HPE aruba networking

Solution overview

Delivering AI-powered single-vendor SASE with edge-to-cloud Zero Trust access

HPE GreenLake

As organizations move to a cloud-centric architecture, where most applications reside in the cloud, and the demand for hybrid work increases, security must evolve in parallel. Traditional architectures rely on perimeter defenses while corporate data is now hosted in SaaS applications and remote workers access corporate resources from anywhere and any device. CIOs and other decision-makers are increasing their focus on Zero Trust Security solutions, but they face challenges in implementing mature Zero Trust solutions for users and things accessing resources from anywhere. Additionally, as security threats become more complex and frequent, IT teams struggle to detect and respond to evolving threats in real time. Traditional monitoring tools generate a high volume of alerts while manual intervention in identifying and resolving issues are time consuming.

Here are the key reasons why a single-vendor SASE platform with edge-to-cloud Zero Trust is critical for modern digital enterprises:

- Traditional security models don't provide consistent and secure access to users and things across different environments including on-premises, cloud-based and remote working, as well as varying device types.
- Legacy VPNs often provide poor user experience. Additionally, VPNs without granular controls can over-extend network privilege, granting users more access to resources than necessary, and increasing security risks.
- Traditional network architectures route application traffic to the data center for security inspection, which is no longer practical, and impacts application performance because most applications now reside in the cloud.
- With corporate data increasingly hosted in SaaS applications, organizations need to take extra steps to protect their data. Corporate data can indeed be stored in both sanctioned and unsanctioned cloud applications (or shadow IT), and may travel over unsecured links, leading to potential risk of data loss.

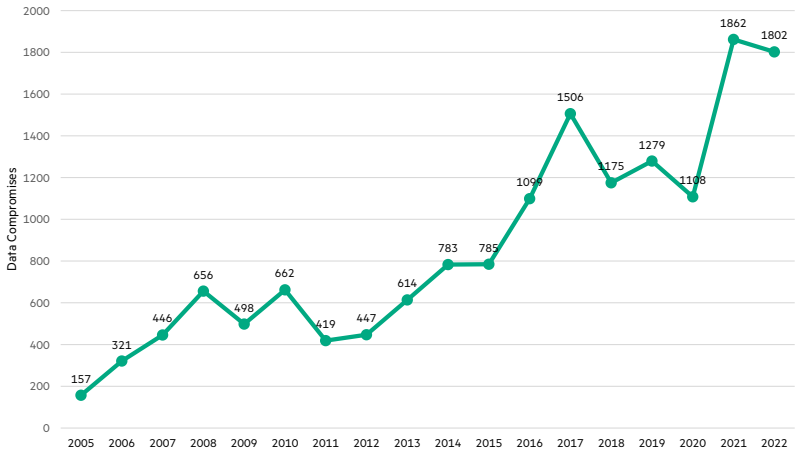

Figure 1. Data compromises in the US[1]

- Employees are vulnerable to web-based threats such as phishing attacks and ransomware when browsing the internet or simply accessing emails.

In 2022, 493 million ransomware attacks were detected by organizations worldwide[2] and around 30 percent of adults worldwide encountered phishing scams. Furthermore, in the fourth quarter of 2022, there were over 1.35 million unique phishing sites worldwide[3].

[1] Source: Annual number of data compromises in the United States, Statista

[2] Annual number of ransomware attacks worldwide from 2017 to 2022, Statista

[3] Phishing - Statistics & Facts, Statista

- Device proliferation and BYOD policies make it difficult to secure various devices accessing the corporate network, locally or remotely. The explosion of IoT devices in recent years, most of which are not owned or managed by IT, has significantly increased the attack surface. However, IoT devices are often built on a simple design and lack sophisticated security mechanisms.
- With evolving cyber threats, IT teams need to automate network and security infrastructure monitoring, and continuously analyze a vast amount of data in real-time. They also need efficient troubleshooting capabilities to quickly identify the root cause of network issues.
- Organizations must comply with regulatory mandates such as NIST, HIPAA, NIS2, and GDPR but often lack the essentials tools and comprehensive reports needed to demonstrate compliance.

To tackle these challenges, organizations can choose between a single-vendor SASE approach and a multi-vendor SASE approach. While a multi-vendor approach allows organizations to integrate new SASE features into an existing security ecosystem, a tight integration of SSE and SD-WAN into a single-vendor SASE platform provides organizations with many benefits including faster deployment, centralized management, consistent security policies, and the ability to adapt seamlessly to the evolving threat landscape.

In fact, Gartner predicts that:

"By 2026, 60% of new SD-WAN purchases will be part of a single-vendor secure access service edge (SASE) offering, up from 15% in 2022[4]."

Converge network and security with a single-vendor SASE solution powered by AI

A single-vendor SASE solution, powered by AI, offers a comprehensive and unified approach to network and security. The integration of various security services such as SD-WAN, SWG (Secure Web Gateway), CASB (Cloud Access Security Broker), ZTNA (Zero Trust Network Access), and AI capabilities into a cohesive platform, streamlines the complexity associated with managing multiple security components, and delivers edge-to-cloud Zero Trust access. This integrated architecture not only simplifies deployment but also ensures unified security policies, centralized management, and consistent Zero Trust access, as well as AI-generated insights, comprehensive visibility, and proactive issue resolution.

What to look for in a single-vendor SASE solution

1. Cloud-native architecture and scalability

A single-vendor SASE platform is designed with a cloud-native architecture, leveraging the scalability and agility of cloud computing. This architecture enables organizations to dynamically allocate resources based on traffic demand, enabling a more efficient and adaptable network.

2. Global network presence

A single-vendor SASE platform provides a global network presence through geographically distributed Point of Presence (PoPs) to ensure consistent performance and low latency, regardless of user location. It simplifies PoP management as organizations only need to manage PoPs from one vendor, contrary to a multi-vendor approach, which requires multiple points of presence from different vendors.

[4] 2023 Magic Quadrant for SD-WAN, Gartner Sep. 2023.

3. Global policy management

A single-vendor SASE solution manages security policies centrally and automatically deploys them globally across the network. This approach streamlines operations, reduces complexity, and helps organizations to deploy and enforce consistent policies effectively.

4. Centralized UI and comprehensive dashboards

A single-vendor SASE solution provides IT teams with the ability to manage all network and security operations in a centralized user interface. It offers enhanced visibility into network traffic, security events and policy enforcement, improving threat detection and incident response. Additionally, it enhances reporting capabilities, providing organizations with the means to demonstrate compliance with regulatory requirements and industry standards.

5. Zero Trust access, data protection, and threat defense

A single-vendor SASE platform seamlessly converges security capabilities such as ZTNA, SWG and CASB into a unified platform:

- ZTNA follows the principle of "never trust, always verify". Unlike VPNs that grant broad access to the corporate network, ZTNA restricts user access to specific applications or microsegments that have been authorized for each user. It also improves user experience by providing multiple Points of Presence (PoPs) instead of a few VPN concentrators involving long backhauls. This approach enforces the principle of least-privilege access. It allows remote workers, as well as third-party users with agentless ZTNA, to connect securely from anywhere.
- CASB identifies and protects all data in SaaS applications, detects shadow IT, and prevents data loss with policies that control what a user can access, download, upload, and share. In inline mode, all communication between the user and the SaaS application is proxied to the closest PoPs to be SSL decrypted and to analyze data in motion. Out-of-band mode uses API-based integrations to allow automatic scanning of data at rest in SaaS apps.
- SWG protects against ransomware, malware, and phishing by inspecting, scanning, and filtering all traffic. It performs various security inspections, including URL filtering, content filtering, and web access control. Additionally, SWG provides policies to restrict access to specific categories of websites such as adult content, gambling, or dangerous sites.
- Firewall as a Service (FWaaS) allows organizations to enforce security policies and inspect traffic regardless of the location, enabling scalable and flexible firewall protection. Secure SD-WANs, part of the SASE solution, offers advanced security capabilities including next-generation firewall, IDS/IPS, DDoS defense and role-based segmentation, enabling organizations to seamlessly replace legacy firewalls in branch offices.

6. Combined SASE capabilities

With a single-vendor SASE solution, organizations can easily combine multiple SASE capabilities to enhance their security posture and inspect traffic in a single pass. SSL inspection is performed only once, improving performance, and reducing complexity. Furthermore, by combining SWG and CASB with DLP, organizations can better monitor user activities to protect sensitive data from leaking out and enforce even more granular controls over web access.

7. Enhanced quality of experience (QoE)

Digital Experience Monitoring (DEM) ensures user productivity by measuring metrics, and monitoring app, device, and network performance over the internet. Advanced SD-WANs also optimize user experience over multi-cloud networking for business-critical applications by exploiting SD-WAN path diversity and automatically selecting the best path for each application. They intelligently steer traffic to the cloud, eliminating the need to backhaul traffic to the data center and optimizing cloud-based traffic. They include WAN optimization to overcome the latency effects of WAN by compressing and deduplicating data and to mitigate the effects of Internet and wireless links that often suffer from packet loss and jitter with Forward Error Correction (FEC).

8. AI

A single-vendor SASE solution includes AI capabilities such as AIOps and generative AI, to improve visibility into connected users and devices, and enable adaptive access control. AI also gives organizations insights into network traffic and security to proactively troubleshoot activities and diagnose network issues. The solution also provides predictive analytics and suggests network and security policy changes to anticipate future threats and issues.

Augmenting SASE with Zero Trust from edge to cloud

Universal Zero Trust access represents a fundamental shift in the approach to network security. It provides consistent and secure access to applications and resources from any location (remote or campus) and enables Zero Trust principles everywhere, while ZTNA solutions focus only on remote work to replace legacy VPN solutions.

Central to this approach is the principle of least-privilege access, ensuring that users and devices access only the resources essential to their tasks. This can be done by micro-segmenting the network based on identity and role, reducing the attack surface, and also with other mechanisms including visibility, multifactor authentication (MFA), access controls, and continuous adjustment of network access based on user/device context.

In 2023, more than 50% of respondents reported considering the adoption of a Zero Trust strategy a top or high priority for their organization[5].

Organizations often struggle to solve these key challenges related to Zero Trust:

- Traditional security models don't provide consistent and secure access across various environments such as on-premises, cloud-based and remote working, as well as multiple device types.
- As organizations commonly operate across various platforms and manage diverse infrastructures, each environment might have its own set of security tools, policies, and access controls, leading to inconsistent security controls across the organization.
- Organizations don't have complete visibility into the devices, activities, and behaviors within the network. IoT device proliferation and BYOD policies make it difficult to secure various devices accessing the corporate network, locally or remotely. Organizations often struggle to identify, authenticate, and authorize these devices.

Advanced single-vendor SASE solutions provide a comprehensive Zero Trust approach, from edge to cloud, by securing access to users and devices located outside or inside the company security perimeter. This approach can be summarized in four steps:

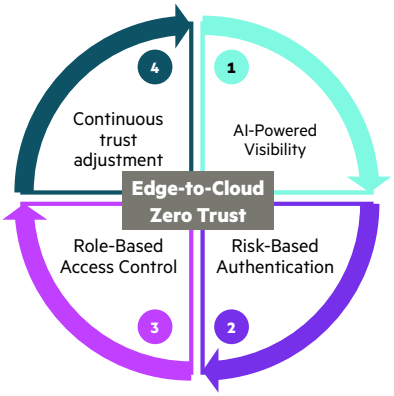

Figure 2. Enforce Zero Trust Access from Edge to Cloud

[5] Statista 2024

1. AI-powered visibility: With the increased adoption of IoT and BYOD policies, advanced single-vendor SASE solutions include AI-powered visibility and profiling so that organizations can quickly identify any type of device based on ML-based classification models.

2. Risk-based authentication: This step enables IT teams to authenticate and authorize every device connecting to the network based on risk and confidence level. To do so, the SASE platform uses standards-based 802.1X enforcement for secure authentication or through integrations with cloud identity stores such as Google Workspace™ or Azure Active Directory™. Authentication mechanisms such as MFA (Multi-Factor Authentication), require users to provide two or more verification factors to access a resource, reducing security risks. In this step, organizations can also implement MAC address authentication for IoT devices that may lack support for 802.1X.

3. Role-based access-control: In this step, IT teams manage role-based access control through a single policy engine for remote work environments, as well as branch and campus environments. Security policy information and any updates related to the user, device type, role, and security posture is propagated to the entire network. Simple Zero Trust policies keep users off the corporate network, ensuring micro-segmentation at the application level, while masking private resources from the internet.

4. Continuous trust adjustment: In an edge-to-cloud Zero Trust approach, it is crucial to adapt access control in real time and update policies based on changes in context such as device type, access location, and device health. Advanced ZTNA solutions use adaptive trust to continuously reassess access rights, ensuring least privilege access per session—without manual intervention. Additionally, they can automatically terminate a session when changes to user groups in the IDP take place.

On campus, intrusion detection and prevention (IDS/IPS) provides an extra layer of security. It performs signature- and pattern-based traffic inspection on LAN (east-west) and WAN (north-south) traffic. Threat logging can be sent to the SASE platform or a third-party SIEM solution to monitor threats in real time. Advanced dashboards, available in the solution, provide real-time visibility into network traffic.

Secure IoT devices with edge-to-cloud Zero Trust

The proliferation of IoT devices has become a major concern for organizations, significantly increasing the attack surface. Based on a simple design, these devices cannot host a security agent, and therefore, they cannot be easily protected. Edge-to-cloud Zero Trust focuses on authenticating and authorizing devices based on their identity, ensuring that only trusted and authenticated IoT devices can connect to the network. Organizations can also define contextual access policies based on factors such as device type, location, and behavior to help enforce security measures tailored to the specific requirements of IoT devices.

Additionally, with centralized policy management and role-based segmentation, edge-to-cloud Zero Trust uses various enforcement points such as switches or secure SD-WANs, to dynamically segment the network and prevent lateral movements. This ensures that IoT traffic remains isolated from mission-critical applications, so that users and IoT devices only communicate with destinations consistent with their role based on identity, access rights, and security posture.

Edge-to-cloud Zero Trust also continuously verifies the identity and security posture of IoT devices before granting access, preventing unauthorized access, and ensuring that only compliant devices are allowed onto the network. The solution also monitors IoT device activities and behaviors to proactively detect security threats associated with IoT devices and trigger appropriate response actions.

The integration of SWG capabilities into the SD-WAN fabric is another measure that helps organizations to safeguard IoT devices against web-based threats. IoT devices can be prone to web-based threats as they generate web traffic when they communicate with cloud services for updates, telemetry, or other purposes. By incorporating SWG capabilities into the SD-WAN fabric, organizations can implement comprehensive web filtering and threat detection mechanisms directly at the network level for all devices. This ensures that IoT devices are shielded from malicious websites, phishing attacks, and other web-based threats without the need for individual security agents.

Security-first, AI-powered unified SASE with HPE Aruba Networking

Security-first, AI-powered unified SASE is part of the HPE GreenLake platform. HPE GreenLake is a portfolio of cloud and as-a-service solutions that helps simplify and accelerate your business. It delivers a cloud experience wherever your apps and data live—edge, data center, colos, and public clouds.

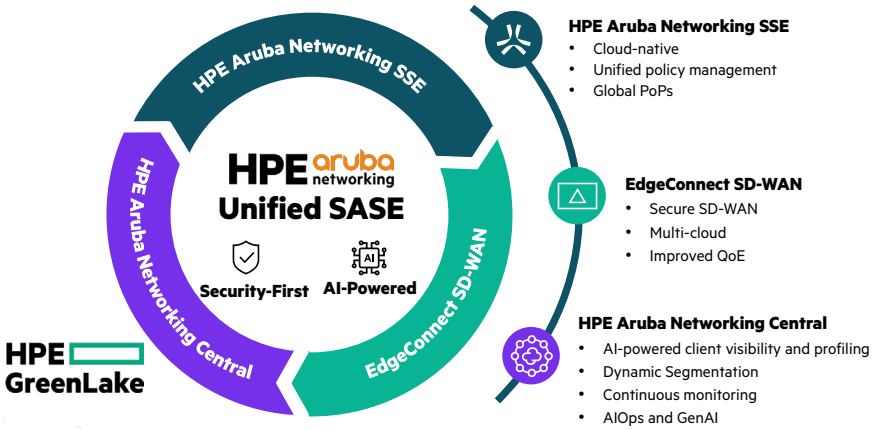

Figure 3. Apply Zero Trust Security controls to protect users and applications, no matter where they connect

HPE Aruba Networking unified SASE enables organizations to embrace security-first, AI-powered networking. Built with Zero Trust principles, the solution ensures a common foundation for networking and security teams and helps demonstrate compliance with cybersecurity standards and regulations. Organizations get advanced visibility and insights, data protection, threat defense, and access control in a single platform. AI-powered networking provides intelligent automation to reduce manual effort, improve visibility and anomaly detection, and enhance monitoring and diagnostics.

HPE Aruba Networking SSE is a unified platform where ZTNA, SWG, CASB, and DEM share a single codebase. All policies are managed from a single user interface, making access control incredibly simple for IT admins. It enables users and authorized third-parties to access resources with agent and agentless ZTNA. Users are protected against web-based threats with SWG, and sensitive data hosted in SaaS applications is securely monitored to prevent data exfiltration with CASB. DEM ensures user productivity by measuring hop-by-hop metrics, and monitoring app, device, and network performance. Additionally, the solution harmonizes access across the world via a cloud-backbone of Amazon Web Services (AWS), Microsoft Azure, Google, and Oracle.

HPE Aruba Networking EdgeConnect SD-WAN fabric comprises EdgeConnect SD-WAN, SD-Branch and Microbranch. It is engineered to deliver secure, high-availability access to network traffic over virtually any combination of links, including MPLS, internet, 4G/5G, and satcom, improving application performance and providing advanced flexibility. The EdgeConnect SD-WAN fabric also supports multi-cloud networking by intelligently steering traffic to the cloud, eliminating the need to backhaul traffic to the data center and optimizing cloud-based traffic. It integrates a next-generation firewall to provide advanced security capabilities across branch offices such as IDS/IPS, DDoS defense, and role-based segmentation. The HPE Aruba Networking EdgeConnect SD-WAN fabric also integrates with SWG, offering comprehensive protection to all users and things on the network without the need to install an SSE agent. This integrated approach allows organizations to seamlessly evolve towards HPE Aruba Networking unified SASE by adding ZTNA and CASB capabilities subsequently.

HPE Aruba Networking Central is a cloud-native management solution that empowers IT with comprehensive AIOps and Generative AI large language models (LLMs), deeper insights, and workflow automation to manage campus, branch, remote, data center, and IoT networks from one dashboard. Paired with the EdgeConnect SD-WAN fabric and HPE Aruba Networking SSE, it provides Zero Trust access for users and devices, including IoT, to private resources regardless of their location. It ensures that they consistently connect to destinations aligned with their role in the business, whether they're in the office, working remotely, or on the go.

HPE Aruba Networking ClearPass provides role- and device-based secure network access control for IoT, BYOD, corporate devices, as well as employees, contractors, and guests across any multivendor wired, wireless, and VPN infrastructure. ClearPass integration within the network infrastructure, including switches and gateways, as well as EdgeConnect SD-WAN and HPE Aruba Networking SSE, augments application intelligence with user and device identity and role-based context to enforce a Zero Trust architecture that dynamically segments the network and continuously adjusts access based on role and identity.

HPE Aruba Networking Central and ClearPass offer a comprehensive set of security functionalities as shown in the following table:

Table 1. HPE Aruba Networking Central and ClearPass Components

Designation	Details
AI-Powered Client Insights	AI-powered Client Insights offers the most granular profiling and visibility in the industry. Client Insights leverages native infrastructure telemetry from access points, switches, and gateways, as well as clients, without requiring installation of physical collectors or agents. ML-based classification models are used to fingerprint, identify, and accurately profile all wired and Wi-Fi connected user and IoT endpoints for policy assignment and enforcement.
ClearPass Device Insights	ClearPass Device Insights provides a full spectrum of visibility across the network by intelligently discovering and profiling all connected devices. This includes detailed device attributes such as device type, vendor, hardware version, and behavior, including applications and resources accessed.
CloudAuth	CloudAuth enables onboarding of end users and client devices either through MAC address-based authentication or through integrations with common cloud identity stores such as Google Workspace or Microsoft Azure Active Directory
ClearPass Policy Manager	ClearPass provides a built-in context-based policy engine with device profiling, posture assessment, onboarding, and guest access options. It supports RADIUS, TACACS+, and 802.1X enforcement for secure authentication. ClearPass also supports MAC address authentication for IoT devices that lack support for 802.1X, and supports multiple authentication/authorization sources (AD, LDAP, SQL). Single sign-on (SSO) works with Ping, Okta, and other identity management tools.
Policy Enforcement Firewall	Role-based user, device, and application policy enforcement firewall provides automated dynamic segmentation for wireless and wired access security
NetConductor	NetConductor enforces granular access control security policies in distributed environments across campus and data center using EVPN/VXLAN open standards to facilitate inline policy enforcement.

HPE Aruba Networking Central includes a full-service AIOps suite that automates common troubleshooting activities including:

- Network Insights to automatically diagnose common network issues,
- AI Search to search troubleshooting tips and solution guides using natural language. AI Search, integrates multiple generative AI (GenAI) Large Language Models (LLMs). Unlike other GenAI networking approaches that use public LLMs, HPE Aruba Networking GenAI was designed with innovative pre-processing and guardrails to improve user experience and operational efficiency by collecting telemetry from nearly four million network-managed devices and more than one billion unique customer endpoints, with one of the largest data lakes in the industry.
- AI Assist to automatically collect log files and troubleshooting data.

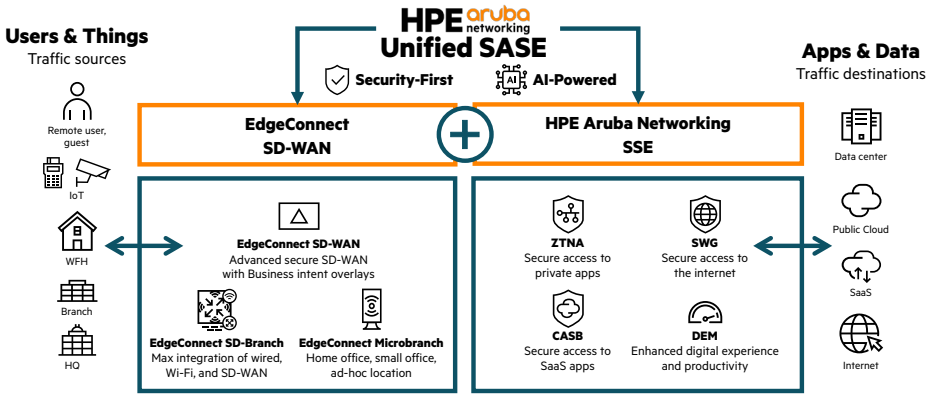

Figure 4. Deploy award-wining EdgeConnect SD-WAN with the cloud-native HPE Aruba Networking SSE platform to build a security-first, AI-powered single-vendor SASE solution

Conclusion

As modern, digital organizations face increasing threats and users connect from anywhere to a cloud-centric network, HPE Aruba Networking unified SASE, powered by AI, introduces a new approach to network security. By integrating Zero Trust Security services into a single-vendor SASE platform, the solution not only simplifies the security landscape but also leverages AI to improve visibility, threat detection, incident response, and troubleshooting. Zero Trust access ensures that trust is never assumed, and every user and device, wherever they connect, undergoes continuous verification, aligning with the highest standards of security. This holistic approach provides organizations with centralized management, consistent security policies, and the ability to adapt seamlessly to the evolving threat landscape. The HPE Aruba Networking security-first, AI-powered unified SASE solution provides organizations with a comprehensive and intelligent strategy to fortify digital enterprises against the complexities of modern cyber threats while ensuring streamlined operations and enhanced resilience.

Make the right purchase decision.
Contact our presales specialists.

Contact us

Visit **ArubaNetworks.com**

SO_AI-Powered-Single-Vendor-SASE_RVK_041624 a00138196ENW

Hewlett Packard Enterprise