aruba
a Hewlett Packard Enterprise company

Proudly Presented By
IOK
IMMER DIE RICHTIGE IT-LÖSUNG.

ÜBERBLICK ÜBER DIE LÖSUNG

Edge-To-Cloud-Sicherheit von Aruba

Ermöglicht sichere Edge-Nutzung und WAN-Transformation

DAS NEUE NETZWERK: EDGE- UND CLOUD-ERWEITERUNG

Das Wachstum am Edge in Form von Remote-Mitarbeitern und einer großen Anzahl neuer IoT-Geräte hat zu einzigartigen Herausforderungen in Bezug auf Onboarding, Transparenz und Sicherheit geführt. Gleichzeitig hat die fortschreitende Migration von Anwendungen in die Cloud die Art und Weise verändert, wie wir an die Netzwerkplanung und die damit verbundenen Sicherheitsanforderungen herangehen. Schließlich wurden die alten Netzwerke nicht für eine Cloud-first-Welt konzipiert. Während die Komplexität des Netzwerks und die Bedrohungen weiter zunehmen, benötigen Unternehmen einen ganzheitlichen, durchgängigen Ansatz, um sicherzustellen, dass Sicherheit und Compliance am Edge, wo sich neue Geräte, Benutzer und Zweigstellen befinden, bis hin zur Cloud, wo wichtige Anwendungen und kritische Daten ein Höchstmaß an Schutz sowie Leistung und Verfügbarkeit erfordern, berücksichtigt werden.

ARUBA ESP (EDGE SERVICES PLATFORM) MIT EDGE-TO-CLOUD-SICHERHEIT

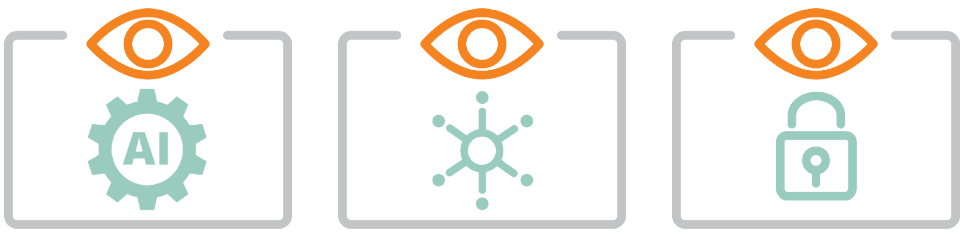
Aruba ESP ist die einzige Architektur, die es Unternehmen ermöglicht, eine ganzheitliche Netzwerkarchitektur zu implementieren, die aus WLAN, Switching, SD-WAN und AIOps besteht und bei der die Sicherheit von Anfang an integriert ist. Mit der Erweiterung um die Aruba EdgeConnect SD-WAN-Plattform kann Aruba seinen Kunden nun helfen, die Vorteile der branchenführenden SD-WAN-Funktionen und gleichzeitig die entscheidenden Zero Trust- und SASE-Sicherheitsgrundlagen zu nutzen.

SICHERHEIT AM EDGE: UMFASSENDE TRANSPARENZ UND ZERO TRUST SEGMENTIERUNG

Angesichts der zunehmenden Verbreitung des IoT, einhergehend mit einer dramatischen Zunahme von Remote-Benutzern, ist die vollständige Transparenz aller Benutzer und Geräte, die sich mit dem Netzwerk verbinden, zu einer immer größeren Herausforderung geworden.Ohne Transparenz sind wichtige Sicherheitskontrollen, die zur Absicherung des Edge erforderlich sind, nur schwer umzusetzen. Automatisierung, KI-basiertes maschinelles Lernen und die Fähigkeit, Gerätetypen schnell zu identifizieren, sind dafür entscheidend. Aruba ClearPass Device Insight nutzt eine Kombination aus aktiven und passiven Erkennungs- und Profilierungstechniken, um das gesamte Spektrum an Geräten zu erkennen, die mit dem Netzwerk verbunden sind oder versuchen, sich mit diesem zu verbinden. Dazu gehören gängige benutzerbasierte Geräte wie Laptops und Tablets. Der Unterschied zu herkömmlichen Tools liegt in der Fähigkeit, die immer vielfältiger werdenden IoT-Geräte zu erkennen, die in modernen Netzwerken immer häufiger anzutreffen sind.

ARUBA ESP (EDGE SERVICES PLATFORM)

Die branchenweit erste Plattform mit einem AI*-gestützten „sechsten Sinn“ für Automatisierung und Schutz



AIOps
AI*-Insights | Networks Analytics Engine
User Experience Insight | Device Insight

Einheitliche Infrastruktur
Wi-Fi | Switching | SD-WAN
Cloud | 5G | Gemeinsamer Data Lake

Edge-to-Cloud Security
Dynamic Segmentation | Zero Trust Policy
Enforcement ClearPass | Orchestrierung der
Cloud-Sicherheit

Abbildung 1: Edge-to-Cloud-Sicherheit ist eine tragende Säule von Aruba ESP

* Die wissenschaftliche Disziplin Artificial Intelligence (AI) / Künstliche Intelligenz (KI) wurde von Marvin Minsky im Jahr 1956 erschaffen. Ursprünglich war damit die Nachbildung der menschlichen Intelligenz gemeint.

Aruba ClearPass Policy Manager ermöglicht die Erstellung von rollenbasierten Zugriffsrichtlinien, die es IT- und Sicherheitsteams ermöglichen, diese Best Practices mit einer einzigen Rolle und den damit verbundenen Zugriffsrechten zu operationalisieren, die überall im Netzwerk angewendet werden können – in der drahtgebundenen oder drahtlosen Infrastruktur, in Zweigstellen oder auf dem Campus. Nach der Profilierung wird den Geräten automatisch die richtige Zugriffskontrollrichtlinie zugewiesen, und sie werden mit Hilfe der dynamischen Segmentierungsfunktionen von Aruba gegenüber anderen Geräten segmentiert. Die Durchsetzung erfolgt über die Policy Enforcement Firewall (PEF) von Aruba, eine vollständige Anwendungsfirewall, diein die Aruba-Netzwerkinfrastruktur eingebettet ist. Darüber hinaus teilt ClearPass jetzt identitätsbasierte Telemetrie mit Aruba EdgeConnect SD-WAN-Appliances, um eine noch differenziertere Segmentierung zu ermöglichen.

EINHEITLICHE SICHERHEIT UND SCHUTZ VOR BEDROHUNGEN IN ZWEIGSTELLEN

Die Bedrohungsabwehrfunktionen von Aruba schützen vor einer Vielzahl von Bedrohungen, darunter Phishing, Denial-of-Service (DoS) und zunehmend verbreitete Ransomware-Angriffe. Unterstützte SD-WAN-Gateways von Aruba führen identitätsbasierte Intrusion Detection and Prevention (IDS/IPS) durch und arbeiten mit Aruba Central, ClearPass Policy Manager und der Policy Enforcement Firewall zusammen. Beim identitätsbasierten IDS/IPS wird eine signatur- und musterbasierte Verkehrsprüfung sowohl des LAN-Verkehrs der Zweigstelle (East-West) als auch des SD-WAN-Verkehrs (North-South) durchgeführt, der durch das Gateway fließt, um eingebettete Sicherheit für das Zweigstellennetzwerk zu bieten. Ein erweitertes Sicherheits-Dashboard innerhalb von Aruba Central bietet IT-Teams netzwerkweite Transparenz, mehrdimensionale Bedrohungsmetriken, Bedrohungsanalysedaten sowie Korrelations- und Incident-Management. Bedrohungsereignisse werden zur Behebung an SIEM-Systeme und ClearPass gesendet.

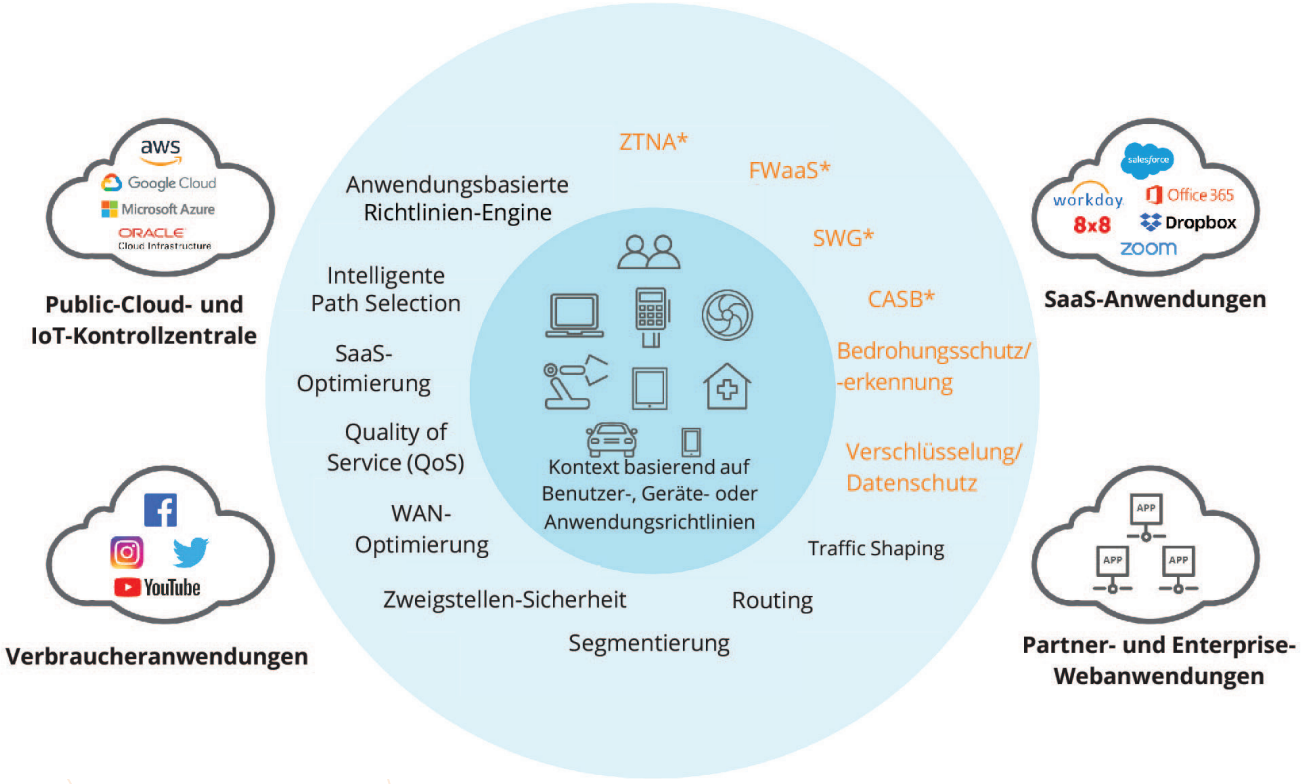


Abbildung 2: Ein sicherer Zugriffsservice wird benötigt, um die digitalen Transformationsinitiativen des Unternehmens zu unterstützen, d.h. die Cloud-first-Strategie und die Mobilitätsanforderungen der Mitarbeiter. In einer robusten SASE-Architektur müssen umfassende WAN-Funktionen mit umfassenden Netzwerksicherheitsfunktionen zusammenarbeiten, um die dynamischen Anforderungen digitaler Unternehmen an einen sicheren Zugriff für Benutzer, Endgeräte und Anwendungen zu unterstützen.

* ZTNA: Zero Trust Network Access
FWaaS: Firewall as a Service
SWG: Secure Web Gateway
CASB: Cloud Access Security Broker

ORCHESTRIERUNG DER CLOUD-SICHERHEIT UND SECURE ACCESS SERVICE EDGE (SASE)

Unternehmen migrieren weiterhin viele ihrer Anwendungen in die Cloud. Da ist es entscheidend, dass SD-WAN- und Sicherheitslösungen mit dem Wandel Schritt halten. Durch die Modernisierung der WAN- und Sicherheitsinfrastruktur können Kunden erhebliche Vorteile sowohl auf der Netzwerk- als auch auf der Sicherheitsseite erzielen. Die Aruba EdgeConnect-Lösung bietet marktführende SD-WAN-Funktionen in Kombination mit einer reibungslosen Orchestrierung mit marktführenden Cloud- Sicherheitsanbietern. Dadurch lässt sich der Aufwand für die Integration von Cloud-basierten Sicherheitsservices in die bestehende Netzwerk- und Sicherheitsinfrastruktur erheblich reduzieren. Durch die Ergänzung dieser Cloud- basierten Sicherheitsservices können Unternehmen die Sicherheit näher zu ihrer Cloud-gehosteten Infrastruktur bringen – wo sie auch hingehört.

ARUBA CENTRAL: BEDROHUNGSANALYSE FÜR DIE GESAMTE INFRASTRUKTUR

Aruba Central ist eine leistungsstarke Cloud-Netzwerklösung, die unübertroffene Einfachheit für moderne Netzwerke bietet. Als Verwaltungs- und Orchestrierungskonsole für Aruba ESP bietet Central einen zentralen Überblick über alle Aspekte von drahtgebundenen und drahtlosen LANs, WANs und VPNs auf dem Campus, in Zweigstellen und Remote-Standorten. Dazu gehört ein erweitertes Sicherheits-Dashboard mit IDS/IPS-Warnungen, Bedrohungsanalysedaten und Korrelation mit Incident- Management-Funktionen.