Solution overview

MODERNIZING SECURITY AND CONNECTIVITY WITH UNIFIED SASE

The shift to distributed, cloud-first enterprises

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 Networking 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.

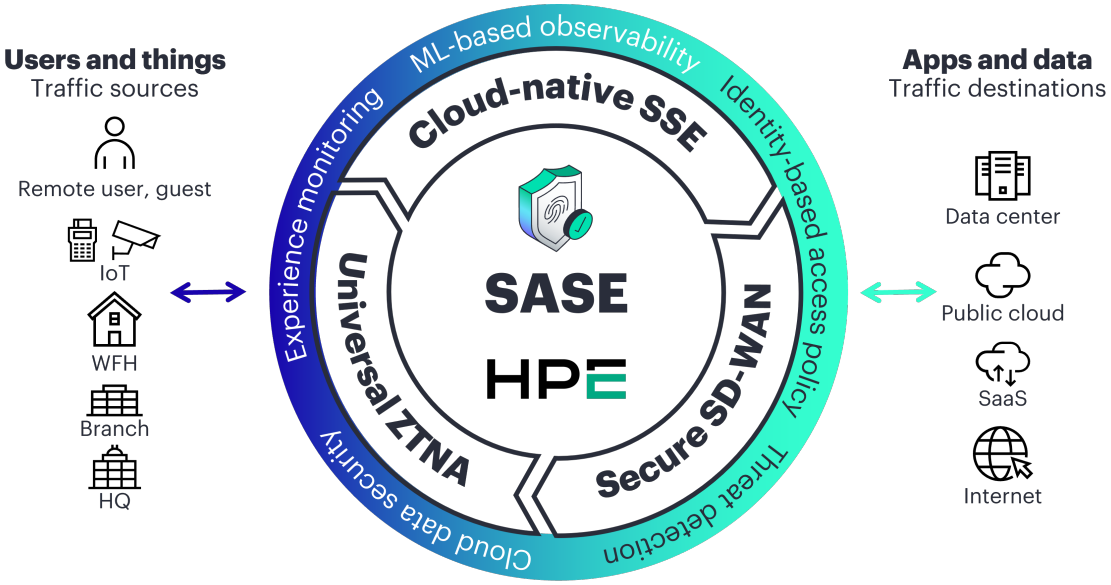


Figure 1. Deliver comprehensive zero trust principles across users, devices, applications, and data

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 Networking SASE is designed, built, and operated as an integrated system.

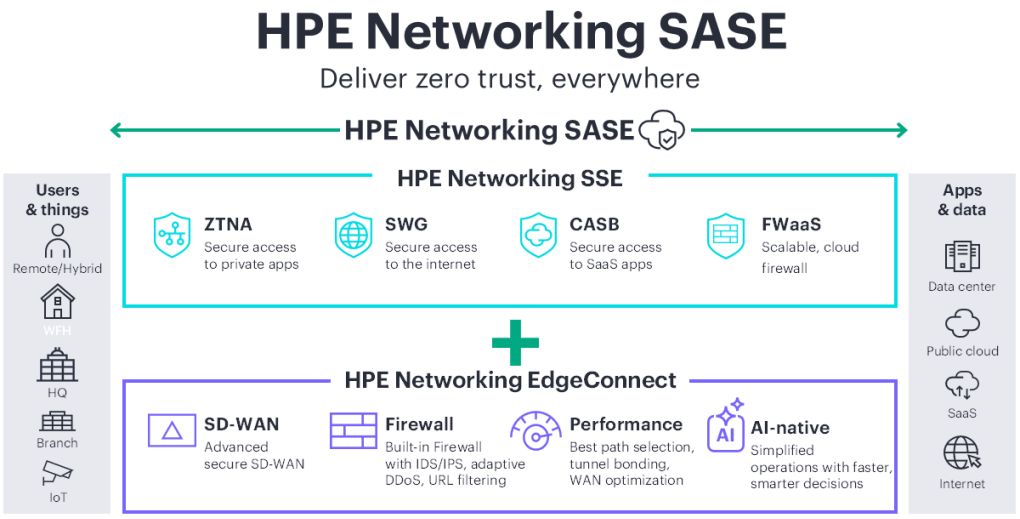


Figure 2. HPE Networking SASE integrates SD-WAN and SSE in a cohesive platform

A key differentiator is the native, fully automated integration between HPE Networking EdgeConnect and HPE Networking SSE. While many vendors rely on fragile 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.

AI-native operations

SASE Copilot delivers AIOps-driven operations using AI-powered analytics and natural language queries powered by generative AI. It streamlines configuration, troubleshooting, and daily management with intelligent insights, guided recommendations, and automated assistance. Administrators can interact more easily with the EdgeConnect platform through natural language search across capabilities, documentation, and APIs—simplifying policy creation, workflow automation, and issue resolution. By enhancing visibility and delivering actionable insights, SASE Copilot reduces downtime, speeds incident response, improves operational efficiency, and supports a more proactive security posture.

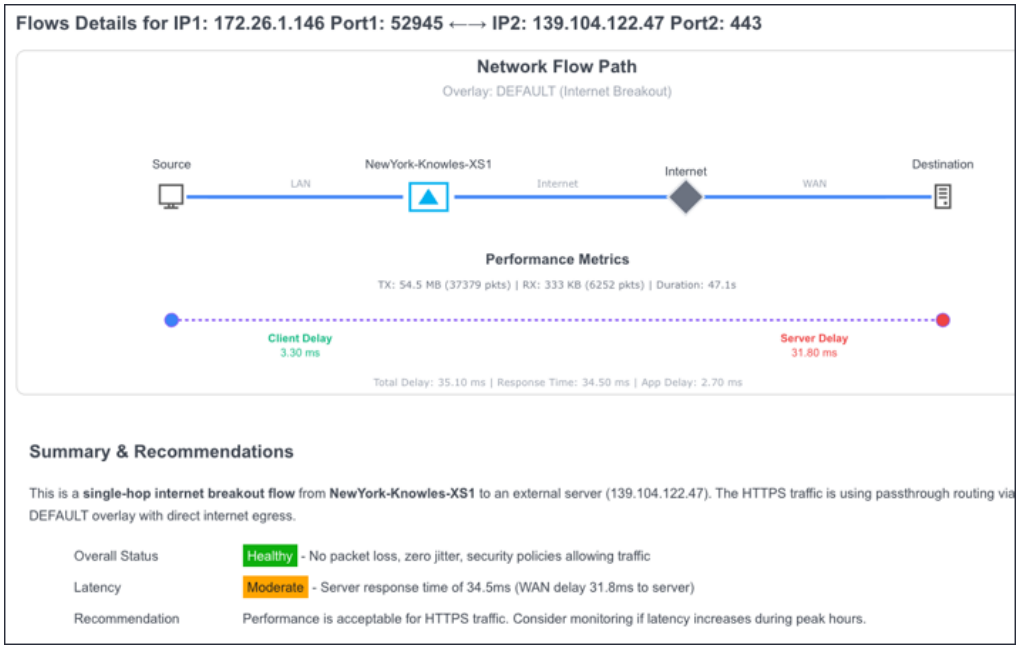


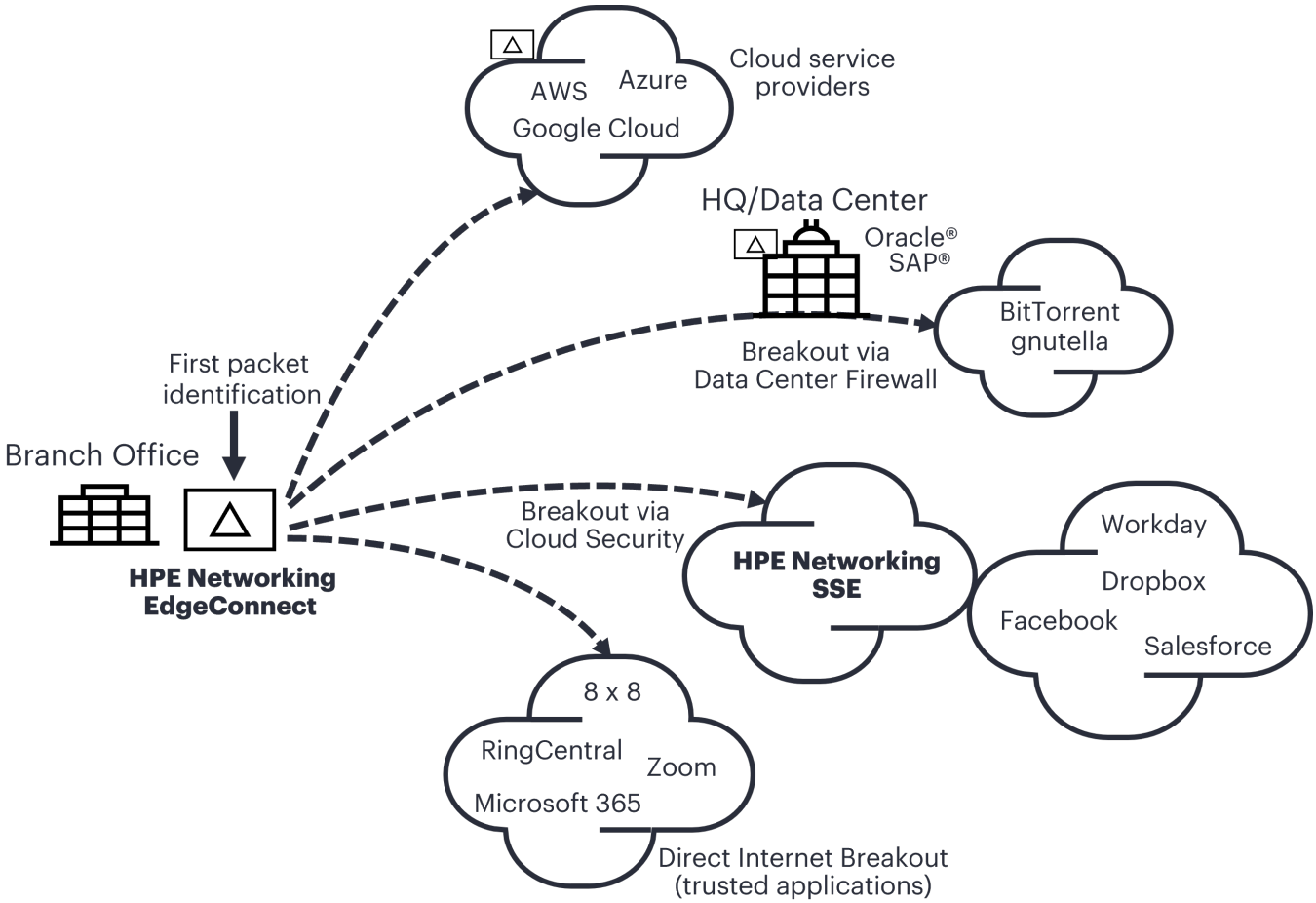
Figure 3. Accelerate issue resolution through natural language interaction and intelligent analytics with SASE Copilot

Cloud-first performance for modern applications

Performance is critical in SASE architectures, where security must not add latency or degrade user experience. HPE Networking EdgeConnect 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 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.



Steer apps intelligently

— Intelligent breakout of SaaS and trusted internet-bound traffic directly to the cloud

Improve SaaS performance

— Avoid backhauling traffic to the data center and improve SaaS application performance

Implement consistent security policies

— Eliminate application security and performance tradeoffs

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 organizations to express networking requirements in terms of application performance, security posture, and business priority. Rather than managing complex routing tables, teams define business intent once and allow the platform to enforce it dynamically across the network.

— **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) automatically restores lost packets by sending parity packets at intervals, eliminating the need for retransmitting packets. Additionally, when traffic is balanced across multiple WAN links using tunnel bonding, Packet Order Correction (POC) ensures packets are delivered in the correct sequence at their destination.

— **AppExpress** adds an additional layer of intelligence by continuously monitoring application experience using both real-time traffic analysis and synthetic polling for business-critical applications. When performance degradation is detected, AppExpress exploits path diversity to automatically select the best path for each application.

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

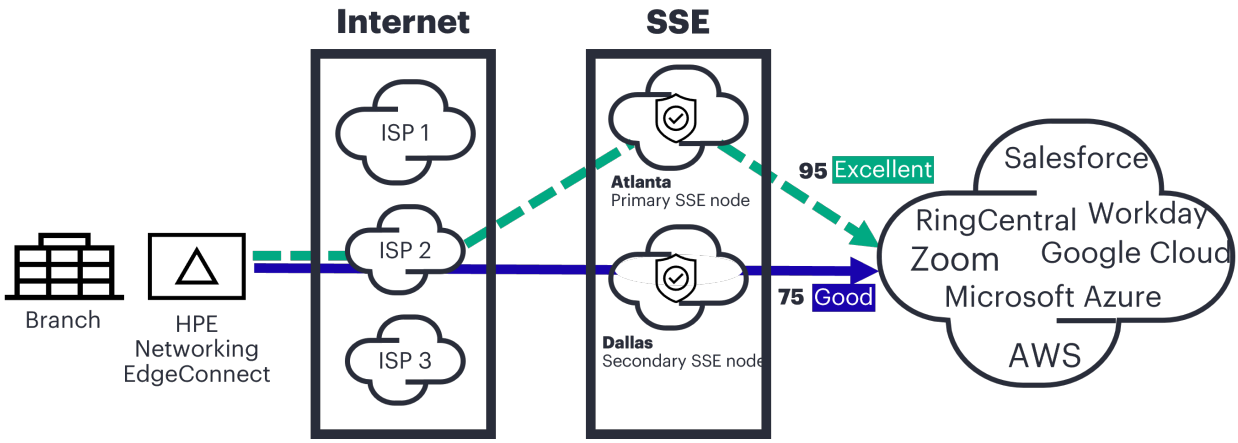


Figure 5. Optimize user experience for business-critical applications with AppExpress, even across SSE routing

Integrated branch security with advanced firewall capabilities

While cloud-delivered security is essential, branches and campuses still require strong local protection. HPE addresses this need by embedding advanced firewall 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 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 analyzed in the security log viewer providing real-time visibility or forwarded to third-party SIEM platforms such as Splunk.

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 Networking EdgeConnect

Simplified ZTNA deployment with an Integrated SSE Connector

The solution simplifies secure access to private applications by embedding an SSE Connector directly in EdgeConnect, enabling ZTNA users to reach private resources through the SD-WAN fabric.

Traditional ZTNA deployments often require organizations to deploy and manage dedicated ZTNA connectors in data centers or cloud environments to provide access to private applications. This adds operational complexity, introduces additional infrastructure to maintain, and can create potential performance bottlenecks.

EdgeConnect eliminates these challenges with a built-in SSE Connector integrated directly into the SD-WAN appliance, removing the need to deploy additional hardware or virtual connectors. This integrated approach reduces deployment complexity, improves performance through local access, enhances resiliency, and accelerates ZTNA adoption without requiring additional infrastructure.

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 SWG tunnel via EdgeConnect, 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.

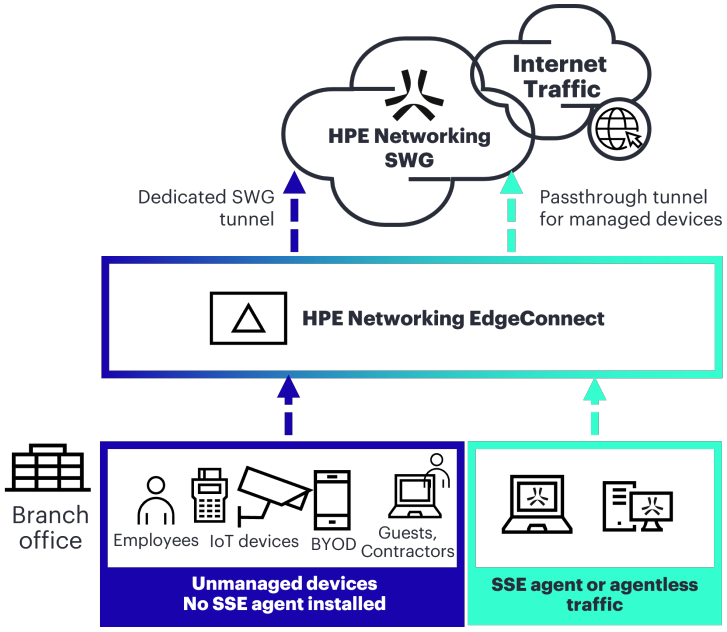


Figure 7. Protect all devices—managed or unmanaged—from web-based threats without installing an SSE agent on each device

Cloud-native SSE with a single policy engine and UI

Complementing SD-WAN, HPE 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 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 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.

— **ZTNA (zero trust network access)** provides identity-driven, least-privilege access to private applications without exposing them to the internet. It replaces legacy VPNs by authenticating users ad devices before access is granted and by preventing lateral movement. It secures access to all private applications, including modern web applications including SSH, RDP, Git, databases, or legacy thick-client applications such as VoIP, ICMP and AS400.

  In addition to agent-based access for managed devices, HPE Networking supports agentless ZTNA, enabling secure access for contractors, partners, and unmanaged devices through browser-based access—without requiring endpoint software.

— **SWG** safeguards users and devices from web-based threats by inspecting all internet-bound traffic for malware, phishing, and risky destinations. It combines advanced SSL inspection, URL filtering, and DNS filtering to provide secure, high-speed internet access while protecting the organization from online threats. DNS filtering blocks domains and IPs based on security policies. Traffic requiring deeper inspection is sent to the nearest SSE point of presence for SSL decryption, followed by URL and content filtering to block malicious or sensitive content according to DLP policies. With inline Data Loss Prevention (DLP), the solution also prevents sensitive data from leaking to the internet.

— **Cloud access security broker (CASB)** delivers visibility and control over SaaS applications by identifying shadow IT, enforcing data protection policies, and monitoring user activity across cloud services. CASB acts as a security broker between users and SaaS platforms, uncovering Shadow IT and ensuring sensitive business data remains protected from cyberthreats. CASB policies are managed centrally within the unified policy engine. The solution enforces data loss prevention (DLP) by blocking risky actions like file downloads and copy/paste, helping organizations meet compliance requirements and prevent data leakage.

Firewall-as-a-Service (FWaaS) enables precise access control while blocking unauthorized communications. It delivers consistent, centralized policy enforcement across branches, remote users, and cloud environments—enhancing visibility, simplifying management, and strengthening a zero trust security posture.

— **Digital experience monitoring (DEM)** provides end-to-end visibility into user experience across applications, network and security layers. DEM continuously monitors application responsiveness, latency and availability, enabling IT teams to quickly identify whether performance issues stem from the network, the application or the cloud.

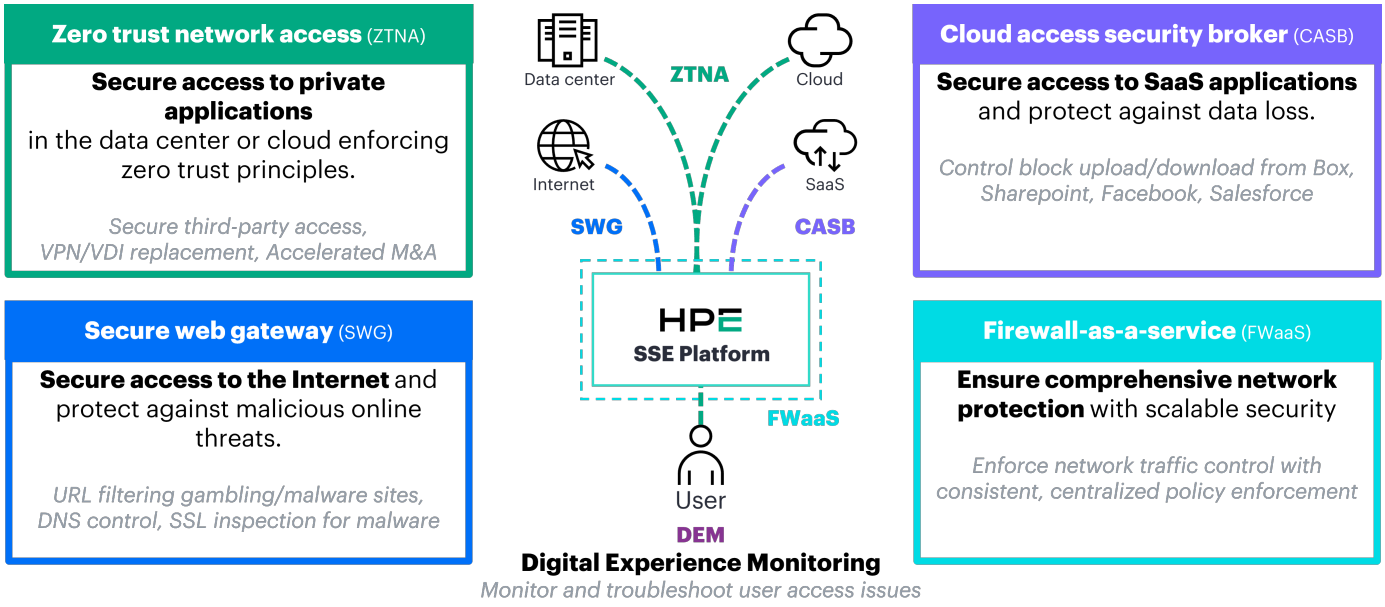


Figure 8. HPE Networking SSE provides advanced cloud-delivered security services including ZTNA, SWG, CASB and FWaaS

Global scale powered by hyperscalers

HPE Networking 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.

The smart routing capability connects multiple PoPs simultaneously to determine the best path, and because all services are co-resident in each PoP, failover and failback are fast. 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 Networking 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 Networking NAC continuously profiles devices using machine learning, identifying type, role, posture, and behavior in real time. This intelligence feeds directly into access control and segmentation decisions, 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.

A cohesive, end-to-end SASE architecture

This end-to-end architecture accelerates SASE adoption, reduces operational complexity, and allows organizations to modernize securely without disruptive changes to their existing infrastructure. In summary, the solution delivers several key advantages:

— **Cloud-first performance:** HPE Networking SASE delivers cloud-first performance by intelligently steering cloud application traffic with first packet iQ, enabling seamless deployment to major cloud providers such as AWS and Azure for end-to-end connectivity. The platform ensures optimal path selection, prioritizes mission-critical applications, and accelerates traffic using advanced features like Path Conditioning, AppExpress, and WAN Optimization.

— **Global scale:** HPE Networking leverages a network of over 500 edge locations built on hyperscaler backbones—including AWS, Azure, and Google Cloud—to provide low latency and elastic scalability. Smart Routing technology selects the best point of presence for each connection, while co-located services in every PoP enable rapid failover and failback for uninterrupted performance.

— **Advanced security:** Security is advanced and comprehensive, with SSE services such as ZTNA, SWG, and CASB delivered through a cloud-native platform using a unified policy engine. Branch locations benefit from built-in firewall capabilities, and universal ZTNA is achieved by combining SASE with AI-powered NAC for adaptive, identity-driven access control.

— **Unified, automated platform:** The unified, automated platform stands out for its fully automated integration between SD-WAN and SSE solutions, streamlining operations, configuration, and troubleshooting with AI-driven analytics and automation through SASE copilot.

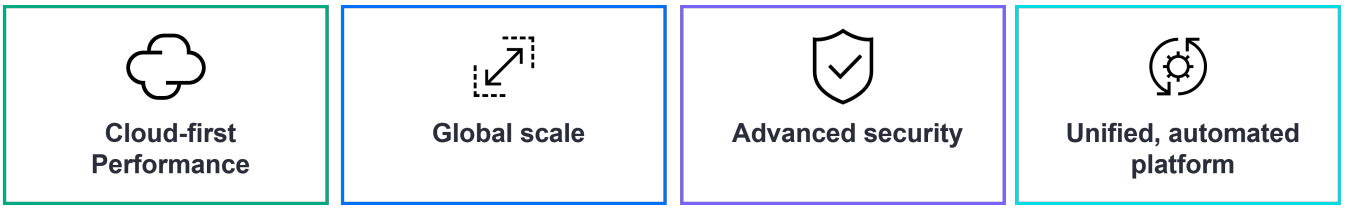


Figure 9. The key advantages of HPE Networking SASE

Simplifying SASE adoption, without compromise

HPE Networking 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, Rev. 1

HEWLETT PACKARD ENTERPRISE

hpe.com