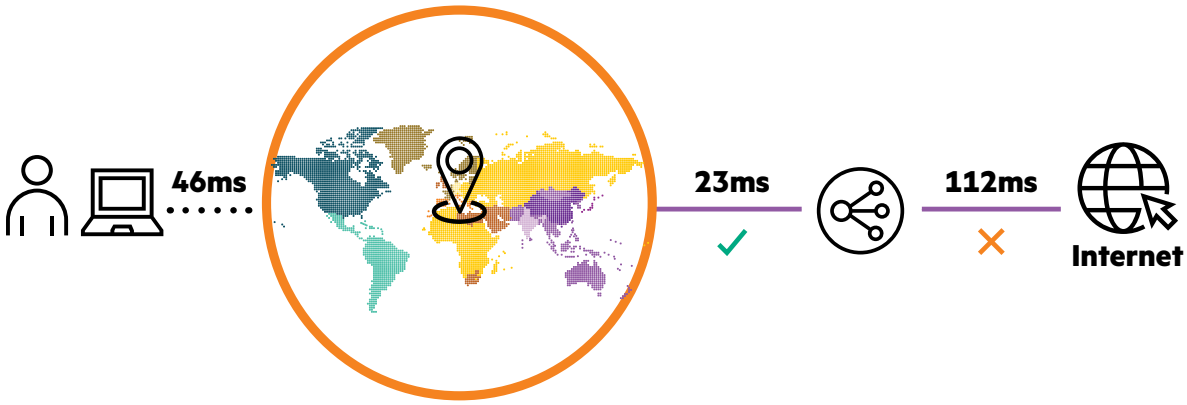
HPE Aruba Networking's DEM is a cloud-delivered Digital Experience Monitoring solution designed to ensure that IT helpdesks remain attuned to end-user device issues. By delivering a seamless and secure digital experience, DEM aligns with the business's need to optimize user experience and increase productivity through better digital experiences.

The platform uncovers performance dips and offers insights into users, departments, or geographies that may be experiencing performance issues. With endpoint telemetry, IT teams can view detailed metrics like CPU usage, resource consumption, memory usage, and Wi-Fi signal strength. Our DEM also features unified application health monitoring, continuously overseeing private, SaaS, and internet applications. Hop-by-hop network path metrics grant visibility into every internet and network hop between a user and business application, ensuring fewer user experience headaches and more peace of mind.





How does DEM work?



1. **A user attempts to access a resource**
   Traffic is forwarded through the HPE Aruba Networking SSE cloud.
2. **Security policies are enforced and user gains access**
   Access controls and policy enforcement take place and the user gains access to the authorized application.
3. **HPE Aruba Networking's DEM runs real-time analysis**
   The data is collected and analyzed in real-time to understand how users interact with the digital services and identify any performance slowdowns or application outages.
4. **Visualize latency identification**
   Admins can see hop-by-hop visibility where latency is occurring and granular visibility down to the individual user and session level.
5. **Experience is optimized for the end-user**
   Based on the insights gained, organizations can make informed decisions to improve their product development and optimize business operations. When issues are detected, DEM tools assist IT teams in quickly identifying the root cause, which speeds up the problem resolution process.

Key DEM features and functions

Network Experience Dashboard: A powerful dashboard that offers visibility into the network path data travels from users to business applications. It's designed to help network administrators quickly identify and pinpoint the cause of latency issues. By providing a detailed hop-to-hop analysis, the dashboard allows for a clear understanding of network performance and the identification of bottlenecks that could affect user experience.

User Experience Dashboard: This serves as a diagnostic tool that swiftly pinpoints latency issues from an individual user's perspective. It provides in-depth insights into each user's interaction with their applications and devices, highlighting areas that may impact performance. This dashboard is particularly useful for IT professionals looking to optimize the end-user experience and ensure smooth operation of business-critical applications.

No monitoring limits: HPE Aruba Networking's DEM is built to accommodate an expansive range of monitoring needs. This means there are no restrictions on the number of users or devices that can be monitored, allowing for scalability and flexibility in network management. Organizations can benefit from comprehensive monitoring capabilities without worrying about hitting any caps or limits.

Real-time probing: This feature sets our DEM service apart from others that rely on synthetic probes. By using real probes that monitor actual application access, the system provides a more accurate reflection of the application's performance and the real user experience. This method ensures that monitoring is based on genuine usage patterns, leading to more reliable data.

No limits to what apps are monitored: HPE Aruba Networking's DEM emphasizes the ability to monitor any application without the need for pre-configurations. Unlike other solutions, which require prior knowledge of the apps to be monitored, this feature allows for spontaneous and comprehensive monitoring of all applications, offering unparalleled flexibility and coverage.

The benefits of DEM

Unified visibility and improved user experience

HPE Aruba Networking's DEM allows administrators to visualize the hop-by-hop latency metrics a user is experiencing across their local internet, the point of presence location, the connector, and the application being accessed. This creates a unified picture of what an end user is experiencing and enabling improved user experience in a hybrid work environment.

Quick resolution for more productivity

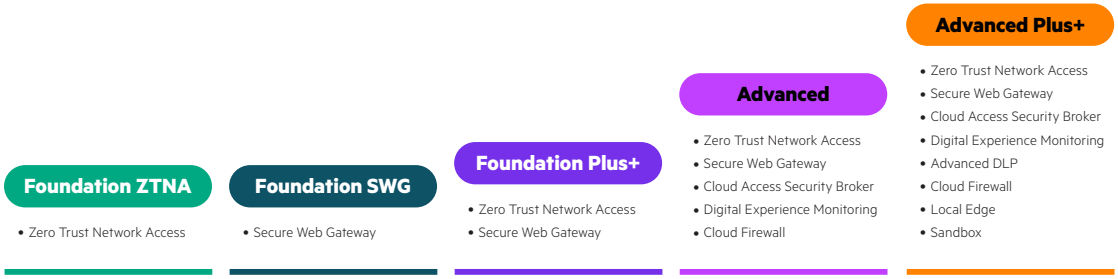
Gaining visibility into performance on unmanaged networks can be challenging; however, DEM allows administrators to quickly identify where a performance issue originates and quickly resolves network related support issues to significantly reduce the time to resolution across the network.

Less support tickets for hybrid work

Increased hybrid work has historically led to increased support tickets relating to network access and decreased visibility across remote network connection and end user experience. Our DEM helps bridge this gap to better support hybrid work across the enterprise.

HPE Aruba Networking SSE packaging

We offer a range of HPE Aruba Networking SSE packages to meet the specific needs of your organization.



Package/bundle	Foundation ZTNA	Foundation SWG	Foundation +	Advanced	Advanced +
Multi-cloud architecture Access to +500 global edge locations across the most reliable cloud providers — AWS, Azure, GCP	✓	✓	✓	✓	✓
Admin portal Centralized access management for admins through a unified UI to enforce zero trust policies across all business resources. (Admin RBAC controls available)	✓	✓	✓	✓	✓
User portal Secure, single access point for users to easily access all their authorized applications in one place	✓	✓	✓	✓	✓
SSE policy tags Smart tagging allows admins to set up granular zero trust policies with just a handful of rules, versus hundreds	✓	✓	✓	✓	✓
SSE agent Lightweight endpoint agent compatible with lap-tops, phones, and tablets devices and operating systems, including Windows, Mac, Linux®, Android™, and iOS	✓	✓	✓	✓	✓
SSE connectors Lightweight VM that front-ends apps to provide a secure, outbound-only, zero trust connection from authorized app to the SSE cloud. (Up to 1,000 connectors)	✓	✓	✓	✓	✓
Universal SSL inspection Enforce SSL Inspection at scale across all forms of traffic — private, SaaS, internet	✓	✓	✓	✓	✓
Analytics and reporting Real-time analytics of all traffic and user behavior within the SSE dashboard. Gain insights from high-level SSE dashboards down to granular individual session logs.	✓	✓	✓	✓	✓
Branch connectivity Secure branch connectivity for internet and internal traffic with IPSec support and easy integration with SD-WAN services	✓	✓	✓	✓	✓
Smart routing Optimize user connectivity through automatic routing across the fastest access path via 500+ edge locations	✓	✓	✓	✓	✓
Partner integrations Integrate with additional services within your Cybersecurity Mesh, such as SIEM, Identity, MDM, Endpoint, and various APIs	✓	✓	✓	✓	✓
Built-in identity Leverage our native HPE Aruba Networking IdP service within SSE — great for third-party access	✓	✓	✓	✓	✓
Multiple IdP support Effortless integration with one or more IdP providers of your choice and enable SAML/SCIM support	✓	✓	✓	✓	✓
Device posture Understand the security posture of end-point devices and enforce security based on their changing context	✓	✓	✓	✓	✓

Package/bundle	Foundation ZTNA	Foundation SWG	Foundation +	Advanced	Advanced +
Log streaming Easy integrate SSE with the SIEM provider of your choice and get even more out of your data with SYS Log and API integrations	✓	✓	✓	✓	✓
Custom block pages and user alerts Help users understand why access is denied with customized block pages and posture block notifications via the agent and minimize IT Tickets in the process	✓	✓	✓	✓	✓
ZTNA					
All ports and protocols Secure access to all private applications with support of all ports and protocols	✓	✗	✓	✓	✓
Robust agentless access Delivers agentless access to private apps for employees, third-parties and BYOD users with a simple web browser. Supported agentless apps: MS SQL, GIT, SSH, RDP, VNC, web apps	✓	✗	✓	✓	✓
Server-initiated flow Enable the support of legacy thick-client apps like VoIP and AS400 with Server-Initiated Flow.	✓	✗	✓	✓	✓
Multi-regional app support Apps in multiple regions are supported across multiple connector zones allowing the best access path to be selected based on latency	✓	✗	✓	✓	✓
DLP for private apps Enable session control and visibility for private applications. Apply DLP policies to scan traffic for malware, run sandbox, and control upload/download actions.	✓	✗	✓	✓	✓
Simplified domain setup Deploying apps with ZTNA is easy with both CNAME and DNS Rewrite. Rewrites eliminates the need for DNS changes allowing for faster application rollout.	✓	✗	✓	✓	✓
SWG					
DNS/URL filtering Proactively block access to malicious sites and content and protect your network integrity and user data	✗	✓	✓	✓	✓
Threat intelligence protection Use smart algorithms and real-time data to block risky URLs and domains based on their content, domain details, and reputation	✗	✓	✓	✓	✓
Data loss prevention (DLP) Prevent data leakage with use of Data Security Profiles, Regex Pattern Matching, and action enforcement for more control, and less risk	✗	✓	✓	✓	✓

Package/bundle	Foundation ZTNA	Foundation SWG	Foundation +	Advanced	Advanced +
Malware and anti-virus scanning Protect against known viruses and malware through repeatable hash and AV scanning — Database signatures	✗	✓	✓	✓	✓
Cloud firewall FWaaS filters network traffic in the SSE cloud and supports all ports and protocols and allows/denies access	✗	✗	✗	✓[1]	✓[1]
CASB					
In-line CASB Track and control activity for over 10,000 SaaS applications with no limit on SSL inspection	✗	✗	✗	✓	✓
Compliance and regulations Predefined Dictionaries and Custom Dictionaries help meet compliance standards (i.e., HIPAA, PCI-DSS, GDPR, NIST)	✗	✗	✗	✓	✓
Advanced DLP Adding to DLP functionality, advanced DLP includes Optical Character Recognition (OCR)	✗	✗	✗	✗	✓
DEM					
Network experience dashboard Gain visibility into the hop-to-hop path between users and business apps and quickly identify and pinpoint the cause of latency issues	Add-on purchase	✗	Add-on purchase	✓	✓
User experience dashboard Swiftly pinpoints latency issues from an individual viewpoint, offering detailed insights into each user's interaction and their devices	Add-on purchase	✗	Add-on purchase	✓	✓
HPE Aruba Networking SSE Add-ons					
Sandbox Test files with real-time sandbox scanning, offering both Fast and Deep Scanning options, while ensuring 99% of files are analyzed in under a minute with no downtime	✗	Add-on purchase	Add-on purchase	Add-on purchase	✓
Local edge Deploy your own software-based SSE Local Edge and bring access even closer to your users and devices at the network's edge (Unlimited number of local edges)	Add-on purchase	✗	Add-on purchase	Add-on purchase	✓
Managed connectors The Managed Connectors service deploys dedicated connectors for organizations, providing them with a Static IP for streamlined access	Add-on purchase	Add-on purchase	Add-on purchase	Add-on purchase	Add-on purchase
Site-based subscription					
SWG bandwidth Gain SWG protection from any HQ, branch, or remote location with dedicated tunnels and no agent requirement. SWG bandwidth includes all Foundation SWG features and is based on consumption, not user licenses. Available individually or with an SSE bundle.	✗	Add-on purchase	Add-on purchase	Add-on purchase	Add-on purchase

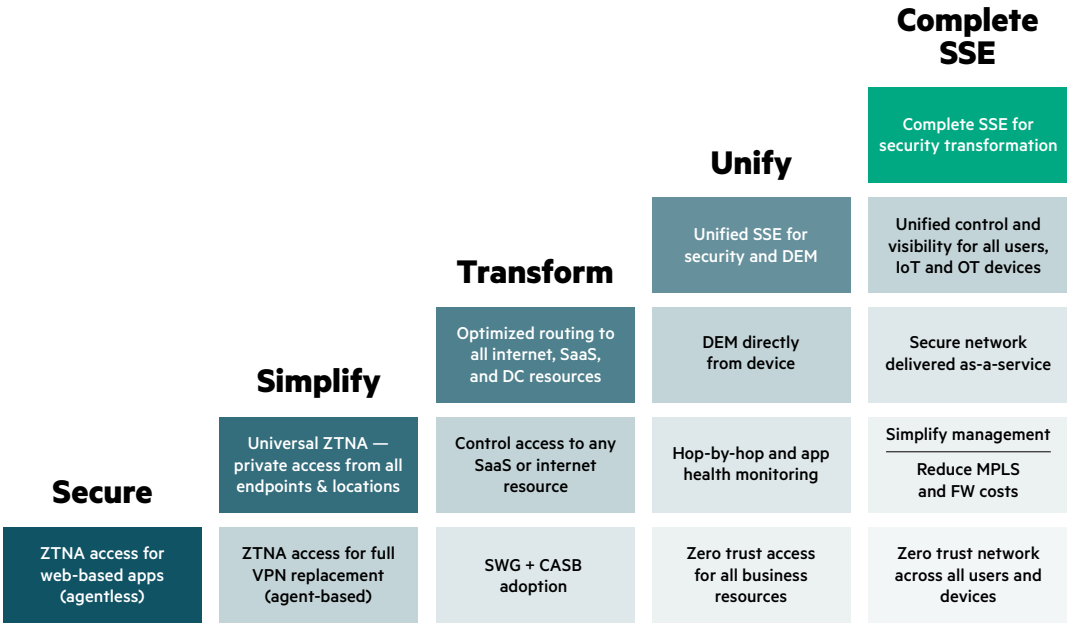
[1] Future availability

Customer success packaging

Package/Bundle	Basic	Select	Premier
Support coverage	Business hours **8am-8pm | Mon-Fri**	24x7x365	24x7x365
Support portal	24x7x365	24x7x365	24x7x365
Architecture and deployment services	N/A	Add-on	Included
Service level agreement	Standard per terms	Standard per terms	Enhanced
Designated customer success manager	N/A	N/A	Included
Deployment health checks	N/A	Add-on	Included Bi-annual
Response time SLA			
Critical	1 Hour	1 Hour	30 Minutes
High	2 Hours	2 Hours	1 Hour
Medium	8 Hours	8 Hours	4 Hours
Low	Next Business Day	Next Business Day	8 Hours

Getting started with HPE Aruba Networking 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 (See below example).



With SSE, security and networking teams no longer must worry about the words “anywhere” and “everywhere”. SSE services like ZTNA, SWG, and CASB allow organizations to gradually substitute outdated security technologies and processes with more efficient, contemporary ones. These modern methods not only promptly tackle urgent security and user requirements, but also offer a flexible platform to cater to future needs.

While most organizations will choose a step-by-step approach to SSE, building on deployment success as they go, the long-term successful implementation of SSE requires an ongoing combination of strategic decisions, technical solutions, user involvement and education, and continuing management and refinement.

In other words, SSE success is a process, one that can quickly start and finish depending on which SSE provider you choose to partner with. Consider HPE Aruba Networking SSE for your SSE project and we’ll walk with you every step of your deployment.

Learn more about HPE Aruba Networking SSE

Connect with an SSE Expert

Take SSE for a free 24-hour test drive

HPE Aruba Networking SSE

Make the right purchase decision.
Contact our presales specialists.

Chat now (sales)

Call now

Visit **ArubaNetworks.com**

Get updates

Hewlett Packard Enterprise

SO_SSE-Overview_A4_RB_102424 a00141561ENW