



MODERNISIERUNG VON SICHERHEIT UND KONNEKTIVITÄT MIT EINHEITLICHEM SASE

Die Umstellung auf verteilte Cloud-First-Unternehmen

Unternehmensnetzwerke und -sicherheit entwickeln sich rasant weiter, während Anwendungen in SaaS- und Public Clouds verlagert werden, Benutzer von überall aus arbeiten und die Gerätevielfalt auf Auftragnehmer, Gäste und IoT-Geräte anwächst. Viele Sicherheitsarchitekturen basieren jedoch immer noch auf perimeterbasierten Modellen oder lose verbundenen Zero Trust-Tools.

Diese Fragmentierung erzeugt Komplexität, Schwachstellen und eine uneinheitliche Durchsetzung von Richtlinien – insbesondere bei nicht verwalteten Geräten und IoT-Geräten – und zwingt IT-Teams zur Verwaltung mehrerer Konsolen und Frameworks, was die Risiken steigert.

Der einheitliche SASE von HPE Aruba Networking vereinfacht den Weg zu SASE und Zero Trust, indem er voneinander getrennte Lösungen durch eine einzige, integrierte Plattform speziell für hybride Cloud-First-Unternehmen ersetzt.

Zero Trust neu denken: von der Fragmentierung zur Integration

Zero Trust gilt als das richtige Sicherheitsmodell für die heutigen Umgebungen. Viele Implementierungen befassen sich jedoch nur mit Teilaspekten des Problems, wie z. B. Remote-Zugriff oder Identitätsmanagement, während Netzwerkfunktionen, Gerätetransparenz und Cloud-Sicherheit unverbunden bleiben. Mit der zunehmenden Verbreitung hybrider Arbeitsmodelle und verteilter Umgebungen erhöhen diese Lücken das Risiko und den operativen Aufwand.

HPE löst dieses Problem mit einer vollständig integrierten Zero Trust-Plattform vom Edge bis zur Cloud, die eine Single-Vendor SASE-Lösung mit KI-basiertem NAC kombiniert. Das ermöglicht ein universelles ZTNA-Modell, bei dem Identität, Gerätestatus und Zugriffsrichtlinien für alle Benutzer und Geräte – ob verwaltet oder nicht, remote oder lokal – einheitlich durchgesetzt werden. Dadurch werden Schwachstellen beseitigt und die Betriebsabläufe von der Zweigstelle bis zur Cloud vereinfacht.

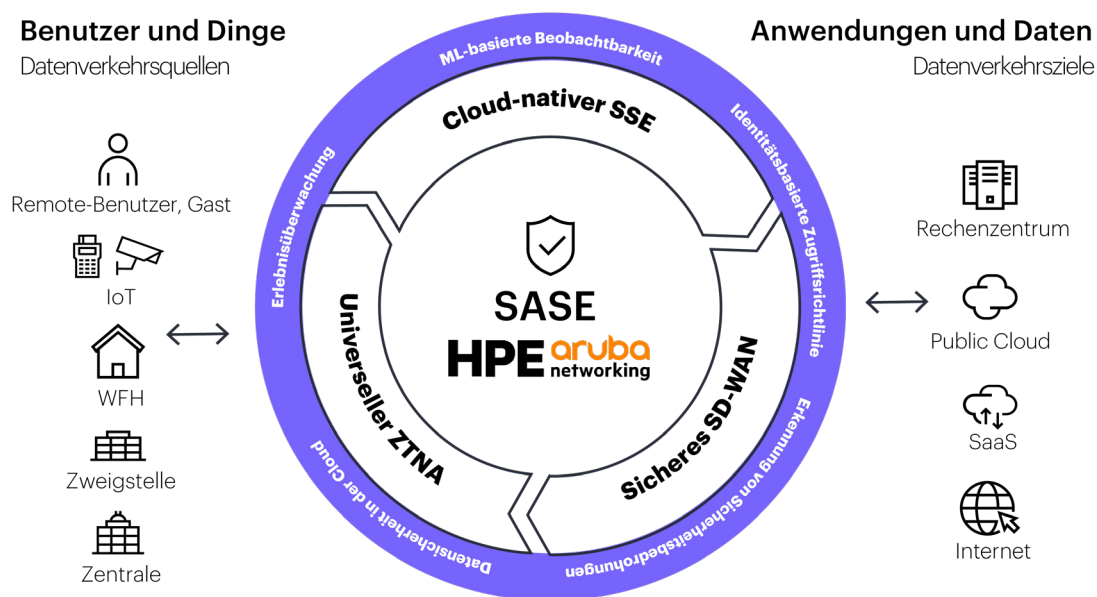


Abbildung 1. Umfassende Umsetzung der Zero Trust-Prinzipien für Benutzer, Geräte, Anwendungen und Daten

Eine einheitliche, als Komplettlösung konzipierte SASE-Plattform

Im Zentrum der Strategie von HPE steht eine einheitliche, zusammenhängende SASE-Architektur, die SD-WAN, Cloud-native SSE-Services und KI-basierte Geräteintelligenz in einer Plattform integriert. Im Gegensatz zu Multi-Vendor-SASE-Lösungen, die aus lose verbundenen Komponenten bestehen, ist der einheitliche SASE von HPE Aruba Networking als integriertes System konzipiert, aufgebaut und betrieben.

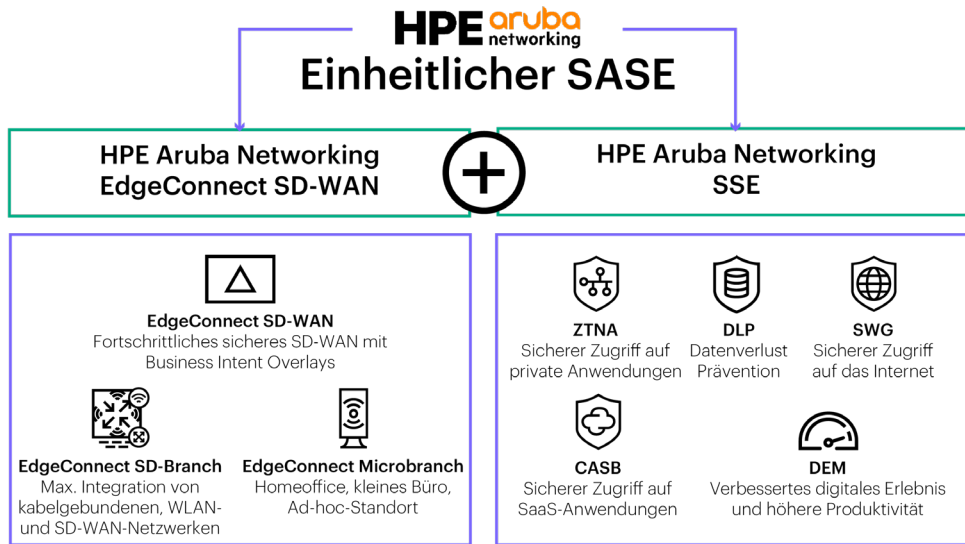


Abbildung 2. Der einheitliche SASE von HPE Aruba Networking integriert SD-WAN und SSE in einer zusammenhängenden Plattform

Ein wesentliches Unterscheidungsmerkmal ist die native, voll automatisierte Integration zwischen HPE Aruba Networking EdgeConnect SD-WAN und HPE Aruba Networking SSE. Während viele Anbieter auf API-Stitching, manuelle Richtlinien synchronisierung oder Service-Chaining setzen, beseitigt HPE diese betrieblichen Abhängigkeiten.

Die Integration erfolgt vollautomatisch, mit sofortiger Verbindung zwischen Edge und SSE-Cloud. Eine manuelle Tunnelkonfiguration, Richtlinienübersetzung oder Synchronisierung ist nicht erforderlich. Dadurch werden Risiken reduziert und die Bereitstellung wird beschleunigt.

Hauptvorteile des einheitlichen SASE von HPE Aruba Networking

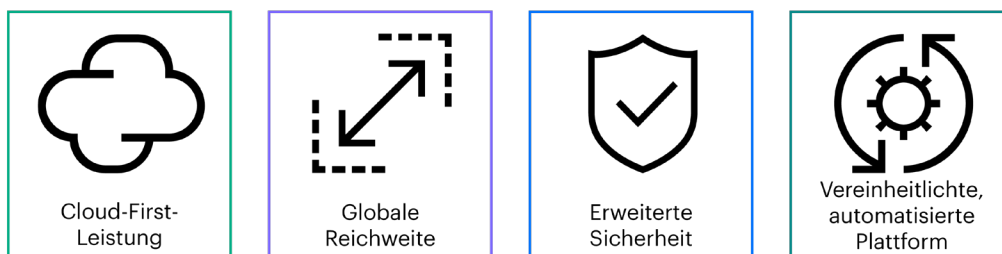


Abbildung 3. Die Hauptvorteile des einheitlichen SASE von HPE Aruba Networking

Cloud-First-Leistung für moderne Anwendungen

Die Leistung ist in SASE-Architekturen essentiell, da die Sicherheit weder zu zusätzlichen Latenzzeiten führen noch die Benutzerfreundlichkeit beeinträchtigen darf. HPE Aruba Networking EdgeConnect SD-WAN wurde für Cloud-First-Datenverkehr entwickelt und verwendet geschäftsorientierte Richtlinien, um Backhauling zu vermeiden und eine konsistente Anwendungsleistung zu gewährleisten.

Die First-Packet-iQ-Funktion identifiziert Tausende von Anwendungen und Domänen bereits im ersten Paket und ermöglicht so eine intelligente Verkehrssteuerung. Mit dieser Funktion können Unternehmen Sicherheitsrichtlinien erstellen, die vertrauenswürdigen Cloud-Anwendungsdatenverkehr, wie z. B. UCaaS-Datenverkehr, direkt ins Internet leiten, während der gesamte übrige Datenverkehr zur Sicherheitsprüfung an eine SSE-Lösung (Security Service Edge) gesendet wird, bevor er an den SaaS-Anbieter oder das Rechenzentrum weitergeleitet wird.

EdgeConnect SD-WAN lässt sich zudem nativ in führende Cloud-Anbieter wie AWS, Microsoft Azure und Google Cloud™ sowie Konnektivitätspartner wie Equinix und Megaport integrieren und verbessert so Leistung, Zuverlässigkeit und Benutzerfreundlichkeit bei der Verbindung von Zweigstellen mit der Cloud.

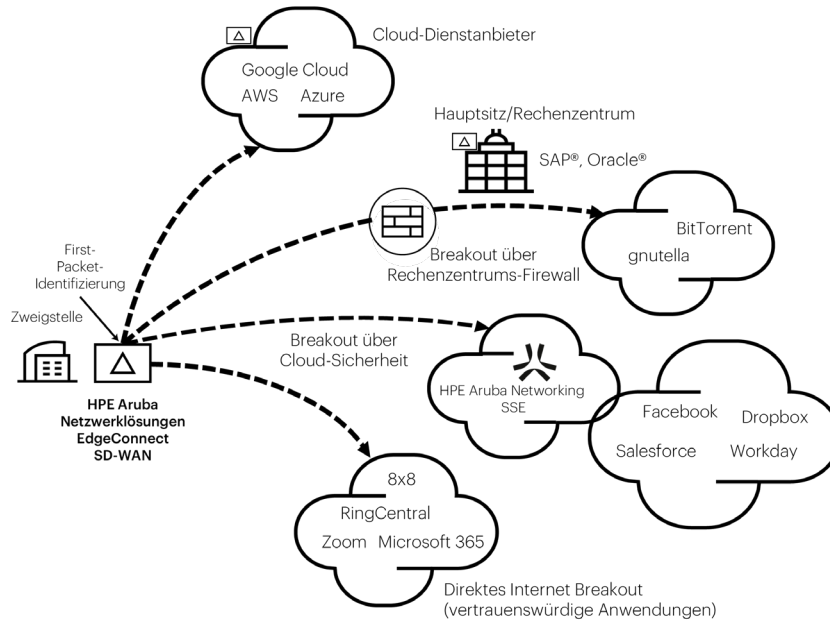


Abbildung 4. Intelligente Steuerung des Datenverkehrs von der Zweigstelle zur Cloud durch First-Packet-Identifizierung

Darüber hinaus bietet die SD-WAN-Lösung WAN-Modernisierungsfunktionen, die Unternehmen bei der Umstellung von traditionellen MPLS-Architekturen auf Cloud-First-Netzwerke mit flexibleren und kostengünstigeren Internetverbindungen unterstützen:

- **Business Intent Overlays** ermöglichen es Teams, Netzwerk-Anforderungen in Bezug auf Anwendungsleistung, Sicherheitsstatus und Geschäftspriorität zu definieren. So kann die Plattform dieses Ziel dynamisch im gesamten Netzwerk durchsetzen, ohne komplexe Routing-Tabellen verwalten zu müssen.
- **Tunnel Bonding** bündelt mehrere WAN-Verbindungen zu einem einzigen logischen Overlay und ermöglicht die Echtzeit-Verkehrssteuerung über Breitband-, MPLS- oder gemischte Verbindungen basierend auf den Unternehmensrichtlinien. Wenn eine Verbindung beeinträchtigt wird oder ausfällt, wird der Datenverkehr automatisch auf verbleibende Pfade oder Backup-Verbindungen umgeleitet, um eine kontinuierliche Konnektivität zu gewährleisten.
- **Pfadkonditionierung** bietet die Leistung einer Standleitung über Standard-Internetleitungen. Paketverluste, Jitter und Latenzzeiten werden reduziert, wodurch die Abhängigkeit von MPLS verringert wird, während gleichzeitig eine vorhersehbare Leistung für Echtzeit- und geschäftskritische Anwendungen gewährleistet bleibt. Die Vorwärtsfehlerkorrektur (Forward Error Correction, FEC) stellt verlorene Pakete ohne erneute Übertragung wieder her, während die Korrektur der Paketreihenfolge (Packet Order Correction, POC) die richtige Reihenfolge über gebündelte Verbindungen hinweg sicherstellt. AppExpress verbessert die Leistung zusätzlich, indem es die Anwendungserfahrung überwacht und bei Erkennung einer Beeinträchtigung automatisch den optimalen Pfad auswählt.
- **Die WAN-Optimierung**, einschließlich TCP-Beschleunigung, Datenkompression und Datendeduplizierung, verbessert die Reaktionsfähigkeit für verteilte Benutzer und bandbreitenbeschränkte Umgebungen zusätzlich und reduziert gleichzeitig die Latenz.

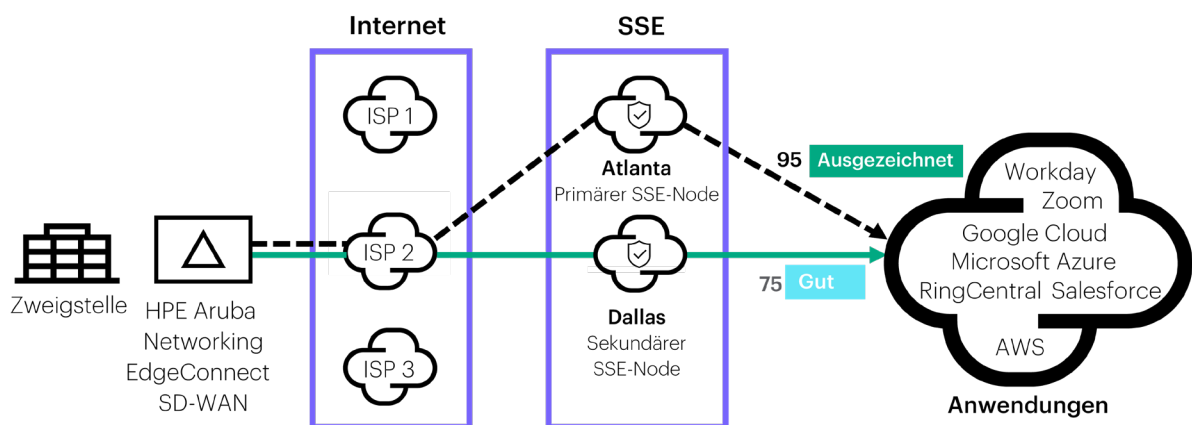


Abbildung 5. Optimierte Benutzererfahrung für geschäftskritische Anwendungen mit AppExpress, auch über SSE-Routing hinweg

Integrierte Sicherheit für Zweigstellen mit fortschrittlichen NGFW-Funktionen

Aus der Cloud bereitgestellte Sicherheit ist zwar unerlässlich, Zweigstellen und Campusgelände benötigen jedoch auch weiterhin einen starken lokalen Schutz. HPE begegnet diesem Bedarf, indem es Next-Generation-Firewall-Funktionen (NGFW) direkt in die SD-WAN-Fabric integriert. Dieser integrierte Stack bietet zustandsabhängige Firewalling-Funktionen, IDS/IPS, rollenbasierte Segmentierung, URL Filtering und adaptiven DDoS-Schutz auf einer einzigen SD-WAN-Plattform, wodurch ältere Zweigstellen-Firewalls überflüssig werden und die operative Komplexität verringert wird.

- **IDS/IPS:** Nutzt signaturbasierte Erkennung zur Identifizierung bekannter Bedrohungen und unterstützt Inline-Blockierung und Out-of-Path-Analyse für Hochleistungsumgebungen. Ereignisse können zur Echtzeit-Transparenz und -Reaktion an SIEM-Plattformen wie Splunk weitergeleitet werden.
- **Adaptive DDoS:** Nutzt maschinelles Lernen, um DoS-Schwellenwerte automatisch auf Basis von Echtzeit-Verkehrsmustern anzupassen, wodurch eine manuelle Feinabstimmung entfällt. Auto Rate-Limiting legt dynamische Basiswerte fest, während Smart Burst ungenutzte Kapazität über Firewall-Zonen verteilt, um den Schutz aufrechtzuerhalten.
- **URL Filtering:** Blockiert schädliche und risikobehaftete Websites mithilfe von maschinellem Lernen, um Domains und URLs in kategorisierte Risikostufen einzuordnen. Reputationsbewertung und Echtzeit-IP-Intelligence helfen bei der Identifizierung neuer Bedrohungen und der konsequenten Durchsetzung von Richtlinien.
- **Rollenbasierte Segmentierung:** Da die Sicherheit in die SD-WAN-Fabric integriert ist, sind Ost-West-Verkehr, IoT-Kommunikation und lokale Übergänge zum Internet standardmäßig geschützt. Die zentrale Segmentierung über LAN und WAN setzt einheitliche Richtlinien durch, wobei ClearPass Identitäts- und Rolleninformationen ergänzt – ganz ohne komplexe VLAN-Architekturen.

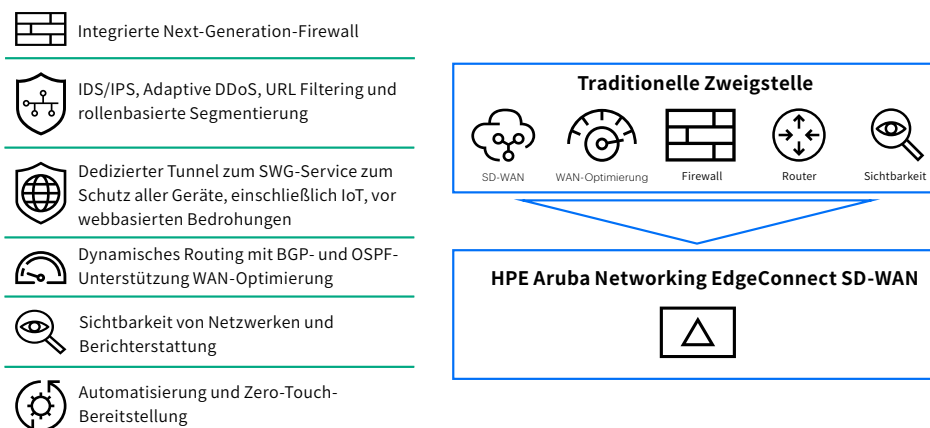


Abbildung 6. Legen Sie Ihre Zweigstellenausrüstung zusammen, indem Sie bisher verwendete Firewalls und Router durch ein sicheres SD-WAN wie HPE Aruba Networking EdgeConnect SD-WAN ersetzen

Umfassende Integration mit einem aus der Cloud bereitgestellten Secure Web Gateway (SWG)

Eine entscheidende Lücke in vielen SASE- und Zero-Trust-Architekturen besteht im Schutz von Geräten, auf denen keine Endpunkt-Agenten ausgeführt werden können, wie z. B. IoT-Sensoren, Drucker, Kameras, medizinische Geräte, industrielle Systeme und Gast-Endgeräte.

HPE begegnet diesem Problem durch die Kombination von rollenbasierter Segmentierung mit einer umfassenden Integration in seine über die Cloud bereitgestellte Softwareentwicklungsplattform. Dieser einheitliche Ansatz bietet Schutz vor Malware, Webfilterung und Bedrohungsabwehr für alle Geräte – ob verwaltet oder nicht – ohne dass ein SSE-Agent erforderlich ist. Der Datenverkehr dieser Geräte wird automatisch über einen dedizierten Tunnel via EdgeConnect SD-WAN geleitet, wodurch ein durchgängiger Schutz auf Netzwerkebene gewährleistet wird, ohne dass Agenten auf jedem Gerät installiert werden müssen. Mit diesem agentenlosen Modell können Unternehmen eine immer größer werdende Angriffsfläche für das IoT sichern, Einblick in das Verhalten von Geräten gewinnen, Segmentierung durchsetzen und böswillige Aktivitäten auf bisher nicht verwalteten Endpunkten verhindern.

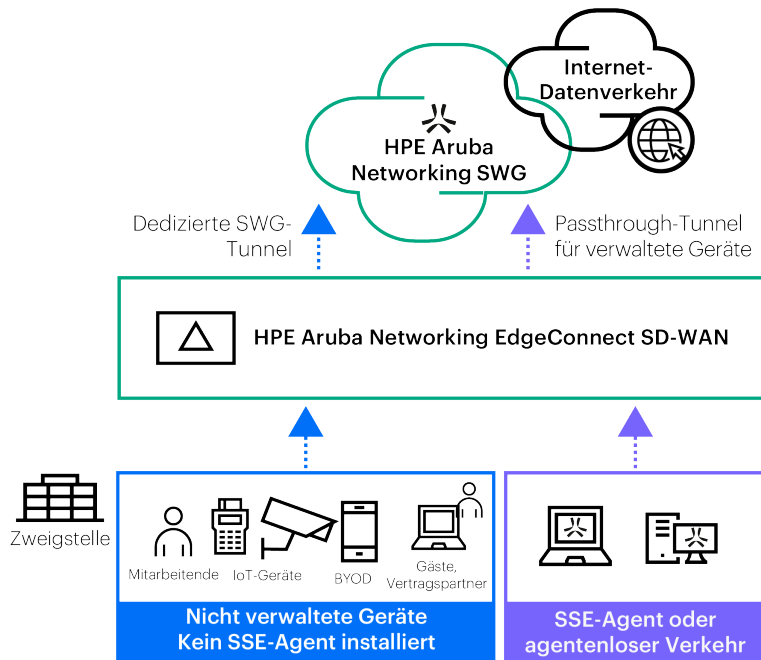


Abbildung 7. Schützen Sie alle Geräte – verwaltete wie nicht verwaltete – vor webbasierten Bedrohungen, ohne auf jedem Gerät einen SSE-Agenten installieren zu müssen

Cloud-nativer SSE mit einer einzigen Richtlinien-Engine und Benutzeroberfläche

Als Ergänzung zu SD-WAN bietet HPE Aruba Networking SSE alle Cloud-basierten Sicherheitsservices über eine einzige Richtlinien-Engine und eine einzige Benutzeroberfläche. Die Funktionen von SWG, ZTNA (Zero Trust Network Access) und CASB (Cloud Access Security Broker) werden einmal festgelegt und für alle Benutzer und Standorte einheitlich durchgesetzt.

Dieses einheitliche Richtlinienmodell macht die Verwaltung separater Richtlinien für verschiedene Sicherheitsservices überflüssig. Änderungen werden automatisch weitergegeben, wodurch Konfigurationsfehler reduziert und Reaktionen auf neu auftretende Bedrohungen beschleunigt werden.

Im Gegensatz zu Architekturen, die auf der Verkettung mehrerer Services über verschiedene Präsenzzpunkte hinweg basieren, bietet HPE Aruba Networking alle Sicherheitsfunktionen innerhalb eines einzigen PoP. Dieses Design vermeidet unnötige Latenz, verbessert die Zuverlässigkeit und vereinfacht die Fehlerbehebung.

Ein umfangreiches Angebot an aus der Cloud bereitgestellten Sicherheitsfunktionen

HPE Aruba Networking SSE bietet eine umfassende Suite von aus der Cloud bereitgestellten Sicherheitsservices zum Schutz von Benutzern, Geräten und Anwendungen in verteilten Umgebungen. Diese integrierten Funktionen bieten identitätsbasierten Zugriff, erweiterten Schutz vor Bedrohungen und detaillierte Kontrolle über Cloud-Services.

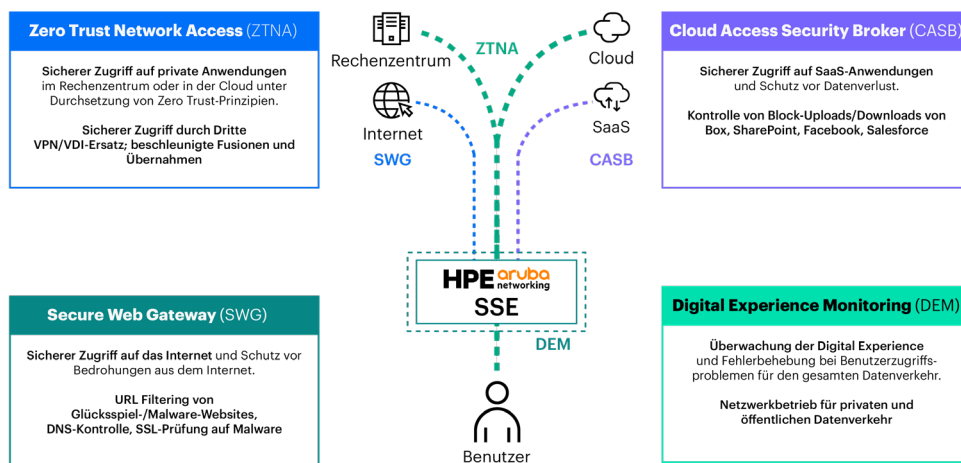


Abbildung 8. HPE Aruba Networking SSE bietet fortschrittliche, aus der Cloud bereitgestellte Sicherheitsservices wie ZTNA, SWG, CASB und DEM

Globale Ebene unterstützt von Hyperscalern

Der einheitliche SASE von HPE Aruba Networking basiert auf einer Hyperscaler-gestützten Infrastruktur mit AWS, Microsoft Azure und Google Cloud und über 500 globalen Edge-Standorten für einen Zugriff mit geringer Latenz sowie elastische Skalierbarkeit.

Intelligentes Routing verbindet mehrere PoPs, um den besten Pfad auszuwählen, während gemeinsam in jedem PoP vorhandene Services ein schnelles Failover und Failback ermöglichen. Dadurch wird sichergestellt, dass die Benutzer für eine gleichbleibende Leistung immer mit dem nächstgelegenen Edge verbunden sind. Die Sicherheitsservices lassen sich dynamisch erweitern, um die Nachfrage zu decken, die Ausfallsicherheit bei Verkehrsspitzen oder Angriffen zu gewährleisten und die Probleme bei der Kapazitätsplanung zu beseitigen.

KI-basierte NAC: Transparenz, Kontext und adaptive Durchsetzung

Ein zentraler Pfeiler des einheitlichen SASE von HPE Aruba Networking ist KI-basierte Netzwerkzugriffsteuerung (NAC) für umfassende Transparenz und Kontextverständnis in der gesamten Umgebung. Vielen herkömmlichen SASE-Lösungen mangelt es an Einblick in die Geräteidentität und das Geräteverhalten, insbesondere für nicht verwaltete Endpunkte.

HPE Aruba Networking NAC erstellt kontinuierlich Geräteprofile mithilfe von maschinellem Lernen und identifiziert Typ, Rolle, Status und Verhalten in Echtzeit. Diese Erkenntnisse fließen in die Zugriffssteuerung und Segmentierung ein und ermöglichen so eine präzise, identitätsbasierte Durchsetzung.

In Kombination mit SASE unterstützt NAC adaptive Zero Trust-Richtlinien, die sich dynamisch an Risiken, Verhaltensanomalien oder Änderungen der Lage anpassen und so sicherstellen, dass die Sicherheit kontinuierlich bewertet und nicht einfach vorausgesetzt wird.

AIOps für optimierte Abläufe

Der SASE-Copilot optimiert Konfiguration und Fehlerbehebung durch KI-gestützte Analysen und Abfragen in natürlicher Sprache, die auf generativer KI (LLM) basieren. Das verbessert die Netzwerkkomplexität, reduziert Ausfallzeiten und liefert umsetzbare Einblicke für eine schnellere Reaktion auf Vorfälle, eine höhere Betriebseffizienz und eine proaktivere Sicherheitsstrategie.



Vereinfachung der SASE-Einführung – ohne Einschränkungen

Der einheitliche SASE von HPE Aruba Networking ist darauf ausgelegt, Unternehmen dort abzuholen, wo sie stehen, und unterstützt eine schrittweise Einführung ebenso wie die vollständige Transformation einer Plattform. Kunden können die Netzwerke ihrer Niederlassungen modernisieren, hybride Arbeitsmodelle absichern, IoT-Umgebungen schützen oder in die Cloud migrieren – ohne Abstriche bei der Leistung, Transparenz oder Sicherheit.

Durch die Beseitigung der Fragmentierung und die Integration von Zero Trust in die Netzwerk-Fabric vereinfacht HPE den Weg zu SASE und ermöglicht es Unternehmen, in einer verteilten Cloud-First-Welt sicher und effizient zu arbeiten.

Weitere Informationen unter

[HPE.com/networking](https://hpe.com/networking)

HPE.com besuchen



Jetzt chatten

© Copyright 2026 Hewlett Packard Enterprise Development LP. Die enthaltenen Informationen können sich jederzeit ohne vorherige Ankündigung ändern. Neben der gesetzlichen Gewährleistung gilt für Produkte und Services von Hewlett Packard Enterprise (HPE) ausschließlich die Herstellergarantie, die in den Garantieerklärungen für die jeweiligen Produkte und Services explizit genannt wird. Die hier enthaltenen Informationen stellen keine zusätzliche Garantie dar. Hewlett Packard Enterprise haftet nicht für technische oder redaktionelle Fehler oder Auslassungen in diesem Dokument.

Google Cloud ist eine eingetragene Marke von Google LLC. Azure, Microsoft und SharePoint sind in den USA und anderen Ländern eingetragene Marken oder Marken der Microsoft Corporation. SAP ist die Marke oder eingetragene Marke der SAP SE oder ihrer Tochterunternehmen in Deutschland und anderen Ländern. Oracle ist eine eingetragene Marke von Oracle und/oder deren Tochterunternehmen. Alle Marken Dritter sind Eigentum der jeweiligen Rechteinhaber.

a00156430DEE

HEWLETT PACKARD ENTERPRISE

hpe.com

