HPE aruba networking

Solution overview

MODERNIZING SECURITY AND CONNECTIVITY WITH UNIFIED SASE

HPE

The shift to distributed, cloud-first enterprises

Enterprise networking and security are rapidly evolving as applications move to SaaS and public clouds, users work from anywhere, and device diversity expands to include contractors, guests, and IoT. Yet many security architectures still rely on perimeter-based models or loosely connected zero trust tools.

This fragmentation creates complexity, blind spots, and inconsistent policy enforcement—especially for unmanaged and IoT devices—while forcing IT teams to manage multiple consoles and frameworks, increasing risk.

HPE Aruba Networking unified SASE simplifies the journey to SASE and zero trust by replacing disconnected solutions with a single, integrated platform built for cloud-first, hybrid enterprises.

Rethinking zero trust: from fragmentation to integration

Zero trust is recognized as the right security model for today's environments. But many implementations address only parts of the problem like remote access or identity, while leaving networking, device visibility, and cloud security disconnected. As hybrid work and distributed environments expand, these gaps increase risk and operational overhead.

HPE solves this with a fully integrated, edge-to-cloud zero trust platform that combines a single-vendor SASE solution and AI-powered NAC. This enables a universal ZTNA model where identity, device posture, and access policies are enforced consistently across all users and devices—managed or unmanaged, remote or on-premises—eliminating blind spots and simplifying operations from the branch to the cloud.

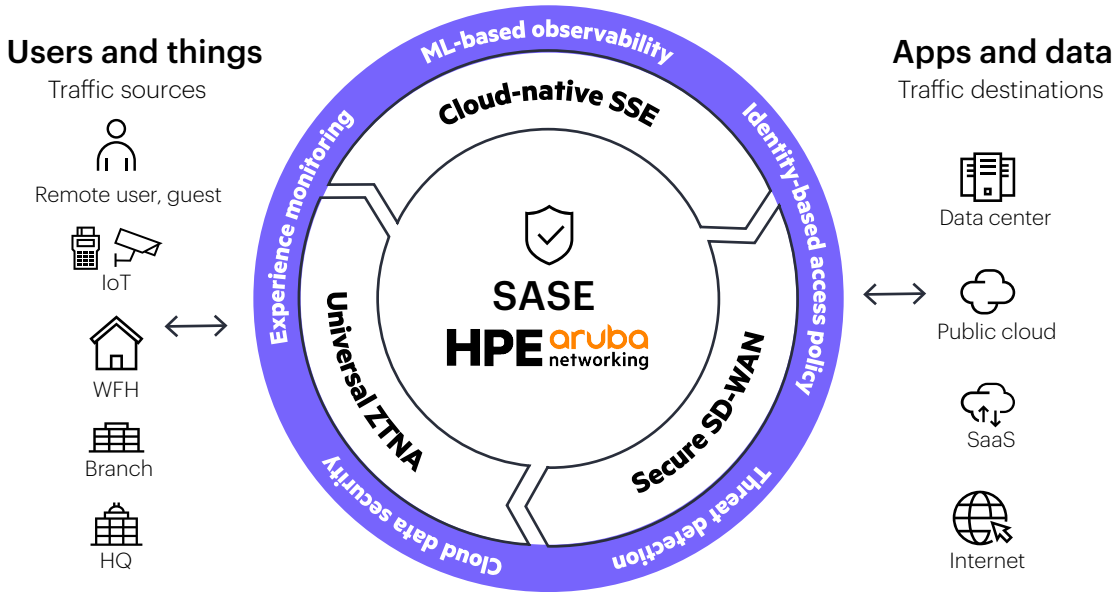

Figure 1. Deliver comprehensive zero trust principles across users, devices, applications, and data

A unified SASE platform, designed end-to-end

At the heart of HPE's strategy is a single, cohesive SASE architecture that integrates SD-WAN, cloud-native SSE services, and AI-powered device intelligence into one platform. Unlike multi-vendor SASE solutions built from loosely connected components, HPE Aruba Networking unified SASE is designed, built, and operated as an integrated system.

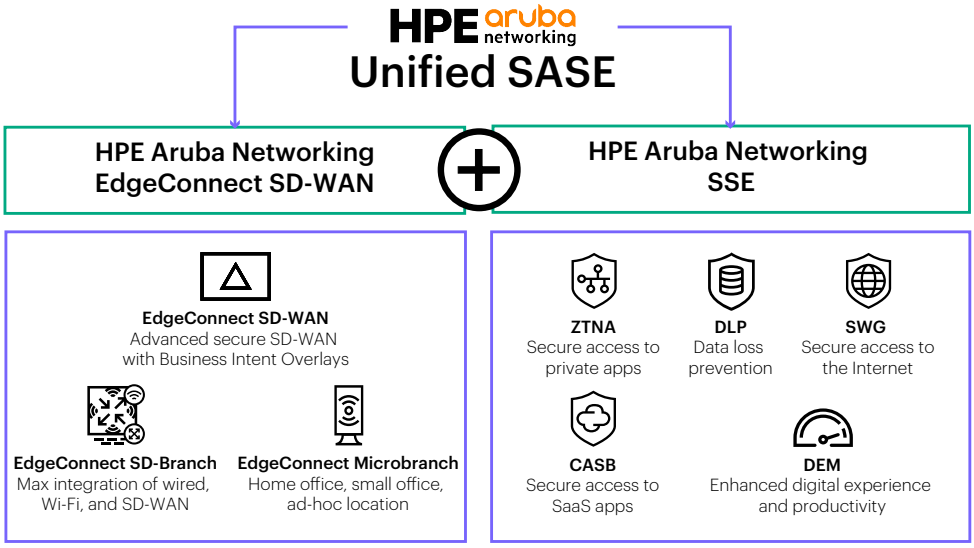

Figure 2. HPE Aruba Networking unified SASE integrates SD-WAN and SSE in a cohesive platform

A key differentiator is the native, fully automated integration between HPE Aruba Networking EdgeConnect SD-WAN and HPE Aruba Networking SSE. While many vendors rely on API stitching, manual policy synchronization, or service chaining, HPE eliminates these operational dependencies.

Integration is automated end-to-end, with instant connectivity between the edge and the SSE cloud. No manual tunnel configuration, policy translation, or synchronization is required, reducing risk and accelerating deployment.

Key advantages of HPE Aruba Networking unified SASE

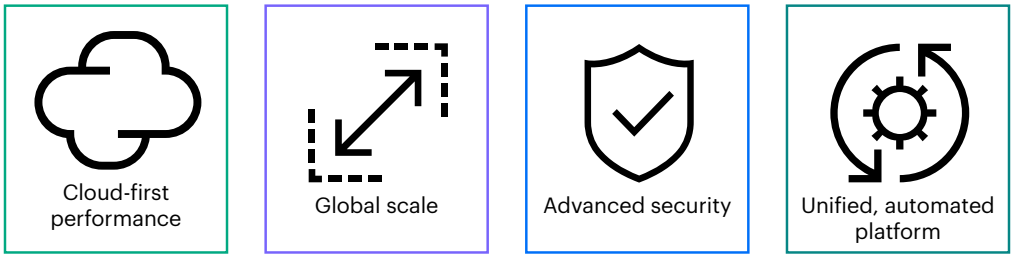

Figure 3. The key advantages of HPE Aruba Networking unified SASE

Cloud-first performance for modern applications

Performance is critical in SASE architectures, where security must not add latency or degrade user experience. HPE Aruba Networking EdgeConnect SD-WAN is built for cloud-first traffic, using business-driven policies to avoid backhauling and deliver consistent application performance.

The first-packet iQ feature identifies thousands of applications and domains on the first packet, enabling intelligent traffic steering. With this feature, organizations can build security policies that send trusted cloud application traffic, such as UCaaS traffic, directly to the internet, while all other traffic, is sent to an SSE (security service edge) solution for security inspection before it is handed off to the SaaS provider or to the data center.

EdgeConnect SD-WAN also natively integrates with leading cloud providers like AWS, Microsoft Azure, Google Cloud™, and connectivity partners like Equinix and Megaport, improving branch-to-cloud performance, reliability, and user experience.

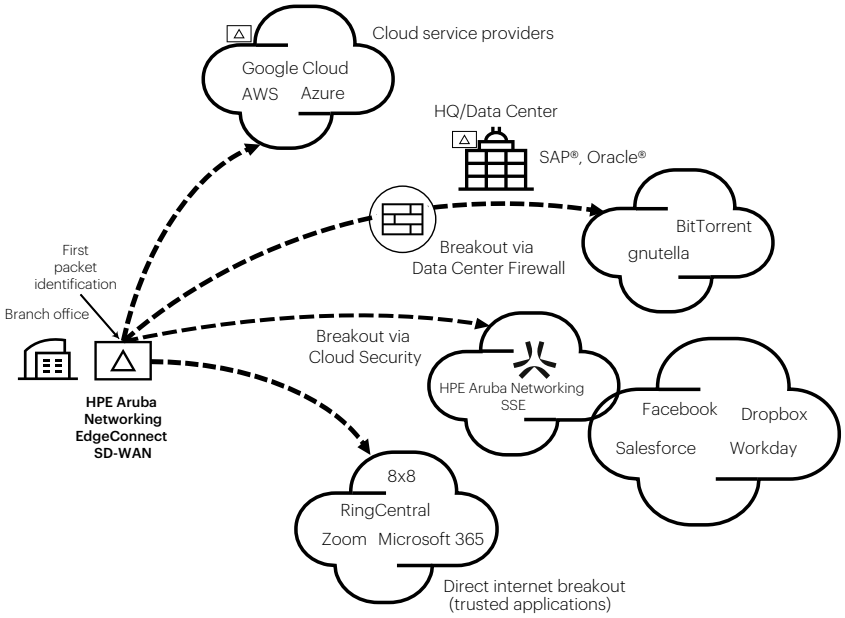

Figure 4. Intelligently steer traffic from the branch to the cloud with first-packet identification

Additionally, the SD-WAN solution provides WAN modernization capabilities that help organizations transition from traditional MPLS architectures to cloud-first networks using more flexible and cost-effective internet connectivity:

— **Business Intent Overlays** allow teams to define networking requirements in terms of application performance, security posture, and business priority, enabling the platform to dynamically enforce intent across the network without managing complex routing tables.

— **Tunnel bonding** aggregates multiple WAN links into a single logical overlay, with real-time traffic steering across broadband, MPLS, or mixed links based on business policies. If a link experiences degradation or failure, traffic automatically shifts to remaining paths or backup connections to ensure continuous connectivity.

— **Path Conditioning** delivers private-line performance over standard internet circuits by mitigating packet loss, jitter, and latency, reducing dependence on MPLS while maintaining predictable performance for real-time and mission-critical applications. Forward Error Correction (FEC) restores lost packets without retransmission, while Packet Order Correction (POC) ensures proper sequencing across bonded links. AppExpress further enhances performance by monitoring application experience and automatically selecting the optimal path when degradation is detected.

— **WAN optimization**, including TCP acceleration, compression, and deduplication, further improves responsiveness for distributed users and bandwidth-constrained environments, while also reducing latency.

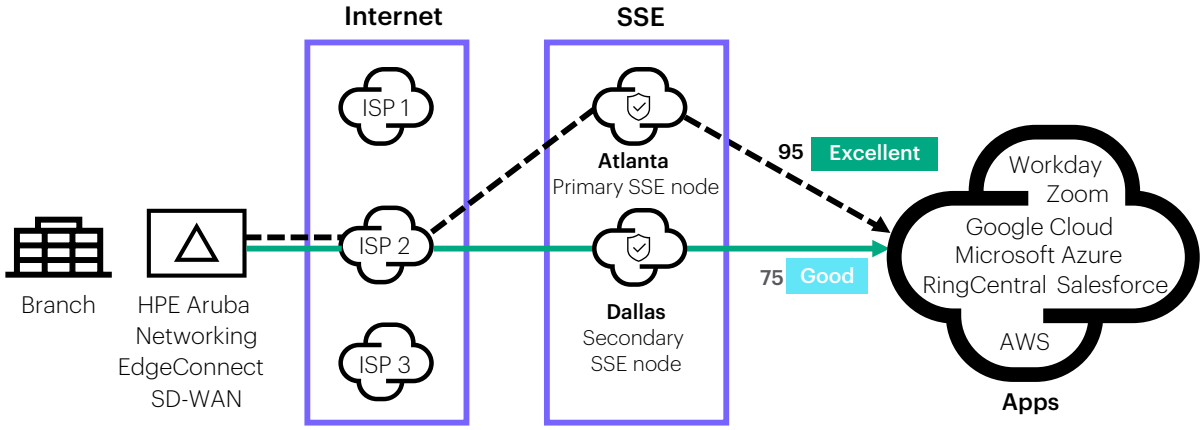

Figure 5. Optimize user experience for business-critical applications with AppExpress, even across SSE routing

Integrated branch security with advanced NGFW capabilities

While cloud-delivered security is essential, branches and campuses still require strong local protection. HPE addresses this need by embedding next-generation firewall (NGFW) capabilities directly into the SD-WAN fabric. This integrated stack delivers stateful firewalling, IDS/IPS, role-based segmentation, URL filtering, and adaptive DDoS protection in a single SD-WAN platform, eliminating legacy branch firewalls and reducing operational complexity.

— **IDS/IPS:** Uses signature-based detection to identify known threats and supports both inline blocking and out-of-path analysis for high-performance environments. Events can be forwarded to SIEM platforms such as Splunk for real-time visibility and response.

— **Adaptive DDoS:** Uses machine learning to automatically adjust DoS thresholds based on real-time traffic patterns, eliminating manual tuning. Auto Rate-Limiting establishes dynamic baselines, while Smart Burst redistributes unused capacity across firewall zones to maintain protection.

— **URL filtering:** Blocks malicious and high-risk sites using machine learning to classify domains and URLs into categorized risk levels. Reputation scoring and real-time IP intelligence help identify emerging threats and enforce policy consistently.

— **Role-based segmentation:** With security embedded in the SD-WAN fabric, east-west traffic, IoT communications, and local internet breakout are protected by default. Centralized segmentation across the LAN and WAN enforces consistent policies, with ClearPass adding identity and role context, without complex VLAN architectures.

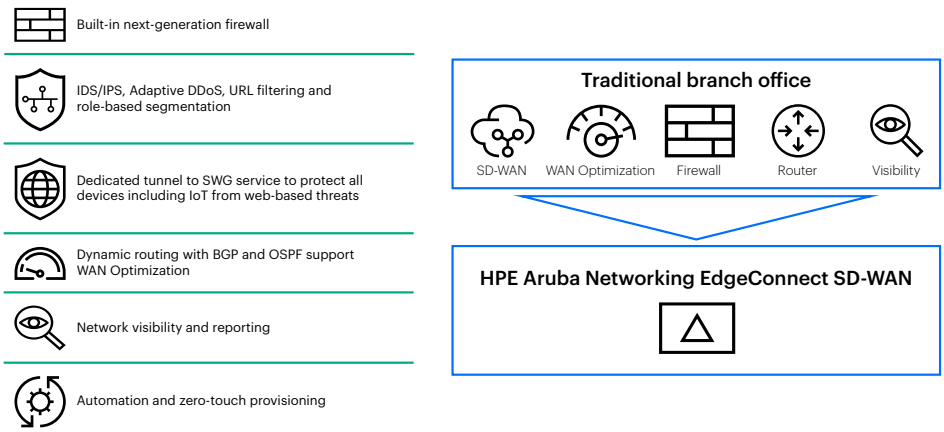

Figure 6. Consolidate branch equipment by replacing legacy firewalls and routers with a secure SD-WAN such as HPE Aruba Networking EdgeConnect SD-WAN

Deep integration with cloud-delivered secure web gateway (SWG)

One critical gap in many SASE and zero trust architectures is protecting devices that cannot run endpoint agents, such as IoT sensors, printers, cameras, medical devices, industrial systems, and guest endpoints.

HPE addresses this by combining role-based segmentation with deep integration to its cloud-delivered SWG. This unified approach provides malware protection, web filtering, and threat prevention for all devices—managed or unmanaged, without requiring an SSE agent. Traffic from these devices is automatically routed through a dedicated tunnel via EdgeConnect SD-WAN, ensuring consistent network-level protection without installing agents on each device. This agentless model helps organizations secure an expanding IoT attack surface, gain visibility into device behavior, enforce segmentation, and prevent malicious activity on previously unmanaged endpoints.

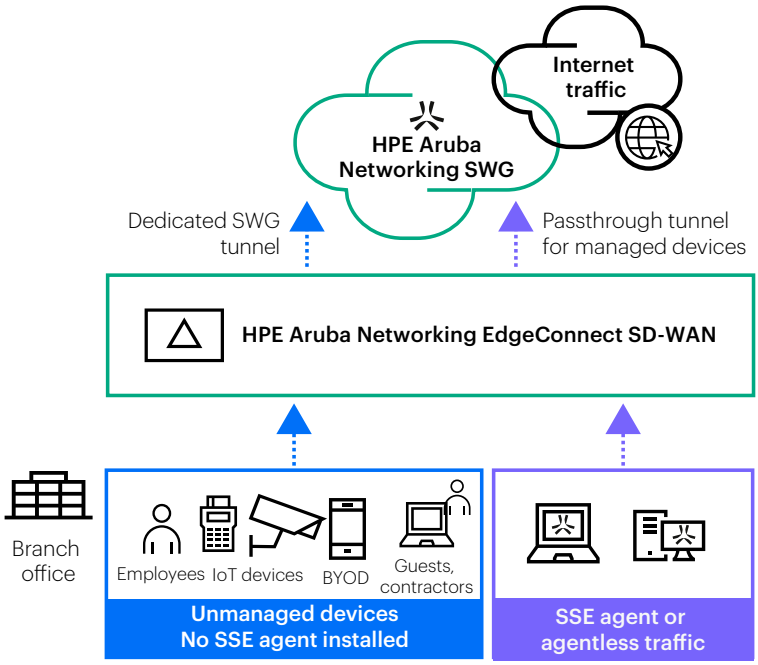

Figure 7. Protect all devices—managed or unmanaged—from web-based threats without installing an SSE agent on each device

Cloud-native SSE with a single policy engine and UI

Complementing SD-WAN, HPE Aruba Networking SSE delivers all cloud-delivered security services through a single policy engine and a single user interface. SWG, ZTNA (zero trust network access) and CASB (cloud access security broker) capabilities are defined once and enforced consistently across all users and locations.

This unified policy model eliminates the need to manage separate policies for different security services. Changes are propagated automatically, reducing configuration errors and accelerating response to emerging threats.

Unlike architectures that rely on chaining multiple services across different points of presence, HPE Aruba Networking delivers all security functions within a single PoP. This design avoids unnecessary latency, improves reliability, and simplifies troubleshooting.

A rich set of cloud-delivered security features

HPE Aruba Networking SSE delivers a comprehensive suite of cloud-delivered security services to protect users, devices, and applications across distributed environments. These integrated features provide identity-driven access, advanced threat protection, and granular control over cloud services.

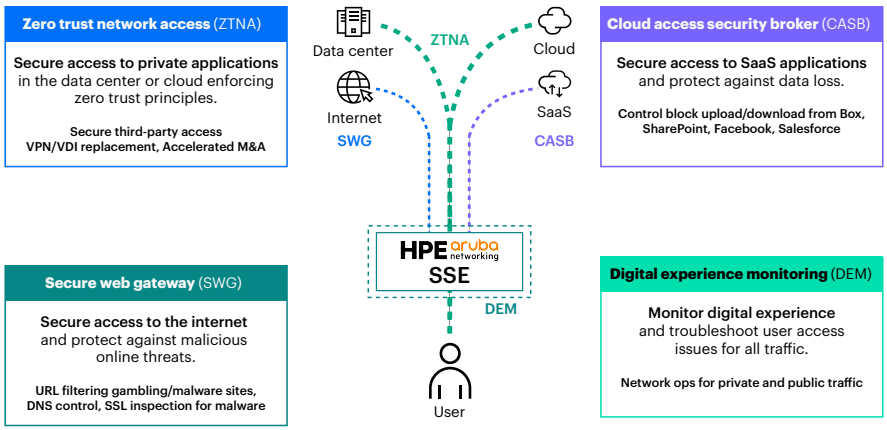

Figure 8. HPE Aruba Networking SSE delivers advanced cloud-delivered security services including ZTNA, SWG, CASB and DEM

Global scale powered by hyperscalers

HPE Aruba Networking unified SASE is built on a hyperscaler-powered infrastructure using AWS, Microsoft Azure, and Google Cloud, with over 500 global edge locations for low-latency access and elastic scalability.

Smart routing connects multiple PoPs to select the best path, while co-resident services in each PoP enable fast failover and failback. This ensures users are always connected to the nearest edge for consistent performance. Security services scale dynamically to meet demand, providing resilience during traffic spikes or attacks and eliminating capacity planning challenges.

AI-powered NAC: visibility, context, and adaptive enforcement

A core pillar of HPE Aruba Networking unified SASE is AI-powered Network Access Control (NAC), providing deep visibility and contextual awareness across the environment. Many traditional SASE solutions lack insight into device identity and behavior, especially for unmanaged endpoints.

HPE Aruba Networking NAC continuously profiles devices using machine learning, identifying type, role, posture, and behavior in real time. This intelligence informs access control and segmentation, enabling precise, identity-driven enforcement.

Combined with SASE, NAC supports adaptive zero trust policies that adjust dynamically based on risk, behavioral anomalies, or posture changes, ensuring trust is continuously evaluated rather than assumed

AIOps for streamlined operations

The SASE copilot streamlines configuration and troubleshooting using AI-driven analytics and natural language queries powered by generative AI (LLMs). This enhances network intelligence, reduces downtime, and delivers actionable insights for faster incident response, greater operational efficiency, and a more proactive security posture.

Simplifying SASE adoption, without compromise

HPE Aruba Networking unified SASE is designed to meet organizations where they are, supporting incremental adoption as well as full platform transformation. Customers can modernize branch networking, secure hybrid workforces, protect IoT environments, or migrate to the cloud—without sacrificing performance, visibility, or security.

By eliminating fragmentation and embedding zero trust into the network fabric, HPE simplifies the journey to SASE, enabling enterprises to operate securely and efficiently in a cloud-first, distributed world.

Visit HPE.com

Learn more at

HPE.com/networking

Chat now

a00156430ENW

HEWLETT PACKARD ENTERPRISE

hpe.com