ARUBA AUF EINEN BLICK

TRANSPARENZ BEI ENDPUNKTEN IN KABELGEBUNDENEN UND KABELLOSEN NETZWERKEN

Die Voraussetzung für erweiterte Sicherheit und Compliance

Früher reichte ein Blick auf den Schreibtisch eines Mitarbeiters, um die mit dem Netzwerk verbundenen Geräte sofort zu erkennen. Diese Zeiten sind längst vorbei. Bring Your Own Device (BYOD) und nicht verwaltete Geräte (z. B. Überwachungskameras) sowie andere immer häufiger im Internet of Things (IoT) verwendete Endpunkte machen es der IT unmöglich, die vollständige Transparenz sicherzustellen.

DIE HERAUSFORDERUNG

Zur Identifizierung der verbundenen Endpunkte sahen die bisher verwendeten Verfahren häufig umfassende Lösungen für die Endpunktverwaltung, Agents und die manuelle Aktualisierung zahlreicher Endpunktdatenbanken vor. Keine dieser Lösungen hat die gewünschten Ergebnisse geliefert, da die IT vollends mit BYOD, der Bereitstellung von Gastzugriffen und nicht autorisierten kabelgebundenen und kabellosen Endpunkten beschäftigt war, die von den Benutzern verwendet werden.

Es wird davon ausgegangen, dass in den nächsten drei Jahren Milliarden von IoT-Geräten Verbindungen mit Netzwerken herstellen werden. Durch die ausführlich dokumentierten Sicherheitslücken der letzten Zeit besteht daher bei den IT-Experten eine große Nachfrage an Funktionen für Transparenz und Berichterstellung. Sie benötigen eine Lösung, die im Gegensatz zu regelmäßigen Updates eine kontinuierliche Überwachung und Profilerstellung ermöglicht – und zwar unabhängig von Standort, Tageszeit und Endpunkttyp.

DIE INTELLIGENTE LÖSUNG ZUR TRANSPARENZ

Die Aruba ClearPass-Familie bietet Netzwerk- und Sicherheitsunternehmen im Vergleich zum Wettbewerb einen einzigartigen Vorteil. Die agentenlose Profilerstellung in Echtzeit kann über eine eigenständige Appliance oder im Rahmen einer umfassenden Lösung zur Durchsetzung von Richtlinien erfolgen.

Beide Lösungen ermöglichen die ständige Identifizierung von Endpunkten und Netzwerkgeräten in kabelgebundenen und kabellosen Netzwerken mit oder ohne AAA als Grundlage, entweder über dynamische oder über statische IP-Adressen. Eine umfassende Dashboard-Ansicht ermöglicht eine einfache Übersicht über alle Endpunkte und deren Anzahl nach Kategorie, Familie und Gerätetyp.

VORTEILE VON ARUBA CLEARPASS

- Automatische Erkennung und Kategorisierung der Endpunkte zur Erfüllung von Sicherheits- und Audit-Anforderungen
- Kontinuierliche Überwachung aller Geräte und Benutzer
- Agentenlose Transparenz ermöglicht die Erkennung von Geräten wie BYOD-Smartphones und IoT
- Gemeinsame Nutzung kontextbezogener Attribute, die die Transparenz auf eine Vielzahl von Sicherheits- und IT-Service-Lösungen ausdehnen
- Keine manuellen Datenbankupdates mehr erforderlich
- Optimierte Netzwerkperformance und Sicherheit durch Informationen zur Anzahl der Endpunkte, zu den Typen und den zugehörigen Attributen

Aruba ClearPass Universal Profiler: Eine eigenständige virtuelle Appliance, die innerhalb von Minuten bereitgestellt und verwendet werden kann. Sie wurde für Unternehmen entwickelt, die noch nicht für eine vollständige NAC-Lösung bereit sind, oder für abgelegene oder eingeschränkte Bereiche, an denen NAC nicht bereitgestellt wird. Diese Appliance lässt sich problemlos an die jeweiligen Skalierungsanforderungen der Unternehmen anpassen.

Aruba ClearPass Policy Manager: Virtuelle oder physische Appliances, die eine umfassende Profilerstellung, die Durchsetzung von Richtlinien in kabelgebundenen und kabellosen Netzwerken mit oder ohne AAA als Grundlage, Gastzugriff, BYOD-Einbindung, Funktionen zur Bewertung von Endpunkten, Berichterstellung und integrierte Sicherheitslösungen von Drittanbietern sowie eine benutzerorientierte Lösungsintegration einschließen.

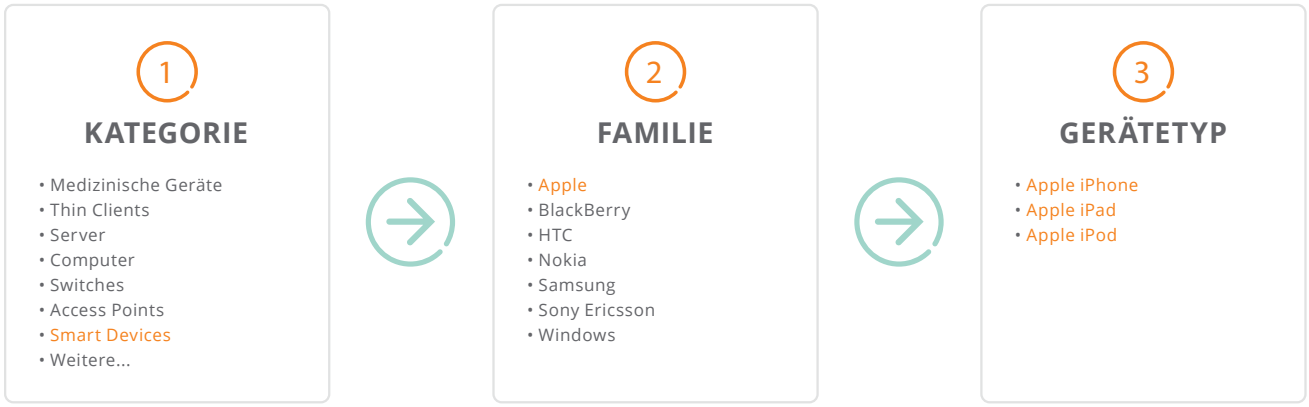

Abbildung 1: Differenzierte Transparenz nach Gerätekategorie, -familie und -typ

Die ClearPass-Familie erkennt Endpunkte mühelos. Dabei werden Attribute identifiziert und ein Profil für diese Attribute erstellt, die wiederum Gerätekategorie, Lieferanten, Betriebssystem, IP-Adresse, Hostname, Besitzer und weitere Informationen ermitteln. Durch die automatisierte und durch die IT anpassbare Klassifizierung der Endpunkte wird sichergestellt, dass neue und unbekannte IoT-Endpunkte in kürzester Zeit der richtigen Gerätefamilie zugeordnet werden, um so die Transparenz und/oder Sicherheit durchzusetzen.

Für zusätzliche Flexibilität stellt ClearPass Optionen für die dynamische Netzwerkerkennung durch Standardnetzwerke oder die Überwachung von SPAN-Anschlüssen bereit. Dies steht im Gegensatz zu den bisher von der IT verwendeten Lösungen für die Netzwerkzugriffssteuerung, die möglicherweise zahlreiche und kostspielige 10G-Anschlüsse für die Spiegelung umfangreicher Endpunktbereitstellungen erforderten.

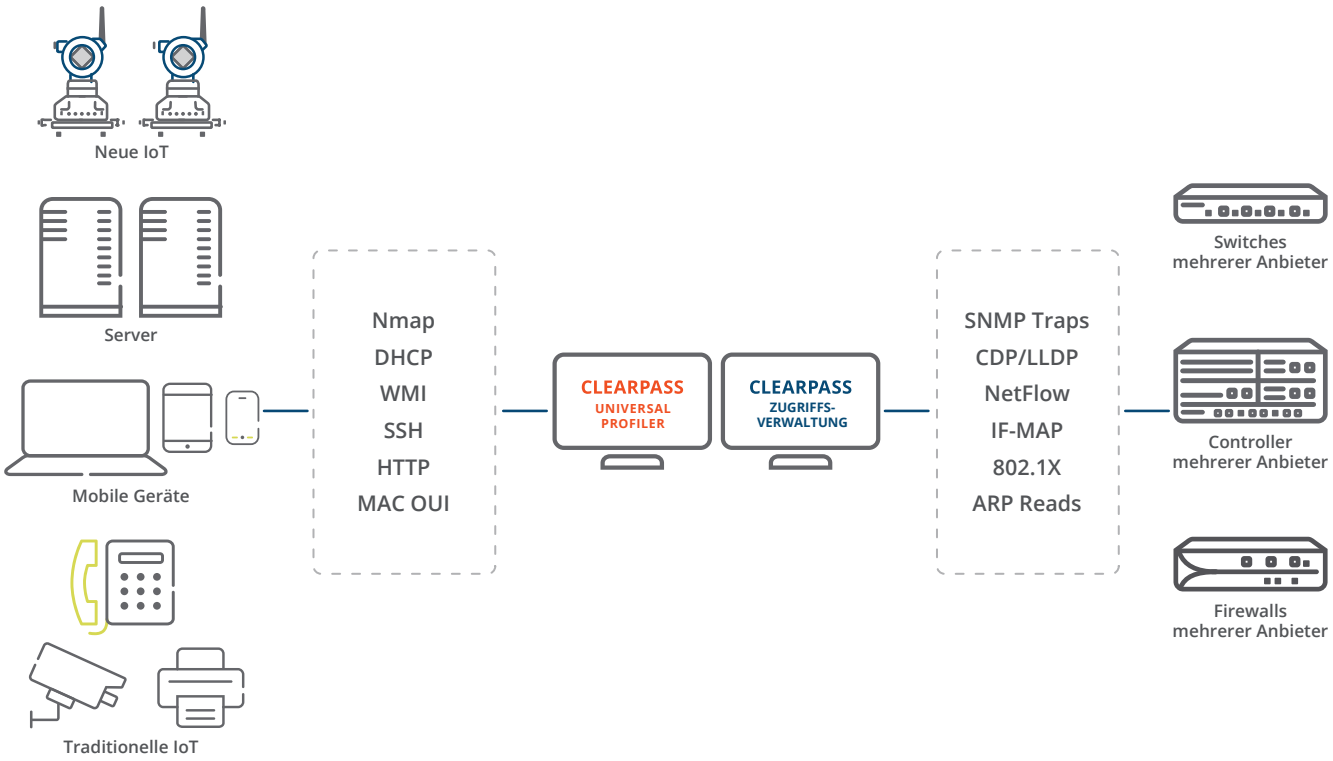

Abbildung 2: Differenzierte Identifizierungs- und Profilerstellungsmethoden

DIFFERENZIERTE ERKENNUNGSMETHODEN

Dank zahlreicher Methoden zur Profilerstellung können differenzierte Endpunktattribute für jedes Gerät gesammelt werden, die zur Identifizierung möglicher Performanceprobleme und Risiken beitragen. Die verbesserte Transparenz und die kontextbezogenen Informationen können sowohl von ClearPass-Lösungen als auch direkt vom ClearPass Policy Manager herangezogen werden, um die Richtlinien hinsichtlich der für den Zugriff berechtigten Geräte und Benutzer zu optimieren und die Reaktionszeit der IT auf potenzielle Gefahren zu senken.

TRANSPARENZ BEI ENDPUNKTEN DURCH LÖSUNGEN VON DRITTANBIETERN

Mit den ClearPass-APIs, Syslog-Benachrichtigungen und der Extensions-Funktion ist der Austausch von Endpunktattributen mit Firewalls, SIEM, Compliance Suites für Endpunkte und anderen Lösungen für das erweiterte Richtlinienmanagement denkbar einfach. Diese Lösungen können die Endpunktattribute erfassen und gemäß den jeweiligen Regeln für die einzelnen Gerätekategorien mit Datenverkehrsmustern abgleichen, um Verbindungen zu optimieren und verdächtigen Datenverkehr zu eliminieren.

WEITERE INFORMATIONEN

Weitere Informationen zu ClearPass Universal Profiler und ClearPass Policy Manager und den einzigartigen Funktionen zur Identifizierung aller Endpunkte, Unterstützung bei der Durchsetzung von Richtlinien und zum besseren Schutz Ihrer kabelgebundenen und kabellosen Netzwerke finden Sie unter www.arubanetworks.com/clearpass.

aruba
a Hewlett Packard Enterprise company

1344 CROSSMAN AVE | SUNNYVALE, CA 94089
1.844.473.2782 | T: 1.408.227.4500 | FAX: 1.408.227.4550 | INFO@ARUBANETWORKS.COM

www.arubanetworks.com IB_Visibility_111616