HPE aruba networking

Lösungsübersicht



Erweiterte Sicherheit mit EdgeConnect SD-Branch

Schutz der Filiale vor neuartigen Bedrohungen mit einem modernen, sicheren SD-WAN

HPE



Hauptvorteile

Die erweiterten Sicherheitsfunktionen in EdgeConnect SD-Branch bieten grundlegende Vorteile:

- Einheitlicher SASE durch enge Integration mit HPE Aruba Networking SSE
- Automatisierte Orchestrierung auf externen Cloud-Sicherheitsanbietern
- Integrierte Sicherheit in kabelgebundenen und Wireless-Netzwerken
- Umfassende dynamische Segmentierung im gesamten verteilten Unternehmen
- Feinmaschige Sicherheitsrichtlinien basierend auf den Rollen der Benutzer und Anwendungen
- Erkennen und Blockieren von Angriffen mithilfe einer täglich aktualisierten Bedrohungsbibliothek
- Erhöhte Transparenz und Echtzeit-Überwachung aller Standorte auf externe Bedrohungen

Einführung

Durch die Verlagerung von Anwendungen in die Cloud und die Umstellung auf hybride Arbeitsmodelle greifen Remote-Benutzer von verschiedensten Orten und über nicht vertrauenswürdige Links auf Unternehmensressourcen zu. Zeitgleich haben Cybersicherheitsrisiken aufgrund der rasanten Zunahme von Geräten, die sich mit dem Netzwerk verbinden, und der in der Cloud gespeicherten vertraulichen Daten, dramatisch zugenommen.

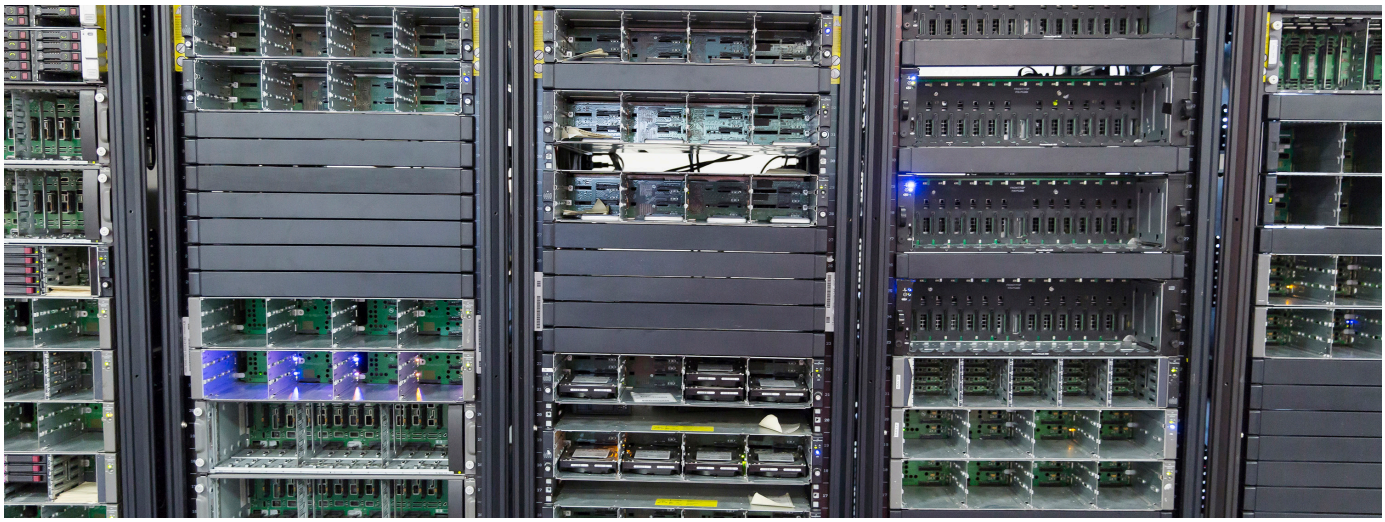
Der Sicherheitsperimeter löst sich allmählich auf. Damit einhergehend definierte Gartner 2019 den Begriff des SASE (Secure Access Service Edge), der SD-WAN mit über die Cloud bereitgestellten Sicherheitsservices, dem sog. SSE (Security Service Edge), kombiniert. So wird eine besser gesicherte und flexiblere Verbindungsmöglichkeit bereitstellt, bei der der Anwendungsverkehr nicht in ein Rechenzentrum zurückgeleitet und eine erweiterte Sicherheitsprüfung direkt in der Cloud durchgeführt wird. In der Tat prognostizierte Gartner[1], dass „bis 2025 mehr als 50% der Unternehmen explizite Strategien zur Einführung von SASE haben werden, im Vergleich zu weniger als 5% im Jahr 2020."

Darüber hinaus muss SASE angesichts der zunehmenden Verbreitung von IoT-Geräten in Unternehmen um ein Zero-Trust-Framework für identitätsbasierte Zugriffssteuerung ergänzt werden, um die Sicherheit zu gewährleisten und Filialen vor Ort vor Sicherheitslücken zu schützen. Denn IoT-Geräte können keine Sicherheitsagenten ausführen, und die Angriffsfläche wird größer.

Durch die Einrichtung und Durchsetzung von Richtlinien in Filialen mittels einer statusabhängigen, anwendungsbezogenen Firewall, einschließlich Deep Packet Inspection (DPI) in Kombination mit Anwendungsklassifizierung und Filterung von Webinhalten, bietet EdgeConnect SD-Branch eine umfassend integrierte SD-WAN-Sicherheit. Eine Engine zur Datenverkehrsprüfung bietet umfangreiche Angriffserkennungs- und präventionsfunktionen (IDS/IPS), die Angriffe blockieren und gleichzeitig einen kontinuierlichen Geschäftsbetrieb gewährleisten.

Die Lösung integriert sich nahtlos in HPE Aruba Networking SSE und bildet so eine einheitliche SASE-Plattform für eine einfachere Einführung und schnellere Bereitstellung von SASE. Um bestimmte Anforderungen zu erfüllen oder um die Lösung in ein bestehendes Sicherheitsökosystem zu integrieren, ist sie außerdem nahtlos mit externen Sicherheitsanbietern integrierbar.
HPE Aruba Networking geht sogar noch einen Schritt weiter und bietet rollenbasierte dynamische Segmentierung im gesamten LAN und WAN, sodass Benutzer und IoT-Geräte Netzwerkziele nur entsprechend ihrer Rolle im Unternehmen erreichen können. Damit wird die Verbreitung externer Bedrohungen im Netzwerk verhindert, was ein zentrales Ziel bei der Sicherung verteilter Unternehmen ist.

[1] Gartner Says Cloud Will Be the Centerpiece of New Digital Experiences, November 2021



Kompromisslose Sicherheit mit EdgeConnect SD-Branch

HPE Aruba Networking bietet die Leistungs- und Kostenvorteile von SD-WAN, und die Sicherheitsfunktionen werden am Edge verwaltet und nicht zurück in das Rechenzentrum oder den Campus gesendet. Um die Integrität des LAN oder WAN zu gewährleisten, lassen sich die Sicherheitsmaßnahmen untergliedern. Das LAN erfordert Absicherungen des Ost-West-Verkehrs, und das WAN verlangt die Sicherung des Verkehrs zwischen Standorten, auch Nord-Süd-Verkehr genannt.

Modernste SD-WAN-Gateways sollten Routing, Erstellung von SD-WAN-Overlays, Sicherheit, Deep Packet Inspection und weitere Funktionen umfassen, die in der Vergangenheit in separaten Anwendungen ausgeführt wurden.

Die folgende Tabelle erklärt die Tools zur Sicherung dieser Netzwerke.

Diese Tabelle zeigt die vielen verschiedenen Sicherheitskomponenten von EdgeConnect SD-Branch. HPE Aruba Networking Gateways unterstützen eine anwendungskonsistente, statusabhängige Firewall[2], Deep Packet Inspection (DPI), Filterung von Webinhalten, VPN-Overlays, IDS/IPS, dynamische Segmentierung, Sicherheits-Dashboards und einen einheitlichen SASE durch die Integration mit HPE Aruba Networking SSE (Security Service Edge).

Tabelle 1. Funktionen zur Sicherung von LAN und LAN-Verkehr

Sicherheitsmerkmal	Details
Statusabhängig und anwendungskonsistent mit Deep Packet Inspection	Benutzer- und Anwendungskonsistenz mit umfassender Richtliniendurchsetzung dank Deep Packet Inspection (DPI)
Angriffserkennung und -prävention (IDS/IPS)	Integrierte Angriffsprävention mit erweiterten Sicherheits-Dashboards
Integration mit SIEM-Tools	Bedrohungsereignisse werden an SIEM-Systeme (Security Information and Events Management) wie beispielsweise Splunk gestreamt.
Filterung von Webinhalten	Bietet die Möglichkeit, Richtlinien basierend auf Standortkategorien zu erstellen
IP-Reputation	Beschränkt automatisch den Datenverkehr von bekanntermaßen schädlichen Quellen
Unified SASE	Integriert sich eng mit HPE Aruba Networking SSE, um eine einheitliche SASE-Plattform zu bilden
Dynamische Segmentierung	Bietet rollenbasierte Segmentierung im gesamten LAN und WAN für verteilte Unternehmen
Sicherheit und Systemhärtung auf Managementebene	Bietet erweiterte Funktionen zur Sicherung der Plattform mit sicherem Booten, Zero-Touch-Bereitstellung und AES256-Verschlüsselung

[2] Weitere Informationen finden Sie im technischen Dokument Unified Policy for the Distributed Enterprise und in der Policy Enforcement Firewall Technical Brief



Statusabhängige, anwendungskonsistente Firewall mit Deep Packet spection

EdgeConnect SD-Branch beinhaltet eine statusabhängige, anwendungskonsistente Firewall mit DPI-Funktionen (Deep Packet Inspection). Es ermöglicht eine feinmaschigere Richtlinienkontrolle und bietet Unternehmen so eine verbesserte Plattform, um neue und aufkommende Bedrohungen zu bewältigen.

Um Transparenz und Kontrolle bieten zu können, erkennt die DPI von EdgeConnect SD-Branch über 3.700 Protokolle und Anwendungen. Die Lösung führt eine DPI des Anwendungsverkehrs durch und stellt sie in einem Dashboard zusammen, das die Bandbreite und Qualität von Anwendungen im Netzwerk überwacht.

Die DPI ermöglicht es Netzwerkadministratoren auch, Firewall-Richtlinien basierend auf Anwendungstyp oder -kategorie zu erstellen. Beispielsweise können Administratoren Richtlinien erstellen, um den Benutzerzugriff auf eine Anwendung oder Anwendungskategorie einzuschränken. Sie können auch Traffic-Shaping-Richtlinien wie Bandbreitenkontrolle und QoS pro Anwendung für Client-Rollen bestimmen und bandbreitenmonopolisierende Anwendungen für eine Gastrolle innerhalb des Unternehmens blockieren.

Angriffserkennung und -prävention (IDS/IPS)

Die Angriffsprävention erkennt schädliche Aktivitäten und ergreift Maßnahmen, wenn ein Angriff erkannt wird. Die Erkennungs-Engine von EdgeConnect SD-Branch überprüft den gesamten Datenverkehr, der das Netzwerk durchläuft, anhand einer signatur- und einer musterbasierten Prüfung mittels einer Bibliothek bekannter Bedrohungen.

Entspricht ein Angriff einem Signaturmuster, ergreift das System Maßnahmen. Die Lösung sendet Warnmeldungen und Benachrichtigungen an den Netzwerkadministrator. Ist IPS aktiviert, wird der Datenverkehr blockiert, um das Unternehmen vor einer schädlichen Aktivität zu schützen. Ergänzend unterstützt die Lösung Netzwerkadministratoren beim Erstellen einer Liste zulässiger Bedrohungen, selbst wenn deren Signatur einem bekannten Muster entspricht.

Die Angriffserkennung liefert Bedrohungsinformationen zu schädlichen Aktivitäten, einschließlich Command and Control, Ransomware, Phishing, Malware, Spyware, Trojanern und Exploit-Kits. Die Lösung wird täglich aktualisiert und stellt sicher, dass Unternehmen den Überblick über die dynamische Bedrohungslandschaft behalten, die sich ständig weiterentwickelt. Sie umfasst mehr als tausend Regeln, untergliedert in 50 Kategorien. Und das Regelwerk wird ständig erweitert: Aus der ganzen Welt gehen Beiträge zu bisher unbekannten Bedrohungen ein. Das Signaturpaket gewährleistet eine optimale Leistung und genaue Erkennung. Die wichtigsten Signaturen werden automatisch auf allen Gateways bereitgestellt, die von HPE Aruba Networking Central verwaltet werden. Die Angriffserkennung wird in HPE Aruba Networking Central unter Sicherheitsmanagement verwaltet (Abbildung 1).

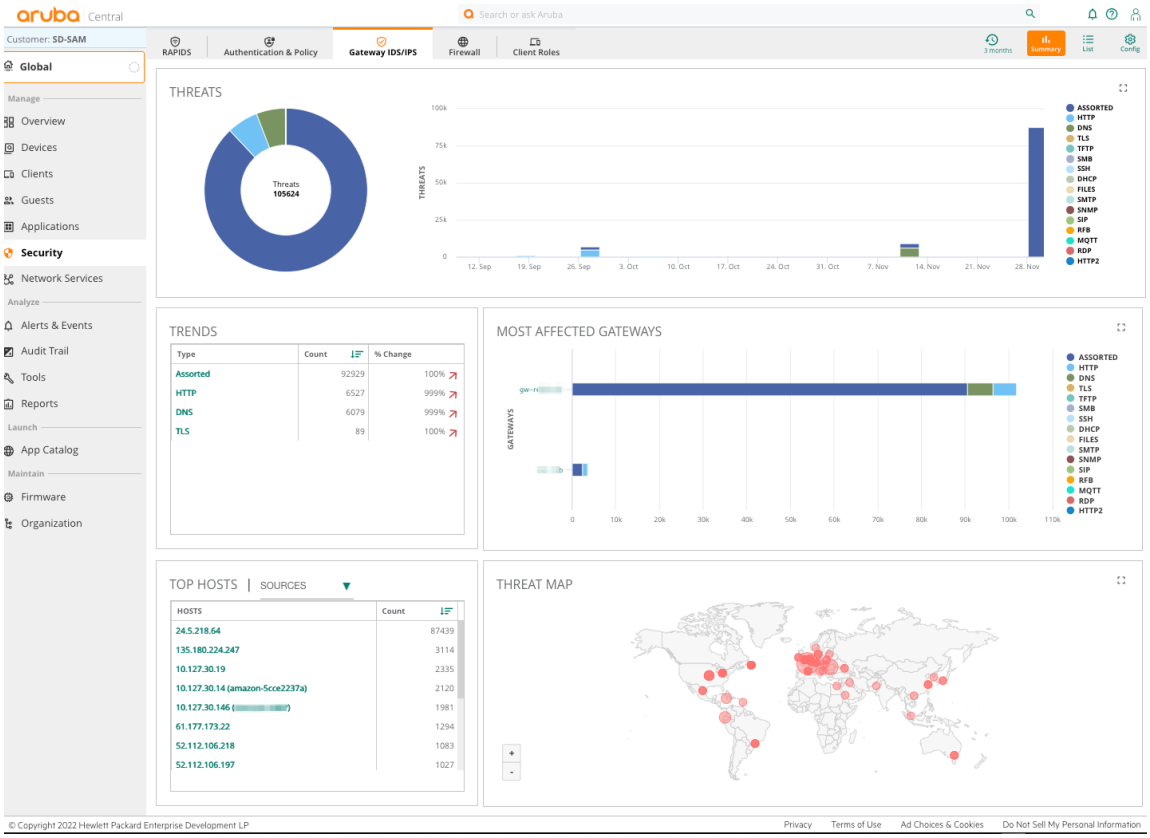


Abbildung 1. Sicherheits-Dashboard für die Angriffsprävention in HPE Aruba Networking Central.

Erkannte Bedrohungen und Warnmeldungen werden in der oberen Kachel zusammengefasst und dargestellt. Diese Bedrohungen werden danach kategorisiert, wie sie in die Filiale gelangen (z. B. über eine HTTP- oder DNS-Anfrage). Auf diesem Dashboard können Sie Bedrohungen im Zeitverlauf sehen und den Benutzer- und Anwendungsverkehr den Bedrohungen zuordnen. Sie können auch Trends für verschiedene Arten von Bedrohungen einsehen.

Die verwendeten Werte beziehen sich auf die Bedrohungskategorie, die Art und Schwere der Bedrohungen sowie die Bedrohungsprävalenz. Sie können Details bis zu den betroffenen Benutzern und Geräten oder der Quelle und dem Ausmaß der Auswirkungen recherchieren. Abbildung 2 zeigt alle Bedrohungen für ein bestimmtes Gerät.

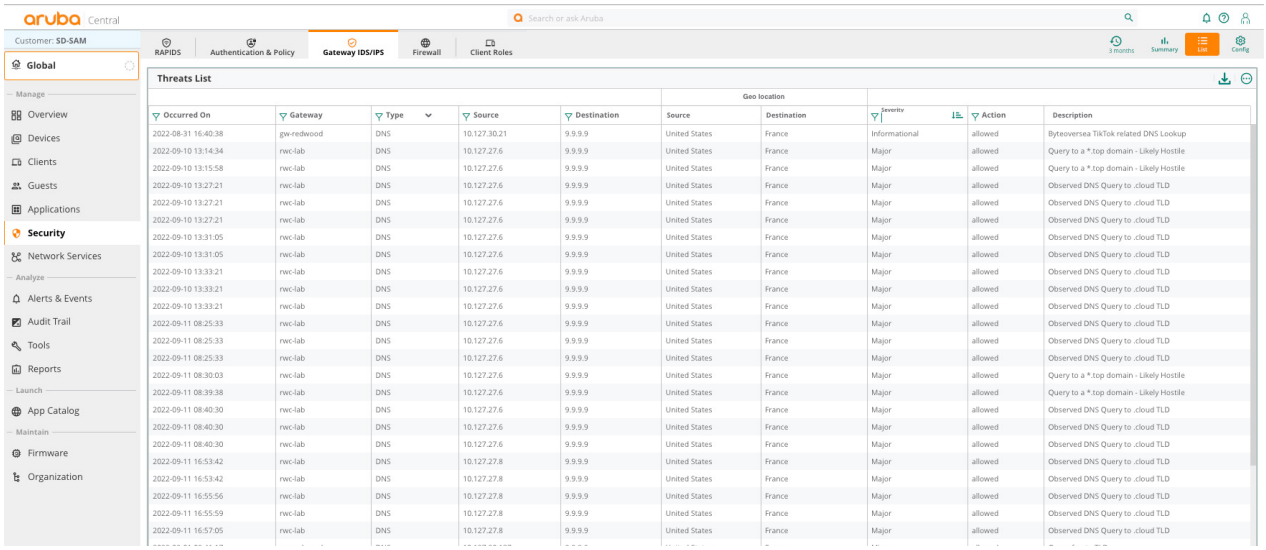


Abbildung 2. Liste der Bedrohungen für ein einzelnes Gerät, die durch detaillierte Aufschlüsselung über das Dashboard erreicht wird.

Neben dem Datum zeigt die Tabelle das Gateway, über das die Bedrohung in die Filiale eingedrungen ist, sowie die Art der Bedrohung, deren Quelle und eine Beschreibung. Sie können auch eine weitere Aufschlüsselung vornehmen, um die Details zu einer bestimmten Bedrohung genauer zu betrachten (Abbildung 3).

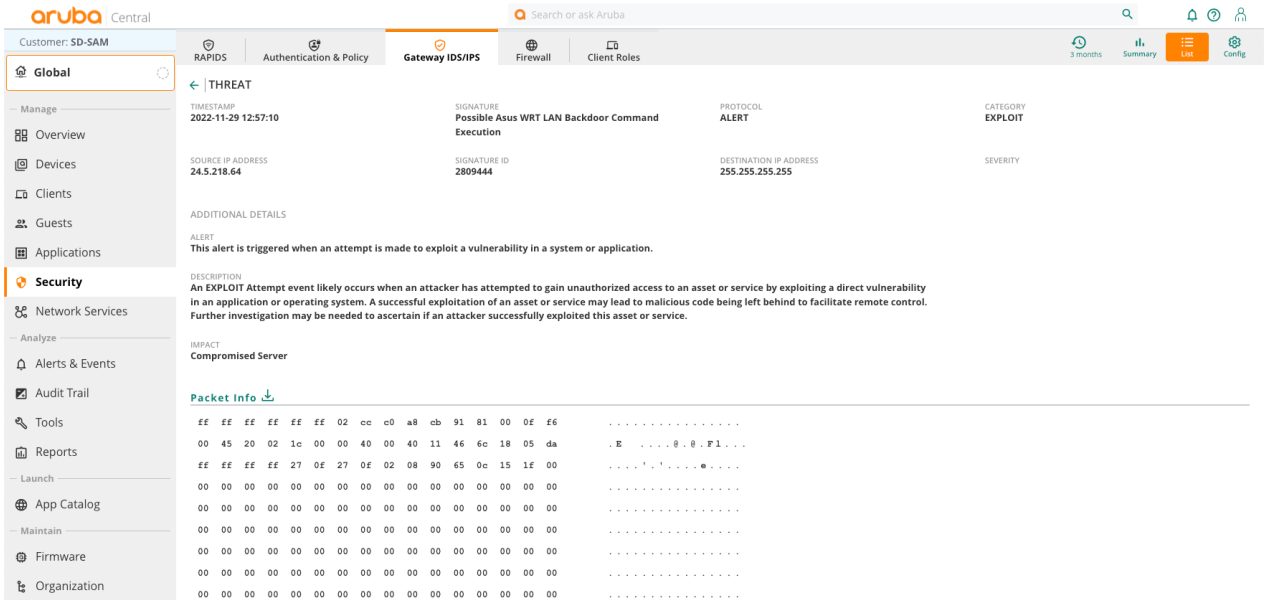


Abbildung 3. Details zu einer Bedrohung

In dieser Ansicht erhalten Sie Informationen über die Art der Bedrohung (Kategorie) und die Bedrohungssignatur. Die Informationen über Sicherheitsbedrohungen in HPE Aruba Networking umfassen ein umfangreiches Signaturpaket und einen Regelsatz mit Zehntausenden Regeln und Dutzenden Kategorien.

Basierend auf den Informationen, die Sie auf der Seite mit den Bedrohungsdetails sehen, können Sie die Richtlinien anpassen (Abbildung 4).

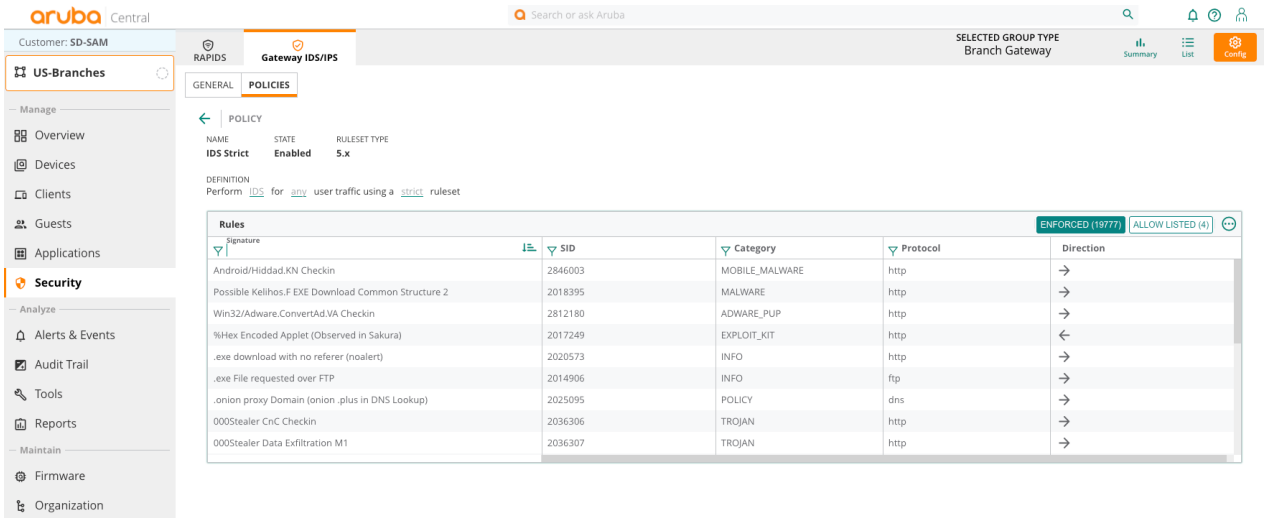


Abbildung 4. Anpassung der Richtlinienregeln für eine Reihe von Bedrohungen

Es gibt integrierte Richtlinien, die Regeln zum Verwerfen oder Zulassen von Paketen definieren, die einer bestimmten Bedrohungssignatur entsprechen. Diese sind in Abbildung 5 zu sehen.

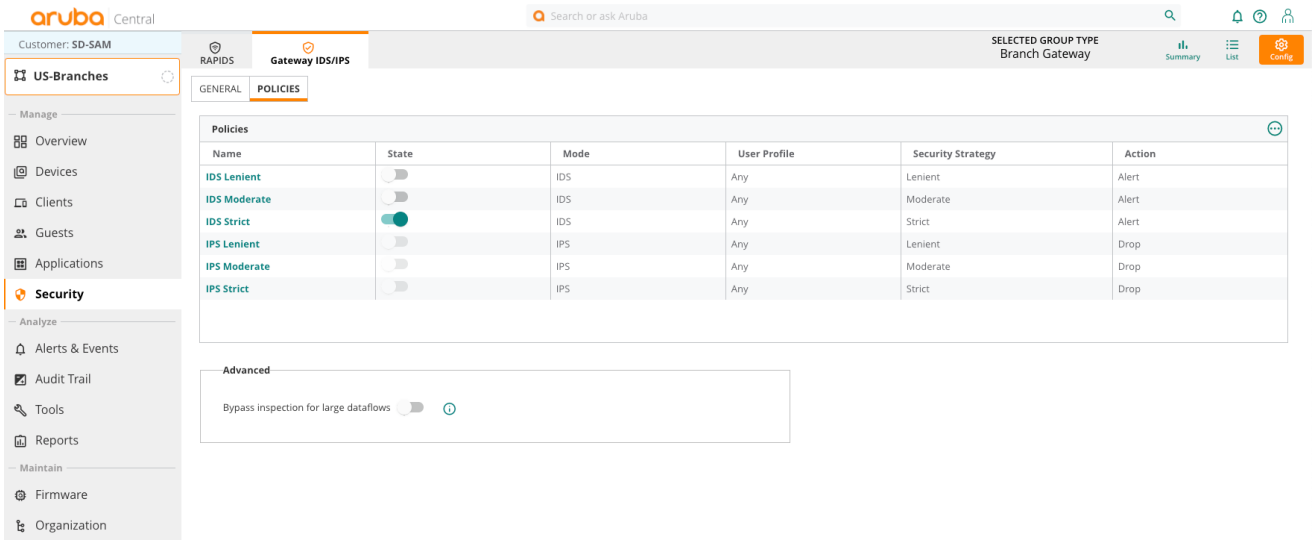


Abbildung 5. Integrierte Richtlinien für das Bedrohungsmanagement.

Sowohl für IDS als auch für IPS kann die Sicherheitsstrategie tolerant, moderat oder streng sein. Diese Einstellungen können Datenverkehr zulassen oder verwerfen oder Warnungen ausgeben.

Integration mit SIEM-Tools

EdgeConnect SD-Branch erfasst Ereignisse im Zusammenhang mit Datenverkehrs- Sessions im Syslog-Nachrichtenformat. Bedrohungsereignisse werden mit dem Central Alert Framework zur Benachrichtigung und Integration mit Protokollierungs- und Sicherheitsanalysetools von Drittanbietern auf Basis festgelegter Schwellenwerte verwaltet.

Ereignisse wie etwa ein Eindringen können an SIEM-Systeme (Security Information and Events Management) wie beispielsweise Splunk gestreamt werden, um die Transparenz und Überwachung zu verbessern. Dadurch können IT-Abteilungen Ereignisse erkennen, die näher betrachtet werden müssen, und so Vorfälle schnell verwalten und beheben.



Abbildung 6. Splunk-Sicherheits-Dashboard

Klassifizierung von Webinhalten, IP-Reputation und Geolocation-Filter

Durch die Filterung von Inhalten werden bestimmte Websites blockiert, die für Unternehmen potenziell schädlich, anstößig und sogar kriminell sein können. Die Filterung von Webinhalten hilft Unternehmen dabei, Websites zu erkennen, die Malware, Spam, Spyware und Phishing-Angriffe verbreiten, sowie Websites mit sensitiven Inhalten (z. B. nicht jugendfreie Inhalte oder Glücksspiele).

Mithilfe von maschinellem Lernen für mehr Geschwindigkeit und höhere Genauigkeit bietet Aruba EdgeConnect SD-Branch eine Klassifizierung von Webinhalten (oder URL-Filterung) und bezeichnet mehr als 80 Website-Kategorien, einschließlich Kategorien mit hohem Risiko.

SD-Branch bietet auch IP-Reputation und Geolocation-Filter, über die sich in Echtzeit das von eingehendem Datenverkehr ausgehende Risiko bestimmen lässt.

Der IP-Reputationsservice liefert einen Echtzeit-Feed bekannter schädlicher IP-Adressen, unterteilt in 10 Kategorien, damit IT-Sicherheitsadministratoren Bedrohungen leicht nach Typ erfassen können. Diese Kategorien umfassen Windows-Exploits, Webangriffe, Phishing, Botnets, Denial-of-Service, Scanner, Proxys, Reputation, Spam-Quellen und mobile Bedrohungen.

Der Service verwendet die Seitenhistorie, Alter, Rang, Standort, Netzwerke, Links, Echtzeitleistung sowie andere Kontext- und Verhaltenstrends, um einen IP-Reputationsindex zu bestimmen, und nimmt eine Klassifizierung in fünf Reputationsstufen – „Vertrauenswürdig", „Geringes Risiko", „Mittleres Risiko", „Verdächtig" und „Hohes Risiko" – vor. Insgesamt klassifiziert die Lösung über 842 Millionen Domänen und über 37 Milliarden URLs.

Der Geolocation-Filterservice verknüpft Quell-/Ziel-IP-Adressen mit einem Standort.

Damit können Unternehmen Richtlinien anwenden, um ein- oder ausgehende Kommunikation mit bestimmten bekannten böswilligen Ländern zuzulassen oder zu unterbinden.

Mit der Filterung von Webinhalten können Unternehmen ihre Beschäftigten vor bösartigen Webinhalten schützen, die Produktivität steigern, Nutzungsrichtlinien einrichten und durchsetzen und sich vor rechtlichen Konsequenzen schützen.

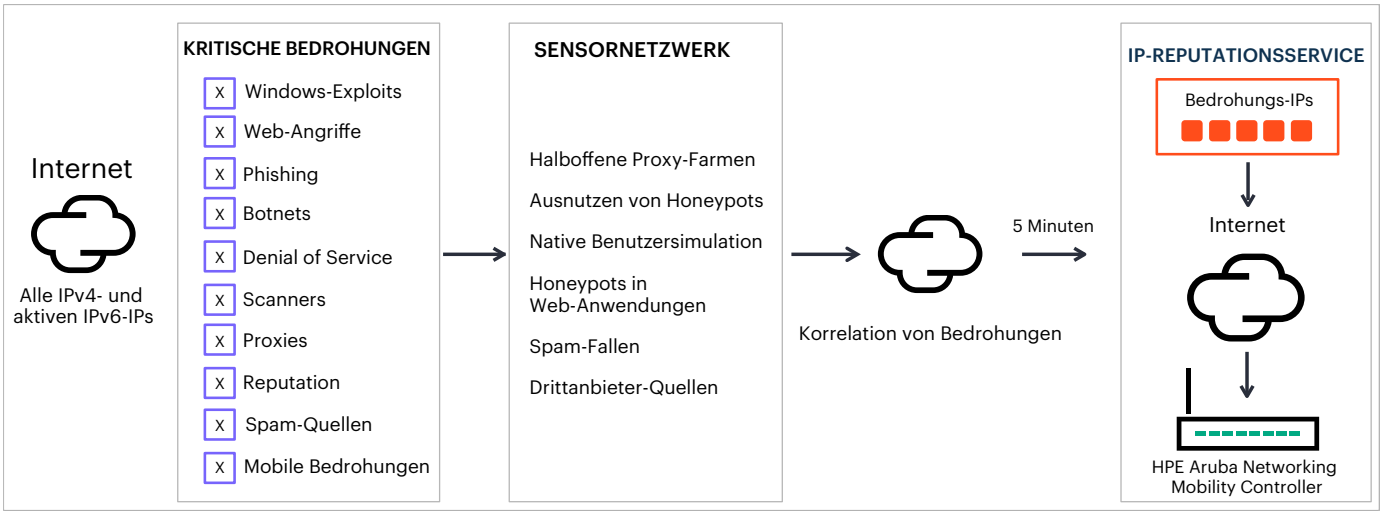


Abbildung 7. Der IP-Reputationsservice verfolgt und filtert externe Bedrohungen in Echtzeit



Einheitlicher SASE

Im Jahr 2019 definierte Gartner den Secure Access Service Edge (SASE), um die Netzwerk- und Sicherheitsherausforderungen zu bewältigen, die sich durch Benutzer ergeben, die sich von verschiedensten Orten aus verbinden und dabei über nicht vertrauenswürdige Links auf vertrauliche Daten in Anwendungen in der Cloud zugreifen. In der Vergangenheit stellten die Mitarbeitenden vor Ort die Verbindung mit einem Unternehmensnetzwerk her und griffen auf Anwendungen zu, die in einem Rechenzentrum gehostet wurden. So war es einfacher, das Netzwerk zu schützen.

Um die Sicherheit in einem jetzt grenzenlosen Unternehmen mit einer hybriden Belegschaft zu gewährleisten, kombiniert SASE Funktionen des SD-WAN mit Leistungen auf Basis von HPE Aruba Networking SSE, darunter ZTNA (Zero Trust Network Access), CASB (Cloud Access Security Broker), SWG (Secure Web Gateway) und DEM (Digital Experience Monitoring).

HPE Aruba Networking SSE bietet eine umfassende Lösung, in der ZTNA, SWG, CASB und DEM auf einer gemeinsamen Codebasis nahtlos zusammenarbeiten. Sämtliche Richtlinien lassen sich über eine zentrale Benutzeroberfläche verwalten, wodurch die Kontrolle für IT-Administratoren vereinfacht wird. Benutzern wird der Zugriff auf Ressourcen per ZTNA mit und ohne Agenten ermöglicht. Benutzer werden mit SWG vor Bedrohungen aus dem Web geschützt, und vertrauliche Daten in SaaS-Anwendungen werden mit CASB sicher überwacht, um die Exfiltration der Daten zu verhindern. Zudem vereinheitlicht die Lösung den Zugriff weltweit mittels eines Cloud-Backbones aus Amazon Web Services (AWS), Microsoft Azure, Google und Oracle.

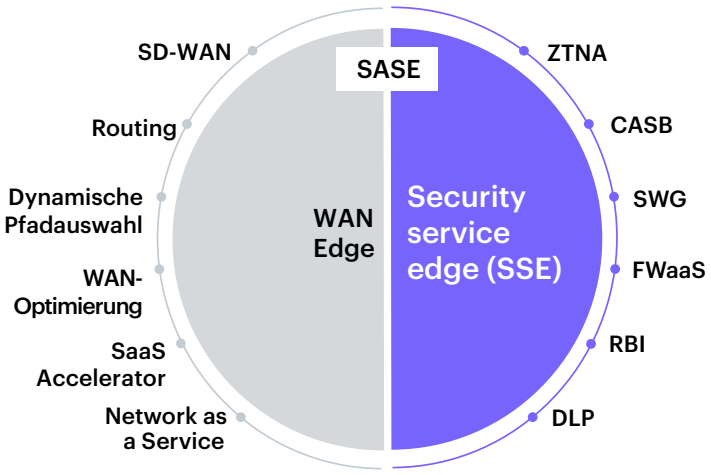


Abbildung 8. SASE-Architektur

Die wichtigsten Funktionen von HPE Aruba Networking SSE:

ZTNA (Zero trust network access): Die Lösung folgt dem Prinzip „Niemals vertrauen, immer überprüfen". Im Gegensatz zu VPNs, die einen weitflächigen Zugriff auf das Unternehmensnetzwerk ermöglichen, schränkt ZTNA den Benutzerzugriff auf bestimmte Anwendungen oder Mikrosegmente ein, die für jeden Benutzer genehmigt werden müssen. Dieser Ansatz wendet den Grundsatz der geringsten Rechte an. Damit können sich Remote-Arbeitskräfte von überall sicher verbinden. Dritte können einen agentenlosen ZTNA nutzen, über den sie sich einfach mit ihren eigenen Anmeldedaten in einem Web-Portal anmelden können, ohne einen ZTNA-Agenten zu installieren.

SWG (Secure web gateway): Das SWG fungiert als Vermittler zwischen Benutzern und Websites, wobei es Schutz vor Bedrohungen wie Ransomware und Phishing bietet. Es führt zahlreiche Sicherheitsinspektionen durch, die URL-Filterung, Filterung von Inhalten und Web-Zugriffskontrolle umfassen. Ergänzend bietet SWG Richtlinien, um den Zugriff auf bestimmte Kategorien von Websites wie Inhalte für Erwachsene, Glücksspiele oder gefährliche Websites einzuschränken.

CASB (Cloud access security broker): Der CASB gewährleistet die Sicherheit vertraulicher Daten in der Cloud. Er identifiziert und erkennt vertrauliche Daten in Cloud-Anwendungen und setzt Sicherheitsrichtlinien wie beispielsweise Authentifizierung und Single Sign-On (SSO) durch. Er überwacht die Benutzeraktivität in Cloud-Services, erkennt mögliche Sicherheitsrisiken und Richtlinienverstöße und verhindert Datenverluste. Der CASB kontrolliert auch Daten-Uploads und -Downloads in SaaS-Anwendungen wie Box, SharePoint, Facebook und Salesforce. Darüber hinaus verhindert der CASB, dass Benutzer nicht autorisierte Cloud-Anwendungen verwenden, und reduziert so das Risiko von Schatten-IT.

DEM (Digital experience monitoring): Durch die Messung von Hop-by-Hop-Metriken und die Überwachung der Anwendungs-, Geräte- und Netzwerkleistung stellt DEM die Produktivität von Benutzern sicher. Mit DEM können IT-Administratoren Konnektivitätsprobleme einfach erkennen und die Mean Time to Resolution verkürzen, um eine reibungslose Benutzererfahrung sicherzustellen.

EdgeConnect SD-Branch integriert sich auch mit mehreren Anbietern für Cloud-Sicherheit, wie etwa Zscaler. Dafür erstellt EdgeConnect SD-Branch sichere Tunnel zwischen SD-Branch- und SSE-Lösungen und automatisiert die Orchestrierung auf SSE-Services.

Ergänzend kann EdgeConnect SD-Branch mit First-Packet-Klassifizierung von Anwendungen bei der Deep Packet Inspection (DPI) bestimmten Netzwerkverkehr auf Basis von Identität oder Anwendung umleiten. Vertrauenswürdige Anwendungen wie Microsoft 365 und Salesforce werden direkt an das Internet weitergeleitet, während Datenverkehr von anderen Cloud-Anwendungen zur weiteren Sicherheitsprüfung zu HPE Aruba Networking SSE oder zu anderen in der Cloud bereitgestellten Sicherheitslösungen gelenkt wird. In einigen Fällen kann der Datenverkehr in das Rechenzentrum geroutet werden, beispielsweise wenn Legacy-Anwendungen im Rechenzentrum gehostet werden oder aus Sicherheitsgründen.

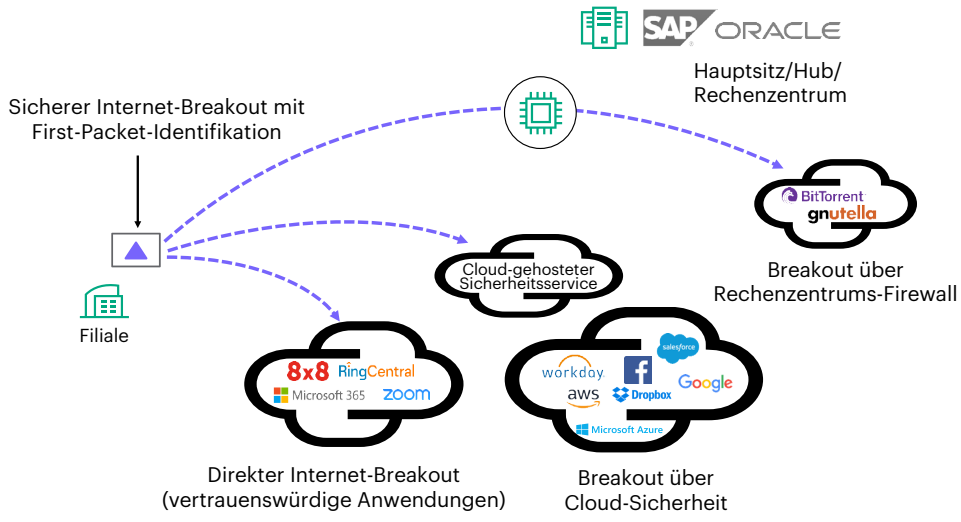


Abbildung 9. Aufbau einer einheitlichen SASE-Plattform mit HPE Aruba Networking und nahtlosem Breakout-Verkehr basierend auf Sicherheitsrichtlinien

Dynamische Segmentierung

Da sich der Sicherheitsperimeter allmählich auflöst, ist SASE zum Schutz von Remote-Benutzern sehr wichtig. Aufgrund der Verbreitung von Geräten im Netzwerk wie beispielsweise IoT-Geräten ist es kritischer geworden, durch die Segmentierung des Netzwerks in Zonen die Angriffsfläche zu verkleinern und so die Verbreitung möglicher Angriffe zu begrenzen.

Daher muss SASE durch ein identitätsbasiertes Zero-Trust-Sicherheits-Framework ergänzt werden, das den Datenverkehr dynamisch segmentiert, sodass Anwender und IoT-Geräte nur Netzwerkziele erreichen können, die ihrer Rolle im Unternehmen entsprechen.

Durch die Segmentierung können Unternehmen nicht nur die Sicherheit und Kontrolle, sondern auch die Anwendungsleistung erhöhen. Netzwerkadministratoren können zum Vermeiden von Überlastungen und zur Priorisierung des Verkehrs konkrete Zonen für geschäftskritische Anwendungen und weitere Zonen für weniger wichtige Anwendungen wie z. B. HLK-Anlagen definieren.

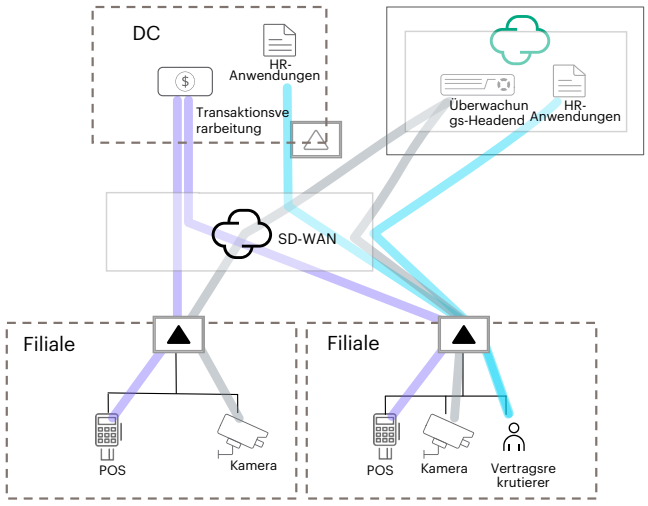
Traditionell haben Unternehmen VLANs definiert, um das Netzwerk zu segmentieren. Die VLAN-Konfiguration bleibt ein komplexer und fehleranfälliger Prozess. Denn Netzwerkadministratoren mussten viele Netzwerkkomponenten sowie Zugriffskontrolllisten (ACLs) manuell konfigurieren, die fest vorgegebene IP-Adressbereiche verwenden, die an bestimmte VLANs gebunden sind. Mit der wachsenden Mobilität, explosionsartigen Zunahme des IoT und immer mehr verteilten Unternehmen ist dieser Ansatz sehr komplex geworden, was zu einer Ausbreitung von VLANs und nicht mehr verwaltbaren Netzwerken führt. Selbst bei einfachsten Konfigurationsänderungen oder beim Client-Onboarding können längere Bereitstellungszyklen und umfangreiche Neukonfigurationen erforderlich sein, die die Produktivität der IT massiv beeinträchtigen.

EdgeConnect SD-Branch verwendet rollenbasierte dynamische Segmentierung, womit Unternehmen das Netzwerk auf einfache und skalierbare Weise über das LAN und WAN segmentieren können, während sie gleichzeitig die Herausforderungen von Mobilität und IoT bewältigen. In Verbindung mit HPE Aruba Networking ClearPass Policy Manager erzwingt EdgeConnect SD-Branch eine Zero-Trust-Architektur und wendet das Prinzip der geringsten Rechte auf den Zugriff an. Es gewährleistet, dass Anwender und Geräte nur mit Zielen kommunizieren, die ihrer jeweiligen Rolle in Bezug auf Identität, Zugriffsrechte und Sicherheitsstatus entsprechen.

Die Integration von ClearPass Policy Manager mit EdgeConnect SD-Branch ergänzt Wissen über die Identität von Benutzern, Geräten und Rollen, um Authentifizierungsprotokolle wie RADIUS, TACACS+ und OAuth2 und mehrere Identitätsspeicher wie Microsoft Active Directory zu unterstützen. Richtlinien werden basierend auf diesen Rollen eingerichtet und an den Gateways von HPE Aruba Networking Central konfiguriert und durchgesetzt. Diese Richtlinien ermöglichen die Autorisierung für den Zugriff auf Anwendungen oder Ziele sowie den gegenseitigen Zugriff (wie die Kommunikation von Benutzern untereinander oder gegenseitigen Zugriff auf Geräte).

Um Transparenzlücken zu schließen, die häufig mit Mobil- und IoT-Geräten einhergehen, bietet HPE Aruba Networking Central eine ML-basierte Klassifizierung aller Clients mit Aruba Client Insights. Diese Funktion nutzt dynamische Vergleiche mit Fingerprints bekannter Clients und die Klassifizierung von MAC-Bereichen für den wahrscheinlichen Fall, dass unbekannte Geräte mit dem Netzwerk verbunden sind.

Um globale Sicherheitsrichtlinien in komplexen, globalen verteilten Netzwerken nahtlos durchzusetzen, beinhaltet



	Kamera	Überwachungs-Headend	POS-Terminal	Transaktionsverarbeitung	Vertragsrekrutierer	HR-Anwendungen
Kamera	✗	✓	✗	✗	✗	✗
Überwachungs-Headend	✓	✓	✗	✗	✗	✗
POS-Terminal	✗	✗	✗	✓	✗	✗
Transaktionsverarbeitung	✗	✗	✓	✓	✗	✗
Vertragsrekrutierer	✗	✗	✗	✗	✗	✓
HR-Anwendungen	✗	✗	✗	✗	✓	✓

Abbildung 10. Ausweitung der dynamischen Segmentierung auf das WAN

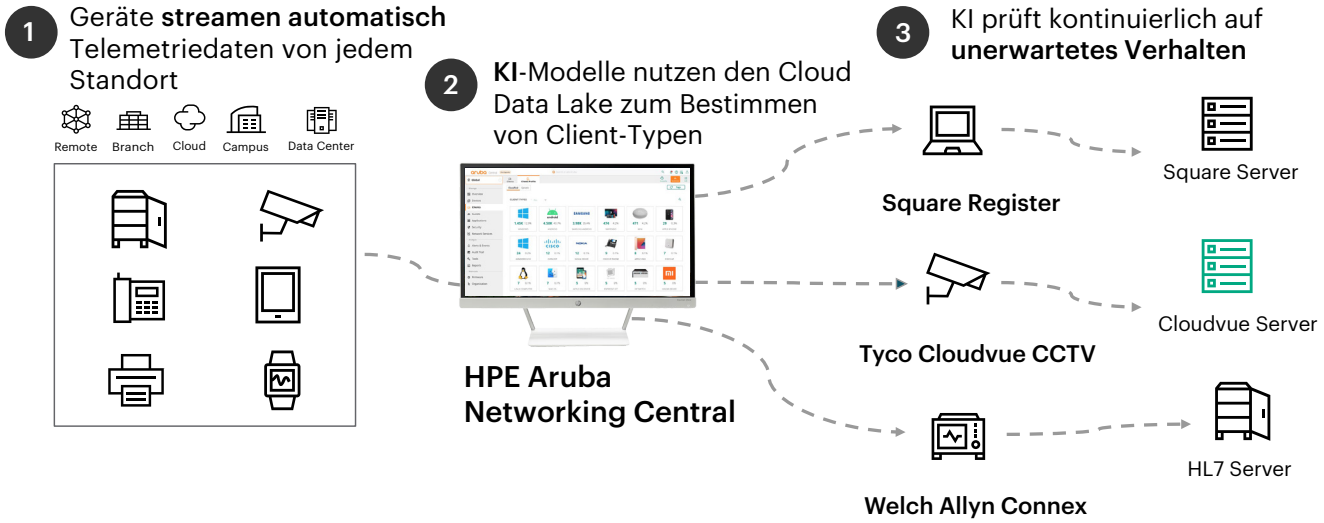


Abbildung 11. HPE Aruba Networking Client Insights verwendet Netzwerk- und Client-Telemetrie mit maschinellem Lernen, um alle kabelgebundenen und WLAN-Endpunkte genau zu identifizieren und zu klassifizieren

HPE Aruba Networking Central NetConductor, der EVPN-, VXLAN- und BGP-Protokolle einsetzt, um die Inline-Richtliniendurchsetzung zu erleichtern. Er erstellt und orchestriert automatisch intelligente Overlays in Verbindung mit einem umfassenden regelbasierten Mikrosegmentierungsmodell auf Basis globaler Rollen in der gesamten Netzwerkinfrastruktur des Unternehmens. Die in Filialen bereitgestellten HPE Aruba Networking Gateways fassen die Client-Verkehrsinformationen mit VXLAN-BGP und IPsec zusammen, die die Rolleninformationen im VXLAN-Header enthalten.

Das Gateway am Zielstandort setzt dann die rollenbasierten Richtlinien für Client-Verkehr um.

Mit anderen Worten: Die einem verbundenen Gerät im Netzwerk zugewiesene Rolle wird mit HPE Aruba Networking Central global definiert. Central leitet dann die Rolleninformationen über den Tunnel-Orchestrator an die Aruba Gateways weiter und weist diese an, Datenverkehr zwischen den Geräten im gesamten WAN zuzulassen oder zu verweigern.

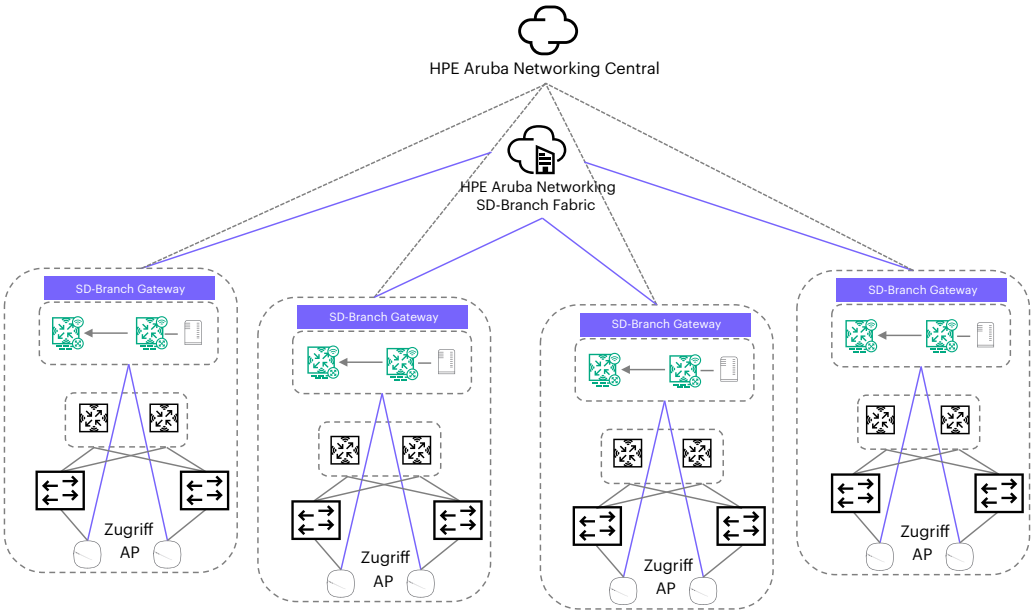


Abbildung 12. Möglichkeit der dynamischen Segmentierung in komplexen, verteilten Netzwerkarchitekturen durch Bereitstellung von EdgeConnect SD-Branch mit NetConductor

NetConductor beinhaltet auch CloudAuth. Damit ist ein reibungsloses Onboarding von Endbenutzern und Client-Geräten durch die Integration mit Cloud-Identitätsspeichern wie Azure Active Directory und Google Workspace oder durch MAC-basierte Authentifizierungen und KI-basierte Client Insights möglich. Dies automatisiert und vereinfacht die Richtliniendefinition für IoT-Geräte mit verhaltensbasierter Profilerstellung mittels KI- oder ML-basierter Klassifizierung und ermöglicht so einen stärkeren Sicherheitsstatus als mit der reinen Verwendung von MAC-Adressen.

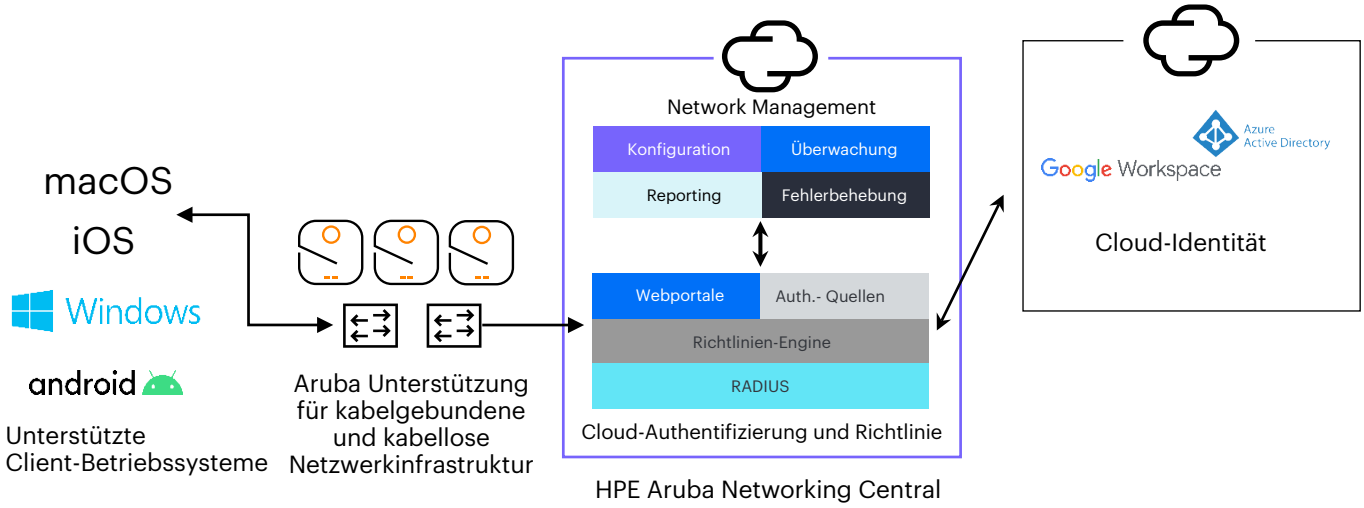
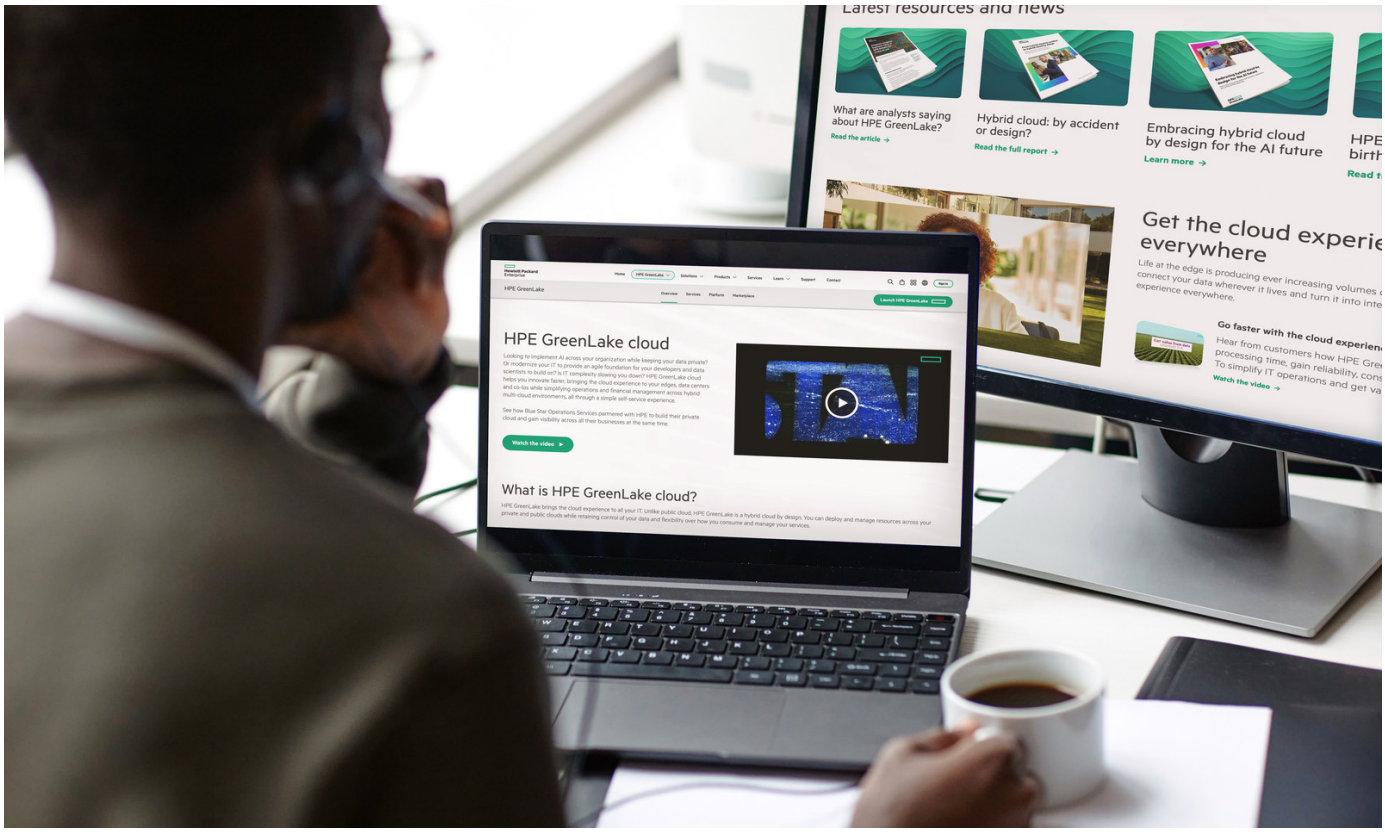


Abbildung 13. CloudAuth Service in NetConductor bietet ein flexibles, leistungsstarkes Framework für die Gewährung des Netzwerkzugriffs



Sicherheit und Systemhärtung auf Managementebene

EdgeConnect SD-Branch[3] verwendet die TPM-Technologie (Trusted Platform Module), einen internationalen Standard, als sicheren, manipulationssicheren Kryptoprozessor. Es handelt sich dabei um einen dedizierten Mikrocontroller, der die Hardware durch die Integration von kryptografischen Schlüsseln in die Geräte schützt. Durch die Verwendung manipulationssicherer Schlüssel können die Geräteintegrität und der Bootcode als unverändert validiert werden, wodurch ein sauberer Startprozess gewährleistet wird. Um diesen Vorgang zu ermöglichen, werden während der Fertigung Bestätigungsschlüssel installiert.

- **Secure Boot:** Um ArubaOS zu laden, erfordert EdgeConnect SD-Branch ein von HPE Aruba Networking ausgestelltes TPM-Zertifikat (Trusted Platform Module). Das TPM-signierte Software-Image schränkt die Kommunikationen stark ein, bis das EdgeConnect SD-Branch Gateway seine Erstkonfiguration von HPE Aruba Networking Central erhält.
- **Sichere Zero-Touch-Bereitstellung:** Um die Kommunikation mit HPE Aruba Networking Central zu sichern, verwendet EdgeConnect SD-Branch das in die HPE Aruba Networking Gateways geladene TPM-Zertifikat. Diese Verbindung nutzt das Transport Layer Security Protokoll (TLS 1.2).
- **WAN Protect ACL:** Eine Standard-ACL schützt die WAN-Seite von EdgeConnect SD-Branch vor externen Bedrohungen. Die Liste wird auf alle als WAN-Ports gekennzeichnete Ports angewandt.

AES-256-Verschlüsselung: EdgeConnect SD-Branch erstellt verschlüsselte IPsec-Tunnel mit AES-256-Bit-Verschlüsselung innerhalb der gesamten SD-WAN-Fabric. IPsec-Tunnel basieren auf dem Internet Key Exchange Protocol Version 2 (IKEv2).
HPE Aruba Networking Gateways nutzen zur beidseitigen Authentifizierung werkseitig installierte TPM-Zertifikate (Trusted Platform Module), um den Aufbau von Overlay-Tunneln zu vereinfachen und zu automatisieren. TPM-Werkszertifikate werden werkseitig auf jedem Gateway installiert. Vom Benutzer hochgeladene Zertifikate werden jedoch bei Bedarf unterstützt. Nur das Protokoll und der UDP-Zielport 4500 müssen für die Einrichtung eines Overlay-IPsec-Tunnels offen bleiben.

HPE Aruba Networking Framework für Zero-Trust-Sicherheit und Compliance

HPE Aruba Networking bietet einen integrierten Ansatz zur Gewährleistung der Zero-Trust-Sicherheit, die LAN-, WLAN- und WAN-Netzwerke umfasst. Dieser Ansatz besteht aus den folgenden fünf Schritten:

- **Transparenz:** Erkennen von Geräten im Netzwerk mithilfe von KI-Methoden
- **Authentifizierung und Autorisierung:** Authentifizierung und Definition von Zugriffsrichtlinien
- **Rollenbasierte Zugriffssicherheit:** Dynamische Bereitstellung des Zugriffs auf einige Netzwerksegmente
- **Kontinuierliche Überwachung:** Erkennen externer Bedrohungen anhand von Warnmeldungen
- **Durchsetzung und Reaktion:** Entsprechende Reaktion auf erkannte Bedrohungen.

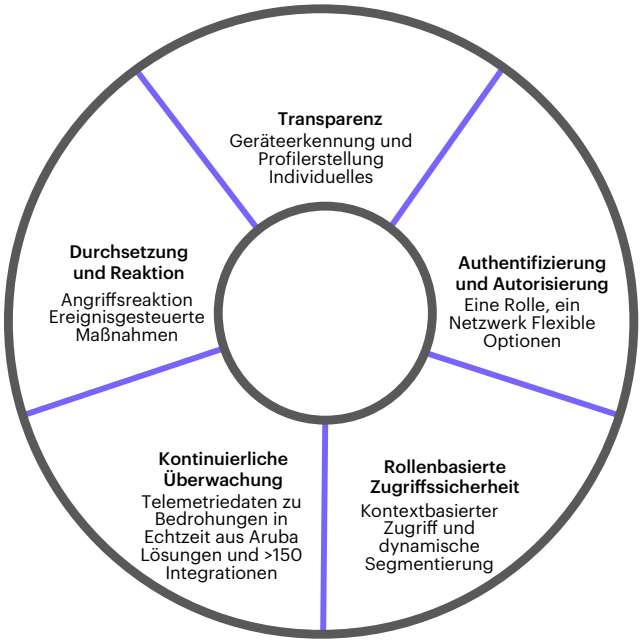


Abbildung 14. Der integrierte Sicherheitsansatz von HPE Aruba Networking (kabelgebundene und Wireless-Sicherheit)

[3] Weitere Informationen finden Sie im Aruba EdgeConnect SD-Branch Leitfaden zur Härtung.

— **Transparenz:** Mit der steigenden Akzeptanz des IoT ermöglicht es HPE Aruba Networking Client Insights Unternehmen, Gerätetypen schnell anhand ML-basierter Klassifikationsmodelle zu erkennen.

— **Authentifizierung:** ClearPass Policy Manager von HPE Aruba Networking erstellt rollenbasierte Zugriffsrichtlinien und authentifiziert jedes Gerät, das sich mit dem Netzwerk verbindet. Es können mehrere Authentifizierungsmethoden verwendet werden. Für Netzwerke, die mit HPE Aruba Networking Central verwaltet werden, ermöglicht Cloud Auth das Onboarding von Endbenutzern und Client-Geräten entweder über MAC oder durch die Integration mit Cloud-Identitätsspeichern wie Google Workspace oder Azure Active Directory.

— **Rollenbasierte Zugriffssteuerung:** EdgeConnect SD-Branch bietet dynamische Segmentierung nach Rollen und Identitäten und gewährleistet eine Zero-Trust-Architektur auf Basis des Zugriffs mit geringsten Rechten. Ergänzend ermöglicht der in HPE Aruba Networking Central enthaltene NetConductor unter Verwendung gängiger Protokolle wie EVPN/VXLAN eine dynamische Segmentierung über große, verteilte Netzwerke.

— **Kontinuierliche Überwachung und Durchsetzung:** EdgeConnect SD-Branch leistet Angriffserkennung und -prävention (IDS/IPS) durch eine signatur- und musterbasierte Prüfung des Filial-LAN-Datenverkehrs (Ost-West) sowie des SD-WAN-Datenverkehrs (Nord-Süd). Das erweiterte Sicherheits-Dashboard in HPE Aruba Networking Central stellt IT-Teams eine netzwerkweite Übersicht, multidimensionale Bedrohungsmetriken, Threat-Intelligence-Daten sowie Korrelations- und Störungsmanagement zur Verfügung. Bedrohungsereignisse werden zur Behebung an SIEM-Systeme und ClearPass gesendet.

Die Tabelle unten zeigt die verschiedenen verfügbaren Sicherheitskomponenten für Aruba EdgeConnect SD-Branch.

Dank seiner fortschrittlichen KI-basierten Identifizierungsfunktionen, dynamischer Segmentierung mit Zero Trust, IDS/IPS, einem einheitlichen SASE und der engen Integration mit zahlreichen externen Cloud-Sicherheitsanbietern sowie der Fähigkeit, Vorfälle im Netzwerk zu überwachen und an SIEM-Lösungen wie Splunk zu streamen, ermöglicht HPE Aruba Networking Unternehmen die Einhaltung umfangreicher Rahmenbedingungen und regulatorischer Standards, wie des NIST CSF Framework, HIPAA und PCI DSS.

Tabelle 2. Verfügbare Sicherheitskomponenten für Aruba EdgeConnect SD-Branch

Sicherheitskomponente	Details
Client Insights	Verwendet Netzwerk- und Client-Telemetrie mit maschinellem Lernen, um alle kabelgebundenen und WLAN-verbundenen Benutzer- und IoT-Endpunkte für die Zuweisung und Durchsetzung von Richtlinien genau zu identifizieren und zu klassifizieren. Überwacht auch das Verhalten von Verkehrsströmen für zusätzliche Sicherheit.
CloudAuth	Ermöglicht das reibungslose Onboarding von Endbenutzern und Client-Geräten entweder durch eine MAC-adressenbasierte Authentifizierung oder durch die Integration mit gängigen Cloud-Identitätsspeichern wie Google Workspace oder Azure Active Directory.
ClearPass Policy Manager	Bietet rollen- und gerätebasierte Netzwerkzugriffskontrolle für IoT, BYOD und Geräte im Unternehmen ebenso wie für Mitarbeitende, Auftragnehmer und Gäste in jeglichen Multivendor-Infrastrukturen, ob kabelgebunden, Wireless oder VPN.
Firewall zur Durchsetzung von Richtlinien	Die rollenbasierte Policy Enforcement Firewall der nächsten Generation für Benutzer, Geräte und Anwendungen verfügt über eine automatisierte dynamische Segmentierungsfunktion für den sicheren kabellosen oder kabelgebundenen Netzwerkzugriff.
Central NetConductor	Konfiguriert automatisch die LAN-, WLAN- und WAN-Infrastruktur im großen Maßstab, um eine optimale Netzwerkleistung zu erzielen und gleichzeitig granulare Sicherheitsrichtlinien für die Zugriffssteuerung durchzusetzen.

HPE Aruba Networking Sicherheitspartner

Um erweiterte Sicherheitsleistungen bereitzustellen, integriert EdgeConnect SD-Branch die Technologiekomponenten zahlreicher Sicherheitspartner, unter anderem Qosmos, Webroot und Proofpoint.

ENEA Qosmos	Mit den integrierten DPI-basierten Informationen zum Datenverkehr von Qosmos lassen sich knapp 3500 Anwendungen erkennen.
WEBROOT®	Die Technologie für maschinelles Lernen von WebRoot klassifiziert Inhalte, Reputation und Standortinformationen für Milliarden von URLs.
proofpoint.	Proofpoint Threat Intelligence bietet Informationen zu schädlichen Aktivitäten und gewährleistet, dass Unternehmen die Bedrohungslandschaft im Blick behalten. Die Daten umfassen über 65.000 Regeln, untergliedert in 50 Kategorien.

Fazit

Aufgrund des zunehmenden Tempos der digitalen Transformation müssen Unternehmen jetzt ihre Netzwerkarchitektur modernisieren, um die Umstellung von Anwendungen auf die Cloud, hybrides Arbeiten und den zunehmenden Bedarf an Bandbreite zu unterstützen. Da sich der Sicherheitsperimeter allmählich auflöst und Cybersicherheitsrisiken steigen, müssen Unternehmen ihre Netzwerk- und Sicherheitsfunktionen in Filialen überholen.

EdgeConnect SD-Branch bietet eine integrierte Lösung, die SD-WAN, Wireless und kabelgebundene Konnektivität mit fortschrittlichen, über die Cloud bereitgestellten Sicherheitsfunktionen kombiniert. Es bietet zahlreiche Mechanismen zum Schutz des verteilten Unternehmens. Dazu gehören:

- Einheitlicher SASE durch Kombination von EdgeConnect SD-Branch mit HPE Aruba Networking SSE
- Automatisierte Orchestrierung auf externen SSE-Anbietern wie Zscaler
- Anwendungskonsistente, statusabhängige Firewall mit Deep Packet Inspection und Angriffserkennung und prävention (Intrusion Detection and Prevention – IDS/IPS)
- Protokollierung von Bedrohungsereignissen, die zur Verbesserung des Störungsmanagements an externe SIEM-Lösungen gestreamt werden können
- Rollenbasierte dynamische Segmentierung, die sicherstellt, dass Benutzer- und IoT-Geräte selbst in komplexen verteilten Umgebungen ihre Ziele entsprechend ihrer Rolle erreichen
- Klassifizierung von Webinhalten, IP-Reputation und Geolocation-Filter
- Datenverschlüsselung über die gesamte SD-WAN-Fabric
- Ausgereifte Plattform mit TPM-Schutz (Trusted Platform Module)

EdgeConnect SD-Branch ist eine zentrale Komponente der Edge Services Platform (ESP) von HPE Aruba Networking. Damit können Unternehmen die digitale Geschäftstransformation durch automatisiertes Netzwerkmanagement, Edge-to-Cloud-Sicherheit und prädiktive KI-basierte Informationen beschleunigen. Es bietet einen einheitlichen Ansatz für das zentrale Management aller Sicherheits- und Netzwerkaspekte mit Wireless-, LAN- und WAN-Konnektivität sowie Network-as-a-Service (NaaS) und gängigen Zero-Trust- und SASE-Sicherheitsframeworks für das gesamte Portfolio. HPE Aruba Networking erweitert AIOps-Funktionen automatisch und überwacht kontinuierlich die Netzwerk- und Anwendungsleistung sowie die Durchsetzung von Sicherheitsrichtlinien. Und bei Beeinträchtigungen oder potenziellen Bedrohungen gewährleistet es eine automatisierte Fehlerbehebung.

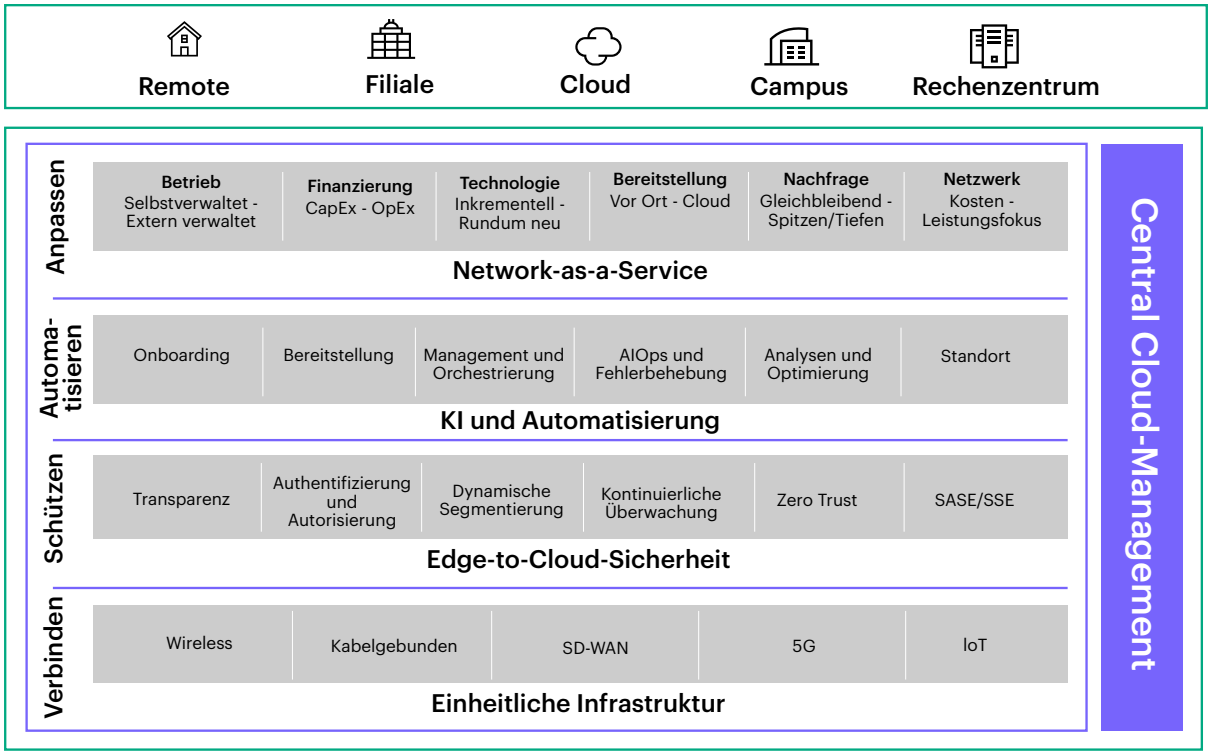


Abbildung 15. Die vier Ebenen der Edge Services Platform von HPE Aruba Networking.



Ressourcen

Die folgenden Ressourcen stehen für Hintergrundinformationen zur Verfügung:

- Einheitliche Richtlinie für das verteilte Unternehmen: Rollenbasierte Richtlinien und Sicherheit im gesamten LAN und WAN
- Technische Übersicht: Firewall zur Durchsetzung von Richtlinien: Funktionen der statusabhängigen Firewall für das Gateway
- Seite zur Edge-to-Cloud-Sicherheit: Das integrierte Framework von HPE Aruba Networking für Transparenz, Kontrolle und KI-basierte Einblicke
- Seite zu Zero Trust und SASE: Die integrierte Zero-Trust- und SASE-Sicherheit in HPE Aruba Networking gewährleistet, dass überall dieselben Zugriffskontrollen angewandt werden
- HPE Aruba Networking SD-WAN Homepage: Funktionen und Vorteile der SD-WAN-Lösung von HPE Aruba Networking
- EdgeConnect SD-Branch Homepage: Funktionen und Vorteile der EdgeConnect SD-Branch Lösung
- Datenblatt: EdgeConnect SD-Branch: Beinhaltet Bestellinformationen für Aruba Virtual Gateways
- Lösungsübersicht für dynamische Segmentierung: Identitätsbasierte Zugriffssteuerung auf globaler Ebene
- Lösungsübersicht für NetConductor: Automatisierung der Konfiguration, Definition und Durchsetzung von Richtlinien auf globaler Ebene

HPE.com besuchen

Chat mit Vertrieb

© Copyright 2025 Hewlett Packard Enterprise Development LP. Die hier enthaltenen Informationen können jederzeit ohne vorherige Ankündigung geändert werden. Die einzigen Garantien für Produkte und Services von Hewlett Packard Enterprise sind in den ausdrücklichen Garantieerklärungen enthalten, die diesen Produkten und Services beiliegen. Aus dem vorliegenden Dokument sind keine weiterreichenden Garantieansprüche abzuleiten. Hewlett Packard Enterprise haftet nicht für technische oder redaktionelle Fehler oder Auslassungen in diesem Dokument.

Alle genannten Marken von Dritten sind Eigentum der jeweiligen Rechteinhaber.

a00093929DEE, Rev. 1

HEWLETT PACKARD ENTERPRISE

hpe.com