HPE aruba networking

Moderne Campus-Netzwerke auf Ihre Art

Bereiten Sie sich auf das Unerwartete vor – mit einem Ansatz, bei dem die Sicherheit im Vordergrund steht, und einem zentralen Punkt für Transparenz und Kontrolle

HPE GreenLake

Bereiten Sie sich auf das Unerwartete vor – mit einem Ansatz, bei dem die Sicherheit im Vordergrund steht, und einem zentralen Punkt für Transparenz und Kontrolle Ihres gesamten Edge-to-Cloud-Campusnetzwerks. In einer Zeit, in der die Auswirkungen von Netzwerken und Sicherheit immer enger miteinander verknüpft sind, müssen leistungsstarke und sichere Konnektivitätsoptionen überall ein stabiles Benutzererlebnis und Schutz für Ihr Unternehmen bieten.

Die wichtigsten Vorteile von sicherheitsorientierter, KI-basierter Vernetzung

- Schaffen Sie eine gemeinsame Grundlage für Netzwerk- und Sicherheitsteams mithilfe eines Security-First-Ansatzes, der Zero Trust, SASE und SSE integriert
- Einfachheit in großem Maßstab durch zentrale Transparenz und Kontrolle
- Vorrangige Konzentration auf die Erfahrung des Endnutzers mit Erkenntnissen und Tests auf Client-Seite
- Höhere IT-Effizienz durch
- KI-basierte Analysen und Automatisierungen
- Einheitliche Verwaltung von WLAN, Switches, VPN und WAN
- IoT-Konvergenz und Integrationen mit führenden Anbietern
- Einheitliche, rollenbasierte Richtlinien für Zero-Trust-Sicherheit
- Auswahl an Optionen für das lokale Cloud- und Vor-Ort-Management
- Flexible Verbrauchs- und Serviceoptionen

Die Anforderungen an heutige Unternehmensnetzwerke sind gewaltig. Die Verbreitung von KI in Unternehmen, hybrider Technologie am Arbeitsplatz sowie der Zustrom von IoT und Mobilgeräten hat die Komplexität erhöht, die ein Unternehmen pflegen und verwalten muss. Die vor über zehn Jahren entwickelten Netzwerkarchitekturen können einfach nicht mit den neuen Leistungs- und Verwaltungsanforderungen sowie den hohen Erwartungen einer zunehmend mobilen Belegschaft Schritt halten. Aufgrund der zunehmenden Häufigkeit von Cyberangriffen und strengerer gesetzlicher Vorschriften wird der Cybersicherheit und der Einhaltung von Vorschriften immer mehr Aufmerksamkeit geschenkt, was zu einer engeren Beziehung zwischen Netzwerk- und Sicherheitsfunktionen geführt hat.

Die Belastung der Unternehmen durch diese digitale Beschleunigung wird bei der Vernetzung von Campus-Standorten noch deutlicher:

1. Die Einführung von Cloud-Services hat die traditionelle lokale Konnektivität, die zur Bereitstellung von Unternehmensdiensten für Benutzer verwendet wird, gestört
2. Die Anforderungen an den hybriden Arbeitsplatz haben die Rolle des traditionellen Büros neu definiert, sodass die regelmäßige Anwesenheit entfällt und die relative Sicherheit der Außenkontrollen umgangen wird
3. Die Knappheit der IT-Ressourcen stellt eine Herausforderung für die Fähigkeit der IT-Abteilung dar, die Erfahrungen der Geschäftsbereiche und Endbenutzer wie in der Vergangenheit aufrechtzuerhalten.

Tolle Benutzererfahrungen sind entscheidend

Trotz der geringeren durchschnittlichen Auslastung in den letzten Jahren wird erwartet, dass die Campus-Netzwerke auf höchstem Leistungsniveau arbeiten, um die Rückkehr der Mitarbeiter ins Büro zu unterstützen. Laut einer kürzlich von Gallup durchgeführten Umfrage unter Mitarbeitern, die remote arbeiten können, arbeiten sieben von zehn in einer Mischform oder vollständig vor Ort. Es wird erwartet, dass der Rest der vollständig remote arbeitenden Mitarbeiter langfristig von drei von zehn auf zwei von zehn zurückgehen wird.[1]

Angesichts dieser Schwankungen in der Nutzung durch die Mitarbeiter, des beispiellosen Wachstums von Collaboration-Tools, OT und IoT sowie des prognostizierten minimalen Wachstums der IT-Ausgaben können veraltete Netzwerke schnell zu einem Engpass für Ihr Unternehmen werden.

[1] Returning to the Office: The Current, Preferred and Future State of Remote Work, Gallup

Damit sich die IT-Abteilung besser an den Prioritäten des Unternehmens orientieren, die Compliance einhalten und die Zufriedenheit der Benutzer aufrechterhalten kann, kann eine vollständige Zero-Trust-Lösung eingesetzt werden. Sie verbindet und schützt alle Benutzer, Gegenstände, Anwendungen und Daten in der gesamten Infrastruktur.

Sicherheitsorientiertes, KI-basiertes Networking für den Campus

Unternehmen, die ihr Netzwerk modernisieren möchten, können zur Bewältigung der folgenden Herausforderungen auf das folgende technische und Service-Framework zurückgreifen:

1. Einführung von Zero-Trust-Sicherheitsdiensten aus der Cloud durch SSE- und SASE-Technologie zur weiteren Reduzierung der Angriffsflächen und zur Sicherung der Nutzer-Anwendungs-Erfahrung.
2. Cloud-native Netzwerkarchitektur, die für Unternehmens-KI, IoT und andere hochskalierbare Hochleistungsanforderungen bereit ist.
3. Leistungsstarke Konnektivitätslösungen, die die Produktivität der Mitarbeiter und hybriden Arbeitsplätze maximieren.
4. IT-Effizienz durch eine moderne Benutzeroberfläche, AIOps und Funktionen zur automatisierten Netzwerkverwaltung.
5. Optionen für ein agiles Network-as-a-Service, die auf Ihre IT-Prioritäten zugeschnitten sind.

Die Netzwerkarchitektur ist optimal auf die Umsetzung Ihrer Sicherheitsprioritäten abgestimmt und besteht aus unterschiedlichen Ebenen, die von einem einzigen Punkt für Transparenz und Kontrolle koordiniert werden.

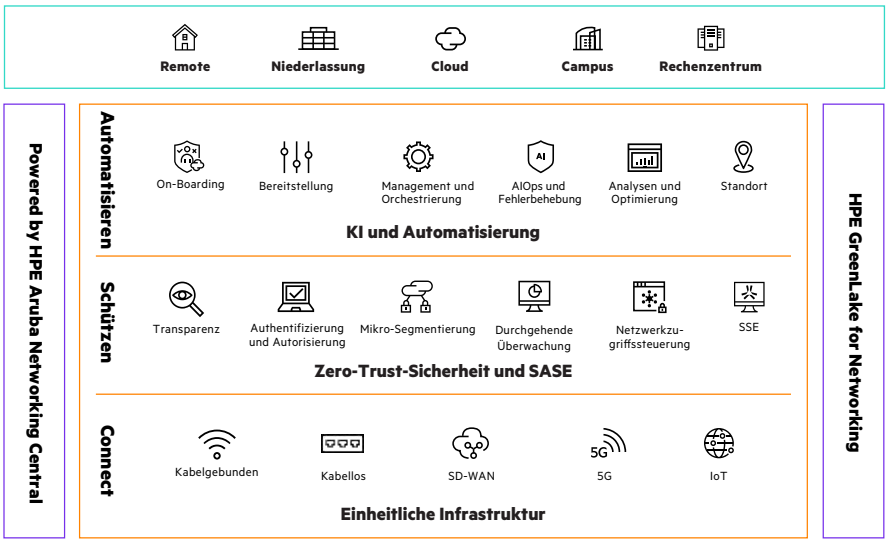

Abbildung 1. Diagramm der sicherheitsorientierten, KI-basierten Netzwerkarchitektur.

1. HPE Aruba Networking Central, ein einziger Punkt für Transparenz und Kontrolle: Central ist eine skalierbare, Cloud-native, Microservices-basierte Plattform, die als Cloud- oder On-Premises-Option verfügbar ist. Central wurde für große und kleine Unternehmen entwickelt und bietet KI-basierte Einblicke, Automatisierung, Sicherheit und Verwaltung für jeden Campus, jede Zweigstelle und jeden hybriden Arbeitsort.

Central integriert außerdem User Experience Insight, dient als Vermittler für IoT-Anwendungen und ermöglicht agentenlose SSE/SASE-Overlays für das Netzwerk von HPE Aruba Networking SSE und ausgewählten Drittanbietern.

Wichtigste Merkmale

- Lifecycle Management von WLAN-, Switching-, SD-WAN-, 5G- und VPN-Infrastruktur
- HPE Aruba Networking Central NetConductor zur Konfigurationsautomatisierung, Richtliniendefinition, Segmentierung und Durchsetzung
- KI-basierte Einblicke, Diagnosen und Abhilfemaßnahmen mithilfe von KI- und maschinellen Lerntools

2. Connect Layer, einheitliche Infrastruktur: Zur Unterstützung der Anforderungen eines hybriden Arbeitsplatzes werden Wireless Access Points (APs) und Netzwerk-Switches von der Zugriffsebene bis zum Campus-Kern eingesetzt, um hohe Leistung und Ausfallsicherheit zu gewährleisten. SD-WAN- und VPN-Gateways bieten zuverlässigen, sicheren Remote-Zugriff und Routing für Cloud- und lokale Workloads. Der kabellose Datenverkehr kann in den meisten allgemeinen oder dezentralen Unternehmensanwendungen lokal überbrückt werden. In größeren Unternehmen kann er über Gateways oder Controller getunnelt werden, um beispielsweise hochmobile Benutzer und Geräte zu unterstützen, die sich in einem mehrstöckigen Bürokomplex bewegen.

Wenn die Anforderungen des Unternehmens über die Unternehmensgrenzen hinausgehen, kann dieselbe physische Infrastruktur in Zweigstellen, kleinen Standorten, zu Hause oder an temporären Standorten bereitgestellt und mit SASE-, SSE- oder VPN-Optionen gesichert werden. Für den Einsatz mobiler Geräte innerhalb und außerhalb des Campus kann auch private 5G-Technologie implementiert werden.

Wichtigste Merkmale

- Wi-Fi-7-, Wi-Fi-6- und -6E-Access Points mit integrierten Bluetooth- und Zigbee-Funkgeräten und USB-Schnittstelle zum Anschluss von IoT-Geräten
- Leistungsstarke, skalierbare Netzwerk-Switches mit integrierten Analysefunktionen, Multi-Gigabit-Ethernet und leistungsstarken PoE-Fähigkeiten
- Private 5G/4G-Funktionen bieten ein unternehmensweites Erlebnis, indem sie die Unternehmenstransparenz, die Sicherheit und die Verwaltung von Assets über Mobilfunknetze hinweg erweitern

Vorteile von Zero Trust

- Begrenzung der Sicherheitsrisiken im Zusammenhang mit anfälligen IoT-Geräten
- Verringerung des Risikos fortgeschrittener Bedrohungen, die die Perimetersicherheit umgehen
- Begrenzung des Schadens, der durch seitliche Bewegungen von Angreifern und infizierten Geräten entsteht
- Verfolgung eines ganzheitlichen Sicherheitsansatzes, unabhängig davon, wer oder was die Verbindung herstellt und woher sie kommt
- Anwendung bewährter Verfahren wie der Mikrosegmentierung für einen „Least-Access"-Ansatz

Erfahren Sie mehr über Zero Trust.

- Ständige Konnektivität mit Live-Upgrades, Gateway-Clustering und Switch-Stacking
- SD-WAN und Routing (OSPF, BGP, Policy-basiertes Routing, Dynamic Path Steering)
- WLAN-, Bridge-, Tunnel- und Mixed-Mode-Bereitstellungsoptionen
- IPv6 für Netzwerke mit höherer Dichte und Bedarf an einem großem Adressbereich

3. Protect Layer, Edge-to-Cloud-Sicherheit: Zum Schutz Ihres Netzwerks und Ihrer Ressourcen wird die Richtlinienverwaltung und Orchestrierung als Overlay über den Connect Layer implementiert. Dadurch besteht die Möglichkeit, zentral erstellte Richtlinien und Verkehrssegmentierungsfunktionen über WLAN, LAN und WAN hinweg zu nutzen, um die Durchsetzung unabhängig vom Standort der Benutzer zu automatisieren. Die Durchsetzungsprinzipien folgen einem Zero-Trust-Modell, das mit SASE- und SSE-Lösungen vereinheitlicht ist, und können innerhalb eines Gateway-Clusters, an einem Zugangspunkt oder verteilt per Switch-Fabric für eine einfache und effiziente Kontrolle zentralisiert werden.

Wichtigste Merkmale

- Schutz für Benutzer-zu-Anwendung-Erfahrungen mit SASE- oder SSE-Technologie (HPE Aruba Networking SSE und EdgeConnect SD-WAN)
- Dynamische Segmentierung oder zentral definierte EVPN-VXLAN-basierte Segmentierung
- Herstellerübergreifend für kabelgebundenes, kabelloses und WAN
- KI-basiertes Endpunkt-/Client-Profiling und Onboarding
- Rollenbasierte Netzwerkzugangssicherheit
- Als Cyber Catalyst ausgewiesene Firewalls der nächsten Generation

4. Automation Layer, KI und Automatisierung: HPE Aruba Networking Central kann zur Verbesserung der Netzwerkleistung, des Zustands und der IT-Effizienz eine Cloud-native Microservices-basierte Plattform und einen datenschutzkonformen Data Lake nutzen, um KI-basierte Netzwerk- und Sicherheitserkenntnisse zu liefern, die dabei helfen, Probleme zu lösen oder zu umgehen. Diese Funktionen werden über Ihr Cloud-verwaltetes Netzwerk von HPE Aruba Networking bereitgestellt und dienen der Konsolidierung des Infrastrukturbedarfs vor Ort sowie der einfacheren Einführung neuer Services, die auch die Nachhaltigkeit durch weniger Wartungsbesuche verbessern. In Verbindung mit dem HPE Sustainability Dashboard bieten die Netzwerke auch Einblicke und Verständnis für Kohlenstoffemissionen und andere Umweltdaten – basierend auf der Validierung durch Dritte.

Wichtigste Merkmale

- Künstliche Intelligenz für IT-Abläufe (AIOps) und maschinelles Lernen
- Automatisiertes On-Boarding, Bereitstellen, Orchestrieren, Analysieren, Verfolgen und Verwalten von Standorten
- Standortdienste und Erweiterbarkeit von IoT und OT
- Überwachung der Benutzererfahrung und synthetische Clienttests mit HPE Aruba Networking UXI

5. Adapt Layer, agiles NaaS: Durch einen flexiblen und nachhaltigen „Services-First"-Ansatz kann der Zweck der Vernetzung von der Bereitstellung technischer Funktionen auf die Erzielung von Geschäftsergebnissen verlagert werden. Die Netzwerknutzung von Hardware, Software und Services ist vollständig an die geschäftlichen (z. B. CAPEX vs. OPEX) und technischen Anforderungen (z. B. On-Premises vs. Cloud) des jeweiligen Unternehmens anpassbar und ermöglicht die Nutzung der neuesten Lösungen und Services von HPE und HPE Aruba Networking.

Wichtigste Merkmale

- Software-as-a-Service
- Netzwerk-as-a-Service
- Professional und Managed Services
- Finanzierung und Übertragung von Anlagen zur Entlastung des End-of-Life-Managements
- Zahlungsaufschub und -erleichterungen
- Phasenweise Implementierung
- Gebraucht und Miete

Tabelle 1. Schlüsselprodukte (nicht exklusiv)

Produkte	Beschreibung
HPE Aruba Networking Central (Optionen für Cloud, On-Premises oder Managed Service Provider)	**Cloud-Natives Netzwerk-Management (Central)** Central ist eine Software-as-a-Service-Lösung, die auf der HPE GreenLake Edge-to-Cloud-Plattform gehostet wird, wobei alle Aktualisierungen des Managementsystems und die Wartung in der Cloud erfolgen. Central kann auch auf Server-Appliances in einem privaten Rechenzentrum bereitgestellt werden. Weitere Informationen.
Access Points für den Innen-/ Außenbereich/ Remote-Zugriff	**Wireless Access Points (APs)** Bieten eine sichere kabellose Multi-Gigabit-Konnektivität für WLAN-Geräte und unterstützen BLE- und Zigbee-Protokolle. Sie wurden speziell für verschiedene Einsatzszenarien entwickelt – für Innen- und Außenbereiche sowie gefährliche Standorte. APs verfügen außerdem über zahlreiche Plattformfunktionen wie Bluetooth und Zigbee, um eine integrierte Netzwerk-Overlay-Konnektivität für IoT-Vorgänge bereitzustellen. Wi-Fi-7- und Wi-Fi-6E-APs fügen GPS/GNSS-Empfänger hinzu, um den Aufbau einer ortsfesten Infrastruktur zu unterstützen. Weitere Informationen.
Zugriffs-/ Aggregations-/ Core-Switches	**Network Access/Aggregation/Core Switches (Switches)** Die Netzwerk-Switches bieten skalierbare, immer verfügbare Hochleistung mit integrierter Analyse und werden auf den Zugangs-, Aggregations- und Kernebenen des Netzwerks eingesetzt, um den Datenverkehr von Clients, Anwendungen und Diensten zu bündeln und als Rückgrat Ihres Unternehmensnetzwerks zu dienen. Weitere Informationen.
Gateways/ Mobility Controller	**Controllers/Gateways (Gateways)** Die Gateways bieten leistungsstarke Verkehrs- und Datensegmentierungs-, Roaming-, VPN- und SD-WAN-Services und werden von Central verwaltet und vor Ort oder in der Cloud bereitgestellt. Sie wurden für Unternehmen entwickelt, die erweiterte Sicherheits-, Routing- und Leistungsfunktionen in Unternehmensumgebungen benötigen. Weitere Informationen.
Security Service Edge (SSE)	**HPE Aruba Networking SSE (Axis) und EdgeConnect SD-WAN** Erhalten Sie sicheren Zugriff mit intelligentem Routing zu jeder Unternehmensressource und kontinuierlicher Überwachung der Erfahrungen, um einen Zero-Trust-Ansatz für jedes Zugriffsereignis zu ermöglichen. Die Integration mit EdgeConnect SD-WAN bietet eine einheitliche SASE-Plattform zur Beschleunigung der Zusammenarbeit zwischen Netzwerk- und Sicherheitsteams. Weitere Informationen.
ClearPass Policy Manager	**Richtlinienmanagement/Profiling/NAC (Central und ClearPass)** Client Insights wird mit HPE Aruba Networking Central geliefert und bietet KI-basierte Client-Transparenz, während Cloud Auth eine Cloud-basierte NAC für Authentifizierung, Autorisierung und Durchsetzung bietet. ClearPass wird vor Ort eingesetzt und ermöglicht eine einheitliche Richtlinienverwaltung für Campus-, Zweigstellen- und Remotenetzwerke verschiedener Anbieter und wird als Hardware oder virtuelle Appliance geliefert. Weitere Informationen.
User Experience Insight	**Benutzer- und Anwendungstests (User Experience Insight)** Simulieren Sie reale Benutzererfahrungen, testen Sie beliebige Anwendungen in beliebigen Netzwerken, und identifizieren Sie mit nur einem Klick die Grundursachen mit dem Cloud-basierten HPE Aruba Networking User Experience Insight. Client-Sensoren werden überall auf Ihrem Gelände eingesetzt, um Ihren Netzwerkadministratoren Echtzeit-Einblicke zu bieten. Weitere Informationen.
HPE Aruba Networking Standortdienste	**Bluetooth-basierte Standortdienste** Die Standortdienste von HPE Aruba Networking eignen sich ideal für den Einzelhandel, das Gesundheitswesen oder andere öffentliche Umgebungen, um nahtlos personalisierte Kundenerlebnisse mit benutzerdefinierten mobilen Apps, Wegbeschreibungen und gezielten Kampagnen zu schaffen. HPE Aruba Networking APs können als Grundlage für die Bereitstellung präziser Standortdienste für den Innenbereich verwendet werden. Weitere Informationen.

Tabelle 2. Schlüsselleistungen (nicht exklusiv)

Produkte	Beschreibung
HPE GreenLake for Networking	**HPE GreenLake for Networking** Konzentrieren Sie sich stärker auf die Erzielung von Geschäftsergebnissen und stimmen Sie Ihre Netzwerkmodernisierungsstrategie mit den Finanzdaten Ihres Unternehmens ab, indem Sie Edge-Konnektivität as-a-Service nutzen. Angesichts kürzerer Planungszyklen und Bedenken hinsichtlich der Netzwerkverwaltung für Cloud- oder Edge-Anwendungen ermöglicht NaaS einen schnelleren Zugriff auf neue Technologien, betriebliche Effizienz und eine vollständige Kontrolle des Änderungsmanagements. Weitere Informationen.
HPE Financial Services	**HPE Financial Services** Mit einem vielseitigen Portfolio an Finanzlösungen kann HPE Financial Services Sie dabei unterstützen, Kapital aus vorhandenen Infrastrukturen freizusetzen, Zahlungen aufzuschieben, gebrauchte Geräte bereitzustellen – und vieles mehr –, um Ihr Unternehmen auf langfristigen Erfolg auszurichten. Weitere Informationen.

Zusammenfassung und Ressourcen

Mit der Weiterentwicklung der Geschäftswelt werden bei der Vernetzung mit der Sicherheit die Netzwerk- und Sicherheitsteams zusammengeführt

Wechseln Sie zu HPE Aruba Networking und nutzen Sie modernste Campus-Netzwerkfunktionen, um die Verwaltung von Edge-to-Cloud-Räumlichkeiten zu vereinfachen, sich wiederholende Aufgaben zu automatisieren und kritische Korrekturen durchzuführen, die das Unternehmen und die Endbenutzererfahrung optimieren. Geben Sie Ihrem Team, was es braucht, um erfolgreich die richtigen Netzwerkbereitstellungs- und -nutzungsmodelle zu liefern und so Ihre Sicherheitsziele zu erreichen.

Die Einführung sicherheitsorientierter, KI-basierter Netzwerke bietet viele konkrete Vorteile. Die Modernisierung des Netzwerks sollte jedoch auf der Grundlage Ihrer Unternehmensstrategie, Ihres Zeitplans, Ihrer Anforderungen und Ihrer Prioritäten erfolgen. Wenn Sie ein Netzwerkupgrade oder eine Cloud-verwaltete Netzwerkmigration planen, bieten die folgenden Ressourcen zusätzliche Einblicke und Empfehlungen:

- HPE Aruba Networking: Es ist Zeit, etwas zu unternehmen
- Modernisierung ohne Kompromisse: Warum Sie HPE Aruba Networking Central zu Instant AP Bereitstellungen hinzufügen sollten
- Modernisierung ohne Kompromisse: Warum von AirWave zu HPE Aruba Networking Central wechseln?

Entscheiden Sie sich für das richtige Produkt. Kontaktieren Sie unsere Presales-Experten.

Chat mit Vertrieb

Anrufen

Besuchen Sie **ArubaNetworks.com**

Updates abrufen

Hewlett Packard Enterprise

SO_Modern-Campus-Networking_RB_100224 a00129689DEE