Lösungsüberblick



HPE aruba networking

Transparenz und Einblick in die heutigen IoT-Netzwerke

Ein KI-basierter Ansatz zur Sicherung von Netzwerkendpunkten mit Client Insights

HPE GreenLake

Angesichts der rasanten Zunahme der Anzahl und Komplexität von Endpunkt-Clients im Netzwerk haben viele Unternehmen Schwierigkeiten, die wachsende Angriffsfläche zu bewältigen. Mit der zunehmenden Verbreitung des Internets der Dinge (Internet of Things, IoT) und neuen Anwendungsfällen durch Initiativen zur digitalen Transformation hat die Einführung von IoT kritische Best Practices für Sicherheit und Compliance zugunsten einer verbesserten betrieblichen Effizienz und besserer Geschäftsergebnisse überholt.

Aufgrund dieser Umstellung sind sich die IT- und Sicherheitsteams häufig nicht darüber im Klaren, wann, wo und welche Arten neuer Clients mit dem Netzwerk verbunden werden. Aufgrund dieses Mangels an Transparenz können sie keine rechtzeitigen Schutzmaßnahmen für die Sicherheit und die Compliance ergreifen. Best Practices würden erfordern, dass jeder neue Kunde genau identifiziert, aufgenommen und einer Richtlinie zugewiesen wird. Aber die IT-Abteilung wird oftmals überrumpelt.

Schwachpunkte in aktuellen Ansätzen

Die vorhandenen Tools zur Netzwerktransparenz konzentrieren sich auf eine recht enge Gruppe von Clients, die mit einfachen Erkennungs- und Profilierungstechniken leicht zu identifizieren sind. Dazu gehört auch die Suche nach weit verbreiteten Smartphones und Laptops mit gängigen Desktop- oder Mobilbetriebssystemen. Mit diesen Techniken lässt sich häufig ein Smartphone mit Android™ von einem Laptop mit Windows unterscheiden.

Die Identifizierung von Clients wie IoT-Geräten ist aus mehreren Gründen besonders schwierig. Einige dieser Gründe sind:

- Viele IoT-Geräte werden von neuen Anbietern hergestellt und können nicht mithilfe standardisierter Erkennungs- und Profilierungstechniken erfasst werden, was eine genaue Profilierung erschwert.
- Häufig gibt es auch IoT-Geräte, die mit generischer Hardware und Software ausgestattet sind, wie z. B. ein Raspberry Pi, der verschiedene Funktionen erfüllt und daher ebenfalls schwer zu entschlüsseln ist.
- Aufgrund ungenauer oder nur teilweiser Profilerstellung werden Clients häufig als generische Windows- oder Linux®-Clients identifiziert, sodass es schwierig ist, präzise Richtlinien anzuwenden.
- Die meisten Lösungen für die Netzwerktransparenz erfordern Kollektoren oder Agenten. Es ist aber nicht immer möglich, Kollektoren an allen Standorten in großem Umfang einzusetzen.

Die Bedeutung des Kontexts

Dieser Wandel erfordert einen umfassenden Ansatz für die Transparenz der gesamten kabelgebundenen und kabellosen Infrastruktur. Dazu müssen keine Agenten eingesetzt werden, und es ist auch nicht erforderlich, sich bei den Clients anzumelden, um zu sehen, was sie sind. Dies bedeutet das vollständige Verständnis des tatsächlichen Verhaltens eines Geräts – welche Protokolle verwendet werden, auf welche Anwendungen und URLs zugegriffen wird und welche Funktion letztendlich ein Client im Netzwerk ausübt. Bei zahlreichen speziell entwickelten IoT-Geräten wie in einem Krankenhaus oder einem Produktionswerk ist dieser umfassende Kontext die einzige Möglichkeit, sie präzise zu erfassen.

Die HPE Aruba Networking Lösung: KI-basierte Client Insights

Die Netzwerkmanagementlösung HPE Aruba Networking Central Cloud von HPE Aruba Networking enthält jetzt KI-basierte Client Insights, die eine der branchenweit detailliertesten Profilierungen und Transparenzen bieten. Client Insights nutzt die native Infrastruktur-Telemetrie von Access Points, Switches und Gateways sowie von Clients, ohne dass die Installation von physischen Erfassungssystemen oder Agents erforderlich ist. Auf maschinellem Lernen (ML) basierende Klassifizierungsmodelle werden genutzt, um eine Vielzahl von Clients in der gesamten kabelgebundenen und kabellosen Infrastruktur zu identifizieren und ein präzises Profil zu erstellen.

Abbildung 1 zeigt, wie Client Insights ML und Crowdsourcing verwendet, um Client-Typen zu identifizieren.

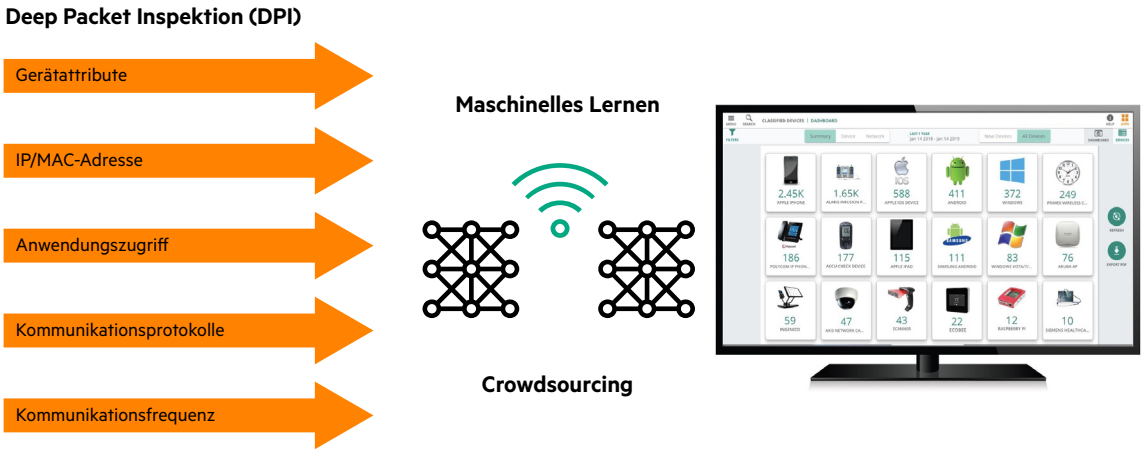


Abbildung 1. Client Insights nutzt fortschrittliches maschinelles Lernen und Crowdsourcing, um jeden Client-Typ genau zu identifizieren.

Diese Leistungsmerkmale werden durch den Einsatz von Deep Packet Inspection (DPI) noch weiter optimiert. Diese liefert zusätzliche Kontext- und Verhaltensinformationen, mit denen sich schwer zu erkennende Geräte, die mit dem Netzwerk verbunden sind, weiter identifizieren lassen. Durch die Nutzung von DPI kann Client Insights eine breitere Palette von Geräteattributen für eine genauere Identifizierung nutzen. Client-Attribute, die Kommunikations- und Verhaltensmuster umfassen, werden analysiert, um dynamisch Cluster ähnlicher Geräte zu bilden.

ML-Modelle werden für ein konstantes Lernen und Aktualisieren dieser Attribute eingesetzt, um so Fingerabdrücke auf dynamische Weise zu aktualisieren und um Klassifizierungsempfehlungen zu bieten. Es wird eine kontrollierte Crowdsourcing-Technologie verwendet, um Fingerabdrücke an mehreren Kundenstandorten zu validieren, bevor sie in die HPE Aruba Networking Klassifikationsdatenbank aufgenommen werden. Dadurch werden Präzision und Vollständigkeit der Klassifizierungsengine gesteigert.

Abbildung 2 zeigt, wie Client Insights Telemetriedaten von HPE Aruba Networking Infrastrukturgeräten verwendet, um Clients zu identifizieren.

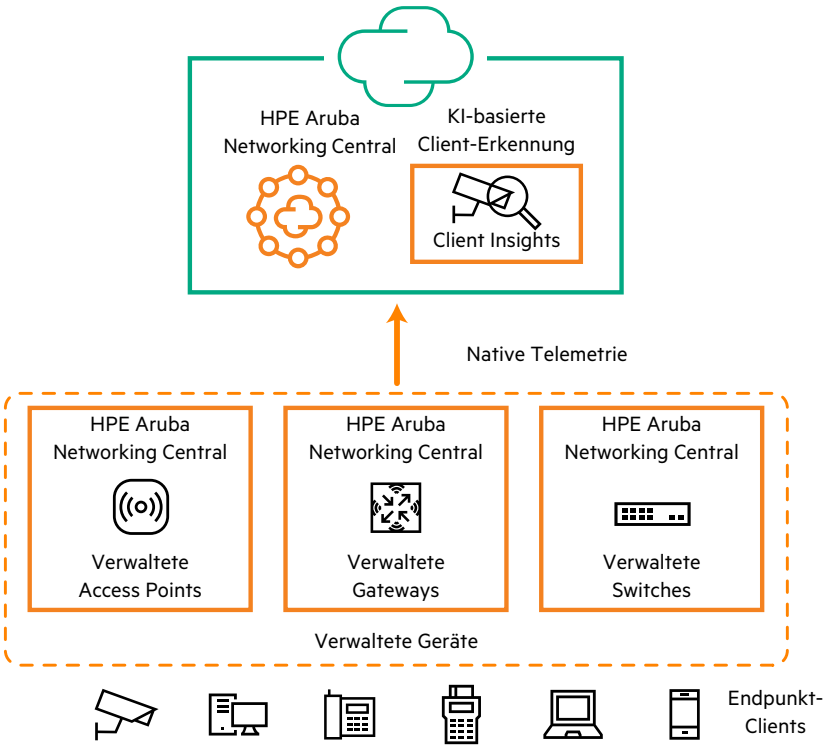


Abbildung 2. Native Telemetriedaten aus der HPE Aruba Networking Infrastruktur werden mithilfe von ML-basierter Klassifizierung zur genauen Identifizierung der verbundenen Clients verwendet

Abbildung 3 zeigt das Dashboard von Client Insights mit verschiedenen Geräten, die unter unterschiedlichen Kategorien aufgelistet sind.

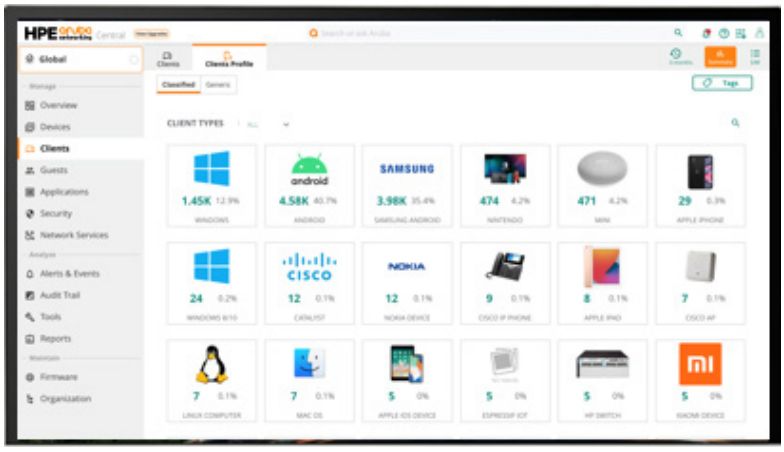


Abbildung 3. Das HPE Aruba Networking Central Cloud Client Insights Dashboard zeigt alle verbundenen Geräte nach Kategorie an.

Für Geräte, die bisher als allgemein angesehen wurden, werden ausgeklügelte ML-Modelle verwendet, um Attribute zu analysieren und ähnliche Clients zusammenzufassen. Da die Clients gruppiert sind, können sie anhand wichtiger Attribute problemlos gekennzeichnet werden. Nach der Kennzeichnung werden neue Clients, die sich mit dem Netzwerk verbinden, automatisch zu ihrem spezifischen Cluster hinzugefügt und entsprechend gekennzeichnet.

In Umgebungen, die nicht von der HPE Aruba Networking Central Cloud verwaltet werden oder für Umgebungen, in denen Netzwerkgeräte von Drittanbietern zum Einsatz kommen, kann HPE Aruba Networking ClearPass Device Insight zur ML-basierten Identifizierung und Profilierung von Clients genutzt werden. HPE Aruba Networking ClearPass Device Insight erfordert die Installation eines physischen oder virtuellen Kollektors und ist separat lizenziert.

Der Wert der automatisierten Durchsetzung von Richtlinien

Transparenz ohne angemessene Kontrolle kann Unternehmen anfällig für Sicherheits- und Compliance-Risiken machen. Client Insights ermöglicht eine kontinuierliche Überwachung der Clients, die in Verbindung mit HPE Aruba Networking ClearPass Policy Manager eine geschlossene End-to-End-Zugriffskontrolle ermöglicht. Dies sorgt für Transparenz und eine automatisierte Durchsetzung von Richtlinien und reduziert den Bedarf an manuellen Eingriffen in kabelgebundenen und kabellosen Netzwerken verschiedener Anbieter erheblich. HPE Aruba Networking ClearPass Device Insight lässt sich außerdem nahtlos in HPE Aruba Networking ClearPass Policy Manager integrieren.

Die automatisierte Durchsetzung von Richtlinien ist für verschiedene Anwendungsfälle geeignet – vom ersten Beitritt eines Clients zum Netzwerk bis hin zu Fällen, in denen ein unerwünschtes Ereignis dazu führt, dass ein Client aufgrund von Sicherheits- oder Compliance-Bedenken entfernt werden muss. Wenn sich beispielsweise eine neue Kamera zum ersten Mal mit dem Netzwerk verbindet, kann sie automatisch als unbekannter Client-Typ erfasst werden, um sicherzustellen, dass sie keine wichtige Infrastruktur oder Server beeinträchtigt. Wenn ein Client kompromittiert wurde oder ein verdächtiges Verhalten zeigt, kann er vollständig in Quarantäne verschoben werden, um ihn zu testen, zu reparieren oder zu ersetzen.

Abbildung 4 zeigt, wie Client Insights in Kombination mit HPE Aruba Networking ClearPass Policy Manager zur automatischen Segmentierung und Durchsetzung funktioniert.

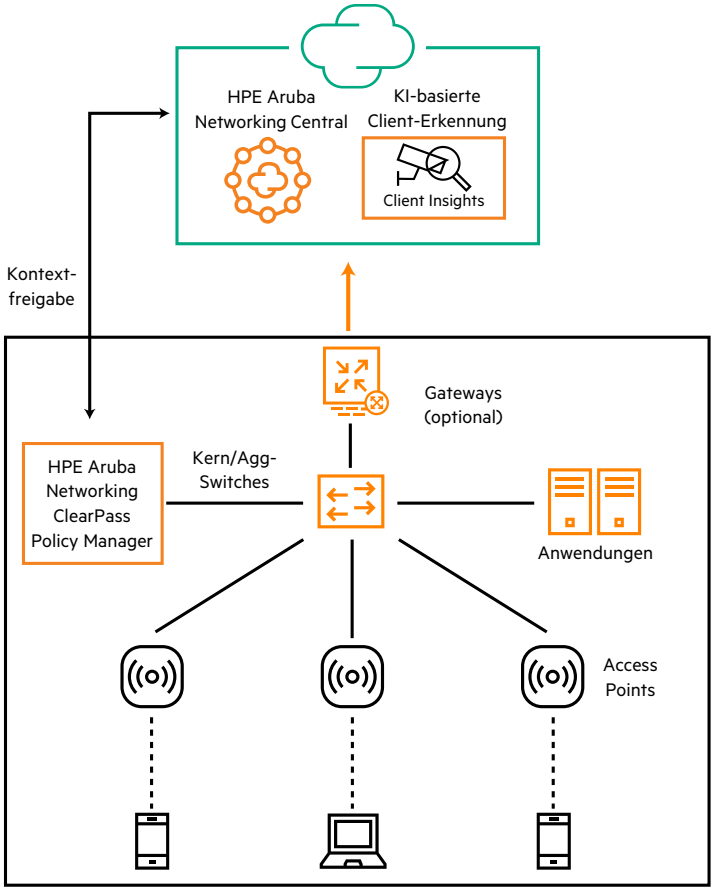
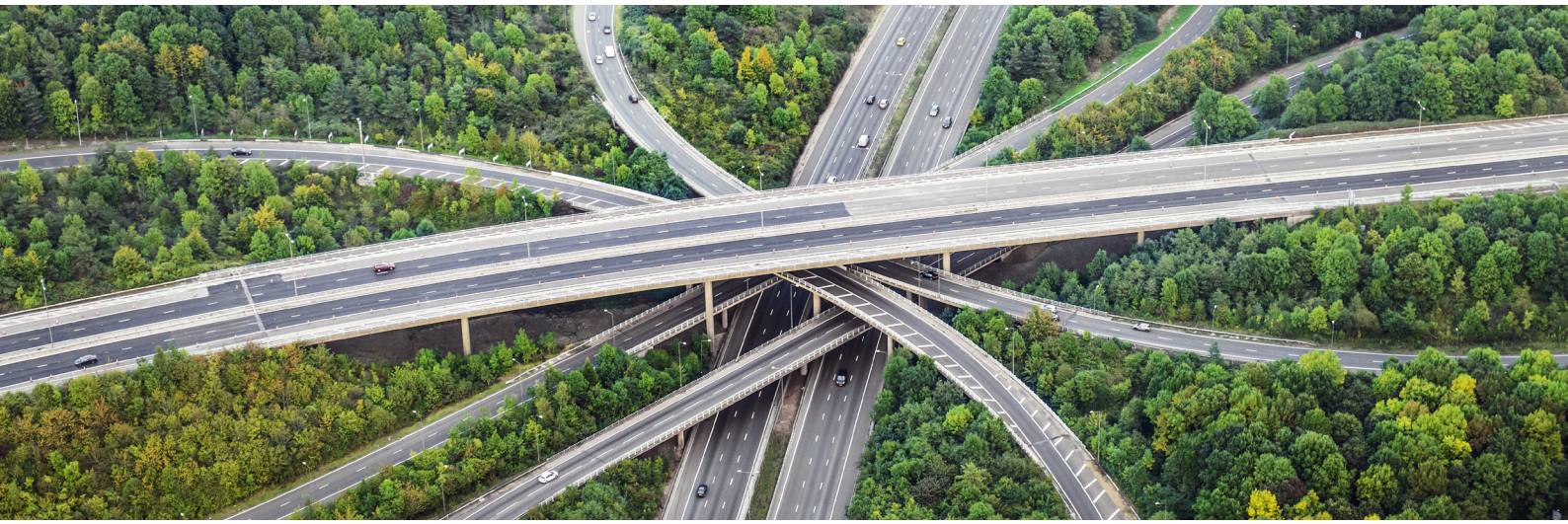


Abbildung 4. Client Insights lässt sich auch mit HPE Aruba Networking ClearPass Policy Manager zur automatischen Segmentierung und Durchsetzung integrieren

HPE Aruba Networking Central Cloud mit Client Insights: Kürzere Time-to-Value

Die Verwaltung geschäftskritischer Anwendungen in zunehmend verteilten Umgebungen steigert die Erwartung an eine verbesserte Verfügbarkeit, Leistung und Sicherheit. HPE Aruba Networking Central Cloud bietet moderne Funktionen, Skalierung, Management und Orchestrierung, einschließlich fortschrittlicher KI/ML- und Sicherheitsfunktionen, mit denen IT-Organisationen aller Größenordnungen überragende Benutzererfahrungen mit erstaunlicher Einfachheit bereitstellen können.

Client Insights nutzt diese einzigartigen Funktionen und die nativen Telemetriedaten aus der Netzwerkinfrastruktur, um den Zeit- und Kostenaufwand für die Bereitstellung zu reduzieren und die Time-to-Value zu beschleunigen. Dieser Ansatz ermöglicht eine zentralisierte, unterbrechungsfreie Erkennung und Überwachung von Netzwerkendpunkten über verteilte Bereitstellungen hinweg und verbessert gleichzeitig die Transparenz und Sicherheit.



Zusammenfassung

Mit der zunehmenden Verbreitung von IoT-Geräten steigt die Zahl der Clients in den Kundennetzwerken weiter an, was neue Anwendungsfälle schafft und gleichzeitig die Angriffsfläche vergrößert. Eine umfassende Transparenz ist unerlässlich, um sicherzustellen, dass die Sicherheit und die Einhaltung von Best Practices mit der betrieblichen Effizienz, die mit der Einführung des IoT einhergeht, Schritt halten.

Die genaue Identifizierung und Erstellung von Kundenprofilen für fein abgestufte rollenbasierte Richtlinien und die Sicherstellung, dass jeder Kunde über das richtige Maß an Zugriffskontrolle zur Verringerung des Gesamtrisikos verfügt, ist nicht mehr nur ein „nice to have“, sondern eine Voraussetzung.

Weitere Informationen finden Sie unter
HPE.com/de/de/Aruba-Central.html

HPE.com besuchen

Chat mit Vertrieb

© Copyright 2025 Hewlett Packard Enterprise Development LP. Die hier enthaltenen Informationen können sich jederzeit ohne vorherige Ankündigung ändern. Neben der gesetzlichen Gewährleistung gilt für Produkte und Services von Hewlett Packard Enterprise (HPE) ausschließlich die Herstellergarantie, die in den Garantieerklärungen für die jeweiligen Produkte und Services explizit genannt wird. Aus dem vorliegenden Dokument sind keine weiterreichenden Garantieansprüche abzuleiten. Hewlett Packard Enterprise haftet nicht für technische oder redaktionelle Fehler oder Auslassungen in diesem Dokument.

Android ist eine Marke von Google LLC. Linux ist in den USA und anderen Ländern eine eingetragene Marke von Linus Torvalds. Windows ist in den USA und/oder anderen Ländern eine Marke oder eingetragene Marke der Microsoft Corporation. Alle genannten Marken von Dritten sind Eigentum der jeweiligen Unternehmen.

a00069032DEE, Rev. 1

Hewlett Packard Enterprise