HPE aruba networking

Broschüre

Einfachere Einführung einer Zero-Trust-Sicherheit

Beschleunigen Sie die Umstellung zu Zero Trust mit einem Security-First KI-Netzwerk

Los geht's >

HPE GreenLake

Inhaltsverzeichnis

Ein Paradigmenwechsel

Innovationen sind für Unternehmen entscheidend. In der heutigen digital orientierten Welt sind ausgezeichnete Erfahrungen das wichtigste Element von Innovationen.

Unternehmen, die ausgezeichnete Erfahrungen bieten, können sich in einem überfüllten Markt hervorheben, Talente aus der ganzen Welt anziehen und bleiben trotz Unsicherheit, Veränderungen und Störungen am Laufen.

Die Konnektivität macht diese ausgezeichnete Erfahrungen möglich. Sie verbindet Menschen miteinander: Einzelhändler:innen mit Kundinnen und Kunden, Mediziner:innen mit Patientinnen und Patienten, Mitarbeiter:innen mit Anwendungen, Geräte mit der Cloud und Daten mit Algorithmen.

Die Konnektivität ist im Dauereinsatz. Sie ist unterbrechungsfrei verfügbar und immer – von jedem Standort – aus zugänglich.

Mit Konnektivität werden ein höheres Maß an Personalisierung, zufriedenstellende Benutzer- und Mitarbeitererlebnisse, Leistungsvorteile und letztendlich Wachstum möglich.

Sie kann die IT jedoch auch verkomplizieren.

Netzwerk- und Sicherheitsteams spielen eine zunehmend strategische Rolle, da Konnektivitäts- und Technologieinitiativen wie generative KI ganz oben auf der Liste der Prioritäten stehen. Gleichzeitig werden die Umgebungen, in denen die Netzwerk- und Sicherheitsteams arbeiten, zunehmend schwierig zu handhaben. Sicherheits-, Datenschutz-, Governance- und Compliance-Maßnahmen entwickeln sich ständig weiter und erfordern koordiniertere Bemühungen. Das macht es Teams, die schon jetzt mit weniger mehr erreichen müssen, umso schwerer.

Was ist Zero Trust?
Zero-Trust-Prinzipien verlangen, dass Benutzer:innen und Geräte ihre Vertrauenswürdigkeit nachweisen, um Zugriff auf die Ressourcen zu erhalten, die sie für ihre Arbeit oder das Ausführen ihrer Funktion benötigen. Dieses Konzept des Zugriffs nach dem Prinzip der geringsten Rechte ist grundlegend für die Sicherheitspraktiken von Zero Trust.

Für Zero-Trust-Sicherheit ist auch eine kontinuierliche Überwachung von Benutzer:innen und Geräten erforderlich. Die Vertrauenswürdigkeit wird kontinuierlich neu bewertet, und wenn sich Benutzer:innen oder Geräte auffällig oder in irgendeiner Weise nicht ihrer Rolle entsprechend verhalten, kann ihr Zugriff eingeschränkt oder entzogen werden. Diese begrenzte und dynamisch bewertete Kontrolle kann dazu beitragen, mögliche Angriffsflächen klein zu halten und Angriffe sogar zu verhindern.

Gute Gründe für Zero-Trust-Sicherheit
Ansätze für die Netzwerksicherheit, die primär auf den Schutz der Peripherie ausgerichtet sind, reichen heute – angesichts wachsender Einführung des IoT; Auswaschung der Grenzen von Unternehmen, da jetzt von überall gearbeitet wird; und zunehmend ausgefeilteren Bedrohungen, die „sichere“ Benutzer:innen und Geräte für bösartige Zwecke ausnutzen – nicht mehr aus.

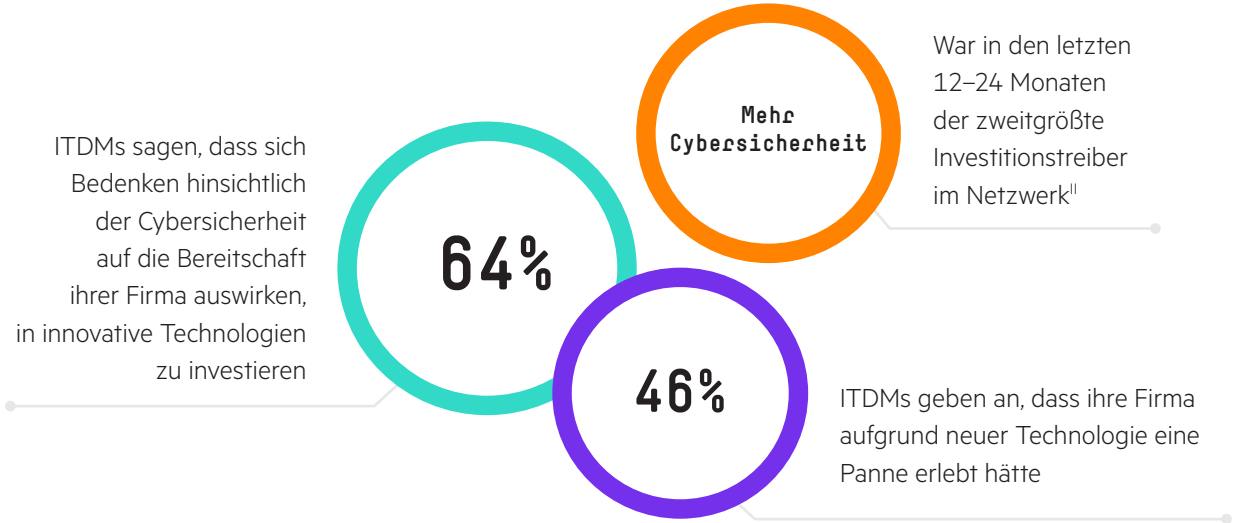
Zunehmender Bedarf an Zero Trust

Konnektivität ist der Schlüssel für Innovationen, und im Zentrum der Konnektivität steht das Netzwerk. Ob Sie im Büro arbeiten, in einem Geschäft einkaufen, sich von einem Café aus anmelden oder eine Überwachungskamera mit einer Cloud-Anwendung verbinden – das Netzwerk ist immer verfügbar.

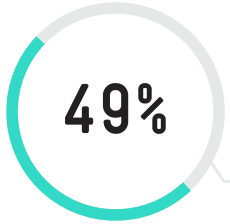
Was ist noch zu erwarten? Nicht erkannte Bedrohungen.

Diese Erwartung ist so tiefgreifend, dass daraus ein neues Modell der Sicherheitsarchitektur entstand: Zero Trust. Zero-Trust-Sicherheitsmodelle gehen davon aus, dass sich immer ein Angreifer in der Umgebung befindet. Demzufolge ist ein eigenes Netzwerk nicht sicherer als ein fremdes.[I]

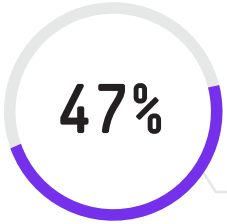
Wie bringen Unternehmen den Bedarf an hoher Leistung und unterbrechungsfreiem Zugriff auf ihr Netzwerk mit dem Bedarf an stabiler Sicherheit in Einklang?



Herausforderungen von Zero Trust



Der Organisationen haben noch keine Zero-Trust-Sicherheit implementiert



Bewerteten ihre Organisation als sehr oder äußerst effektiv bei der Reduzierung von Bedrohungen in der Angriffslandschaft

Der Organisationen, die als äußerst effektiv darin eingestuft werden, mit einer sich ständig verändernden Bedrohungslandschaft Schritt zu halten, haben – im Gegensatz zu den übrigen 50 % – Zero-Trust-Sicherheit eingeführt[III]

Obwohl die Akzeptanz von Zero Trust in den letzten Jahren zugenommen hat, stellt die Umsetzung für viele Unternehmen immer noch eine Herausforderung dar. Dafür gibt es zahlreiche Gründe.

1. **Ein Paradigma – kein Produkt**. Zero Trust ist kein einzelnes Produkt oder eine einzelne Lösung, die „von der Stange" erworben werden kann. Es handelt sich um eine Reihe von architektonischen Leitprinzipien, die immer wieder verfeinert und in der Infrastruktur und durch Festlegung von Richtlinien umgesetzt werden müssen. Das heißt, es ist keine einmalige Initiative. Eine ausgereifte Vision von Zero Trust zu entwickeln kann einige Zeit in Anspruch nehmen, da sich Sicherheitsdenkweisen ändern und Prozesse angepasst werden.

2. **Bereichsübergreifende Anforderungen.** Zero Trust erstreckt sich über die Technologiebereiche in einem Unternehmen und betrifft nicht nur Netzwerke, sondern auch Benutzer:innen, Geräte, Anwendungen und Workloads an Campus-Standorten, in Filialen, Rechenzentren, in der Cloud und darüber hinaus. Koordination, Kontrolle und Konsistenz sind kritisch, aber angesichts der verschiedenen Umgebungen schwer zu erreichen.
3. **Fragmentierte Leistungen.** Die Funktionen der Zugriffskontrolle, die Zero-Trust-Architekturen unterstützen, erstrecken sich in der Regel über mehrere Technologielösungen, die oftmals aus Einzelteilen zusammengeschustert werden. Mit der Zeit erhöht dieser Patchwork-Ansatz nicht nur die architektonische und betriebliche Komplexität, sondern setzt das Unternehmen auch Sicherheitslücken, Inkonsistenzen bei Richtlinien und deren Durchsetzung sowie potenziellen Cybersicherheitsrisiken durch unbeabsichtigte Lücken aus.[IV]
4. **Team-Zusammenarbeit.** Die Bereitstellung erfolgreicher Innovationen, die den Anforderungen der Zero-Trust-Sicherheit entsprechen, erfordert häufig, dass die Netzwerk- und Sicherheitsteams zusammen arbeiten, um gemeinsame Ziele zu verfolgen: erstklassige Erfahrungen bereitzustellen und dabei das Unternehmen vor immer häufiger auftretenden und raffinierteren Angriffen zu schützen. Uneinheitliche Tools und fehlende gemeinsame Kontrollen und Daten können zu isolierten Abläufen führen, die das Erreichen gemeinsamer Geschäftsresultate behindern.

Die neue Rolle des Netzwerks

Es ist wichtig, Innovationen mit Zero-Trust-Grundsätzen zu verbinden – und Innovationen basieren auf Konnektivität. Das bedeutet, dass das Netzwerk als Teil eines gesamten Zero-Trust-Sicherheitsökosystems nun eine wesentliche Rolle spielt.

Für IT-Führungskräfte ist es jetzt an der Zeit, über das Netzwerk als Zero-Trust-Sicherheitslösung nachzudenken.

Auch wenn keine einzelnen Anbieter oder Lösungen den kompletten Schutz bieten, den eine Organisation braucht, ist ein Netzwerk mit integrierter Zero-Trust-Sicherheit eine Grundlage, um die Implementierung von Sicherheitsanforderungen zu vereinfachen und die Sicherheit an kritischen Zugangspunkten zu steigern. In seiner Doppelrolle, dass es die Konnektivität möglich macht und die Cybersicherheit verteidigt, wird das Netzwerk ganz natürlich zu einem Ort der Zusammenarbeit und Kooperation zwischen Netzwerk- und Sicherheitsteams.

Ihre Netzwerkentscheidung ist wichtig für den Schutz des Unternehmens.

Ein einfacherer Weg zur Zero-Trust-Sicherheit

Security-First KI-Netzwerk

Beschleunigen Sie die Umstellung zu Zero Trust mit dem Security-First KI-Netzwerk von HPE Aruba Networking. So bietet das Security-First KI-Netzwerk von HPE Aruba Networking eine allgemeine Zero-Trust-, KI-Grundlage, die Netzwerk- und Sicherheitsteams nutzen können, um innovative Geschäftsergebnisse und sichere, besondere Erlebnisse zu schaffen, ohne die Cybersicherheit zu gefährden.

Ein Security-First KI-Netzwerk von HPE Aruba Networking erleichtert die Einführung von Zero-Trust-Sicherheit und unterstützt die Compliance mit Cybersicherheitsstandards und -vorschriften. Unternehmen erhalten damit die Möglichkeit, das Netzwerk als Sicherheitslösung zu nutzen. Das Netzwerk kann jetzt umfassendere Transparenz und Einblicke, ein zentralisiertes Richtlinienmanagement, Datensicherung, Bedrohungsabwehr und Zugriffssteuerung über eine einzige Plattform bereitstellen. Mit diesen integrierten Zero-Trust-Sicherheitsfunktionen wird das Netzwerk selbst zur wichtigen Verteidigungslinie, die sich in die Elemente des Sicherheitsökosystems integriert. Die Sicherheit nimmt zu, ohne dass zusätzliche Komplexität durch mehrere verschiedenartige Tools oder den kostspieligen und störenden Komplettaustausch der vorhandenen Infrastruktur entsteht.

KI-basierte Netzwerke vervielfachen auch die Personalkraft eines Unternehmens – ein entscheidender Faktor, da die rechtlichen Rahmenbedingungen weiter und die Talentlücken größer werden sowie Cyber-Bedrohungen zunehmen. Mit dem HPE Aruba Networking Security-First KI-Netzwerk können Teams von einer intelligenten Automatisierung profitieren, die den manuellen Aufwand reduziert, die Transparenz und Anomalienerkennung verbessert sowie die Überwachung und Diagnoseprogramme stärkt. All das stellt sicher, dass ein Unternehmen keinem unnötigen Risiko ausgesetzt ist.

Wie macht ein Security-First KI-Netzwerk die Einführung von Zero-Trust-Sicherheit einfacher?

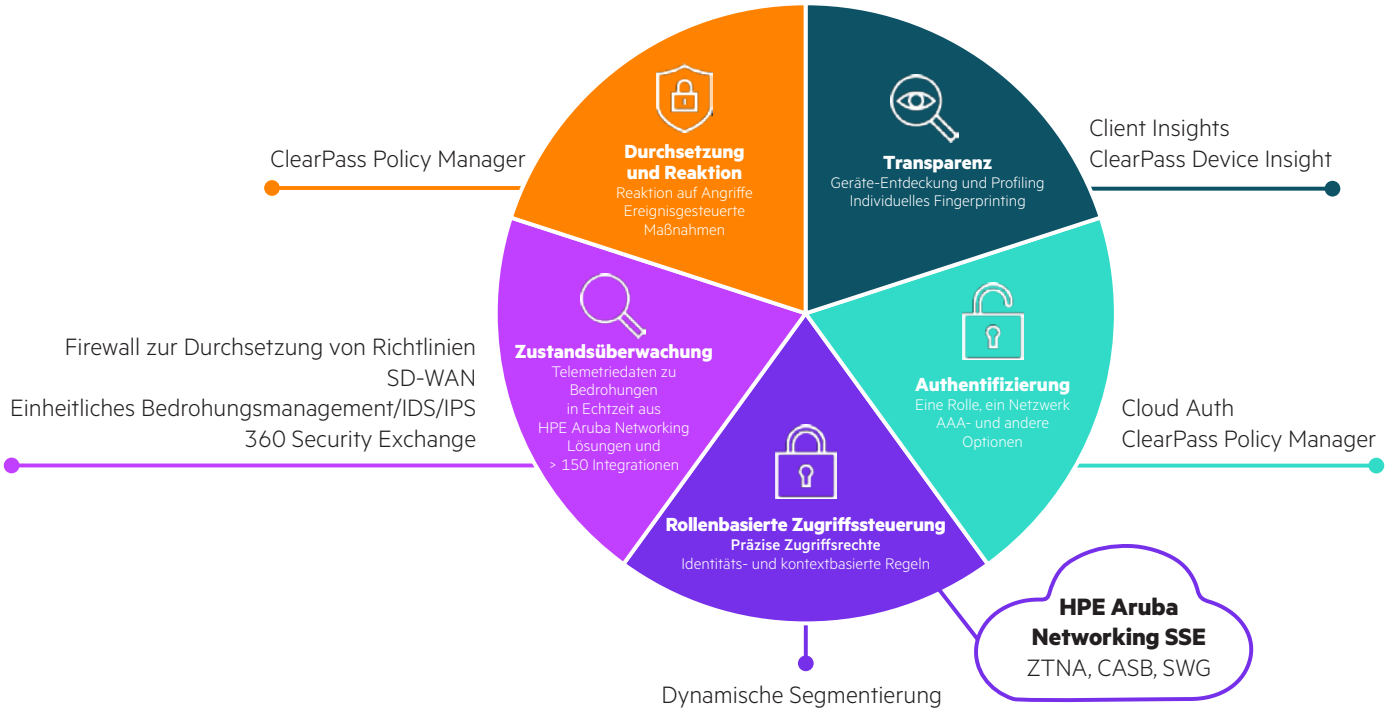
1. Liefert **umfassende Transparenz** für eine gemeinsame Erkenntnisquelle für Teams und Tools
2. Bietet **ein globales Richtlinienmanagement** für einfachere Definitionen und Anwendungen von Richtlinien
3. Stärkt **die Edge-to-Cloud-Umsetzung** für optimierte Leistung und konsistente Kontrolle
4. Ist **KI-gestützt** und verbessert dadurch die Effizienz und Sicherheit

Erwägen Sie die Einführung einer Zero-Trust-Sicherheit? Berücksichtigen Sie die Grundvoraussetzungen.

„Idealerweise sollten Sie einige Fragen zu jedem Benutzer oder Gerät in Ihrem Netzwerk beantworten können: Wer sind Sie? Welche Rechte sollten Sie in diesem Netzwerk haben? Und wie kann ich diese durch eine Richtlinienkontrolle durchsetzen?"

– Jon Green, Chief Technology Officer und Chief Security Officer, HPE Aruba Networking, Hewlett Packard Enterprise[v]

HPE Aruba Networking Zero-Trust-Sicherheitsfundament

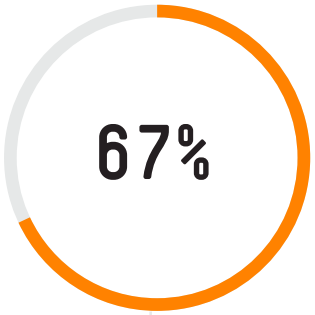


Im Gegensatz zu anderen Ansätzen, bei denen eine Reihe von unzusammenhängenden Sicherheitslösungen nachträglich in der Netzwerkinfrastruktur angelegt werden müssen, bietet das Security-First KI-Netzwerk von HPE Aruba Networking integrierte Zero-Trust-Lösungen, die als natürlicher Bestandteil einer Standard-Netzwerkbereitstellung geplant, konzipiert und betrieben werden. Die HPE Aruba Networking Lösungen lassen sich auch nahtlos in das übrige Sicherheitsökosystem integrieren, um auf Informationen aus der Sicherheitsumgebung zu reagieren, den Schutz zu steigern und den Betrieb zu vereinfachen.

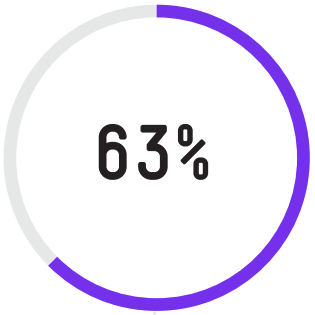
Umfassende Transparenz

Mit einer Datenquelle arbeiten

Die Zero-Trust-Sicherheit beginnt mit der Transparenz zu verbundenen Benutzer:innen und Geräten. Dennoch bestehen in vielen Unternehmen weiterhin Sicherheitslücken aufgrund mangelnder Transparenz und Kontrolle der Benutzer- und Geräteaktivitäten. Ein großer Teil der Lücke geht auf die wachsende Zahl von IoT-Geräten zurück, die mit Unternehmensnetzwerken verbunden sind und die Angriffsfläche des jeweiligen Unternehmen deutlich vergrößern. Erschwerend kommt hinzu, dass IoT-Geräte oftmals von anderen Geschäftsbereichen als der IT installiert und verwaltet werden, was zu mangelnder Transparenz beiträgt.



Der Befragten gaben an, dass die Identifizierung und Authentifizierung von IoT-Geräten, die auf ihr Netzwerk zugreifen, für die Sicherheitsstrategie ihres Unternehmens von entscheidender Bedeutung ist



Der Befragten meinten, es mangele ihren Sicherheitsteams an Transparenz und Kontrolle über die Aktivitäten aller Geräte, die mit ihrer IT-Infrastruktur verbunden sind [VII]

Das Security-First KI-Netzwerk erleichtert Teams die Implementierung von Sicherheitkontrollen mit Zero Trust und bietet damit umfassende Transparenz und Kontrolle. Wenn sich auf der Grundlage einer Datenquelle gute Entscheidungen treffen lassen, werden Netzwerk- und Sicherheitsabläufe optimiert. So können Teams fundierte Entscheidungen darüber treffen, wie Risiken überwacht und verwaltet werden müssen.

Die Vorteile umfassender Transparenz

- Sicher wissen, wer und was sich in Ihrem Netzwerk befindet, und Verhalten und Zustand kontinuierlich überwachen
- Daten für andere Elemente des Sicherheitsökosystems (wie etwa SIEMs) freigeben, um Meldungen und Informationen aus der Infrastruktur bereitzustellen
- Integrierte Analysen des Netzwerkverkehrs und Verhaltensgrundregeln nutzen, um Angriffe frühzeitig zu erkennen, eventuell abzuwehren oder die Ausbreitung zu verhindern

HPE Aruba Networking Lösungen

Die Cloud-basierte Netzwerkmanagementlösung HPE Aruba Networking Central umfasst KI-gestützte Transparenz und Profilerstellung mit Client Insights. Client Insights analysiert die native Infrastruktur-Telemetrie unmittelbar von Access Points, Switches, Gateways und Clients, ohne dass die Installation von physischen Erfassungssystemen oder Agents erforderlich ist. Client Insights bietet eine genaue KI-/ML-Geräteprofilerstellung mit 99 % Genauigkeit bei bekannten Clients und einer Unbekanntenrate von < 5 % für eine Vielzahl von Endgeräten, die sich mit dem Netzwerk verbinden,[VIII] einschließlich zahlreicher IoT-Geräte in der gesamten kabelgebundenen und kabellosen Infrastruktur. In Umgebungen, die nicht vom Cloud-basierten HPE Aruba Networking Central verwaltet werden oder in denen Netzwerkgeräte von Drittanbietern zum Einsatz kommen, kann HPE Aruba Networking ClearPass Device Insight zur ML-basierten Identifizierung und Profiling von Clients genutzt werden.

Bis zu 99 % Profilgenauigkeit für mit dem Netzwerk verbundene Geräte – einschließlich IoT-Geräte

Wie vereinfachen rollenbasierte Richtlinien die Einführung von Zero-Trust-Sicherheitsframeworks?
Mit Rollen ist es möglich, Richtliniendefinitionen über Netzwerke hinweg zu übertragen, unabhängig vom geografischen Standort oder Verbindungspunkt zum Netzwerk. Geeignete Richtlinien können Benutzer:innen und Geräten dauerhaft begleiten, wenn diese sich im Unternehmen – vom Hauptstandort über die Filiale ins Homeoffice und anderswo hin – bewegen.

Globale Richtlinien

Richtlinien, die Benutzer:innen folgen

Sobald Benutzer:innen oder Geräte bekannt und profiliert sind, besteht der nächste Schritt in einem Zero-Trust-Sicherheitsframework darin, die Identität der Person oder des Gerätes bei jeder Verbindung zu authentifizieren und die entsprechenden Zugriffskontrollrichtlinien zuzuweisen. Das Definieren und Verwalten von Richtlinien kann jedoch eine Herausforderung sein, wenn sich die Geschäftsdynamik ändert, sich Arbeitskräfte von überall aus anmelden und IoT-Geräte hinzukommen. Ansätze, die auf standort- oder netzwerkspezifischen Konstrukten wie IP-Adressen oder Subnetzen basieren, können zu Komplexität und Inflexibilität im Netzwerk führen und Sicherheitsrisiken im Zusammenhang mit Inkonsistenzen bei der Definition und Anwendung schaffen.

Mithilfe globaler Richtlinienfunktionen in einem Security-First KI-Netzwerk können Unternehmen ihre Reichweite vergrößern, indem übergeordnete Richtlinien basierend auf Identität und Rollen bestimmt und angewendet werden. Die Rollen gelten für das gesamte Unternehmen. Die aufwendige Wartungen von Zugangskontrollen für jedes Gerät im Betrieb wird damit vermieden. Richtlinien auf Basis von Unternehmensabsichten machen die Richtlinien-Workflows einfacher, indem sie aus den Komplexitäten und Änderungen der zugrundeliegenden physikalischen Netzwerke ausgegliedert werden, sodass sowohl Netzwerk- als auch Sicherheitsteams gezielt verwalten können.

Vorteile globaler Richtlinien

- Richtlinien einmal bestimmen und überall anwenden. Aufwendige Wartungen von Zugangskontrollen und Inkonsistenzen, die das Risiko erhöhen, werden damit vermieden
- Richtlinien ständig lückenlos überwachen und umsetzen und Benutzer:innen, Geräte, Daten und Anwendungen konstant steuern – ganz gleich, wo sie sich befinden und womit sie sich verbinden
- Bieten Netzwerk- und Sicherheitsteams eine „gemeinsame Toolbox“ zum Optimieren der Netzwerkleistung und Durchsetzen granularer Sicherheitsrichtlinien

HPE Aruba Networking Lösungen

HPE Aruba Networking ClearPass authentifiziert Benutzer:innen und Geräte anhand zahlreicher Identitätsquellen, beispielsweise über Active Directory. Mithilfe einer umfassenden Richtlinien-Engine, die präzise Zugriffsrechte ermöglicht, kontrolliert ClearPass, welche Benutzer:innen und Geräte auf welche Ressourcen zugreifen können. Die Richtlinien folgen Benutzer:innen und Geräten nahtlos durch kabellose, kabelgebundene und Wide Area Networks – selbst in einer Umgebung mit Komponenten verschiedener Anbieter.

Für Netzwerke, die mit HPE Aruba Networking Central verwaltet werden, ermöglicht die Cloud-native Netzwerkzugriffssteuerungslösung (NAC) Cloud Auth das reibungslose Onboarding von Endbenutzer:innen und Client-Geräten entweder durch eine MAC-Adressen-basierte Authentifizierung oder durch die Integration mit gängigen Cloud-Identitätsspeichern, um automatisch die richtige Ebene des Netzwerkzugriffs zuzuweisen.

Für Hybrid- und Remote-Benutzer:innen und Dritte, wie etwa Auftragnehmende und Zeitarbeitskräfte, beschränkt HPE Aruba Networking SSE Zero Trust Network Access (ZTNA) über einen Trust Broker den Zugriff auf bestimmte Anwendungen oder Mikrosegmente, die für diese Person gemäß Definition über eine einzige globale Richtlinienschnittstelle genehmigt wurden. Die kontinuierliche Überwachung stellt sicher, dass Richtlinien automatisch an Änderungen der Identität, des Standorts und des Gerätezustands angepasst werden. Durch diesen Zusammenhang kann Zero Trust bei jedem Zugriffsereignis einfacher sichergestellt werden.

Durchsetzung vom Edge bis zur Cloud

Konsistente Richtliniendurchsetzung für Benutzer:innen, Anwendungen, Daten und Geräte

Zero-Trust-Sicherheitsframeworks basieren auf der Durchsetzung von Richtlinien. Sie stellen sicher, dass Benutzer:innen und Geräte nur Zugriff auf die benötigten Ressourcen haben; und nur solange kein Verdacht besteht, dass sie an einem Angriff beteiligt sind.

Mit dem Security-First KI-Netzwerk von HPE Aruba Networking können Unternehmen eine rollenbasierte Zero-Trust-Durchsetzung an jedem Kontrollpunkt implementieren. Das Security-First KI-Netzwerk setzt rollenbasierte Richtlinien für alle Benutzer:innen, Geräte, Daten und Anwendungen durch – ganz gleich, wie oder wo oder womit sie sich verbinden. Eine Inline-Richtliniendurchsetzung innerhalb der Switch-Infrastruktur verhindert, dass der Verkehr beim Umsetzen der Sicherheitsrichtlinien in die Enge getrieben wird. Dadurch werden die Leistung und das Benutzererlebnis verbessert und gleichzeitig weniger Ressourcen verbraucht – ohne den Zugriff oder den Schutz zu beeinträchtigen.

Vorteile der Edge-to-Cloud-Umsetzung

- Setzt Richtlinien überall durch – einschließlich auf dem Endgerät, am Access Point, Access Switch, SD-WAN Gateway, Top-of-Rack Switch im Rechenzentrum, am Hauptstandort und über die Cloud
- Unterstützt die Kooperation und Zusammenarbeit von Netzwerk- und Sicherheitsteams, da Richtlinien dazu beitragen, eine optimale Netzwerkleistung zu erzielen, und gleichzeitig das Unternehmen schützen
- Verringert die Anzahl externer Sicherheitslösungen, die zur Durchsetzung der für Zero-Trust- und Compliance-Frameworks benötigten Zugriffskontrollen erforderlich sind, sowie die damit verbundene Komplexität

HPE Aruba Networking Lösungen

Die dynamische Segmentierung von HPE Aruba Networking separiert den Netzwerkverkehr basierend auf Identität und zugehörigen Zugriffsberechtigungen und setzt den Zugriff auf Anwendungen und Daten mit Zero Trust nach dem Prinzip der geringsten Rechte vom Edge bis zur Cloud um. Da die dynamische Segmentierung mehrere Durchsetzungsmodelle – zentral und dezentral – unterstützt, kann die IT-Abteilung je nach den Anforderungen ihrer Umgebung eines oder beide Modelle verwenden. Die zentralisierte Regeldurchsetzung übernimmt die Policy Enforcement Firewall, eine komplette, in die HPE Aruba Networking Netzwerkinfrastruktur integrierte Anwendungsfirewall. Verteilte Inline-Durchsetzung innerhalb der Gateway- und Switch-Infrastruktur wird von HPE Aruba Networking Central NetConductor bereitgestellt. Dabei handelt es sich um eine Full-Stack-Lösung, die weit verbreitete Technologie wie EVPN/VXLAN verwendet, um ein intelligentes Netzwerk-Overlay zu schaffen, das sich für schnelle Netzwerkbereitstellung im Unternehmen sowie besonders hohe Skalierbarkeit für Netzwerk- und Sicherheitsautomatisierung eignet.

Unternehmen können auch HPE Aruba Networking EdgeConnect SD-WAN einsetzen und mithilfe einer integrierten, durchgängigen Next Generation Firewall konsistente Sicherheitsrichtlinien umsetzen, die sich über WAN und LAN erstrecken, einschließlich IDS/IPS, DDoS-Schutz und unternehmensweiter Mikro-Segmentierung. Mithilfe integrierter NGFW-Services können Unternehmen ihr Zweigstellennetzwerk und Sicherheitsfunktionen konsolidieren. So lassen sich veraltete Firewalls und Router in Filialen eliminieren.

Durch einen vereinfachten und automatisierten Mikrosegmentierungsprozess über eine benutzerfreundliche, Point-and-Click-Benutzeroberfläche erleichtert der HPE Aruba Networking Fabric Composer die Implemetierung von Zero-Trust-Sicherheit im Rechenzentrum. Der HPE Aruba Networking CX 10000 Switch stellt verteilte Mikrosegmentierung, Ost-West-Firewalling, Verschlüsselung und Telemetrie-Services inline über jeden Anschluss und näher an kritischen Unternehmensanwendungen bereit, sodass keine zusätzlichen Firewalls erforderlich sind

„Führende Unternehmen werden Zero-Trust-Architekturen einführen, bei denen die Aufgabe des Netzwerks nicht darin besteht, alles mit allem zu verbinden, sondern vielmehr darin, als Durchsetzungsebene für Sicherheitsrichtlinien zu agieren. Für Benutzer, die auf Anwendungen zugreifen, können Sicherheitsrichtlinien in der Cloud durchgesetzt werden. Aber für viele Verkehrsflüsse (besonders für IoT-Geräte mit deren zugehörigen Services) wird es effizienter sein, Sicherheitsrichtlinien in Zugriffsgeräten wie Access Points, Switches und Routern automatisch bereitzustellen.“

– David Hughes, Chief Product und Technology Officer, HPE Aruba Networking, Hewlett Packard Enterprise[IX]

Was ist KI-Networking?
KI-Networking ist ein neu definierter Begriff und soll ausdrücken, wie künstliche Intelligenz für den IT-Betrieb (AIOps) auf WLAN-, Switching- und WAN-Umgebungen angewendet wird.

KI-automatisierter Betrieb

Im großen Maßstab verwalten und schützen

Die heutige Wirtschaftswelt ist komplexer geworden und schwieriger zu navigieren als je zuvor. Wer heute ein Zero-Trust-Netzwerk pflegen und sichern will, braucht umfassende Transparenz und Automatisierung. Die künstliche Intelligenz verspricht, das menschliche Potenzial zu vervielfachen. So können Unternehmen Risiken deutlich senken, um die Sicherheit zu verbessern und Teams mehr Freiraum zu geben, geschäftliche Vorteile zu schaffen.

Ein Security-First KI-Netzwerk bietet Teams die Leistungsstärke maschinellen Lernens in Kombination mit vollständiger netzwerk- und benutzerzentrierter Telemetrie zur Erfassung von Daten aller Benutzer:innen, Geräte und Netzwerke. Sicherheitsteams können diese Daten zur Unterstützung der Implementierung von Zero-Trust-Sicherheit und kontinuierlichen Überwachung nutzen und so Angriffe verhindern und eindämmen. Die Netzwerkteams profitieren von der Möglichkeit, langwieriges Onboarding, Bereitstellungen und Aufgaben zur Richtlinien-Harmonisierung automatisieren zu können.

Die Vorteile eines KI-automatisierten Betriebs

- Automatisierung von Netzwerkmanagement und Sicherheitsaufgaben zur Verringerung des benötigten manuellen Aufwands für die Sicherung und Verwaltung des Netzwerks
- Verbesserung der Transparenz und Kontrolle von Benutzer:innen und Geräten im Netzwerk und Erkennung von Anomalien zur besseren Angriffserkennung und -verhinderung
- Verbesserte Überwachung und Diagnosen, um handlungsrelevante Einblicke zu erhalten, die Netzwerk- und Sicherheitsteams nutzen können

KI-automatisierter Betrieb mit HPE Aruba Networking

HPE Aruba Networking Central ist eine Cloud-native Netzwerk- und Sicherheitsmanagementkonsole für die gesamte HPE Aruba Netzwerkinfrastruktur. Als zentraler Punkt für Transparenz und Kontrolle für die Aruba ESP (Edge Services Platform) bietet Central AIOps, Workflow-Automatisierung und erweiterte Sicherheitsfunktionen zur Vereinheitlichung aller Vorgänge an Hauptstandorten, Zweigstellen sowie in Rechenzentrums- und Remote-Arbeitsumgebungen.

Central nutzt KI und erweiterte Analysen, um allgemeine Netzwerk- und Sicherheitsmanagement- und Betriebsvorgänge zu automatisieren – mit intelligenter Überwachung von Netzwerk, Anwendungen und Geräten, die Teil des Data Lake sind, rund um die Uhr. Diese Funktionen basieren auf ML-Modellen, die konstant mit Netzwerkleistungsdaten eines vielfältigen und globalen Kundenstamms von HPE Aruba Networking geschult werden. Die KI-gestützten Leistungen von Central umfassen:

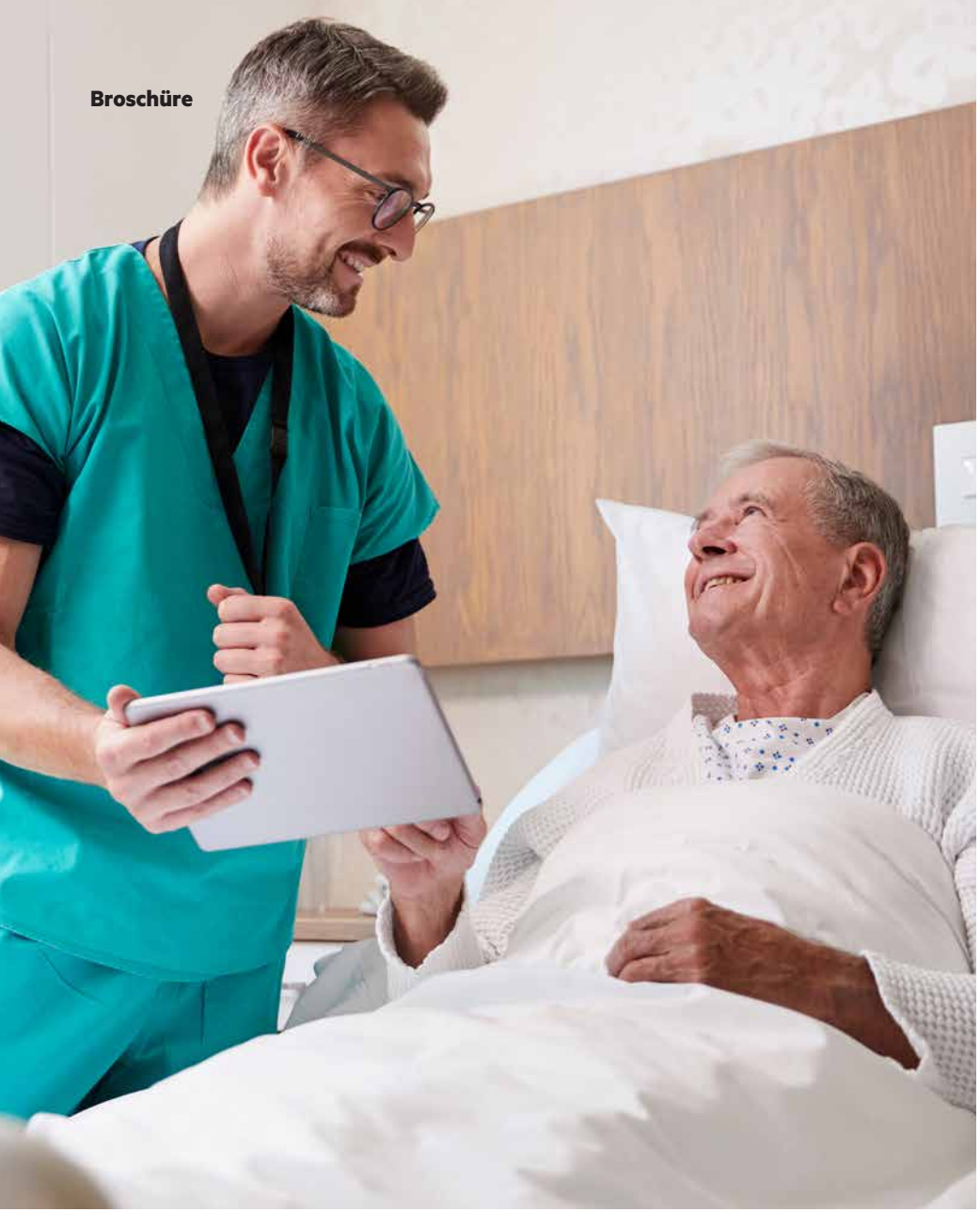
- Automatische Erkennung und Diagnose von Problemen beim Einsatz dynamischer Baselines, mit integrierter Anomalieerkennung für präzise Problemerkennung, Ursachenermittlung und Problembehebung mit nahezu 95 % Genauigkeit[X]
- ML-Modelle in Verbindung mit Deep Packet Inspection zur genauen Erkennung und Profilierung von Clients in der gesamten kabelgebundenen und kabellosen Infrastruktur ohne physische Erfassungssysteme oder Agenten
- Firmwareempfehlungen, um den Aufwand für die manuelle Nachverfolgung von Firmware-Upgrades zu vermeiden und das Risiko mangelnder Compliance aufgrund von Sicherheitsschwachstellen zu senken

Die KI-gestützten Leistungen von HPE Aruba Networking Central basieren auf dem größten Data Lake der Branche

2,7
Millionen Geräte

200
Millionen Clients

>30
Branchen



Bethesda Health Group

Das Security-First KI-Netzwerk bei der Arbeit

Kundenerfahrungen

Neben hochgradig personalisierter häuslicher Pflege bietet die Bethesda Health Group lebendige und vielfältige Seniorengemeinschaften, die auf einzigartige Art und Weise die Stadtteile im Großraum St. Louis widerspiegeln. Damit hat sie sich über 135 Jahre einen landesweiten Ruf als vertrauenswürdiger Partner für Senioren und deren Familien aufgebaut. Die 1100 Arbeitskräfte der Organisation bieten an 16 Standorten individuelle, hochwertige, innovative und mitfühlende Pflege.

Um seine zunehmend mobile und technikaffine Belegschaft und Wohnbevölkerung zu unterstützen, hat Bethesda seine Betriebsabläufe umgestaltet und eine Cloud-First-Strategie eingeführt. Mithilfe leistungsstarker Konnektivität werden Services bereitgestellt, Zugriffe auf eine Vielzahl von Anwendungen ermöglicht, und die Bewohner können mit ihren Pflegeteams, ihrer Familie und ihren Freunden in Kontakt bleiben. Durch diese Transformation entstand auch der Bedarf an verbesserter Cybersecurity und der Einführung von Zero Trust.

Bethesda arbeitete schon für das kabelgebundene, kabellose und softwaredefinierte WAN (SD-WAN)-Netzwerk mit HPE Aruba Networking zusammen und beschloss nun, seine Infrastruktur durch die Einführung einer vollständig Cloud-basierten Secure Access Service Edge (SASE)-Plattform und des HPE Aruba Networking Security Service Edge (SSE) zu verbessern. Diese konsolidiert mehrere sichere Zugriffsfunktionen in einem einzigen, benutzerfreundlichen Cloud-Service, der Richtlinien basierend auf Änderungen im Benutzer-, Geräte- und Anwendungskontext automatisch anpasst.

Nach der Bereitstellung des SD-WAN wollte Bethesda die Zugriffssicherheit verbessern und Audit-Anforderungen erfüllen. Mit HPE Aruba Networking ClearPass konnte Bethesda seine Zugriffssteuerung über eine granulare, richtlinienbasierte Lösung für kabelgebundene und kabellose Netzwerke automatisieren – und das magere IT-Personal hielt die Lösung für eingängig und benutzerfreundlich.

Bethesda schätzte HPE Aruba Networking Central auch für die Bereitstellung des KI-gestützten und Cloud-basierten Managements zur weiteren Vereinheitlichung seiner kabelgebundenen und kabellosen Infrastruktur.

„Wir haben eine umfassende und sichere Netzwerkinfrastruktur gewonnen, sodass wir großen kabelgebundenen, WLAN- und SD-WAN-Bedarf mit einem kleinen IT-Team stemmen können – ohne das Budget zu sprengen.“

– Michael Keller, Leiter des Bereichs Information Technology, Bethesda Health Group[XII]

Ganzen **Artikel lesen**

Zero-Trust-Sicherheit bereitstellen

Die Einführung einer Zero-Trust-Sicherheit ist ein langer Weg. Sie wissen nicht, wo Sie anfangen sollen? Bestimmen Sie anhand dieser Checkliste mit Funktionen die richtigen nächsten Schritte:

- ✓ Haben Sie Einblick in jedes Gerät in Ihrem Netzwerk, ob Sie es verwalten oder nicht?
- ✓ Verfügen Sie über konsistente Methoden für die Zuweisung von Privilegien an Benutzer:innen und Geräte?
- ✓ Setzen Sie Sicherheitsstandards durch, bevor ein Gerät im Netzwerk zugelassen wird?
- ✓ Setzen Sie rollenbasierte Zugriffsrichtlinien konsistent überall im gesamten Netzwerk durch?
- ✓ Können Sie anhand aller verfügbaren Daten kontinuierlich den Sicherheitsstatus einer Person überwachen?

Weitere Informationen zum Security-First KI-Netzwerk von HPE Aruba Networking finden Sie unter

arubanetworks.com/products/security/

[I] Rose, S.; Borchert, O.; Mitchell, S.; Connelly, S. Zero Trust Architecture. NIST Special Publication 800-207. National Institute of Standards and Technology. August 2020.

[II] Das „Innovationen oder Risiken"-Dilemma. Hewlett Packard Enterprise. 2023.

[III] The 2023 Global Study on Closing the IT Security Gap: Addressing Cybersecurity Gaps from Edge to Cloud. Ponemon Institute. März 2023.

[IV] The 2023 Global Study on Closing the IT Security Gap: Addressing Cybersecurity Gaps from Edge to Cloud. Ponemon Institute. März 2023.

[V] Was ist der Stand bei Zero-Trust-Sicherheit? HPE Aruba Networking. April 2023.

[VI] The 2023 Global Study on Closing the IT Security Gap: Addressing Cybersecurity Gaps from Edge to Cloud. Ponemon Institute. März 2023.

[VII] The 2023 Global Study on Closing the IT Security Gap: Addressing Cybersecurity Gaps from Edge to Cloud. Ponemon Institute. März 2023.

[VIII] KI-basierte Netzwerkinfrastruktur: Die Lösung für eine effiziente IT. 2022.

[IX] Hughes, D. Five top networking and security trends for 2024. Januar 2024.

[X] HPE Aruba Networking Central KI-basiertes, Cloud-verwaltetes Networking für Zweigstellen-, Campus-, Remote- und Rechenzentrumsnetzwerke. 2023.

[XI] HPE Aruba Networking Central KI-basiertes, Cloud-verwaltetes Networking für Zweigstellen-, Campus-, Remote- und Rechenzentrumsnetzwerke. 2023.

[XII] Bethesda Health Group. 2024 https://www.arubanetworks.com/resources/case-studies/bethesda-health-group/

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

Kontakt

Besuchen Sie **ArubaNetworks.com**

Hewlett Packard Enterprise

BR_EasingZeroTrustSecurityadoption_DT_020124 a00137590dee