Brochure

HPE aruba networking

Streamline your SASE journey with security-first, AI-powered networking

HPE GreenLake

Secure modern, cloud-centric organizations

In today's dynamic digital landscape, organizations often struggle to secure their distributed environments, optimize performance, and comply with regulations. With the proliferation of unmanaged devices, such as IoT, implementing zero trust principles presents significant operational challenges.

Additionally, legacy network architectures hinder agility and scalability for cloud-centric operations, impacting application performance and user experience. With increasing cyber threats and sensitive data now hosted in SaaS applications, organizations have difficulties securing access to cloud applications and data across diverse locations and devices, necessitating a unified approach to networking and security.

To tackle these challenges, HPE Aruba Networking offers a comprehensive four-step approach that integrates advanced security measures with SASE and zero trust capabilities powered by AI, delivering secure access, advanced threat defense, data protection and improved user experience. With this approach, organizations can streamline their SASE journey with a security-first, AI-powered networking strategy. Steps include:

1. **Modernize your network.** Optimize your WAN connections and use AI to create a more intelligent network that enhances user experience.
2. **Protect your branch.** Elevate branch security with secure SD-WAN and Secure Web Gateway (SWG), establishing the foundation for SASE.
3. **Simplify third-party access.** Secure users, devices, and data with unified SSE.
4. **Scale protection using AI.** Turn your network into a security solution designed to enhance security of AI resources and protect against AI-accelerated threats using AI-powered, built-in zero trust security.

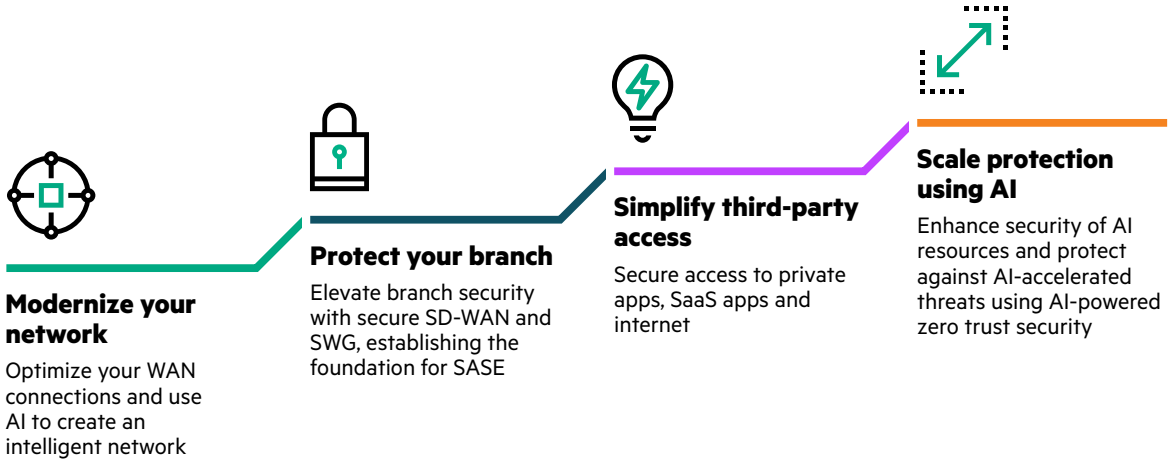


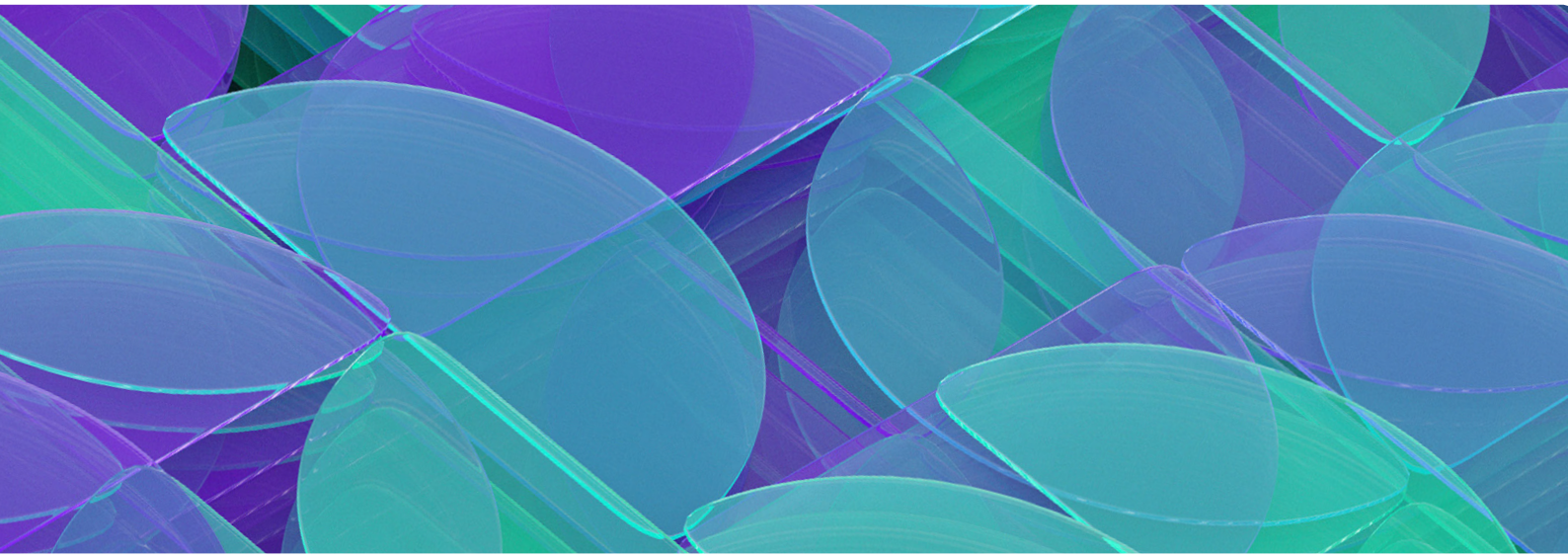
Figure 1. Advance your SASE journey at your own pace to implement zero trust from edge to cloud.

Advance you SASE journey with security-first, AI-powered networking

To achieve SASE, a four-step approach is essential to streamline and accelerate your journey to SASE:

Step 1: Modernize your network by optimizing WAN connections and using AI to create a more intelligent network that enhances user experience.

Traditional network architectures, which often rely on MPLS and data center-centric designs, struggle to meet the dynamic demands of modern cloud-centric operations. These architectures typically backhaul traffic to centralized



data centers, leading to latency issues, reduced application performance, and inefficient use of bandwidth. Cloud applications, such as SaaS platforms hosted on AWS, Azure, and Google Cloud™, require direct and optimized connectivity to ensure optimal performance and user experience. Moreover, critical applications like real-time voice and video suffer from latency, packet loss, and jitter issues when routed through traditional MPLS networks, impacting productivity and user satisfaction.

HPE Aruba Networking EdgeConnect SD-WAN enhances application performance over broadband connections through several key mechanisms:

- Tunnel bonding aggregates multiple links, effectively increasing available bandwidth and improving network resilience.
- Path conditioning techniques mitigate common issues like jitter and packet loss that affect broadband links, ensuring smoother data delivery.
- WAN optimization, including TCP protocol acceleration and data reduction, minimizes latency effects caused by geographical distances, thereby enhancing overall user experience and productivity.

With application-first packet identification and intelligent routing, EdgeConnect SD-WAN ensures direct and optimized paths for cloud-hosted applications. Virtual SD-WAN instances can be seamlessly deployed within leading public cloud providers such as Azure, AWS, and Google Cloud, enhancing network performance and responsiveness. Additionally, EdgeConnect SD-WAN AppExpress optimizes SaaS traffic by dynamically directing traffic to the nearest point of presence (PoP) and selecting the best path based on synthetic polling and real-time traffic observations.

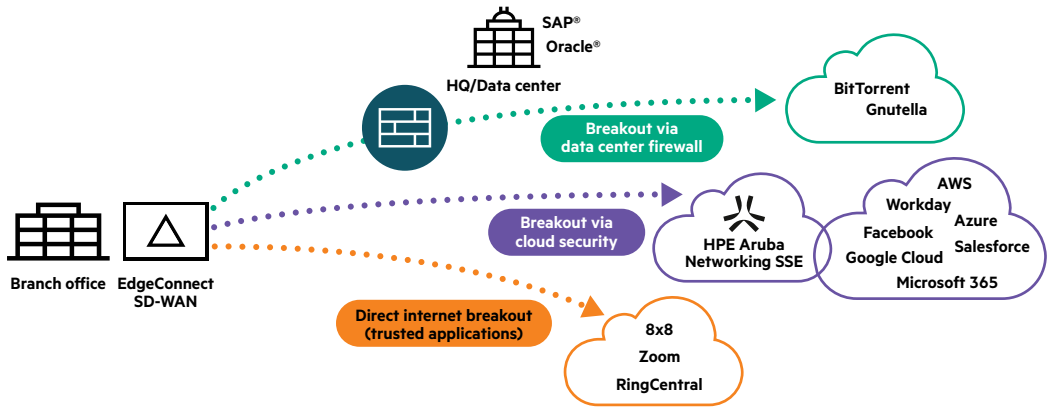


Figure 2. Intelligently steer cloud-destined traffic to the cloud with EdgeConnect SD-WAN.

AIOps, part of HPE Aruba Networking Central, enhances network intelligence by automating configuration and troubleshooting activities. The solution significantly improves resolution times using natural language queries, by leveraging generative AI and large language models (LLMs), and through actionable recommendations, ensuring the network continues to work at peak levels.

Key features

First Packet iQ	Identifies more than 10,000 applications and more than 300 million web domains on the first packet, enabling intelligent routing of cloud-destined traffic and prioritization of critical applications.
Cloud Integration	Deploys virtual SD-WAN instances within major public cloud providers (AWS, Azure, Google Cloud, Oracle Cloud) to optimize connectivity and performance for cloud-hosted applications.
Performance Optimization	Utilizes path conditioning to provide private-line-like performance over broadband with techniques such as adaptive Forward Error Correction (FEC) and Packet Order Correction (POC) to reconstruct lost packets and reorder any out-of-sequence packets. Tunnel bonding combines multiple links, increasing available bandwidth, while WAN optimization techniques mitigate latency effects through TCP protocol acceleration and data reduction methods.
AppExpress	Optimizes user experience for business-critical applications such as Zoom, Workday, SAP, Microsoft 365, and other applications by automatically selecting the best path for each application, leveraging synthetic polling and real-time user traffic observations.
AIOps	HPE Aruba Networking Central, which powers HPE Aruba Networking EdgeConnect SD-Branch, includes AIOps capabilities such as AI Insights to automatically diagnose common network issues, AI Assist to collect log files and troubleshooting data, and AI Search, which uses natural language (generative AI with LLMs) to greatly enhance user experience, with search-driven navigation, faster trouble-shooting, and intelligent document summarization.

Key benefits

- **Improved application performance:** Enhances user experience with faster response times and reduced latency for cloud applications.
- **Cost efficiency:** Reduces reliance on expensive MPLS circuits by leveraging broadband and internet links without sacrificing performance.
- **Scalability and flexibility:** Allows easy setup of new branch offices and adapts to dynamic cloud environments.

Step 2: Protect your branch by elevating branch security with secure SD-WAN and SWG, establishing the foundation for SASE.

Branch offices and remote locations are prone to security breaches and web-based threats due to the increased reliance on cloud services, BYOD (Bring Your Own Device) policies, and the proliferation of IoT devices. Traditional security approaches, based on branch firewalls, are inadequate for addressing the diverse security needs of distributed environments. They are difficult to manage and require local technical expertise, leading to inconsistent security policies across branch locations.

Furthermore, users and devices, including IoT, accessing the internet are susceptible to web-based threats such as malware, phishing attacks, and malicious websites, while standalone SWG solutions frequently fail to offer comprehensive security for both managed and unmanaged devices, leaving gaps in protection.

EdgeConnect SD-WAN integrates a robust suite of security features including a next-generation firewall with IDS/IPS, DDoS protection, and role-based segmentation, enabling organizations to seamlessly replace legacy branch firewalls. Centralized management of security policies eliminates the need for local technical expertise, streamlining operations across distributed environments. With fine-grained segmentation based on user roles and identity, EdgeConnect SD-WAN enhances security by isolating IoT device traffic from critical business applications, reducing exposure to potential threats.

Enhance protection with SWG

Furthermore, when augmented with SWG, SD-WAN provides comprehensive protection against web-based threats for all users and devices connected to the enterprise network, eliminating the need to install an SSE agent on every device.

To achieve this, HPE Aruba Networking SWG inspects all web traffic for malicious content, including encrypted traffic, and blocks access to harmful websites. The solution uses URL filtering, content filtering, SSL inspection, and malware detection to safeguard against phishing attacks, malicious websites, and unauthorized access attempts. It can also be combined with DLP to prevent the leakage of sensitive data and monitor user activity.

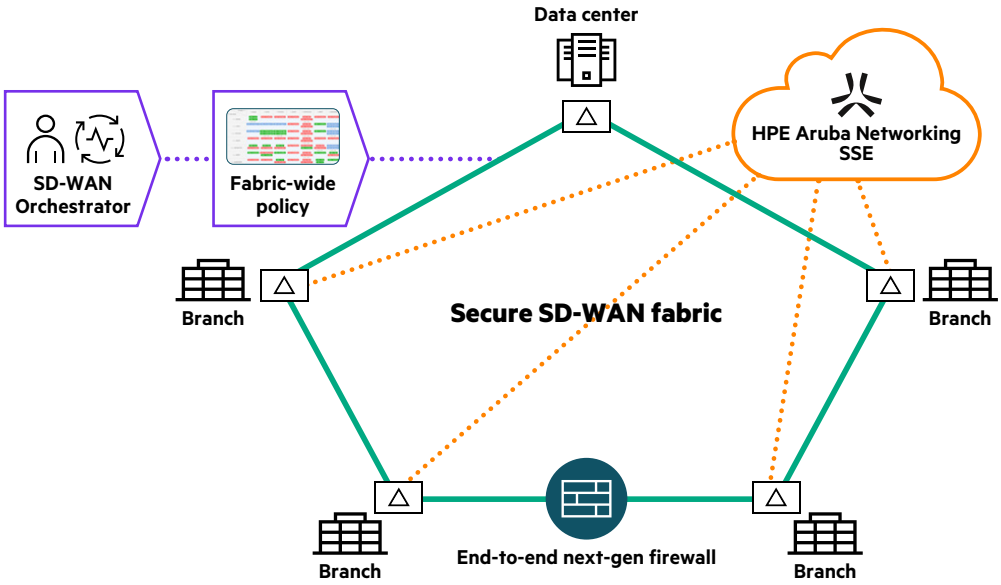


Figure 3. Build an end-to-end secure SD-WAN fabric with EdgeConnect SD-WAN.

Key features

Built-in, next-generation firewall	Simplifies the replacement of legacy branch firewalls while offering advanced threat protection such as IDS/IPS, DDoS defense and role-based segmentation.
Role-based segmentation	Enforces granular security policies based on user roles and device identity, isolating IoT traffic from mission-critical applications to mitigate potential risks.
Integration with HPE Aruba Networking ClearPass	Enhances security posture by integrating identity and role information, facilitating the implementation of zero trust principles with fine-grained segmentation within the SD-WAN fabric.
SD-WAN augmented with SWG	Protects all devices, managed and unmanaged, against web-based threats without requiring SSE agents on individual devices, ensuring comprehensive network security.
Secure Web Gateway (SWG)	Provides real-time threat protection, blocks malware and phishing, and enforces content filtering to control access to inappropriate content, ensuring a safe web browsing experience. Combined with DLP, sensitive information is secured.

Key benefits

- **Unified security management:** Centralizes security policy enforcement and management across distributed locations, reducing complexity and operational overhead.
- **Comprehensive threat protection:** Enhances defense against web-based threats, malware, and phishing attacks without compromising network performance.
- **Improved compliance posture:** Ensures adherence to regulatory requirements and industry standards (e.g., GDPR, HIPAA) through role-based segmentation and enforcement of security policies.

Step 3: Simplify third party access and secure users, devices, and data with unified SSE.

While cloud-centric organizations must effectively safeguard their employees against web-based threats with SWG, they must also protect sensitive data now hosted in cloud applications. They must also meet the needs of hybrid workers and third-party contractors by giving them access to the resources they need.

- Remote workers and third-party contractors require secure access to corporate resources and applications from various locations and devices. Traditional VPN solutions pose security risks by providing broad network access after authentication, even to resources that are not needed, increasing the potential for unauthorized data access and breaches. Managing and securing access for third-party entities, such as contractors, without compromising security posture and compliance requirements is a complex task for IT teams.
- As sensitive data is now hosted in SaaS applications, organizations lack visibility and control over data stored and accessed within sanctioned and unsanctioned SaaS applications. Shadow IT and the adoption of cloud services by lines of business without IT oversight increase the risk of data exposure, compliance violations, and unauthorized access. Traditional security measures fail to provide comprehensive protection and monitoring capabilities across cloud environments, leaving sensitive data vulnerable to breaches and insider threats.

In addition to SWG, HPE Aruba Networking offers ZTNA and Cloud Access Security Broker (CASB) capabilities in a unified platform to address remote access, SaaS security, and web-based threat challenges comprehensively.

ZTNA implements zero trust principles to verify user identities and device health before granting access to corporate applications and resources. It ensures least-privilege access and continuous authentication to mitigate risks associated with unauthorized access and data breaches.

CASB provides visibility and control over data stored and accessed within SaaS applications. CASB monitors user activities, enforces data loss prevention (DLP) policies, and detects anomalous behavior to prevent data exfiltration and ensure compliance with regulatory requirements. CASB functions in two modes: In the inline mode, all communication between the user and the SaaS application is proxied to the closest access points of presence to be SSL decrypted and go through the single policy engine. For data at rest, API-based CASB integrations allow automatic scanning of SaaS apps and IaaS platforms for protection.

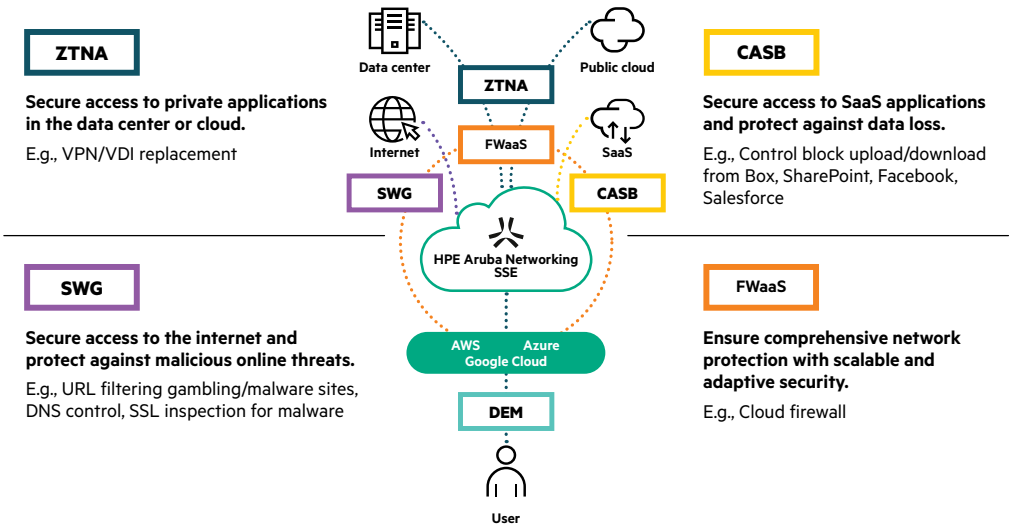


Figure 4. Transforming secure business access with HPE Aruba Networking SSE.

Key features	
ZTNA	Ensures secure remote access based on least-privilege access, by verifying each user and device before granting access to applications.
Agentless ZTNA	Facilitates seamless onboarding of third-party contractors without the need for installing an ZTNA agent.
CASB	Provides visibility and control over SaaS applications, ensuring data security and compliance. It enforces security policies, prevents data breaches, and detects threats in cloud environments.
Single UI with single policy engine	Simplifies operations and facilitates faster response by centralizing management and policy configuration.
Global presence	Maintains a global presence with over 500 edge locations, reducing latency and eliminating long backhauls, simplifying PoP management often associated with multi-vendor SASE deployments.
Shared codebase	Allows for integrated SSE capabilities such as combining SWG, CASB, DLP, SSL inspection, to avoid redundant use of security functions such as SSL inspection.
Continuous authentication	Dynamically evaluates user and device posture throughout the session, adapting access controls based on contextual factors such as location, device type, and behavior.

Key benefits

- **Comprehensive security posture:** Integrates ZTNA, CASB, and SWG functionalities into a unified SSE platform to enforce consistent security policies and protect against evolving threats across distributed environments.
- **Enhanced data protection:** Ensures confidentiality, integrity, and availability of sensitive data by preventing unauthorized access and data leakage within SaaS applications.
- **Operational efficiency:** Simplifies access management and security administration with centralized policy enforcement, real-time monitoring, and proactive threat detection capabilities.

Step 4: Scale protection using AI. Turn your network into a security solution designed to enhance security of AI resources and protect against AI-accelerated threats using AI-powered, built-in zero trust security.

Attackers are increasingly leveraging AI to develop more sophisticated threats, requiring advanced threat defense strategies that also leverage AI capabilities to improve protection and strengthen zero trust security.

Protecting AI infrastructure is also critical. Unmanaged devices like IoT generate significant amounts of data for AI, yet they are particularly vulnerable as they communicate with cloud services for tasks like machine learning training, updates, and telemetry. Additionally, bring-your-own-device (BYOD) and devices from third-party users frequently operate outside traditional IT oversight, posing risks of compromise without detection. This scenario creates potential

In the digital age, organizations must cope with distributed and heterogeneous environments, which can create serious risks of data breaches and non-compliance as corporate data are accessed from anywhere and from any device.

entry points for cyber-attacks and introduces concerns about AI poisoning from maliciously manipulated or corrupted data. As organizations confront these challenges, integrating AI-driven security measures becomes crucial to effectively safeguarding against evolving threats and securing AI workloads.

Achieving comprehensive visibility, enforcing global policies, and ensuring security across all endpoints and applications allow organizations to implement zero trust from edge to cloud. Universal ZTNA represents a fundamental shift in the approach to network security, extending the ZTNA use case to on-premises. Universal ZTNA provides access from any locations and devices (including IoT) and enables zero trust principles everywhere, while ZTNA solutions only focus on remote working to replace legacy VPN solutions.

HPE Aruba Networking offers foundational support for universal ZTNA, with continuous improvements to enhance functionality. This is done through a comprehensive set of functionalities that includes AI-powered visibility, cloud-based authentication, role-based access control, and continuous trust adjustment.

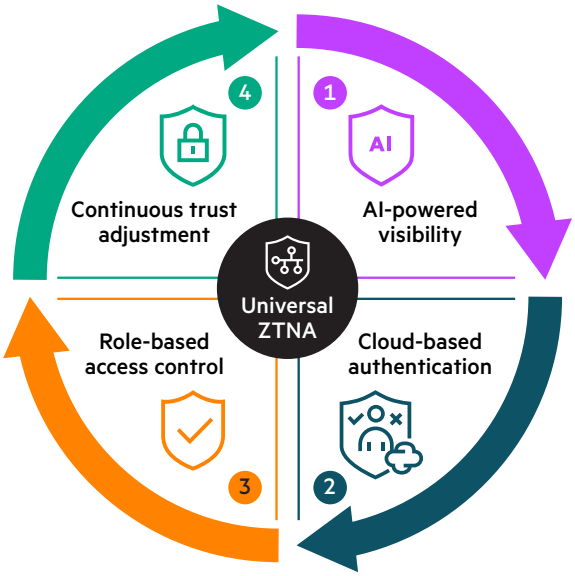


Figure 5. HPE Aruba Networking Universal ZTNA framework

The HPE Aruba Networking framework for zero trust includes the following capabilities.

1. **AI-powered visibility:** HPE Aruba Networking Central includes AI-powered visibility and profiling with **Client Insights**. With this functionality, organizations can quickly identify any device type — with up to 99% profiling accuracy of known devices, and less than 5% rate of unknowns — through ML-based classification models, which dynamically analyze device attributes like traffic patterns and behavioral characteristics. This enables not only automated device fingerprinting to support zero trust security, but also the ability to use behavior baselines to spot anomalies that can indicate compromise and attack.
2. **Cloud-based authentication:** Authenticate and authorize every device connecting to the network. HPE Aruba Networking ClearPass supports RADIUS, TACACS+, and 802.1X enforcement for secure authentication. HPE Aruba Networking Central Cloud Auth integrates with cloud identity stores, such as Google Workspace™ or Azure Active Directory.
3. **Role-based access control:** HPE Aruba Networking ZTNA and HPE Aruba Networking Central enforce role-based access via a global policy engine for on-premises and remote users and devices using techniques such as dynamic segmentation based on least-privilege access.
4. **Continuous trust adjustment:** Adapt policies and access control in real time based on changes in context such as device type, access location, and device health. This phase is enhanced through bidirectional communication with the rest of the security ecosystem via the HPE Aruba Networking 360 Security Exchange.

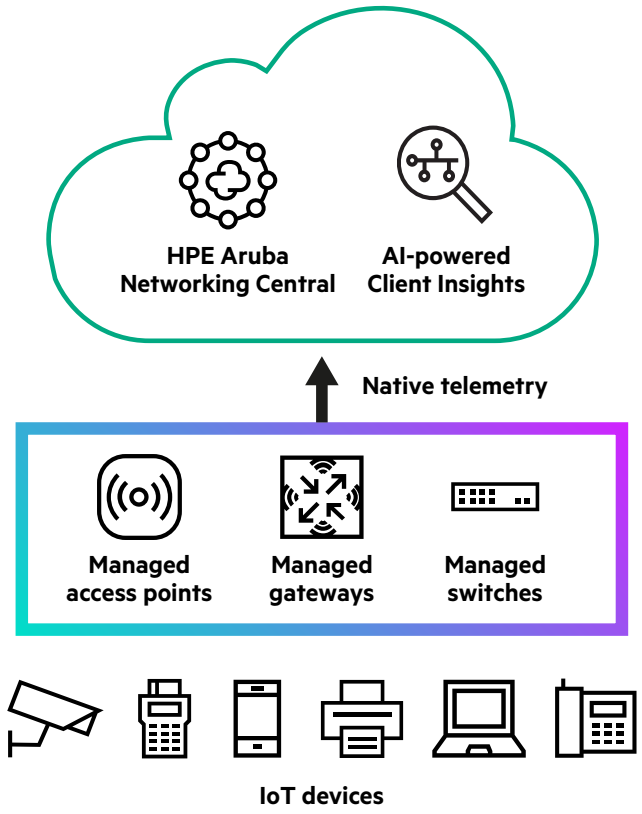


Figure 6. AI-powered visibility with HPE Aruba Networking Client Insights

By adding SD-WAN and other SSE capabilities such as SWG, CASB, and FWaaS, organizations can achieve zero trust from edge to cloud — enforcing secure access to internal resources, SaaS, and the internet from anywhere and any device, protecting data, applications and other corporate resources from cyber threats. With HPE Aruba Networking

Central, organizations can manage their wired, wireless, and WAN infrastructure from a single, cloud-native platform, providing centralized control and end-to-end visibility to transform their network into a robust zero trust architecture powered by AI.

Finally, HPE Aruba Networking supports compliance with industry standards and regulations such as NIST, HIPAA, GDPR, and PCI DSS through a comprehensive zero trust approach that encompasses remote locations, branch, and campus locations, as well as detailed reports on web usage and security incidents.

Key features

AI-powered visibility	Uses ML-based classification models to fingerprint, identify, and accurately profile all connected user and IoT endpoints for precise policy assignment and enforcement.
Comprehensive AIOps suite	Provides a full-service AIOps suite that automates common troubleshooting activities. It includes AI Search, which uses generative AI and LLMs to provide troubleshooting tips and solution guides based on natural language queries.
Dynamic segmentation	Enforces granular access controls based on user identities, device attributes, and contextual factors to prevent lateral movement and contain AI-accelerated threats.
Certified interoperability	Via the HPE Aruba Networking 360 Security Exchange, certified interoperability between HPE Aruba Networking and partner technologies ensures optimal security and hassle-free operation.

Key benefits

- **Enhanced threat intelligence:** Improves threat detection and response capabilities with AI-driven insights and behavioral analytics, minimizing the impact of AI-accelerated threats.
- **Regulatory compliance:** Supports regulatory compliance through role-based access, continuous monitoring, comprehensive dashboards, and AI-driven insights.
- **Operational resilience:** Enhances operational resilience by proactively recommending policy updates and previewing changes before implementation, accelerating attack response while ensuring that the changes will not adversely affect network operations.

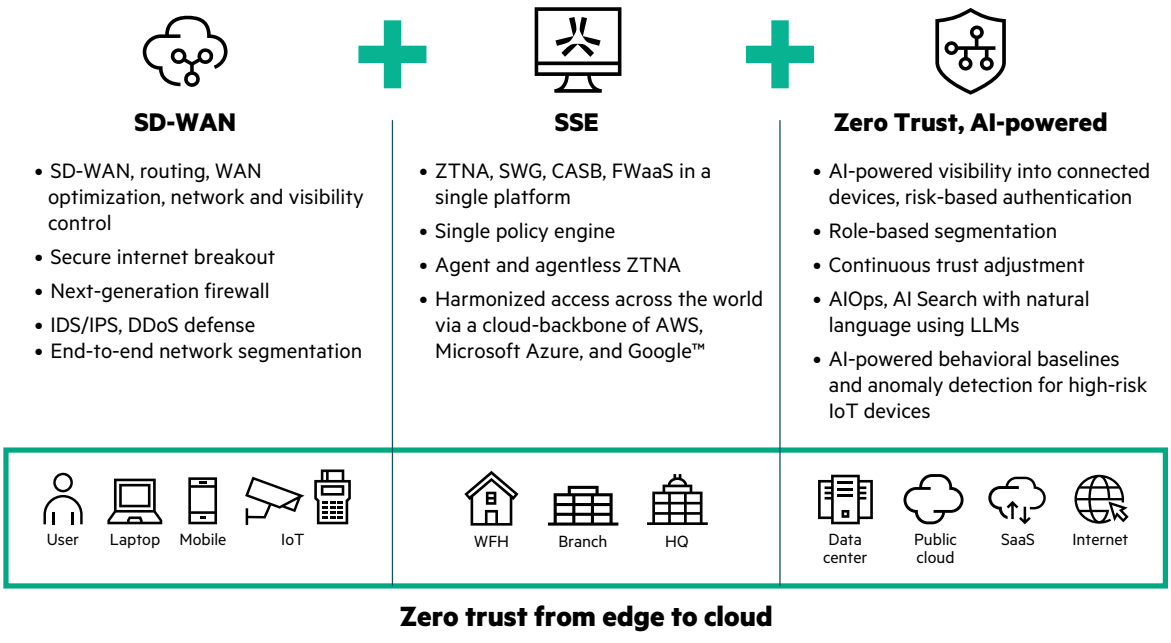


Figure 7. Edge-to-cloud zero trust with security-first, AI-powered networking

Conclusion

In the digital age, organizations must cope with distributed and heterogeneous environments, which can create serious risks of data breaches and non-compliance as corporate data are accessed from anywhere and from any device. The proliferation of IoT devices has increased the attack surface making it even more difficult to protect the organization. HPE Aruba Networking enables organizations to navigate their SASE journey confidently with advanced security and AI-driven insights to achieve zero trust from edge to cloud. By addressing critical challenges such as network modernization, branch security, data protection, threat defense, and AI-powered security, HPE Aruba Networking delivers a scalable, high-performance solution tailored for modern enterprises from network modernization with SD-WAN to a security-first, AI-powered networking approach based on intrinsic zero trust principles.

Learn more at

For more information on how HPE Aruba Networking can streamline your SASE journey, visit our website:

HPE Aruba Networking SASE

Visit **ArubaNetworks.com**

Make the right purchase decision.
Contact our presales specialists.

Contact us

BR_Streamline-SASE-Journey_A4_RB_072624 a00141672ENW

Hewlett Packard Enterprise