aruba
a Hewlett Packard Enterprise company

Implementierung von identitätsbasierten Zero-Trust- und SASE-Architekturen

SO NUTZT MAN DIE NETZWERKZUGRIFFSSTEUERUNG, UM DAS UNTERNEHMEN ZU SCHÜTZEN

Inhalt

Warum sich die Sicherheit weiterentwickeln muss

Die Herausforderungen für die Netzwerksicherheit haben sich mit der zunehmenden Dezentralisierung der Belegschaft, der Überflutung des Netzwerks mit neuen IoT-Geräten und den immer raffinierteren und hartnäckigeren Angriffen deutlich erhöht. Herkömmliche Sicherheitsansätze, die sich in erster Linie auf den Netzwerkrand konzentrieren, sind als primäre Sicherheitsstrategie unwirksam geworden.

Moderne Netzwerksicherheit muss nicht nur imstande sein, eine ständigen Veränderungen unterworfene Menge von Benutzer:innen und Geräten aller Art zu bewältigen, sondern auch mit zunehmend häufigeren Bedrohungen fertig werden, die auf bisher für sicher gehaltene Teile der Netzwerkinfrastruktur abzielen.
Um dieses Problem anzugehen, wurden zwei große Netzwerksicherheitsinitiativen ins Leben gerufen, die als Leitfaden für die Planung, den Entwurf und die Implementierung sicherer Netzwerke zur Unterstützung einer umfassenden IT-Schutzstrategie dienen.
Mit dem Federal Information Systems Management Act (FISMA) aus dem Jahr 2014 wurde das National Institute of Standards and Technology (NIST) beauftragt, eine Reihe von allgemeinen Sicherheitsrichtlinien und eine Architektur zu entwickeln, die sich zur Zero-Trust-Architektur entwickelt hat. Im Jahr 2019 definierte Gartner das Secure Access Service Edge (SASE)-Konzept, um der Tatsache Rechnung zu tragen, dass der IT-Zugang und die entsprechenden Sicherheitsdienste in der Cloud verfügbar sein werden.

Zero Trust und SASE stützen sich auf Identität

Ein grundlegendes Prinzip der Zero-Trust- und SASE-Architekturen ist, dass der Zugang zu IT-Ressourcen nicht allein davon abhängen sollte, wo oder wie sich ein Client verbindet. Mit anderen Worten: Das Netz ist grundsätzlich nicht vertrauenswürdig, und es muss eine „Overlay"-Sicherheitsstruktur hinzugefügt werden, die auf einer genau definierten, identitätsbasierten Architektur basiert, die den Datenverkehr auf die Pfade und Ressourcen beschränkt, die ausdrücklich zugelassen wurden. Darüber hinaus können diese Architekturen den Sicherheits-„Lebenszyklus" eines Endpunkts abdecken, von der Authentifizierung und Autorisierung bis hin zur kontinuierlichen Überwachung und Angriffsabwehr.

Ziel ist es, den Client zu authentifizieren und dann seine Konfiguration und seinen Status kontinuierlich mit einer Reihe von akzeptablen Sicherheitszuständen zu vergleichen, um sicherzustellen, dass er keine Schwachstellen einführt oder an einem Angriff beteiligt ist. In diesem Leitfaden erfahren Sie, wie Sie eine Zero Trust- und SASE-Architektur mit Identität als Grundlage implementieren.

Unterstützung beider Frameworks durch die Bewältigung der 5 wichtigsten Herausforderungen im Bereich der Sicherheit

1 **Blinde Flecken im Netzwerk beseitigen.** Ziel ist es, alle mit dem Netzwerk verbundenen Geräte zu erkennen und zu profilieren – auch IoT-Geräte, die nicht in den Zuständigkeitsbereich des Netzwerk- und Sicherheitsteams fallen.

2 **Überprüfen Sie die Identität, bevor Sie Zugang gewähren.** Beginnend mit 802.1X gibt es viele Authentifizierungsverfahren, die sicherstellen, dass nur legitime Benutzer und Geräte eine Verbindung zum Netzwerk herstellen, einschließlich neuer Lösungen für IoT-Geräte.

3 **Vergleichen Sie die Endpunktkonfiguration mit Compliance-Baselines und nehmen Sie gegebenenfalls Korrekturen vor.** So kann das Sicherheitsteam Konfigurationsrichtlinien definieren und durchsetzen, die die Anwendung der entsprechenden Patches und Updates widerspiegeln.

4 **Richten Sie den Zugriff auf IT-Ressourcen mit den wenigsten Rechten ein, indem Sie den Datenverkehr auf der Grundlage identitätsbasierter Richtlinien segmentieren.** Nachdem die Identität und die Übereinstimmung der Konfiguration bestätigt wurden, kann dem Benutzer oder Gerät eine Reihe von IT-Privilegien zugewiesen werden, die durch vordefinierte Zugriffsrichtlinien in der Netzwerkinfrastruktur durchgesetzt werden.

5 **Überwachen Sie den Sicherheitsstatus des Benutzers und des Geräts sowie bidirektionale Kommunikation mit anderen Elementen des Sicherheitsökosystems kontinuierlich.** Reduzieren oder eliminieren Sie die Zugangsrechte, wenn es Anzeichen dafür gibt, dass ein mit dem Netzwerk verbundener Benutzer oder ein Gerät kompromittiert wurde.

Wissen, was sich in Ihrem Netzwerk befindet

Die Fähigkeit alle kabellosen und -gebundenen Geräte, die mit dem Netzwerk verbunden sind, breit gefächert und präzise zu erkennen – von herkömmlichen IT-verwalteten Geräten bis hin zu zuvor unerkannten IoT-Geräten, wie Kameras, Medizingeräten und anderen schwer zu erkennenden Endpunkten – stellt eine essentielle Sicherheitskontrolle dar.

Der effektivste Ansatz nutzt mehrere Erkennungsmethoden, um ein breites Sortiment an Gerätetypen zu finden und zu klassifizieren. Die fortschrittlichsten Lösungen nutzen maschinelles Lernen, um kontextuelle und Verhaltensinformationen konstant zu evaluieren, Fingerabdrücke dynamisch zu aktualisieren und Empfehlungen für zuvor nicht gesehene Geräte abzugeben.

Zur Unterstützung der granularen Segmentierung des Datenverkehrs können Geräteerkennung und –profilierung in Zugriffsrichtlinien integriert werden, um eine durchgängige Zugriffskontrolle von der Sichtbarkeit bis zur Durch-setzung der Netzwerkinfrastruktur zu ermöglichen. Auf der Grundlage einer bestimmten Richtlinie können Geräten automatisch Zugriffsrechte zugewiesen werden, oder sie können unter Quarantäne gestellt werden, wenn sie die Konfigurationsanforderungen nicht erfüllen oder sich bösartig oder unsicher verhalten.

Was Sie jetzt tun können

- **Erstellen Sie ein Geräteinventar, was alles mit dem Netzwerk verbunden ist.**
- **Überwachen Sie kontinuierlich auf neue Geräte und Verbindungen.**
- **Nutzen Sie Cloud-basierte Fingerabdruck-Datenbanken, um auf Profile für bisher nicht gesehene Geräte zuzugreifen.**

Stellen Sie konsistente Authentifizierung für die Zuweisung von Privilegien sicher

Nachdem ein(e) Benutzer(in) oder ein Gerät bekannt und profiliert wurde, ist der nächste Schritt, die Identität bei jeder Anmeldung im Netzwerk zu authentifizieren. Organisationen können sich auf sichere Authentifizierung unter Verwendung von normenbasierter 802.1X-Durchsetzung verlassen. Authentifizierung von MAC-Adressen kann auch für IoT- und Headless-Geräte verwendet werden, die eventuell keinen Support für 802.1X bieten. Darüber hinaus hat die Wi-Fi-Allianz vor kurzem einen Wi-Fi-ZERTIFIZIERTEN Easy Connect™ Standard definiert, um zertifizierte IoT-Geräte sicher aufzunehmen.

Umfangreicher Gastzugang vereinfacht die Workflow-Prozesse für Besucher und ermöglicht Rezeptionist:innen, Mitarbeitenden und anderem nicht zur IT-Abteilung gehörenden Personal die Erstellung von temporären Gastzugängen für sicheren drahtlosen und drahtgebundenen Internetzugriff. Mobil-freundliche Portale mit sehr guten Anpassungsmöglichkeiten bieten benutzerfreundliche Anmeldungsvorgänge mit Selbstregistrierung, Sponsor-Freigabe und Erstellung von Bulk-Zugangsdaten.

Was Sie jetzt tun können

- **Eine Authentifizierungslösung einrichten, die mit mehreren Protokollen und Schnittstellen mit einer Vielzahl von Identitätsdatenbanken arbeiten kann.**
- **Richten Sie ein Gastportal ein, um Besucher nahtlos aufzunehmen.**
- **Implementieren Sie 802.1X-Authentifizierung für sowohl verkabelte als auch kabellose Verbindungen und priorisieren Sie WLAN-EasyConnect-fähige Geräte für IoT-Anwendungen.**

Einhaltung der Compliance durchsetzen

Die Einhaltung der Compliance und die Bewertung der Sicherheitslage sind wichtige Sicherheitskontrollen, die vom Netzwerk ausgeführt werden können. Während des Autorisierungsprozesses werden für bestimmte Geräte Zustandsprüfungen durchgeführt, um sicherzustellen, dass sie die von der IT-Abteilung festgelegten Konfigurationsstandards einhalten, einschließlich Patch-Levels, Virenschutz, Antispyware und Firewall-Richtlinien. Geräte, die Compliance-Standards nicht einhalten, können entweder automatisch mit einem dauerhaften Agenten repariert oder zur weiteren Nachverfolgung an ein firmeneigenes Portal weitergeleitet werden.

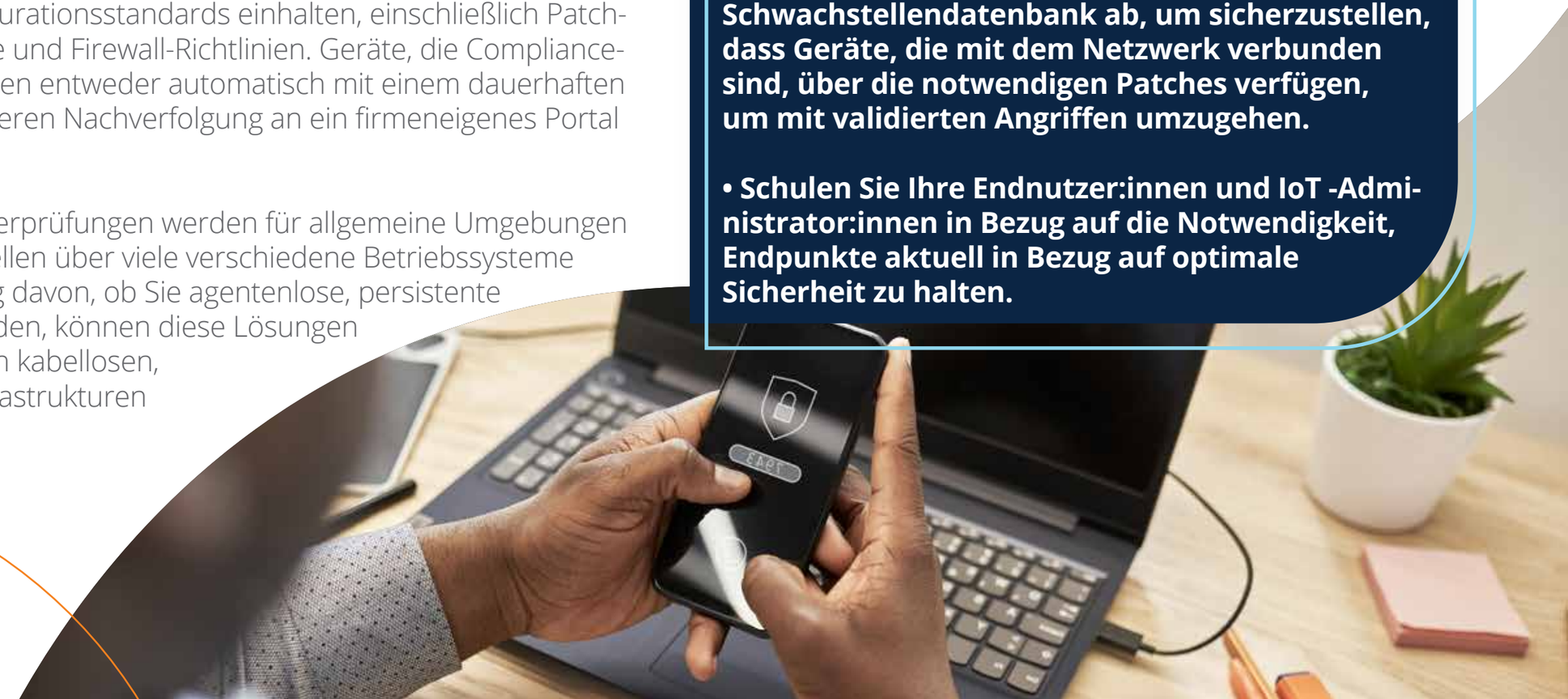
Haltungsbasierte Sicherheitsüberprüfungen werden für allgemeine Umgebungen erstellt und können Schwachstellen über viele verschiedene Betriebssysteme hinweg eliminieren. Unabhängig davon, ob Sie agentenlose, persistente oder auflösbare Clients verwenden, können diese Lösungen zentral kompatible Endpunkte in kabellosen, kabelgebundenen und VPN-Infrastrukturen identifizieren.

Was Sie jetzt tun können

• Legen Sie Standards für Konfiguration, Version, und Patch-Levels fest, die für Endpunktzugriff auf das Netzwerk erforderlich sind.

• Schließen Sie ein Abonnement bei einer Schwachstellendatenbank ab, um sicherzustellen, dass Geräte, die mit dem Netzwerk verbunden sind, über die notwendigen Patches verfügen, um mit validierten Angriffen umzugehen.

• Schulen Sie Ihre Endnutzer:innen und IoT -Administrator:innen in Bezug auf die Notwendigkeit, Endpunkte aktuell in Bezug auf optimale Sicherheit zu halten.



Nutzen Sie Identität, um Netzwerk-Traffic dynamisch zu segmentieren

Das Herzstück der NIST Zero-Trust-Architektur ist eine Zusammenarbeit von zwei wichtigen Netzwerkkomponenten:

- Eine Richtlinien-Engine/Administrator(in), die/der die Bedingungen festlegt, unter denen ein(e) Benutzer(in) oder ein Gerät eine Verbindung zum Netzwerk herstellen kann und welche Zugriffsrechte ihr/ihm zustehen, basierend auf dem Authentifizierungs- und Compliance-Prozess, den er/sie durchlaufen muss

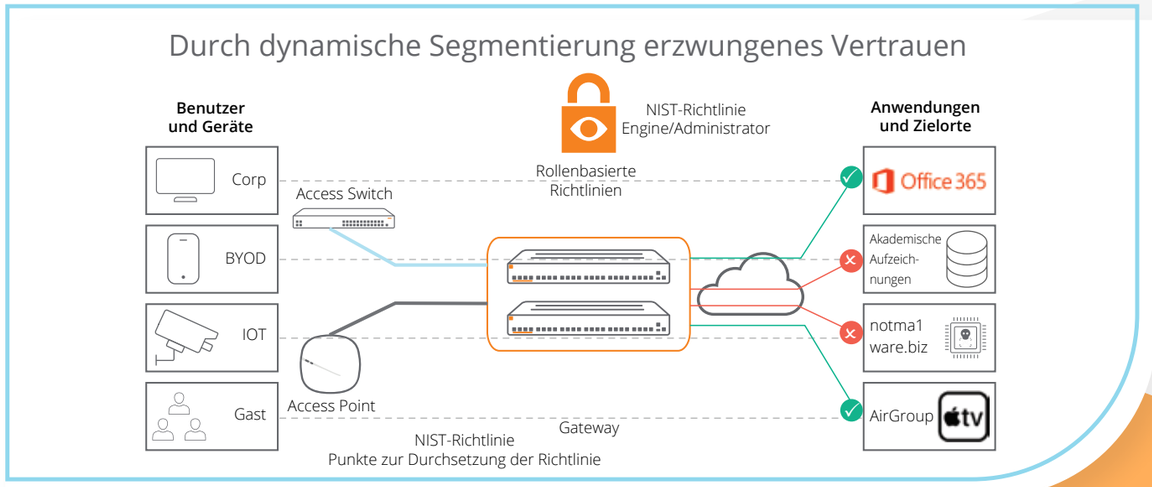
- Ein Richtliniendurchsetzungspunkt, der die von der Richtlinien-Engine gelieferten Zugriffsanweisungen interpretiert und durchsetzt

Gemeinsam bilden sie Echtzeit- oder dynamische Traffic-Segmentierung. Diese Art der Kontrolle kann jedoch nicht nachträglich zu einem Netzwerk hinzugefügt werden, das ohne Überlegungen zur Verwaltung und Durchsetzung eines identitätsbasierten Zugriffs aufgebaut wurde, der in Echtzeit an Änderungen des Endpunkt- und Netzwerkstatus angepasst werden muss.

Die Fähigkeit zur Mikrosegmentierung des Traffics auf Basis von Identität und Rolle ergibt zwei Hauptvorteile:

Dynamischer Prozess: Die rollenbasierte Richtlinie wird einem kabelgebundenen Port oder einer drahtlosen Verbindung auf der Grundlage von Faktoren wie der Zugriffsmethode des Clients zugewiesen. Auch kontextbezogene Daten wie Tageszeit, Gerätetyp usw. können einbezogen werden, sodass das IT-Personal nicht länger statische Attribute zur Zugriffskontrolle verwenden muss.

Feinkörnige Segmentierung: Dadurch kann der Client-Verkehr auf der Grundlage von Berechtigungen in der Zugriffsrichtlinie segmentiert werden. Die Mikrosegmentierung ermöglicht verbesserte Sicherheits- und Leistungsvorteile, da die Zugriffskontrollen viel granularer sein können als schwer zu verwaltende VLAN-Zuweisungen und von der Netzwerkinfrastruktur durchgesetzt werden.

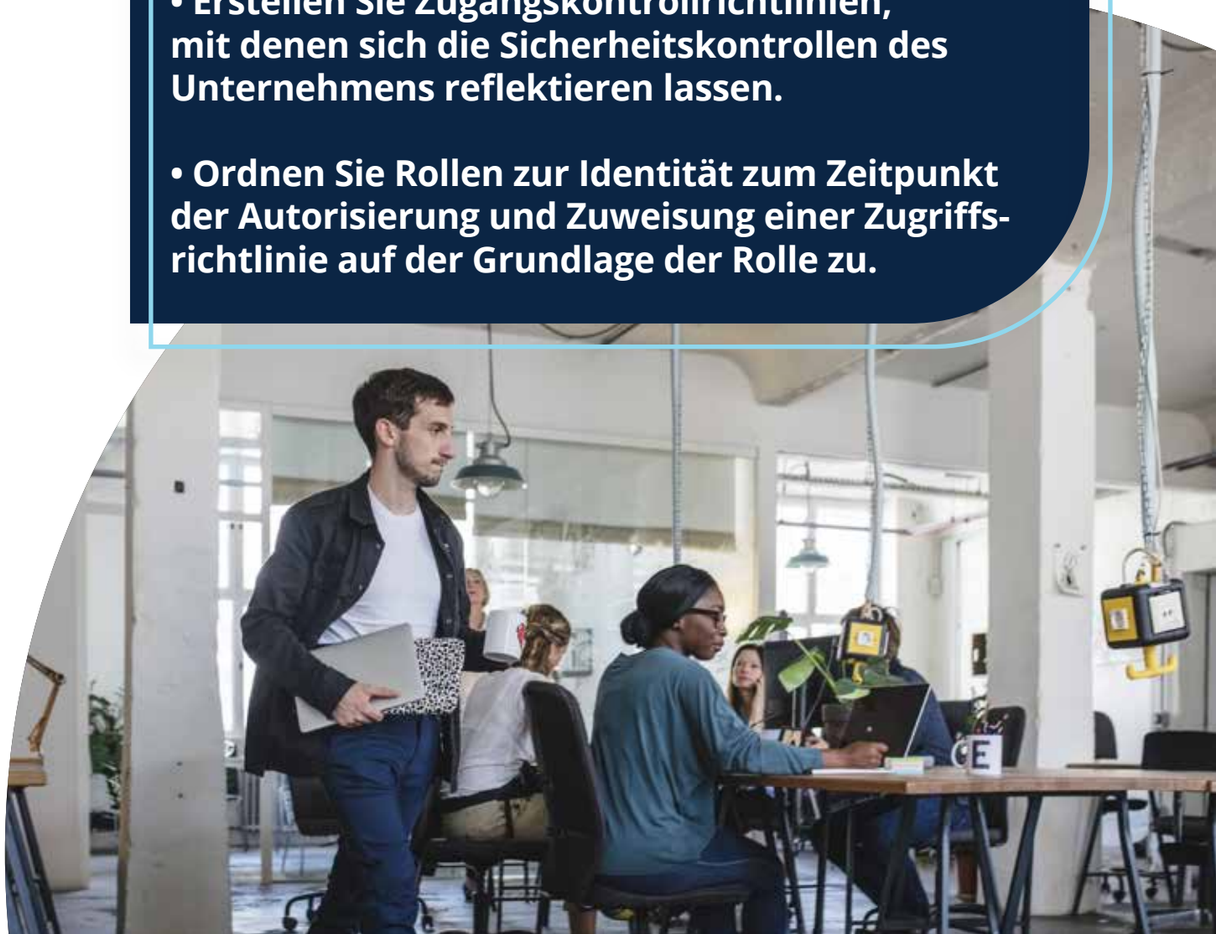


Wenn VLANs nicht ausreichen: Verwendung von EVPN-VXLAN zur Erweiterung Netzwerksegmentierung im globalen Maßstab

Die Verbreitung von Endgeräten aufgrund von BYOD, Mobilität am Arbeitsplatz und IoT führt zu einem Bedarf an feineren Segmentierungsstrategien, um verschiedene Profile von Benutzern, Geräten und Datenverkehr auf globaler Basis zu trennen – über das hinaus, was traditionelle VLANs bieten können. Moderne Netzwerk-Switches haben die Möglichkeiten zur Konfiguration und Richtliniendurchsetzung erweitert und umfassen nun auch Industriestandards wie EVPN-VXLAN für mehr Flexibilität, globale Skalierbarkeit und Interoperabilität mit Drittanbietern. EVPN-VXLAN ermöglicht es Unternehmen, geografisch verteilte Standorte über eine virtuelle Layer-2-Überbrückung zu verbinden, und hat sich vor allem aufgrund der Einschränkungen herkömmlicher VLAN-basierter Netzwerke zu einem beliebten Netzwerkrahmen entwickelt. VXLAN kapselt Layer-2-Ethernet-Frames in Layer-3-UDP-Pakete ein, d. h. virtuelle Layer-2-Subnetze können sich über darunter liegende Layer-3-Netze erstrecken und die Netzwerksegmentierung über physikalische Zuordnungen hinweg ausweiten.

Was Sie jetzt tun können

- **Etablieren Sie Benutzer- und Gerätegruppen mit ähnlichen Zugangsberechtigungen zu IT-Assets.**
- **Erstellen Sie Zugangskontrollrichtlinien, mit denen sich die Sicherheitskontrollen des Unternehmens reflektieren lassen.**
- **Ordnen Sie Rollen zur Identität zum Zeitpunkt der Autorisierung und Zuweisung einer Zugriffs-richtlinie auf der Grundlage der Rolle zu.**



Erstellen Sie eine tiefe Integration mit dem Sicherheitsökosystem

Wie sowohl im NIST-Zero-Trust-Architektur- als auch im SASE-Rahmenwerk hervorgehoben wird, müssen Unternehmen in der Lage sein, die besten Sicherheitslösungen einzusetzen und sicherzustellen, dass ihr gesamtes Sicherheitsökosystem kommuniziert und das Bewusstsein für Angriffe und die Reaktion darauf koordiniert.

Ein entscheidender Vorteil dieses Ansatzes besteht darin, dass Unternehmen ihre bestehenden Sicherheitsinvestitionen nutzen können, indem sie Lösungen wie Next-Generation Firewall (NGFW)- und Security Information and Event Management (SIEM)- Technologien nahtlos in ihre Netzwerkzugriffssteuerungslösungen integrieren. Dadurch wird die Bindung an eine einzige Lösung vermieden, die zu kostspieligen Upgrades und einer einzigen Produktquelle führt. Ein Netzwerksicherheits-Framework, das sich in das breitere Sicherheitsökosystem integriert, bietet die besten Elemente einer einheitlichen Lösung mit der Flexibilität einer offenen Architektur.

Der Kontext wird zwischen den einzelnen Komponenten für eine durchgängige Durchsetzung und Sichtbarkeit von Richtlinien geteilt. Dadurch kann die Zugangskontrolllösung auf sich ändernde Bedrohungen für Benutzer:innen und Geräte reagieren, nachdem diese sich beim Netzwerk authentifiziert haben.

Was Sie jetzt tun können

- **Erstellen Sie eine umfassende, auf Zero Trust und SASE basierende Sicherheitsstrategie, um Ihre Sicherheitsinvestitionen zu steuern.**
- **Stellen Sie sicher, dass Ihre Sicherheitslösungen offen sind und sich nahtlos in Ihre Netzzugangskontrolle integrieren lassen.**
- **Entwerfen Sie Richtlinien, die das Netzwerk zu einem Verbündeten bei der Erkennung und Reaktion auf Angriffe machen.**

Wie Aruba dazu beitragen kann: Die Aruba Edge Services Platform bietet Zero Trust und SASE Edge-to-Cloud-Sicherheitslösungen

Die Aruba Edge Services Platform (ESP) unterstützt Zero-Trust- und SASE-Architekturen, indem sie Geräteerkennung, Authentifizierung, Konfigurationserzwingung, rollenbasierte Zugriffskontrolle, integrierte richtlinienbasierte Datenverkehrssegmentierung und kontinuierlichen Schutz vor Bedrohungen bietet – alles in einer einzigen Lösung:

Aruba Central Client Insights:

Die Sicherheits- und Netzwerkteams sind ständig auf der Suche nach Geräten, die ohne die entsprechenden Kontrollen mit dem Netz verbunden sind. Client Insights nutzt eine ganze Reihe passiver und aktiver Erkennungstechniken sowie KI-Fingerprinting, um sicherzustellen, dass jedes Gerät gefunden und profiliert wird.

ClearPass:

ClearPass führt eine breite Palette von Funktionen der Zero-Trust-Architektur aus. Es beginnt mit einer Reihe von Authentifizierungsdiensten zur Identifizierung von Benutzer:innen und Geräten. Auf der Grundlage der Identität weist der ClearPass-Richtlinienmanager eine Reihe von Zugriffsberechtigungen zu, die vom Aruba-Netzwerk durchgesetzt werden. ClearPass OnGuard führt eine fortschrittliche Endpunktbewertung und -behebung durch, um sicherzustellen, dass Sicherheits- und Compliance-Anforderungen erfüllt werden, bevor Benutzer:innen und Geräte eine Verbindung zum Netzwerk herstellen.

Dynamische Segmentierung:

Die marktführende dynamische Segmentierungslösung von Aruba ist ein entscheidendes Element der in Aruba ESP integrierten Edge-to-Cloud-Sicherheit. Es ermöglicht den Zugriff auf IT-Ressourcen mit den geringsten Rechten, indem es den Datenverkehr auf der Grundlage von Rollen und zugehörigen Zugriffsberechtigungen segmentiert. Die dynamische Segmentierung vereinheitlicht den rollenbasierten Zugriff und die Durchsetzung von Richtlinien über kabelgebundene, drahtlose und WAN-Netzwerke hinweg und stellt sicher, dass Benutzer:innen und Geräte nur mit Zielen kommunizieren können, die ihrer Rolle entsprechen – so bleibt der Datenverkehr sicher und getrennt.

Policy Enforcement Firewall (PEF):

Die Firewall zur Richtliniendurchsetzung (Policy Enforcement Firewall, PEF) ist eine zustandsabhängige Layer-7-Firewall, die auf Aruba Wireless Access Points, Gateways und Controllern aktiviert werden kann. PEF ist der begleitende Durchsetzungspunkt für ClearPass-Richtlinien und erzwingt eine richtlinienbasierte Segmentierung des Datenverkehrs pro Benutzer und pro Gerät für kabelgebundene, drahtlose und WAN-Konnektivität.

Central NetConductor:

Mit dieser Suite mit Cloud-nativen Netzwerkverbindungs- und Sicherheitsservices können Unternehmen jeder Art und Größe die kabelgebundene, drahtlose und WAN-Infrastruktur automatisch konfigurieren, um eine optimale Netzwerkleistung zu erzielen und gleichzeitig die granularen Sicherheitsrichtlinien für die Zugriffskontrolle durchzusetzen, die die Grundlage für Zero-Trust- und SASE-Architekturen bilden. Mit Central NetConductor kann die dynamische Segmentierung über die Cloud verwaltet werden, mit der Möglichkeit, Zugriffsrichtlinien zentral zu definieren und durchzusetzen, entweder in einer verteilten oder zentralen Weise, je nach Wahl des Overlay.

Aruba 360 Security Exchange:

Die Sicherheitsprodukte von Aruba lassen sich in eine Vielzahl von IT-Systemen von Drittanbietern integrieren, um eine durchgängige Richtliniendurchsetzung und Transparenz für mobile und IoT-Geräte zu gewährleisten. Der ClearPass Policy Manager ist bidirektional in über 150 Sicherheits- und Verwaltungsprodukten von Drittanbietern integriert, um identitätsbasierte Informationen für das Ökosystem bereitzustellen und Informationen über Bedrohungen und Angriffe zu erhalten, die als Grundlage für politische Entscheidungen dienen.

Das Pentagon modernisiert die drahtgebundene und drahtlose Konnektivität auf allen Klassifizierungsebenen mit der Infrastruktur von Aruba

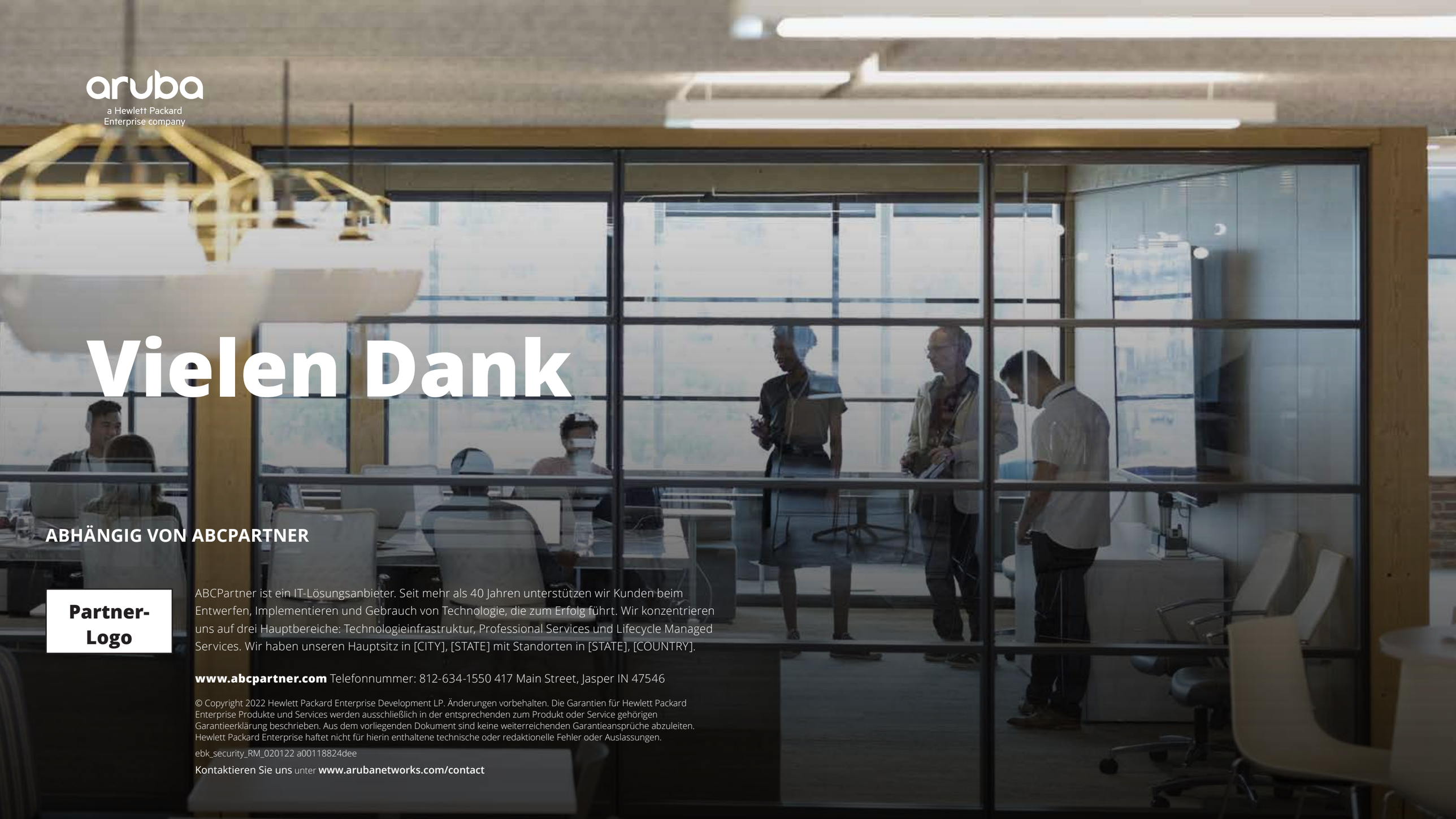
Das Pentagon, der Hauptsitz des US-Verteidigungsministeriums, modernisiert seine klassifizierten und nicht klassifizierten Netzwerke, um täglich Zehntausende von Geräten zu unterstützen. Die ESP-basierte Architektur von Aruba wird dem Pentagon eine automatisierte Netzwerkinfrastruktur zur Verfügung stellen, die manuelle Prozesse wie Port-Mapping und die anfängliche Switch-Konfiguration überflüssig macht. Darüber hinaus wird der Einsatz von Aruba ClearPass Policy Manager für die sichere Netzwerkzugriffssteuerung auf alle Netzwerke erweitert.

Sicherheits-anforderungen	Zero-Trust- und SASE-Architektur	Aruba-Lösungen
Wissen, was sich in Ihrem Netzwerk befindet	Ein Unternehmen schützt Resourcen, indem es definiert, welche Ressourcen vorhanden sind	**Aruba Client Insights**
Alle Benut-zer:innen und Geräte authentifizieren	Erstellen, Speichern und Verwalten von Unterneh-mensbenutzerkonten und Identitätsdatensätzen	**ClearPass Policy Manager**
Stellen Sie sicher, dass die Konfi-gurations- und Compliance-Richt-linien eingehalten werden	Sammeln von Informationen über den aktuellen Zustand der Unternehmensressource und Anwenden von Aktualisie-rungen auf Konfiguration und Softwarekomponenten	**ClearPass OnGuard**
Zuweisung und Durchsetzung von Zugangsrichtlinien im Netzwerk	Jede Authentifizierung und Auto-risierung von Ressourcen erfolgt dynamisch und wird strikt durch-gesetzt, bevor der Zugriff über die Koordination zwischen einer Richtlinien-Engine und einem Richtliniendurchsetzungspunkt erlaubt wird	**Dynamische Segmentierung aktiviert durch:** **- ClearPass, PEF mit Aruba Access Points und Gateways** **- Central NetConductor, Policy Manager und Echtzeit-Durchsetzung über Aruba Switches und Gateways**
5. Bi-direktionale Kommunikation mit dem Sicher-heitsökosystem und Reaktion auf Angriffe	Echtzeit- (oder Echtzeit-nahe) Rückmeldung über die Sicher-heitslage von Unternehmensinfor-mationssystemen; Integration mit Sicherheitsinformations- und Ereignisverwaltungssystemen	**ClearPass Policy Manager/ Aruba 360 Security Exchange**

Zusammenfassung

Netzwerklösungen mit integrierter Unterstützung für Zero-Trust- und SASE-Architekturen bieten ein starkes, integriertes Sicherheitsfundament. Ohne umfassende Unterstützung für alle fünf wichtigen Sicherheitsanforderungen sind Unternehmen gezwungen, komplizierte, nicht integrierte Lösungen zusammenzustellen, die Lücken in ihrem Schutz hinterlassen.

Sind Sie startbereit? Weitere Informationen finden Sie unter:
https://www.arubanetworks.com/de/connect-and-protect/



aruba
a Hewlett Packard
Enterprise company

Vielen Dank

ABHÄNGIG VON ABCPARTNER

Partner-Logo

ABCPartner ist ein IT-Lösungsanbieter. Seit mehr als 40 Jahren unterstützen wir Kunden beim Entwerfen, Implementieren und Gebrauch von Technologie, die zum Erfolg führt. Wir konzentrieren uns auf drei Hauptbereiche: Technologieinfrastruktur, Professional Services und Lifecycle Managed Services. Wir haben unseren Hauptsitz in [CITY], [STATE] mit Standorten in [STATE], [COUNTRY].

www.abcpartner.com Telefonnummer: 812-634-1550 417 Main Street, Jasper IN 47546

ebk_security_RM_020122 a00118824dee

Kontaktieren Sie uns unter **www.arubanetworks.com/contact**