HPE aruba networking

Lösungsübersicht

Einführung in HPE Aruba Networking SSE

Ortsunabhängiger sicherer Zugriff auf alle Benutzer, Geräte und Anwendungen mit einer einzigen SSE-Plattform

HPE

Die Herausforderungen bei modernen Sicherheitslösungen

Es ist nicht zu übersehen, dass sich in der globalen Geschäftswelt ein enormer Wandel vollzogen hat. Immer mehr Benutzer, Anwendungen und Geräte agieren heute außerhalb des Schutzperimeters der herkömmlichen Netzwerksicherheit. IT-Führungskräfte erkennen nach jahrelangem Ringen mit herkömmlichen Netzwerksicherheitslösungen, dass der Sicherheitsbereich endlich einer dringenden Transformation bedarf. Unter Berücksichtigung der Anforderungen moderner Unternehmen erfinden sie die Grundbausteine des sicheren Zugriffs neu.

Gleichzeitig bestätigen Branchenanalysten den Wert dieses wegweisenden Schritts hin zu cloudbasierten Sicherheitslösungen aufgrund zunehmender Mobilität und der umfassenden Cloud-Einführung. Sie stellen eine neue Gruppe von Technologien unter der Bezeichnung Security Service Edge (SSE) in den Fokus, mit denen Teams ihre Strategien für sicheren Zugriff für alle Benutzer, Geräte und Anwendungen auf einfache und konsolidierte Weise modernisieren können. Die HPE Aruba Networking SSE-Lösung passt hervorragend zu dieser Entwicklung und bietet universellen, sicheren Zugriff, der auf die Anforderungen der sich ständig verändernden Geschäftswelt von heute zugeschnitten ist.

Was ist SSE?

Security Service Edge (SSE) ist eine umfassende cloudbasierte Lösung, die sicheren Zugriff, Transparenz und Governance für alle Geschäftsanwendungen gewährleistet. Sie stellt ein vereinheitlichtes Sicherheitsmodell dar, das wichtige Kernkomponenten wie Zero Trust Network Access (ZTNA) zum Schutz privater Anwendungen, Secure Web Gateway (SWG) für die Kontrolle des Internetzugriffs, Cloud Access Security Broker (CASB) zur Sicherung von SaaS-Anwendungen und Digital Experience Monitoring (DEM) enthält, um eine optimierte digitale Erfahrung bei allen Arten von Zugriffen zu gewährleisten. Diese Service-Konvergenz repräsentiert die Zukunft sicherer Konnektivität – ein einzigartiger, cloudzentrierter Service, mit dem IT-Abteilungen die Fähigkeit erlangen, den Zugriff auf Benutzer und Anwendungen zu regeln, unabhängig von ihrem physischen Standort, den von ihnen verwendeten Geräten oder den Netzwerken, mit denen sie sich verbinden.

HPE Aruba Networking SSE mag zunächst nur wie ein weiteres Akronym im umfangreichen IT-Lexikon wirken, es hat jedoch für moderne Arbeitsplätze einen besonderen Wert, weil es zur Hälfte ein SSE ist, während WAN Edge Services die andere Hälfte ausmachen.

Detailansicht SASE

Abbildung 1 zeigt, wie Gartner eine übergreifende SASE-Cloud-Infrastruktur definiert hat.

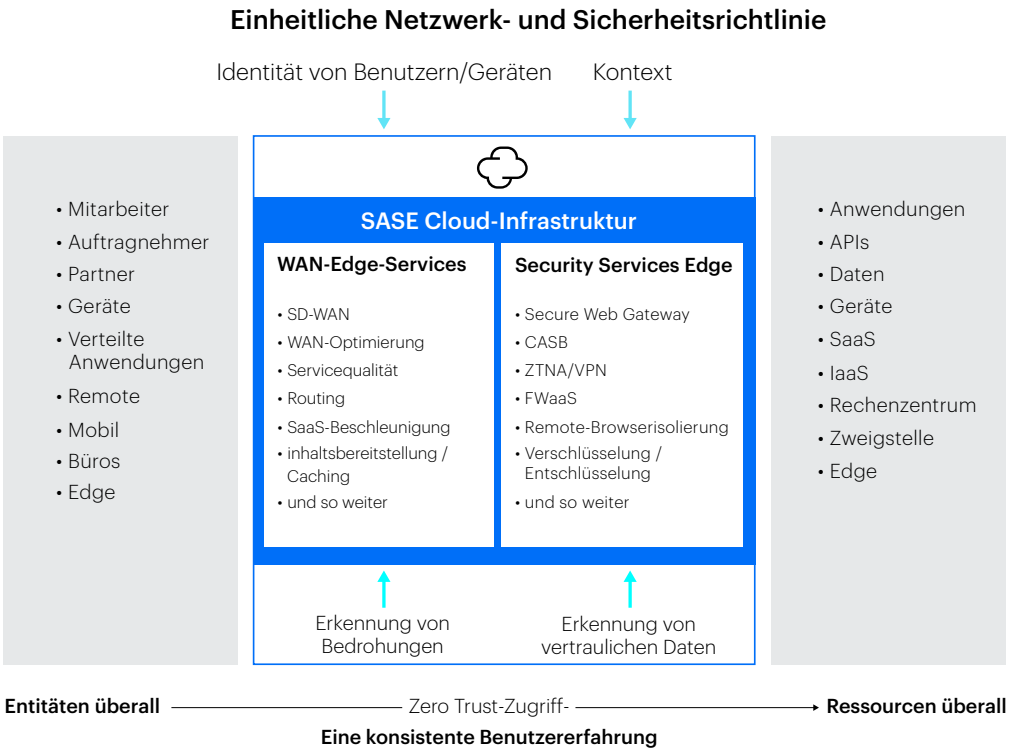

Abbildung 1. Detaillierte Ansicht eines umfassenden SASE-Frameworks

Schlüsseltechnologien in HPE Aruba Networking SSE

— **Zero Trust Network Access (ZTNA)**
ZTNA stellt eine enorme Verbesserung gegenüber dem herkömmlichen VPN-Zugriff auf private Anwendungen dar, da es den Anwendungszugriff auf Remote- und Hybrid-Benutzer ausweitet und nach der Authentifizierung nur den Zugriff auf autorisierte Ressourcen erlaubt. ZTNA stellt im Wesentlichen sicher, dass beim Zugriff auf Anwendungen keinem Benutzer oder Gerät standardmäßig vertraut wird. Stattdessen müssen alle Benutzer und Geräte robuste Identitätsüberprüfungsprozesse durchlaufen, um Zugriff auf entsprechende Ressourcen zu erhalten. Darüber hinaus wird das Prinzip der geringsten Zugriffsrechte angewandt, d. h. die Benutzer können nur auf die von den Administratoren genehmigten Anwendungen und Daten zugreifen.

— **Secure Web Gateway (SWG)**
SWG ist ein zentraler SSE-Service, der den Internetzugang verwaltet, indem er Unternehmensrichtlinien anwendet und verhindert, dass unerwünschter und unbekannter Internetverkehr in das interne Netzwerk eines Unternehmens gelangt. SWG schützt Benutzer vor dem Zugriff auf bösartige Websites, aus dem Internet eingeschleusten Viren und Malware und ermöglicht ihnen gleichzeitig den Zugriff auf Ressourcen, die sie für ihre Arbeit benötigen.

— **Cloud Access Security Broker (CASB)**
Ein CASB erweitert die SSE-Sicherheitsfunktion. Er setzt die Sicherheitsrichtlinien für den Zugriff und die Vermeidung von Datenverlusten durch, wenn Benutzer und Services auf verschiedene Unternehmensressourcen zugreifen (ob cloudbasiert, private Anwendungen usw.), und trägt zur Einhaltung der Sicherheitsrichtlinien des Unternehmens und der Branche bei.

— **Digital Experience Monitoring (DEM)**
Mit DEM können Unternehmen Ihren Mitarbeitern ein Benutzererlebnis bieten, das ihre Produktivität und Sicherheit gewährleistet. DEM überwacht die digitale Erfahrung der Benutzer, um sicherzustellen, dass das System mit Spitzen in der CPU-Auslastung, Netzwerkausfällen und Leistungsproblemen von Anwendungen umgehen kann. Gleichzeitig erhält die IT-Abteilung Einblicke und Metriken zu jedem Internet- und Netzwerkschritt.

Die Vorteile von HPE Aruba Networking SSE

HPE Aruba Networking SSE stellt eine moderne Alternative zu herkömmlichen netzwerkbasierten Sicherheitstechnologien (Firewalls, VPN-Gateway-Appliances und Web-Gateway-Appliances) dar und bietet einen Mehrwert für mehrere Teams.

Zu den Sicherheitsvorteilen von HPE Aruba Networking SSE gehören:

— universelle Sicherheit bei Zugriffen für alle Benutzer (Mitarbeiter und Dritte gleichermaßen), Geräte und Anwendungen

— einfachere Beseitigung von Angriffsflächen und Angriffsvektoren

— Minimierung der Auswirkungen von Ransomware- oder Malware-Angriffen, indem laterale Bewegungen reduziert werden

— Implementierung des Prinzips der geringsten Zugriffsrechte mit Zero Trust-Richtlinien

— Schutz vor Datenexfiltration durch verbesserte Kontrolle der Daten

— Verringerung blinder Flecken beim Thema Sicherheit, indem Transparenz und Kontrolle über die Schatten-IT erlangt werden

— Aktivierung von SSL-Verschlüsselung im großen Maßstab mit der Cloud

— eine zentrale Ansicht für universelle Transparenz und Zugriff auf alle Aktivitäten

Die Netzwerkvorteile von HPE Aruba Networking SSE sind ebenso überzeugend und umfassen Folgendes:

— Unterstützung aller Anwendungen – gleich ob Legacy- oder Cloud-Anwendungen – mit einer Single-Access-Lösung

— Minimierung des Anbieterwildwuchses und Vereinfachung der Networking-Services

— kein erweiterter Zugriff auf das Unternehmensnetzwerk, Zugriff wird auf bestimmte Anwendungen gewährt

— Segmentierung des Zugriffs auf einer granularen individuellen Basis, ohne Netzwerkzugriff und ohne Bedarf an einer Netzwerksegmentierung

— Optimierung der Konnektivitätspfade und Reduzierung der Latenzzeiten dank intelligentem Routing

— Reduzierung von Ausfällen und Downtime durch eine präzise Fehlerbehebung, bei der das digitale Erlebnis gewahrt wird

— beschleunigte Bereitstellung und mühelose Skalierung mit einer Cloud-Architektur

HPE Aruba Networking SSE revolutioniert den Ansatz von Unternehmen für die Netzwerksicherheit und -konnektivität mit einem agileren, sichereren und effizienteren Modell, das den Anforderungen moderner Unternehmen gerecht wird.

Die Elemente von HPE Aruba Networking SSE

HPE Aruba Networking **SSE Cloud**
Mit über 500 globalen Edge-Standorten, die auf dem Backbone von AWS, Microsoft, Azure und Google Cloud Platform™ ausgeführt werden, verbindet die SSE-Cloud auf der Grundlage intuitiver Zero Trust-Richtlinien alle autorisierten Benutzer sicher mit allen Geschäftsanwendungen.

HPE Aruba Networking **Benutzerportal**
Die Oberfläche für Endbenutzer, über die alle Benutzer basierend auf ihrer Identität und der festgelegten Zugriffsrichtlinie alle agentenbasierten oder agentenlosen Anwendungen, für die sie eine Berechtigung haben, anzeigen und problemlos per Mausklick aufrufen können.

HPE Aruba Networking **Richtlinien-Tags**
Mit dem logischen Tagging-System von HPE Aruba Networking SSE können IT-Administratoren innerhalb weniger Minuten detaillierte Zero Trust-Richtlinien definieren. Richtlinien können für Anwendungsgruppen, einzelne Anwendungen, Benutzergruppen, einzelne Benutzer, Standorte, Gerätestatus und weitere Kriterien definiert werden, was die Festlegung von Richtlinien vereinfacht.

HPE Aruba Networking **SSE Agent**
Der HPE Aruba Networking SSE Agent ist ein schlanker Agent, der auf dem Computer des jeweiligen Endbenutzers ausgeführt wird. Der SSE-Agent führt eine Analyse des Gerätestatus durch, verschlüsselt den Datenverkehr und leitet ihn dann automatisch zur HPE Aruba Networking SSE Cloud weiter. Der SSE-Agent passt die Zugriffsrechte kontinuierlich an Kontextänderungen an und unterstützt Anwendungen, für die ein Thick-Client-Zugriff erforderlich ist. Der SSE-Agent unterstützt sogar VoIP- (Peer-to-Peer) und serverinitiierte (ICMP) Abläufe. Für webbasierte Anwendungen ist kein Agent erforderlich. Stattdessen können Benutzer den agentenlosen Zugriff mit einem einfachen Browser nutzen.

HPE Aruba Networking **SSE Connector**
Der HPE Aruba Networking SSE Connector wird häufig paarweise bereitgestellt und ist eine schlanke virtuelle Maschine, die als Frontend für Ihre privaten Anwendungen eingesetzt wird, wenn Sie den ZTNA-Service nutzen. Der HPE Aruba Networking SSE Connector stellt eine sichere, ausschließlich ausgehende Verbindung mit Authentifizierung zwischen der Anwendung und der HPE Aruba Networking SSE Cloud her. Der SSE-Connector verschleiert den Standort Ihres Netzwerks und Ihrer Anwendungen und legt niemals IPs offen, wodurch er die Angriffsfläche und das Risiko internetbasierter Angriffe minimiert. Darüber hinaus spielt der SSE-Connector eine wichtige Rolle bei der Bereitstellung von Anwendungen für Benutzer ohne Netzwerkzugriff und bei der Bekämpfung des Risikos lateraler Bewegungen durch das Herstellen von Eins-zu-Eins-Verbindungen.

Wie funktioniert HPE Aruba Networking SSE?

HPE Aruba Networking SSE wurde entwickelt, um Unternehmen in einer einzigen Lösung umfassende Sicherheit beim Zugriff auf verschiedene Anwendungen zu bieten, sei es im Internet, in der Cloud oder privat gehostet. Und so funktioniert es:

1. **Der Benutzer versucht, auf die Anwendung zuzugreifen:** Ein Benutzer versucht, von einem beliebigen Standort auf der Welt auf eine Unternehmensanwendung zuzugreifen.
2. **HPE Aruba Networking SSE vermittelt Anfragen:** Die Anfrage wird vom nächstgelegenen unserer 500 Edge-Standorte empfangen, wodurch Teams möglicherweise risikoreiche Pass-Through-Verbindungen vermeiden können. HPE Aruba Networking SSE wird zur ersten Anlaufstelle und vermittelt alle Zugriffsanfragen im großen Maßstab.
3. **Der Benutzer wird identifiziert und authentifiziert:** Die HPE Aruba Networking SSE Plattform nutzt SAML- und SCIM-Attribute von einem internen oder externen IdP (ID-Provider), um den Benutzer oder die Entität zu identifizieren, die versucht, auf eine Ressource zuzugreifen. Dabei kann es sich um einen Mitarbeiter, einen Drittanbieter oder Partner handeln.
4. **Zero Trust-Richtlinien werden durchgesetzt:** Die HPE Aruba Networking SSE Plattform setzt kontextbasierte Zugriffsrichtlinien durch, beispielsweise auf der Grundlage der Identität der Benutzer, des Gerätestatus, des Benutzerstandorts usw. Die Durchsetzung der SSE-Richtlinien basiert auf Zero Trust-Prinzipien. Dies bedeutet, dass Benutzern nur Zugriff auf genau die Ressourcen gewährt wird, zu deren Nutzung sie berechtigt sind. Der Zero Trust-Zugriff wird für alle Anwendungstypen erzwungen, einschließlich privater Anwendungen, SaaS-Anwendungen und Internet-Browsing.
5. **Daten werden auf Bedrohungen überprüft:** Die HPE Aruba Networking SSE Plattform scannt den gesamten Datenverkehr auf Bedrohungen mit universeller SSL-Prüfung, Data Loss Prevention, URL-Filterung, Malware- und Antivirenscans sowie Sandboxing. Darüber hinaus umfasst die HPE Aruba Networking SSE Plattform Firewall-as-a-Service (FWaaS)-Funktionen, die vor externen Bedrohungen und Datenexfiltration schützen.
6. **Der schnellste Zugriffsweg wird ermittelt:** Der HPE Aruba Networking SSE Service nutzt Smart Routing über die Multi-Cloud-Architektur (AWS, Azure, GCP™), wobei automatisch der optimale Zugriffsweg über unsere 500 globalen Edge-Standorte auf der ganzen Welt ermittelt wird.
7. **Der Benutzer erhält Zugriff:** Nch der Identifizierjng, Verifizierimg und Einstufung des Benutzers als als sicher wird diesem über den schnellen Zugriffspfad Zugriff auf die jeweilige Ressource gewährt.
8. **Der Zugriff wird kontinuierlich überwacht und kontrolliert:** Die Leistung der HPE Aruba Networking SSE Plattform endet aber nicht nach der Herstellung der sicheren Verbindung. Sie überwacht kontinuierlich die Benutzeraktivitäten und Transaktionen und stellt sicher, dass verdächtiges Verhalten erkannt und kontrolliert wird.
9. **Der Zugriff wird bei Kontextänderungen angepasst:** Die HPE Aruba Networking SSE Plattform passt sich an aktuelle Bedrohungen und Änderungen im Benutzerverhalten, der Gerätefunktion und dergleichen an, um Risiken zu minimieren und einen robusten Sicherheitsstatus aufrechtzuerhalten.

In allen Phasen des Prozesses bietet die HPE Aruba Networking SSE Lösung Transparenz und Kontrolle über alle Interaktionen zwischen Benutzern und Anwendungen und gewährleistet die Sicherheit, ohne das Benutzererlebnis zu beeinträchtigen.

Abbildung 2 zeigt die Funktionsweise der HPE Aruba Networking SSE Plattform im Detail.

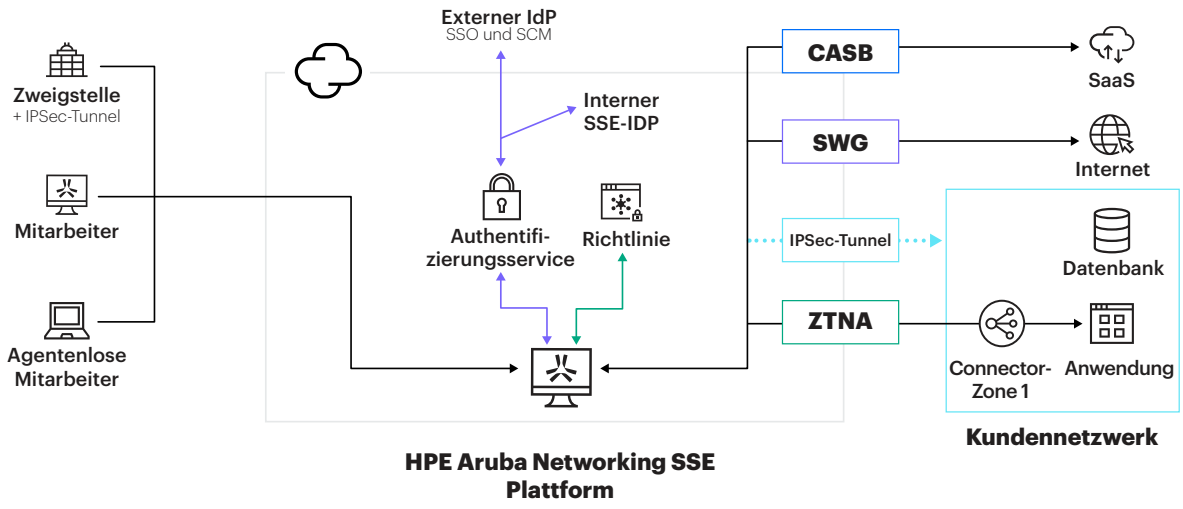

Abbildung 2. Architekturansicht der HPE Aruba Networking SSE Plattform

Was macht HPE Aruba Networking SSE einzigartig?

Nicht alle SSE-Lösungen sind gleich und die HPE Aruba Networking SSE-Lösung wurde von Grund auf mit der Zielsetzung entwickelt, den Bedarf der Kunden auf eine Weise zu erfüllen, die andere Anbieter nicht leisten können.

Universelle Sicherheit: ein neuer Sicherheitsstandard

Mit HPE Aruba Networking SSE erhalten Sie umfassende Sicherheit. Die Lösung bietet eine zentrale, sichere Konnektivitätsplattform, die den Zugriff für alle Benutzer, Geräte und Anwendungen sichert. Genießen Sie alle Funktionen an einem Ort: eine Cloud, eine Schnittstelle und einen Regelsatz für umfassenden Schutz.

Vereinfachtes Management: Ihre Kommandozentrale

HPE Aruba Networking SSE vereinfacht das Sicherheitsmanagement. Unsere intuitive, zentrale Ansicht verbessert die betriebliche Effizienz und minimiert den Verwaltungsaufwand. Die Plattform bietet ein einfaches und dennoch detailliertes Richtlinien- und Zugriffsmanagement und ermöglicht eine rationalisierte, aber fein abgestimmte Kontrolle über Ihr gesamtes Unternehmensnetzwerk.

Ausfallsichere Multi-Cloud-Architektur: das Rückgrat Ihres Unternehmens

HPE Aruba Networking SSE ist skalierbar und für die Cloud konzipiert, um die wachsenden und sich entwickelnden Leistungsanforderungen Ihres Unternehmens zu erfüllen. Unsere Multi-Cloud-fähige HPE Aruba Networking SSE Architektur ist skalierbar und flexibel, basiert auf den zuverlässigsten Cloud-Plattformen (AWS, Azure und GCP) und verfügt über mehr als 500 globale Edge-Standorte[1], wodurch sicherer Zugriff in unmittelbarer Nähe zu Endbenutzern ermöglicht wird.

Smart Routing: der schnelle Weg zur Konnektivität

Intelligenz ist ein fester Bestandteil der HPE Aruba Networking SSE Plattform. Die Konnektivität wird automatisch optimiert, indem die Route mit der geringsten Latenz für die Verbindung globaler Benutzer über alle weltweiten Edge-Standorte hinweg gesucht wird, was die Leistung verbessert und Ausfallzeiten reduziert. Diese intelligente Plattform zeichnet sich durch Folgendes aus:

— **Beschleunigter, multiregionaler Zugriff:** HPE Aruba Networking SSE verbindet Benutzer schnell mit Anwendungen, indem es den kürzesten Pfad zur nächstgelegenen Version der Anwendung findet. Dies sorgt für mehr Zuverlässigkeit und ein besseres Nutzungserlebnis.

— **TCP-Optimierung:** Die HPE Aruba Networking SSE Lösung hält Verbindungen stabil und verlässlich, indem sie die Art und Weise anpasst, wie Datenpakete gesendet werden. Dies ist entscheidend für die reibungslose Ausführung der Anwendungen und für ein großartiges Benutzererlebnis.

Diese wichtigen Funktionen von HPE Aruba Networking SSE bringen eine optimierte Sicherheit, Leistung und Verwaltung mit sich, sodass Benutzer von einem besseren Erlebnis und IT-Administratoren von effizienteren Abläufen profitieren.

[1] "Secure Access to All Corporate Resources from Anywhere with HPE Aruba Networking SSE," by SANS Research Program, HPE, June 2024.

Lösungsübersicht

ZTNA von HPE Aruba Networking ist auf die Anforderungen einer modernen, hybriden Belegschaft ausgelegt und bietet schnellen, sicheren Zugriff auf Unternehmensressourcen, während IT-Abteilungen gleichzeitig transparente Einblicke und die Kontrolle behalten.

ZTNA

Weil immer mehr Unternehmen auf eine mobile Belegschaft setzen und die Nutzung der Cloud vorantreiben, haben entsprechend viele Teams angesichts der neuen Situation Schwierigkeiten, das gleiche Maß an Sicherheit und Kontrolle zu erreichen, das sie einst hatten. ZTNA von HPE Aruba Networking ist eine moderne Lösung, die sicheren Zugriff auf private Anwendungen bietet. Im Rahmen des umfassenderen HPE Aruba Networking SSE Frameworks stellt unser ZTNA sicher, dass nur berechtigte Benutzer auf autorisierte private Anwendungen zugreifen können. Das verkleinert die Angriffsfläche und erhöht die Sicherheit. ZTNA arbeitet nach dem Prinzip der geringsten Zugriffsrechte. Dabei wird den Benutzern nur der minimale Zugriff gewährt, den sie für die Ausführung ihrer Aufgaben benötigen.

Der ZTNA-Service unterstützt eine Vielzahl von agentenbasierten oder agentenlosen Anwendungen, darunter moderne Web-Anwendungen, aber auch bisher verwendete Thick-Client-Anwendungen. Benutzer profitieren vom schnellen Zugriff auf lokale und cloudbasierte Anwendungen, ohne sich wiederholt anmelden zu müssen oder den Standort der Anwendung zu kennen, wodurch ein nahtloses Zugriffserlebnis entsteht. Darüber hinaus bietet ZTNA adaptive Zugriffskontrollen, bei denen der Kontext von Zugriffsanforderungen kontinuierlich ausgewertet wird, um die Berechtigungen dynamisch basierend auf dem Benutzerverhalten und anderen Faktoren anzupassen.

ZTNA macht Schluss mit herkömmlichen VPN-Lösungen und bietet eine detaillierte, richtlinienbasierte Zugriffskontrolle, die auf Zero Trust-Sicherheit ausgerichtet ist. ZTNA von HPE Aruba Networking ist auf die Anforderungen einer modernen, hybriden Belegschaft ausgelegt und bietet schnellen, sicheren Zugriff auf Unternehmensressourcen, während IT-Abteilungen gleichzeitig transparente Einblicke und die Kontrolle behalten. Dieser Ansatz erhöht nicht nur die Sicherheit, sondern verbessert auch das allgemeine Benutzererlebnis mit einem schnellen und zuverlässigen Zugriff auf erforderliche Anwendungen.

Wichtige Merkmale und Funktionen von ZTNA

Sicherer Zugriff auf alle privaten Anwendungen
Sicherer Zugriff auf alle privaten Anwendungen, einschließlich moderner Web-Anwendungen (SSH, RDP, Git, DB usw.) oder bisher verwendete Thick-Client-Anwendungen (VOIP, ICMP, AS400 usw.).

Agentenbasierter oder agentenloser Zugriff
Zugriff auf private Anwendungen, mit oder ohne Agenten. Integrationen in beliebige SSO-Lösungen sorgen für ein reibungsloses Benutzererlebnis.

Minimierte Angriffsfläche
Minimierte Angriffsfläche durch Eliminierung aller offenliegenden Netzwerk- und Anwendungs-IPs. Machen Sie Ihr Netzwerk für das offene Internet und Angreifer unsichtbar, während Sie den Benutzern nur Zugriff auf bestimmte private Anwendungen gewähren, jedoch niemals vollständigen Netzwerkzugriff.

Geringste Zugriffsrechte
Mit einfachen Zero Trust-Richtlinien auf Grundlage von Identität und adaptivem Kontext können Unternehmen unkompliziert das Prinzip der geringsten Zugriffsrechte bis auf die Anwendungsebene durchsetzen. Keine komplexe Mikrosegmentierung erforderlich, nur Zero Trust-Durchsetzung.

SSL-Prüfung für private Anwendungen
Nutzen Sie SSL-Prüfungen im großen Maßstab, um zu ermitteln, wer auf welche URLs zugegriffen hat, und heruntergeladene Dateien anzuzeigen, verwendete Befehle zu betrachten und Warnmeldungen zu erhalten.

Unterstützung aller Ports und Protokolle
Anders als bei anderen ZTNA-Lösungen wird VPN durch unseren ZTNA vollständig ersetzt, da alle Ports und Protokolle unterstützt werden. So können Unternehmen in Technologien und Plattformen investieren, die bei der Konsolidierung helfen und Legacy-Technologien überflüssig machen.

Wie funktioniert ZTNA?

Abbildung 3 bietet einen Überblick darüber, wie ZTNA in einer Geschäftsumgebung funktioniert.

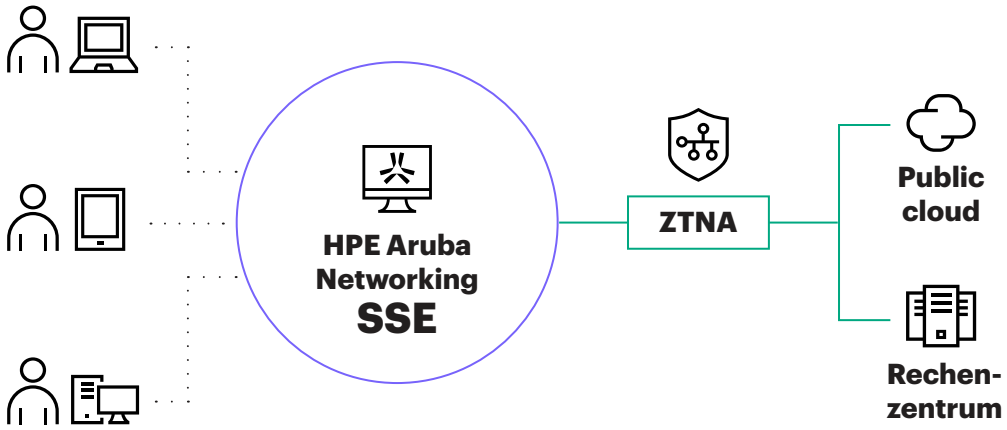

Abbildung 3. Architekturansicht des HPE Aruba Networking ZTNA-Service

1. **Ein Benutzer versucht, auf eine private Anwendung zuzugreifen**
   Sichern Sie den Zugriff auf alle Ports und Protokolle – sogar VoIP und ICMP – und unterstützen Sie den Zugriff mit und ohne Agent
2. **Der ZTNA-Service vermittelt die Anfrage**
   Anstatt den VPN-Konzentrator im Unternehmensnetzwerk anzupingen, geht die Anfrage zur Auswertung direkt an die HPE Aruba Networking SSE Plattform.
3. **Der ZTNA-Service validiert die Identität und Richtlinie**
   Überprüfen Sie die Benutzeridentität und setzen Sie die Zero Trust-Richtlinie durch. Zugriffsrechte werden bei Änderungen an Inhalten (Gerätestatus, Standort usw.) automatisch angepasst.
4. **ZTNA identifiziert den nächstgelegenen HPE Aruba Networking SSE Connector**
   Sobald der Zugriff gewährt wird, signalisiert die HPE Aruba Networking SSE Cloud dem nächstgelegenen HPE Aruba Networking SSE Connector, der ausschließlich mit der HPE Aruba Networking SSE Cloud kommuniziert, eine sichere ausgehende Verbindung mit der privaten Anwendung herzustellen.
5. **ZTNA stellt eine sichere Verbindung zur Ressource her**
   Der ZTNA-Service stellt die Konnektivität zwischen dem Benutzer und der Anwendung über eine ausgehende Verbindung her. So werden private Anwendungen im Internet unsichtbar, Benutzer können nicht auf das Netzwerk zugreifen und erhalten eine sicherere Verbindung zu wertvollen Anwendungen.
6. **ZTNA überprüft den Datenverkehr und überwacht das Benutzererlebnis**
   Der ZTNA-Service überprüft weiterhin den Datenverkehr der privaten Anwendung und das Benutzerverhalten, um potenzielle Bedrohungen zu erkennen und davor zu warnen. Gleichzeitig wird das allgemeine Benutzererlebnis verbessert.

Vorteile des ZTNA

— **Universeller Zugriff leicht gemacht:** ZTNA vereinfacht den Zugriff auf Unternehmensressourcen mit einem konsistenten und nahtlosen Verbindungserlebnis unabhängig vom Standort des Benutzers. Wenn Mitarbeiter von zu Hause oder im Büro arbeiten, stellt ZTNA sicher, dass sie schnellen und zuverlässigen Zugriff auf alle erforderlichen Unternehmensressourcen haben.

— **Schnellere Zugriffsgeschwindigkeiten:** ZTNA steigert die Produktivität durch eine Optimierung des Datenverkehr-Routings, mit der sichergestellt wird, dass der schnellste und effizienteste Weg zur erforderlichen Ressource verwendet wird. Dies wird ohne manuelles Eingreifen von Benutzern oder IT-Mitarbeitern erreicht, wodurch die Latenz im Datenverkehr reduziert und die Gesamtleistung verbessert wird.

— **Geringere Angriffsfläche mit Zero Trust:** Mit dem Grundsatz „Niemals vertrauen, immer überprüfen" minimiert ZTNA die Angriffsfläche. Die Technologie macht private Ressourcen im Internet unsichtbar und setzt das Prinzip der geringsten Zugriffsrechte durch, wodurch sichergestellt wird, dass nur autorisierte Benutzer auf das Netzwerk und seine Ressourcen zugreifen können. Dieser Ansatz verringert das Risiko unbefugter Zugriffe und möglicher Datenschutzverletzungen erheblich.

— **Reduzierung des Verwaltungsaufwands:** ZTNA optimiert das Management von Remote-Zugriffen. Die Technologie macht herkömmliche VPN-Lösungen und einen Großteil des damit verbundenen Sicherheits-Stacks für eingehende Verbindungen überflüssig. Unternehmen können alle Aspekte des Remote-Zugriffs – Richtlinien, Anwendungen, Geräte, Benutzer und Daten – über eine einzige Schnittstelle verwalten, was die Administration und bedarfsabhängige Skalierung vereinfacht.

SWG

HPE Aruba Networking SWG ist ein SWG-Service der nächsten Generation, mit dem der Zugriff auf das Internet an allen Arbeitsplätzen mühelos und sicher wird. Der Cloud-Service fungiert als Sicherheitsbroker zwischen mobilen Benutzern, Büros und Niederlassungen einer Organisation und dem offenen Internet. HPE Aruba Networking SSE prüft den Internetverkehr und vermittelt die schnellstmögliche Verbindung über die Cloud, sodass Unternehmen verschiedene netzwerkzentrierte Outbound-Gateway-Appliances als Teil einer größeren HPE Aruba Networking SSE Plattform ersetzen können.

Unsere SWG-Lösung bietet eine fließende SSL-Datenverkehrsprüfung mit einer Proxy-Architektur für die automatische Vermittlung von Verbindungen zum Internet. Der SWG-Service umfasst anpassbare Zugriffskontrollen, die Zero Trust auf den Internet- und SaaS-Zugriff anwenden und gleichzeitig die Benutzer vor Bedrohungen schützen. Darüber hinaus ist er mit Datensicherungsfunktionen ausgestattet, die Einblick in die Benutzeraktivität bieten und Inline-DLP-Kontrollen (Data Loss Prevention) anwenden, um Datenlecks zu verhindern. Der SWG-Service ermöglicht außerdem die einfache Erkennung und Verhinderung komplexer Angriffe durch den Schutz mit Threat Intelligence, Malware- und Virenscans, Cloud-Firewall-Funktionen und Sandboxing in Echtzeit.

Wichtige Merkmale und Funktionen von SWG

DNS/URL-Filterung: Blockiert proaktiv den Zugriff auf bösartige Websites und Inhalte und schützt so die Integrität Ihres Netzwerks und Ihrer Benutzerdaten. Dazu werden DNS-Abfragen abgefangen und die URLs anhand einer ständig aktualisierten Datenbank bekannter bösartiger Websites analysiert. Bei Erkennung einer Übereinstimmung wird der Zugriff auf die Site blockiert, um mögliche Sicherheitsverletzungen zu verhindern.

Schutz mit Threat Intelligence: Diese Schutzebene nutzt fortschrittliche Algorithmen und Bedrohungsdaten in Echtzeit und blockiert den Zugriff auf riskante URLs und Domänen. Dabei werden der Inhalt, die Domänendetails und der Reputationswert jeder Website bewertet. Websites mit verdächtigen oder bösartigen Merkmalen werden eingeschränkt, wodurch das Risiko von Cyber-Bedrohungen verringert wird.

DLP für den Internetzugriff: DLP verhindert, dass vertrauliche Daten die Grenzen des Unternehmens verlassen, auch im Internetverkehr. DLP für den Internetzugriff verwendet Datensicherheitsprofile, in denen festgelegt ist, welche Daten vertraulich sind, und vergleicht Regex-Muster, um alle Daten zu scannen und solche zu erkennen, die mit den Profilen übereinstimmen. Wenn eine Übereinstimmung gefunden wird, werden vordefinierte Aktionen durchgesetzt, um den Datenfluss zu steuern und das Risiko von Datenlecks zu verringern.

Malware- und Antivirenscans: Schützen Sie sich vor bekannten Viren und Malware durch Hash-Matching und Antiviren-Scantechniken. Dateien und Datenpakete werden gescannt und mit einer Datenbank mit Signatur-Hashes abgeglichen, die nachweislich mit Malware in Verbindung stehen. Bei Hash-Übereinstimmungen wird die Datei als bösartig gekennzeichnet und es werden entsprechende Maßnahmen ergriffen, um die Bedrohung zu neutralisieren.

Cloud-Firewall (FWaaS): Die Cloud-Firewall (oder FWaaS) filtert den Netzwerkverkehr innerhalb der HPE Aruba Networking SSE Cloud. Sie unterstützt alle Ports und Protokolle und ermöglicht eine detaillierte Kontrolle des Netzwerkzugriffs. Richtlinien können so konfiguriert werden, dass Datenverkehr anhand verschiedener Kriterien zugelassen oder verhindert wird. Dadurch wird sichergestellt, dass nur legitimer Datenverkehr zugelassen und potenzielle Bedrohungen blockiert werden.

Echtzeit-Sandboxing: Die Sandbox-Funktion ermöglicht Echtzeit-Scans von Dateien in einer sicheren, isolierten Umgebung mit gleichermaßen schnellen und gründlichen Analyseoptionen. Durch das dynamische Scannen von 100 % des Datenverkehrs in Sekundenschnelle wird eine umfassende Erkennung von Sicherheitsbedrohungen gewährleistet.[2] Auf diese Weise können sich Unternehmen proaktiv gegen moderne Cyber-Bedrohungen verteidigen, ohne die Produktivität der Benutzer zu beeinträchtigen.

Wie funktioniert SWG?

Abbildung 4 bietet einen Überblick darüber, wie SWG in einer Geschäftsumgebung funktioniert.

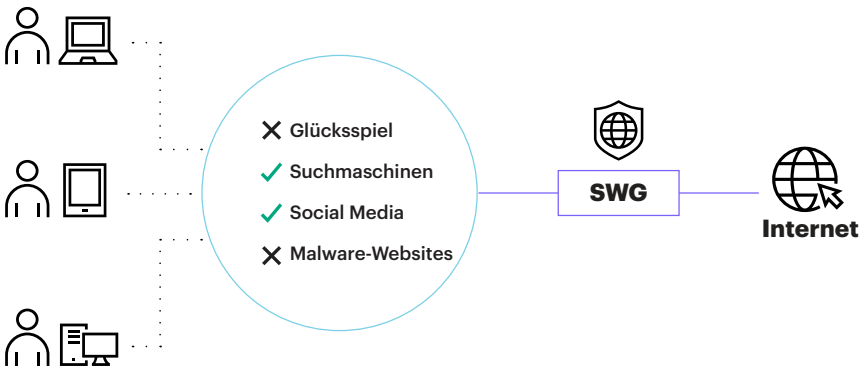

Abbildung 4. Architekturansicht des HPE Aruba Networking SWG-Service

1. **Mitarbeiter im Büro oder unterwegs versuchen, auf das Internet zuzugreifen**
   Der Datenverkehr wird über den HPE Aruba Networking SSE Agenten automatisch zum nächstgelegenen Edge-Standort geroutet.

2. **Der SWG-Service überwacht den Datenverkehr über Proxys**
   Es wird erkannt, dass der Datenverkehr zum Internet fließt, worauf er an den SWG-Service innerhalb der HPE Aruba Networking SSE Cloud geleitet wird.

3. **SWG validiert die Identität und wendet die Richtlinie an**
   Durch Sicherheitskontrollen – wie URL/DNS-Filterung, Bedrohungsschutz, Malware-Scans, Sandboxing und die Cloud-Firewall – wird der Zugriff auf bekannte bösartige und riskante Websites blockiert.

4. **SWG verbindet Benutzer fließend mit Internetressourcen**
   Nachdem die Zugriffskontrollen angewendet wurden und wenn die Internetressource die Sicherheitsanforderungen erfüllt, wird der Benutzer über eine sichere, verschlüsselte Verbindung mit dem Internet verbunden.

5. **SWG bleibt inline und überwacht die Benutzererfahrung**
   Wenn sich der Sicherheitsstatus ändert, wird der Zugriff automatisch gesperrt. Administratoren können die Aktivität beobachten und eine hohe Zugriffsleistung sicherstellen.

[2] Advanced Threat Protection for Web Apps & File Upload, Perception Point.

Vorteile von SWG

- **Transparenz und Kontrolle:** SWG von HPE Aruba Networking liefert umfassende Einblicke in den Internetverkehr und die Benutzeraktivität im gesamten Unternehmen. Dies ermöglicht eine detaillierte Überwachung und Kontrolle des Internetzugriffs und stellt sicher, dass nur sicherer und richtlinienkonformer Datenverkehr zugelassen wird. SWG hilft bei der Durchsetzung von Nutzungsrichtlinien und verhindert den Zugriff auf bösartige oder unangemessene Websites.
- **Datenschutz:** Eine der Hauptfunktionen unseres SWG-Services besteht im Schutz vertraulicher Daten vor dem Verlust oder dem Zugriff durch unbefugte Parteien. Dafür wird der ausgehende Datenverkehr auf vertrauliche Informationen überprüft, wobei Übertragungen blockiert werden, wenn sie gegen Datensicherungsrichtlinien verstoßen. Dies ist für die Einhaltung gesetzlicher Vorschriften und den Schutz geistigen Eigentums von entscheidender Bedeutung.
- **Erkennung und Vermeidung:** Unser SWG ist mit erweiterten Funktionen zur Erkennung von Sicherheitsbedrohungen ausgestattet, die ein breites Spektrum an Cyber-Bedrohungen wie Malware, Phishing-Angriffe und sonstige internetbasierte Angriffe identifizieren und blockieren. Durch die Analyse des Webverkehrs kann SWG verhindern, dass diese Bedrohungen die Benutzer erreichen oder das Netzwerk kompromittieren.
- **Sicherheit im großen Maßstab:** Wenn Unternehmen wachsen und ihren Betrieb erweitern, ist eine SWG-Skalierung möglich, mit der eine einheitliche Sicherheit für alle Benutzer und Standorte gewährleistet wird. Unabhängig davon, ob Mitarbeiter im Büro, an einem Remote-Standort oder mithilfe von Cloud-Services arbeiten, stellt das SWGs sicher, dass ein gleichbleibendes Sicherheitsniveau angewendet und Schutz vor Bedrohungen geleistet wird – unabhängig davon, woher der Datenverkehr stammt oder wo sich die Benutzer befinden.

CASB

Unter Schatten-IT versteht man die Nutzung von Anwendungen und Services ohne ausdrückliche Genehmigung der IT-Abteilung.

CASB von HPE Aruba Networking ist eine moderne CASB-Lösung, die die Cloud-Sicherheit verbessern und den Zugriff auf SaaS-Anwendungen für Unternehmen sichern soll. Unser CASB dient als Sicherheitsvermittler zwischen Benutzern und SaaS-Anwendungen, bietet Inline-CASB-Schutz für Daten während der Übertragung, reguliert effektiv Datenflüsse, deckt Schatten-IT auf und verhindert Datenverluste.

HPE Aruba Networking CASB bietet End-to-End-Transparenz und ermöglicht eine zentrale Verwaltung von Benutzerzugriffen, Downloads und Freigabeberechtigungen. Die Funktionsweise des CASB ist unkompliziert: Er leitet den Datenverkehr über einen Proxy weiter, um riskante Pass-Through-Verbindungen zu vermeiden, validiert Identitäten, wendet Richtlinien an und verbindet Benutzer sicher mit Ressourcen, während er gleichzeitig den Datenverkehr prüft und das Benutzererlebnis überwacht.

Unser CASB legt den Schwerpunkt auf Benutzerfreundlichkeit und Skalierbarkeit und bietet sicheren Zugriff auf moderne Cloud-Services und -Anwendungen. In unserer Cloud-zentrierten Welt zielt der CASB als Teil der umfassenderen HPE Aruba Networking SSE Plattform darauf ab, von Anfang an einen Mehrwert durch verbesserte Transparenz, Compliance und Datensicherheit zu liefern.

Wichtige Merkmale und Funktionen des CASB

- **Inline-CASB:** Der Inline-CASB von HPE Aruba Networking fungiert als Wächter zwischen den Benutzern Ihres Unternehmens und den SaaS-Anwendungen/Cloud-Services. Er setzt bei Bewegungen von Daten in die Cloud und aus der Cloud Sicherheitsrichtlinien in Echtzeit durch. Dieser Prozess kann Authentifizierung, Verschlüsselung und andere Sicherheitskontrollen umfassen.
- **SSL-Prüfung für die CASB-Steuerung:** Mit der SSL-Prüfung für SaaS können Teams verschlüsselten SSL/TLS-Verkehr untersuchen, um potenzielle Bedrohungen oder Datenlecks zu stoppen, bevor sie auftreten. Durch die Entschlüsselung des Datenverkehrs kann der CASB Sicherheitsrichtlinien zum Schutz vertraulicher Daten anwenden.
- **Unbegrenzte SaaS-Anwendungen zur SSL-Prüfung:** Unser CASB bietet unbegrenzte Kapazitäten zur Überprüfung des SSL/TLS-Verkehrs über eine beliebige Anzahl von SaaS-Anwendungen hinweg und gewährleistet eine umfassende Abdeckung ohne Leistungsbedenken.

— **Einblick in Anwendungen und Schatten-IT:** Sie erhalten Einblick in SaaS-Anwendungen und Schatten-IT, um die mit der Nutzung genehmigter und nicht genehmigter Apps verbundenen Risiken besser zu verstehen und zu verwalten.

— **Detaillierte Kontrolle eingeschränkter Aktionen:** Mit CASB können Administratoren detaillierte Richtlinien festlegen, die bestimmte Aktionen wie Hochladen, Herunterladen, Teilen von Daten usw. beim Arbeiten in jeglichen SaaS-Anwendungen einschränken. Dies ist eine wichtige Voraussetzung zum Schutz vor Datenverlusten und zur Gewährleistung der Einhaltung verschiedener Vorschriften.

— **DLP für SaaS-basierte Anwendungen:** DLP-Tools tragen zum Schutz vertraulicher Daten in SaaS-Anwendungen bei, indem potenzielle Datenschutzverletzungen oder unbefugte Zugriffe überwacht, erkannt und blockiert werden.

- **DLP-Regex/Wörterbuchabgleich:** DLP kann reguläre Ausdrücke (Regex) und Wörterbuchabgleiche verwenden, um vertrauliche Daten zu identifizieren und zu schützen. Dies ermöglicht detailliertere und flexiblere Datensicherheitsrichtlinien für den Abgleich mit bestimmten Mustern oder Begriffen in Dateien.

- **Optische Zeichenerkennung (OCR, Optical Character Recognition):** OCR-Technologie wandelt Textbilder, etwa gescannte Dokumente oder Fotos, in bearbeitungsfähige und durchsuchbare Daten um. Dies ist besonders nützlich für die Verarbeitung von Dokumenten, die vertrauliche Informationen wie Sozialversicherungsnummern enthalten.

— **Compliance mit vordefinierten und benutzerdefinierten Wörterbüchern:** Es können vordefinierte und benutzerdefinierte Wörterbücher erstellt werden, um die Compliance mit bestimmten Vorschriften wie HIPAA, PCI DSS, DSGVO und NIST sicherzustellen. Diese Wörterbücher enthalten Begriffe und Muster, die für jede Verordnung einzigartig sind und Organisationen dabei helfen, ihren Compliance-Verpflichtungen nachzukommen.

Wie funktioniert CASB?

Abbildung 5 bietet einen Überblick darüber, wie CASB in einer Geschäftsumgebung funktioniert.

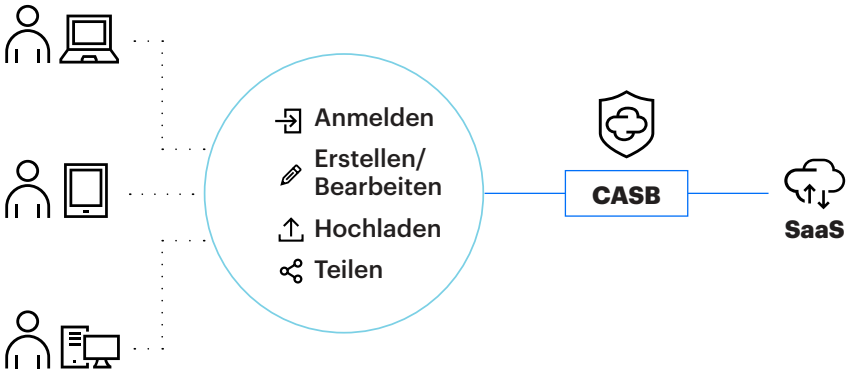

Abbildung 5. Architekturansicht des HPE Aruba Networking CASB-Service

1. **Ein Benutzer versucht, auf einen Cloud-Service zuzugreifen**
   Der Benutzer versucht, auf eine SaaS-Anwendung oder IaaS-Plattform zuzugreifen. Der Datenverkehr wird über den HPE Aruba Networking SSE Agenten automatisch zum nächstgelegenen Edge-Standort geroutet.
2. **Der CASB-Service überwacht und kontrolliert den Datenverkehr**
   Der Datenverkehr wird direkt in die HPE Aruba Networking SSE Cloud geleitet und dort einer SSL-Prüfung unterzogen.
3. **Der CASB validiert die Identität und wendet die Richtlinie an**
   Nach Anwendung des Inline-CASB und der Datensicherungskontrollen (z. B. Uploads, Downloads und Freigabeaktivitäten, optische Zeichenerkennung, Compliance) werden die Zugriffsrechte automatisch auf der Basis von Kontextänderungen in Echtzeit angepasst.
4. **CASB stellt eine sichere Verbindung zur SaaS-Ressource her**
   Durch eingeschränkte Aktionen wird dem Benutzer ein sicherer SaaS-Zugriff gewährt, während gleichzeitig nicht autorisiertes Verhalten eingeschränkt wird, um Datenverlust zu verhindern und die Einhaltung von Vorschriften durchzusetzen.
5. **CASB bleibt inline und überwacht die Benutzererfahrung**
   Administratoren erhalten Einblick in sämtliche Benutzeraktivitäten beim Zugriff auf die SaaS-Anwendung. Wenn sich der Sicherheitsstatus ändert oder der Benutzer unbefugte Aktivitäten versucht, wird der Zugriff neu bewertet und die Administratoren werden benachrichtigt.

Die Vorteile von CASB

— **Verbesserte Datensicherheit:** Der CASB von HPE Aruba Networking bietet Echtzeit-Scanning und Überwachung der Datennutzung und des Datenflusses zum und vom SaaS-Anbieter. Hierzu gehören DLP-Funktionen, die vertrauliche Daten schützen, indem sie die unbefugte Weitergabe verhindern und die Durchsetzung von Datensicherheitsrichtlinien gewährleisten.

— **Transparenz und Kontrolle:** Mit CASB erhalten Unternehmen detaillierte Transparenz und Kontrolle über ihre Cloud-Umgebung. Teams können den gesamten Benutzerverkehr sehen, ermitteln, welche Cloud-Anwendungen die Benutzer verwenden, und detaillierte Steuerelemente anwenden, um zu verwalten, wie auf Daten zugegriffen wird und diese verwendet werden.

— **Compliance:** Unser CASB unterstützt Unternehmen bei der Einhaltung von Datenschutzbestimmungen durch die Durchsetzung von Unternehmensrichtlinien zur Cybersicherheit in mehreren Cloud-Umgebungen. Er liefert Risikobewertungen und Schätzwerte für Benutzer und Anwendungen, die für das Management der Compliance-Anforderungen nützlich sind.

— **Bedrohungsminderung:** Unser CASB bietet Schutz vor bekannten und unbekannten Bedrohungen, einschließlich Anti-Malware und Antivirenprogrammen. Der CASB erkennt ungewöhnliches Verhalten in Cloud-Anwendungen, identifiziert Risiken wie Ransomware, kompromittierte Benutzer und betrügerische Anwendungen und kann Bedrohungen automatisch beheben, um Unternehmensrisiken zu begrenzen.

— **Betriebliche Effizienz:** Durch die Konsolidierung mehrerer Methoden für die Durchsetzung von Sicherheitsrichtlinien an einem einzigen Punkt ermöglicht der CASB Unternehmen, ihren Sicherheitsbetrieb zu optimieren. Diese Integration vereinfacht das Management von Sicherheitsrichtlinien und reduziert die Komplexität der Sicherung mehrerer Cloud-Services.

DEM

Das DEM von HPE Aruba Networking ist eine cloudbasierte Digital Experience Monitoring (DEM)-Lösung, mit der IT-Helpdesks stets auf Probleme mit den Geräten der Endbenutzer vorbereitet bleiben. DEM stellt ein nahtloses und sicheres digitales Erlebnis sicher und ist abgestimmt auf die Unternehmensanforderungen, das Benutzererlebnis zu optimieren und die Produktivität durch bessere digitale Erlebnisse zu steigern.

Die Plattform erkennt Leistungseinbrüche und bietet Einblicke in Benutzer, Abteilungen oder Regionen, bei denen diese möglicherweise auftreten. Mithilfe der Endpunkttelemetrie können IT-Teams detaillierte Metriken wie CPU-Auslastung, Ressourcenverbrauch, Speichernutzung und WLAN-Signalstärke einsehen. Unser DEM verfügt außerdem über eine einheitliche Überwachung des Anwendungsstatus, mit der private, SaaS- und Internetanwendungen kontinuierlich beaufsichtigt werden. Hop-basierte Netzwerkmetriken bieten Einblick in jeden Internet- und Netzwerk-Hop zwischen einem Benutzer und einer Unternehmensanwendung, wodurch Probleme für die Benutzer reduziert und die Sicherheit gesteigert werden kann.

Abbildung 6 zeigt die Dashboard-Ansicht des DEM-Service von HPE Aruba Networking.

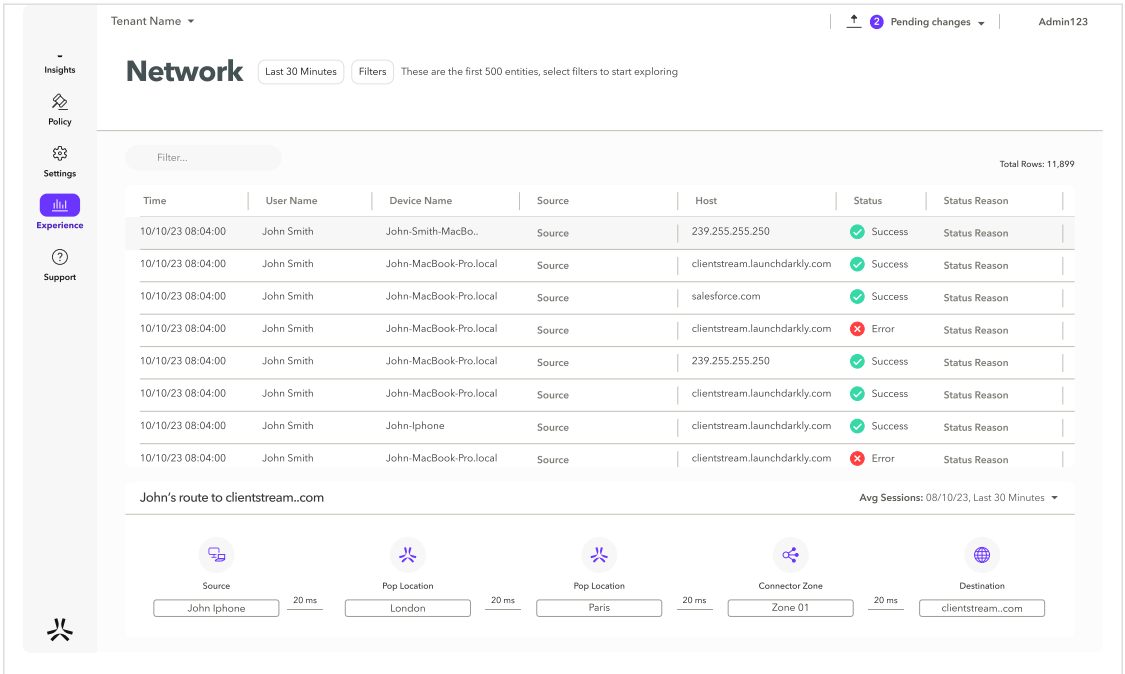

Abbildung 6. Dashboard-Ansicht des HPE Aruba Networking DEM-Service

Wie funktioniert DEM?

Abbildung 7 bietet einen Überblick darüber, wie DEM in einer Geschäftsumgebung funktioniert.

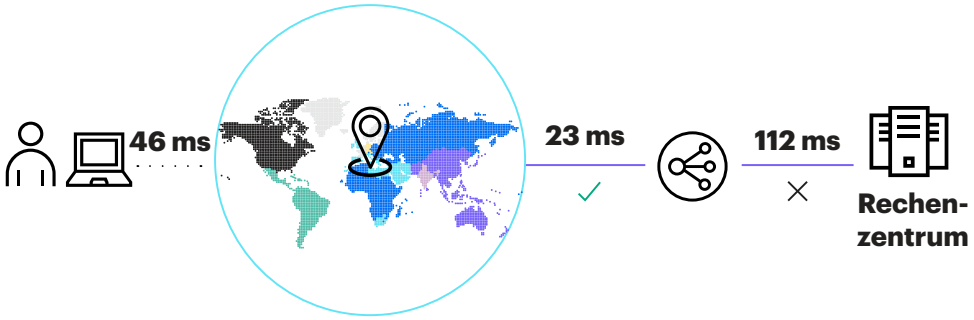

Abbildung 7. Architekturansicht des HPE Aruba Networking DEM-Service

1. **Ein Benutzer versucht, auf eine Ressource zuzugreifen**
   Der Datenverkehr wird über die HPE Aruba Networking SSE Cloud geleitet.

2. **Sicherheitsrichtlinien werden durchgesetzt und Benutzer erhalten Zugriff**
   Nach Zugriffskontrollen und der Durchsetzung von Richtlinien erhält der Benutzer Zugriff auf die autorisierte Anwendung.

3. **Das DEM von HPE Aruba Networking führt Echtzeitanalysen durch**
   Die Daten werden in Echtzeit erfasst und analysiert, um zu verstehen, wie Benutzer mit den digitalen Services interagieren, und um Leistungseinbußen oder Anwendungsausfälle zu erkennen.

4. **Identifizierte Latenzen werden visualisiert**
   Administratoren können durch Hop-basierte Transparenz sehen, wo Latenzen auftreten, und transparente Einblicke bis auf die Ebene einzelner Benutzer und Sitzungen erhalten.

5. **Das Erlebnis wird für den Endbenutzer optimiert**
   Auf der Grundlage der gewonnenen Erkenntnisse können Unternehmen fundierte Entscheidungen zur Verbesserung ihrer Produktentwicklung und Optimierung ihrer Geschäftsabläufe treffen. Wenn Probleme erkannt werden, unterstützen DEM-Tools die IT-Teams dabei, schnell die Hauptursache zu identifizieren, was den Problemlösungsprozess beschleunigt.

Wichtige Merkmale und Funktionen von DEM

Dashboard für das Netzwerkerlebnis: Ein leistungsstarkes Dashboard für Einblicke in den Netzwerkpfad der Datenübertragung von Benutzern zu Geschäftsanwendungen. Es soll Netzwerkadministratoren dabei helfen, die Ursache von Latenzproblemen schnell zu identifizieren und zu lokalisieren. Durch die Bereitstellung einer detaillierten Hop-to-Hop-Analyse unterstützt das Dashboard ein klares Verständnis der Netzwerkleistung und die Identifizierung von Engpässen, die das Benutzererlebnis beeinträchtigen könnten.

Dashboard für das Benutzererlebnis: Dieses Dashboard dient als Diagnosetool, das Latenzprobleme aus der Sicht eines einzelnen Benutzers schnell erkennt. Es bietet detaillierte Einblicke in die Interaktion jedes Benutzers mit seinen Anwendungen und Geräten und hebt Bereiche hervor, die die Leistung beeinträchtigen können. Dieses Dashboard ist besonders nützlich für IT-Fachkräfte, die das Endbenutzererlebnis optimieren und einen reibungslosen Betrieb geschäftskritischer Anwendungen sicherstellen möchten.

Unbeschränkte Überwachungsmöglichkeit: Das DEM von HPE Aruba Networking ist darauf ausgelegt, ein breites Spektrum an Überwachungsanforderungen abzudecken. Dies bedeutet, dass es keine Beschränkungen hinsichtlich der Anzahl der Benutzer oder Geräte gibt, die überwacht werden können, was Skalierbarkeit und Flexibilität für das Netzwerkmanagement bringt. Unternehmen können von umfassenden Überwachungsfunktionen profitieren, ohne sich Gedanken über das Erreichen von Obergrenzen oder Beschränkungen machen zu müssen.

Echtzeit-Probing: Diese Funktion ist ein Alleinstellungsmerkmal unseres DEM-Services gegenüber anderen, die auf synthetischem Probing basieren. Durch die Verwendung des echten Probings, das den tatsächlichen Anwendungszugriff überwacht, liefert das System ein genaueres Bild der Anwendungsleistung und des tatsächlichen Benutzererlebnisses. Mit dieser Methode wird sichergestellt, dass die Überwachung auf echten Nutzungsmustern basiert, was zu zuverlässigeren Daten führt.

Keine Beschränkungen hinsichtlich der überwachten Anwendungen: Das DEM von HPE Aruba Networking stellt die Fähigkeit in den Mittelpunkt, jede Anwendung ohne Vorkonfigurationen zu überwachen. Im Gegensatz zu anderen Lösungen, die vorherige Kenntnisse über die zu überwachenden Anwendungen erfordern, ermöglicht diese Funktion eine spontane und umfassende Überwachung aller Anwendungen und bietet eine einzigartige Flexibilität und Abdeckung.

Die Vorteile von DEM

Einheitliche Transparenz und verbessertes Benutzererlebnis
Mit dem DEM von HPE Aruba Networking können Administratoren Hop-basierte Latenzmetriken visualisieren, die das Erlebnis eines Benutzers beim Zugriff über sein lokales Internet auf den Point-of-Presence-Standort, den Connector und die Anwendung beschreiben. Dadurch entsteht ein einheitliches Bild des Endbenutzererlebnisses, womit die Benutzererfahrung in einer hybriden Arbeitsumgebung verbessert werden kann.

Schnelle Problemlösungen für mehr Produktivität
Einblick in die Leistung nicht verwalteter Netzwerke zu gewinnen, kann sehr schwierig sind. Mit DEM können Administratoren jedoch schnell feststellen, wo ein Leistungsproblem seinen Ursprung hat, und netzwerkbezogene Supportprobleme schnell lösen, um die Zeit bis zur Lösung des Problems im gesamten Netzwerk deutlich zu verkürzen.

Weniger Support-Tickets für hybride Arbeitsformen
Die Zunahme hybrider Arbeitsformen hat in der Vergangenheit zu einer Zunahme der Support-Tickets im Zusammenhang mit Netzwerkzugriffen und einer verringerten Transparenz bei Remote-Netzwerkverbindungen und bezüglich des Endbenutzererlebnisses geführt. Unser DEM hilft, diese Lücke zu schließen, um hybride Arbeit im gesamten Unternehmen besser zu unterstützen.

HPE Aruba Networking SSE Pakete

Wir bieten eine Reihe von HPE Aruba Networking SSE Paketen an, die auf die spezifischen Anforderungen Ihres Unternehmens abgestimmt sind.

Abbildung 8 zeigt die verschiedenen Pakete, die HPE Aruba Networking SSE anbietet.

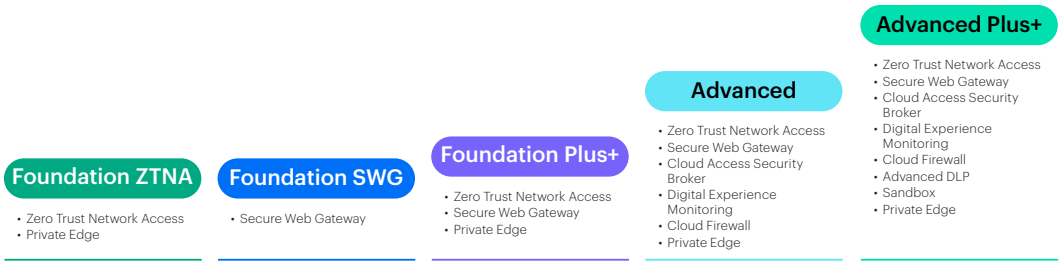

Abbildung 8. HPE Aruba Networking SSE Pakete

Tabelle 1. Pakete und Bundles für HPE Aruba Networking SSE

Paket/Bundle	Foundation ZTNA	Foundation SWG	Foundation +	Advanced	Advanced +
Multi-Cloud-Architektur Zugriff auf über 500 globale Edge-Standorte bei den zuverlässigsten Cloud-Anbietern wie AWS, Azure, GCP	✓	✓	✓	✓	✓
Admin-Portal Zentrales Zugriffsmanagement für Administratoren über eine einheitliche Benutzeroberfläche, um Zero Trust-Richtlinien für alle Unternehmensressourcen durchzusetzen. (Admin-RBAC-Kontrollen sind erhältlich)	✓	✓	✓	✓	✓
Benutzerportal Sicherer, zentraler Zugriffspunkt für Benutzer, um auf alle ihre autorisierten Anwendungen zugreifen	✓	✓	✓	✓	✓
HPE Aruba Networking SSE Richtlinien-Tags Durch Smart Tagging können Administratoren detaillierte Zero Trust-Richtlinien mit nur einer Handvoll Regeln anstelle von Hunderten einrichten	✓	✓	✓	✓	✓
HPE Aruba Networking SSE Agent Schlanker Endpunkt-Agent, der mit Laptops, Telefonen und Tablets sowie Betriebssystemen wie Windows, Mac, Linux®, Android™ und iOS kompatibel ist	✓	✓	✓	✓	✓
HPE Aruba Networking SSE Connectoren Schlanke virtuelle Maschine, die als Front-End für Anwendungen dient, um eine sichere, ausschließlich ausgehende Zero Trust-Verbindung von autorisierten Anwendungen zur HPE Aruba Networking SSE Cloud bereitzustellen. (Bis zu 1.000 Connectoren)	✓	✓	✓	✓	✓
Universelle SSL-Prüfung Durchsetzung von SSL-Inspektionen im großen Maßstab für alle Arten von Datenverkehr – privat, SaaS, Internet	✓	✓	✓	✓	✓
Analysen und Reporting Echtzeitanalyse des gesamten Datenverkehrs und Benutzerverhaltens im HPE Aruba Networking SSE Dashboard. Einblicke über übergeordnete HPE Aruba Networking SSE Dashboards bis hin zu detaillierten individuellen Sitzungsprotokollen	✓	✓	✓	✓	✓
Konnektivität an Zweigstellen Sichere Zweigstellenkonnektivität für Internet und internen Datenverkehr mit IPSec-Unterstützung und einfacher Integration in SD-WAN-Services	✓	✓	✓	✓	✓
Smart Routing Optimierung der Benutzerkonnektivität durch automatisches Routing über den schnellsten Zugriffsweg über mehr als 500 Edge-Standorte	✓	✓	✓	✓	✓
Partnerintegrationen Integration zusätzlicher Services in Ihr Cybersicherheits-Mesh, wie SIEM, Identity, MDM, Endpoint und verschiedene APIs	✓	✓	✓	✓	✓

Paket/Bundle	Foundation ZTNA	Foundation SWG	Foundation +	Advanced	Advanced +
Integrierte Identität Nutzung unseres nativen HPE Aruba Networking IdP-Services innerhalb von HPE Aruba Networking SSE – ideal für den Zugriff durch Dritte	✓	✓	✓	✓	✓
Unterstützung mehrerer IdPs Mühelose Integration eines oder mehrerer IdP-Provider nach Wahl und Aktivierung von SAML/SCIM-Unterstützung	✓	✓	✓	✓	✓
Gerätestatus Erkenntnisse über den Sicherheitsstatus von Endpunkten und Durchsetzen von Sicherheitsmaßnahmen auf Grundlage ihres sich ändernden Kontextes	✓	✓	✓	✓	✓
Protokoll-Streaming Einfache Integration von HPE Aruba Networking SSE in den SIEM-Anbieter Ihrer Wahl und verbesserte Datennutzung mit SYS Log- und API-Integrationen	✓	✓	✓	✓	✓
Benutzerdefinierte Sperrseiten und Benutzerwarnungen Bessere Aufklärung der Benutzer, warum der Zugriff verweigert wird, durch benutzerdefinierte Sperrseiten und Benachrichtigungen zu Sperrungen über den Agenten, sowie Minimierung der Anzahl von IT-Tickets	✓	✓	✓	✓	✓
ZTNA					
Alle Ports und Protokolle Sicherer Zugriff auf alle privaten Anwendungen mit Unterstützung aller Ports und Protokolle	✓	×	✓	✓	✓
Robuster agentenloser Zugriff Bietet Mitarbeitern, Dritten und BYOD-Benutzern agentenlosen Zugriff auf private Anwendungen über einen einfachen Webbrowser. Unterstützte agentenlose Anwendungen: MS SQL, GIT, SSH, RDP, VNC, Web-Anwendungen	✓	×	✓	✓	✓
Serverinitiierter Flow Aktivierung der Unterstützung älterer Thick-Client-Anwendungen wie VOIP und AS400 mit serverinitiierten Flows.	✓	×	✓	✓	✓
Multiregionale Anwendungsunterstützung Unterstützung von Anwendungen in mehreren Regionen über mehrere Connector-Zonen hinweg, sodass anhand der Latenz der beste Zugriffspfad ausgewählt werden kann.	✓	×	✓	✓	✓
DLP für private Anwendungen Aktivieren der Sitzungssteuerung und Transparenz für private Anwendungen. Anwendung von DLP-Richtlinien, um den Datenverkehr auf Malware zu scannen, Sandboxing auszuführen und Upload-/Download-Aktionen zu steuern.	✓	×	✓	✓	✓

Paket/Bundle	Foundation ZTNA	Foundation SWG	Foundation +	Advanced	Advanced +
Vereinfachte Domäneneinrichtung Vereinfachte Domäneneinrichtung mit ZTNA über CNAME und DNS Rewrite Durch Rewrites sind keine DNS-Änderungen mehr erforderlich, sodass die Anwendung schneller bereitgestellt werden kann.	✓	×	✓	✓	✓
Private Edge Bereitstellung Ihres eigenen softwarebasierten HPE Aruba Networking SSE Private Edge, um den Zugriff noch näher an Ihre Benutzer und Geräte am Edge des Netzwerks heranzubringen (unbegrenzte Anzahl lokaler Edges)	✓	×	✓	✓	✓
SWG					
DNS/URL-Filterung Proaktives Blockieren von Zugriffen auf bösartige Websites und Inhalte und Schutz der Integrität Ihres Netzwerks und Ihrer Benutzerdaten	×	✓	✓	✓	✓
Schutz mit Threat Intelligence Verwendung intelligenter Algorithmen und Echtzeitdaten, um riskante URLs und Domänen basierend auf deren Inhalt, Domänendetails und Reputation zu blockieren	×	✓	✓	✓	✓
DLP Verhindern von Datenverlusten durch den Einsatz von Datensicherheitsprofilen, Regex-Mustervergleichen und Durchsetzung von Aktionen für mehr Kontrolle und weniger Risiko	×	✓	✓	✓	✓
Malware- und Antivirenscans Schutz vor bekannten Viren und Malware durch wiederholbare Hash- und AV-Scans – Datenbanksignaturen	×	✓	✓	✓	✓
Cloud-Firewall FWaaS filtert den Netzwerkverkehr in der SSE-Cloud, unterstützt alle Ports und Protokolle und erlaubt/verweigert den Zugriff	×	×	×	✓[3]	✓[3]
CASB					
Inline-CASB Verfolgen und Kontrollieren von Aktivitäten in über 10.000 SaaS-Anwendungen ohne Einschränkung bei der SSL-Prüfung	×	×	×	✓	✓
Compliance und Regulierung Vordefinierte und benutzerdefinierte Wörterbücher zur besseren Einhaltung von Compliance-Standards (z. B. HIPAA, PCI-DSS, DSGVO, NIST)	×	×	×	✓	✓
Erweiterte DLP Ergänzung der DLP-Funktionalität, umfasst OCR	×	×	×	×	✓
DEM					
Dashboard für das Netzwerkerlebnis Hop-basierte Einblicke in den Pfad zwischen Benutzern und Unternehmensanwendungen sowie Identifizierung und Lokalisierung der Ursache von Latenzproblemen	Add-on-Kauf	×	Add-on-Kauf	✓	✓

[3] Zukünftig verfügbar

Paket/Bundle	Foundation ZTNA	Foundation SWG	Foundation +	Advanced	Advanced +
Dashboard für das Benutzererlebnis Identifiziert Latenzprobleme schnell aus individueller Sicht und bietet detaillierte Einblicke in die Interaktion jedes Benutzers und seiner Geräte	Add-on-Kauf	×	Add-on-Kauf	✓	✓
HPE Aruba Networking SSE Add-ons					
Sandbox Testen von Dateien mit Sandbox-Scan in Echtzeit. Dieser bietet sowohl schnelle als auch gründliche Scan-Optionen und scannt gleichzeitig dynamisch 100 % des Datenverkehrs in Sekundenschnelle.[4]	×	Add-on-Kauf	Add-on-Kauf	Add-on-Kauf	✓
Managed Connectors Bereitstellung dedizierter Connectoren für Unternehmen und einer statischen IP für optimierte Zugriffe durch diesen Service	Add-on-Kauf	Add-on-Kauf	Add-on-Kauf	Add-on-Kauf	Add-on-Kauf
Standortbasiertes Abonnement					
SWG-Bandbreite SWG-Schutz von jeder Zentrale, Zweigstelle oder jedem Remote-Standort aus mit dedizierten Tunneln und ohne Agentenanforderung. Die SWG-Bandbreite umfasst alle Funktionsmerkmale von Foundation SWG und wird nach Verbrauch und nicht nach Benutzerlizenzen abgerechnet. Einzeln oder mit HPE Aruba Networking SSE Bundle erhältlich.	×	Add-on-Kauf	Add-on-Kauf	Add-on-Kauf	Add-on-Kauf

[4] Advanced Threat Protection for Web Apps & File Upload, Perception Point

Customer Success Pakete

Tabelle 2. Customer Success Pakete für HPE Aruba Networking SSE

Paket/Bundle	Basic	Select	Premier
Support-Abdeckung	Geschäftszeiten **8–20 Uhr | Montag bis Freitag**	24x7x365	24x7x365
Support-Portal	24x7x365	24x7x365	24x7x365
Architektur- und Bereitstellungsservices	-	Add-on	Enthalten
Service Level Agreement	Standard gemäß Bedingungen	Standard gemäß Bedingungen	Erweitert
Eigener Customer Success Manager	-	-	Enthalten
Integritätsprüfungen der Bereitstellung	-	Add-on	Inbegriffen, alle zwei Jahre
SLA für Reaktionszeit			
Kritisch	1 Stunde	1 Stunde	30 Minuten
Hoch	2 Stunden	2 Stunden	1 Stunde
Mittel	8 Stunden	8 Stunden	4 Stunden
Niedrig	Nächster Arbeitstag	Nächster Arbeitstag	8 Stunden

Erste Schritte mit HPE Aruba Networking SSE

Zu Beginn Ihrer Umstellung auf HPE Aruba Networking SSE sollten Sie Ihren Ausgangspunkt bestimmen. Eine sorgfältige Planung und Priorisierung der wichtigsten Anwendungen, Daten, Ressourcen und Benutzertypen ist der Schlüssel zu einer erfolgreichen Bereitstellung. Eine beliebte Bereitstellungsmethode besteht darin, HPE Aruba Networking SSE in einem schrittweisen Ansatz zu starten, wie in Abbildung 9 dargestellt.

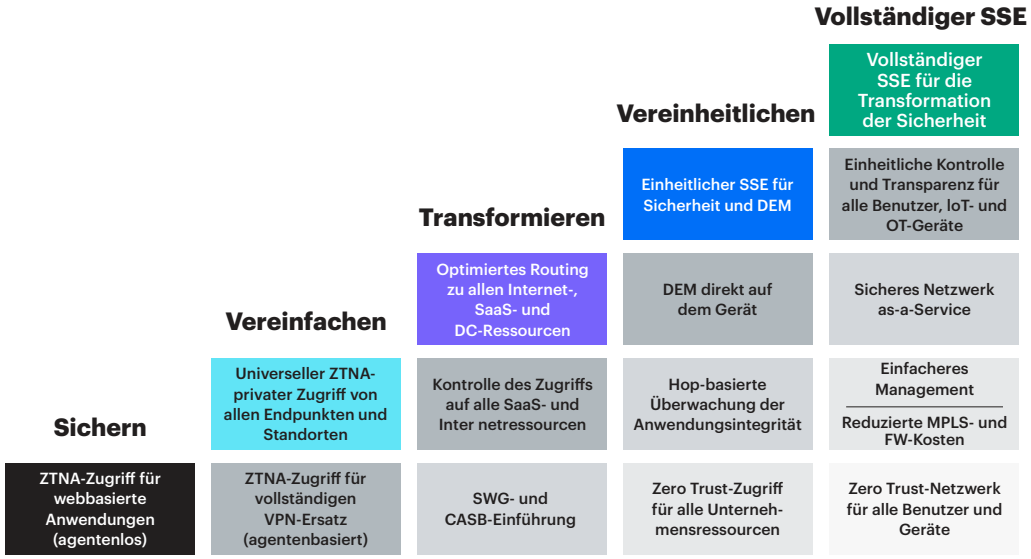

Abbildung 9. Ein schrittweiser Ansatz zur vollständigen Bereitstellung von HPE Aruba Networking SSE

Weitere Informationen

HPE Aruba Networking SSE Experten kontaktieren

HPE Aruba Networking SSE 24 Stunden lang kostenlos testen

HPE Aruba Networking SSE

HPE.com besuchen

Mit HPE Aruba Networking SSE müssen sich Sicherheits- und Netzwerkteams keine Gedanken mehr über die Bedeutung von „irgendwo“ und „überall“ machen. Mit HPE Aruba Networking SSE Services wie ZTNA, SWG und CASB können Unternehmen veraltete Sicherheitstechnologien und -prozesse schrittweise durch effizientere, zeitgemäße ersetzen. Mithilfe dieser modernen Methoden können Sie nicht nur dringende Sicherheits- und Benutzeranforderungen umgehend bewältigen, sie bieten Ihnen auch eine flexible Plattform für die Erfüllung zukünftiger Anforderungen.

Die meisten Unternehmen wählen zwar einen schrittweisen Ansatz für HPE Aruba Networking SSE und bauen dabei auf erfolgreichen Bereitstellungen auf. Für die langfristig erfolgreiche Implementierung von HPE Aruba Networking SSE ist jedoch eine durchgängige Kombination aus strategischen Entscheidungen, technischen Lösungen, der Einbindung und Schulung von Benutzern sowie fortlaufender Verwaltung und Verfeinerung erforderlich.

Mit anderen Worten: Der Erfolg von HPE Aruba Networking SSE ist ein Prozess, der schnell beginnen und enden kann, je nachdem, mit welchem HPE Aruba Networking SSE Anbieter Sie zusammenarbeiten. Ziehen Sie HPE Aruba Networking SSE für Ihr SSE-Projekt in Betracht. Wir besprechen mit Ihnen jeden Schritt der Bereitstellung in Ihrer Umgebung.

Jetzt chatten

a00141561DEE, Rev. 2

HEWLETT PACKARD ENTERPRISE

hpe.com