HPE aruba networking

IoT-Schutz mit Zero Trust-Sicherheit und KI skalieren

im Kampf gegen die Entwicklung von Sicherheitsbedrohungen durch KI und IoT

Der Siegeszug der KI führt für fast alle Unternehmen zu erhöhten Risiken. Daher benötigen die Sicherheitsteams ein neues, vertrauenswürdiges Tool in ihrem Sicherheitsarsenal: ein sicherheitsorientiertes, KI-gestütztes Netzwerk, das die Sicherheit an jedem Verbindungspunkt erhöht und einen umfassenden Schutz vor IoT-basierten Risiken bietet.

HPE GreenLake

94 % der befragten IT-Führungskräfte gaben im Bericht „Architect an AI Advantage“ an, dass ihre Sicherheitsrisiken durch KI gewachsen sind.[1] Viele dieser Bedrohungen dürften den IT-Teams zwar bekannt sein, eine bedeutende Risikoquelle könnte jedoch unentdeckt bleiben: IoT-Geräte.

IoT-Geräte führen zu einem rapiden Wachstum der Angriffsfläche

Seit Jahren spielen IoT-Geräte eine wichtige Rolle in Unternehmen, da sie wertvolle Daten generieren können. Mit dem Aufkommen neuer KI-Modelle, die nach kontextreichen und vielfältigen Daten für das Trainieren und Nutzen von Modellen verlangen, wächst die Menge und Vielfalt der IoT-Geräte, die zu Unternehmensnetzwerken hinzugefügt werden.

Die Anbindung von IoT-Geräten an Unternehmensnetzwerke birgt Risiken für Unternehmen. IoT-Geräte können auf das Internet zugreifen, sind aber oft mit weniger Sicherheitsvorkehrungen ausgestattet als übliche Endbenutzergeräte. Außerdem sind sie häufig „kopflos“, d. h. ohne direkte Benutzerinteraktion kontrollierbar. Erschwerend kommt hinzu, dass diese Geräte oft außerhalb des Zuständigkeitsbereichs von Netzwerk- und Sicherheitsteams angeschlossen und verwaltet werden. Die beschleunigte Einführung von IoT-Geräten in Unternehmensnetzwerken führt zu einer erheblichen Erweiterung der potenziellen Angriffsfläche.

Dieser Trend ist unter Bedrohungsakteuren nicht unbemerkt geblieben. Im Jahr 2024 verzeichneten Forscher einen Anstieg von IoT-Malware-Angriffen um 400 % in verschiedenen Branchen.[2] Angreifer kennen die Sicherheitslücken und Schwachstellen, die durch vernetzte IoT-Geräte in Unternehmensnetzwerken entstehen, und versuchen, diese auszunutzen. Sie nehmen IoT-Geräte ins Visier, um sich unbefugten Zugriff zu verschaffen, Daten zu exfiltrieren und sogar Daten zu beschädigen oder zu zerstören, die für das Training von KI-Modellen verwendet werden – eine Angriffsart, die als „AI Poisoning“ bezeichnet wird.

In Anbetracht dieser Umstände benötigen Unternehmen neue Schutzkonzepte. Als Ausgangspunkt können umfassende Sichtbarkeit und Beobachtbarkeit dazu beitragen, das Verhalten von Entitäten (einschließlich IoT-Geräte) im Netzwerk genau zu identifizieren und zu analysieren. Unternehmen müssen auch in der Lage sein, Richtlinien zu definieren, zu nutzen und durchzusetzen, um sich vor Bedrohungen in dem großen Umfang zu schützen, den die umfassende Einführung des IoT erfordert.

[1] HPE, Architect an AI Advantage

[2] Deloitte, Global Cyber Threat Intelligence (CTI): Annual Cyber Threat Trends, März 2024

Bekämpfung von Bedrohungen durch KI mit einem KI-basierten Security-first-Netzwerk

Für den Erfolg von Unternehmen im KI-Zeitalter spielt das Netzwerk eine entscheidende Rolle. Ob es sich um herkömmliche On-Premises-Verbindungen oder das Internet und die Cloud handelt, die Mission des Netzwerks ist es, Daten und Ressourcen zu sammeln, zu sichern und nach Bedarf jederzeit und überall zur Verfügung zu stellen. Angesichts der Bedrohungslage und der Allgegenwärtigkeit des Netzwerks im KI-Zeitalter muss es noch eine weitere Funktion erfüllen: Sicherheit.

KI-basiertes Security-first-Networking von HPE Aruba Networking kann dazu beitragen. Das auf Zero Trust-Sicherheitsgrundsätzen basierende, KI-basierte Netzwerk bietet eine gemeinsame Grundlage, die Sicherheits- und Netzwerkteams nutzen können, um einzigartige Benutzererlebnisse zu schaffen und die Einführung von KI zu unterstützen – ohne den Schutz vor Cyberangriffen zu beeinträchtigen. Durch die Kombination von KI-basierten Identitätsinformationen und -analysen, Sicherheitsrichtlinien und Edge-to-Cloud-Durchsetzung schützt HPE Aruba Networking Daten, Infrastrukturen und Anwendungen für KI in großem Umfang – was immer wichtiger wird, weil KI-Ressourcen im gesamten Unternehmen, einschließlich IoT-Geräten und -Daten, zunehmend zu Angriffszielen werden. Mit den HPE Aruba Networking-Lösungen erhalten Unternehmen KI-basierte Transparenz, Richtlinienverwaltung, Bedrohungsabwehr und Zugriffskontrolle über eine zentrale Kontrolloberfläche.

Mithilfe von Netzwerktelemetrie und Einblicken, die auf dem branchenführenden Data Lake basieren,[1] liefert HPE Aruba Networking eine Sicherheitskomplettlösung mit Transparenz, Netzwerkerkennung und Reaktion direkt in HPE Aruba Networking Central.[2] Damit können Unternehmen sicher erkennen, welche Geräte mit dem Netzwerk verbunden sind, das Geräteverhalten beobachten und analysieren, Anomalien erkennen und Maßnahmen ergreifen – alles von KI unterstützt und in HPE Aruba Networking Central bereitgestellt.

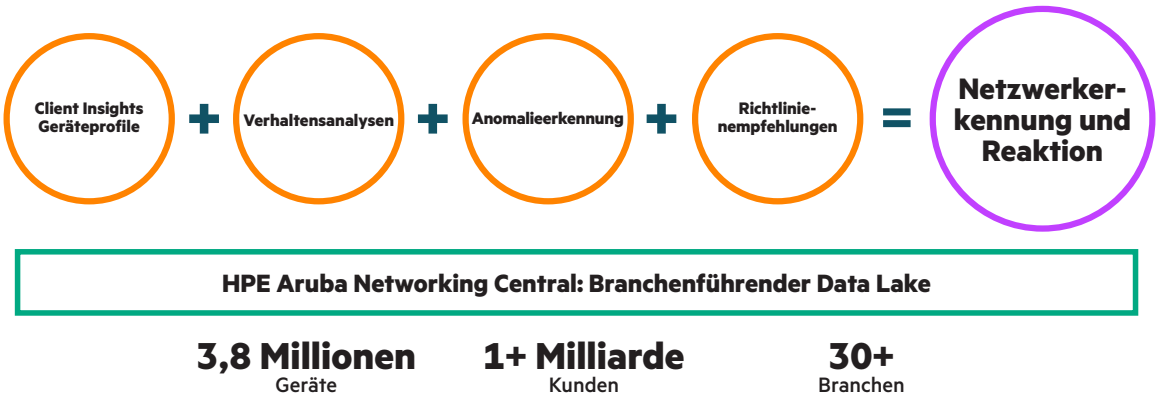

Abbildung 1. KI-gestützte Netzwerkerkennung und Reaktion, einschließlich präziser Geräteidentifizierung, Erkennung von Anomalien und rollenbasierter Richtlinienempfehlungen

KI-basierte Geräteprofile

Aktuelle Ansätze für Netzwerktransparenz sind oft unzureichend, wenn es um die Identifizierung von IoT-Geräten geht. IoT-Geräte, die von spezialisierten Anbietern hergestellt werden, folgen möglicherweise nicht den Standardmethoden für die Profilerstellung. Einige IoT-Geräte verwenden generische Hardware und Software, was eine genaue Profilerstellung erschwert. Aber eine unscharfe Profilerstellung kann zu generischen Kategorisierungen wie „Windows“ oder „Linux®“ führen, was die Durchsetzung von Richtlinien erschwert. Darüber hinaus beruhen die meisten Transparenzlösungen auf Collectors oder Agenten, die sich nur schwer in großem Umfang an mehreren Standorten einsetzen lassen.

HPE Aruba Networking löst diese Probleme, indem es mit KI-basierten Client Insights, einer in HPE Aruba Networking Central integrierten Sicherheitslösung, die branchenweit detaillierteste Profilerstellung und Transparenz bietet.[3] Client Insights nutzt native Infrastruktur-Telemetrie von Access Points, Switches, Gateways und Clients, ohne dass die Installation von physischen Collectors oder Agenten erforderlich ist. ML-basierte Klassifizierungsmodelle werden genutzt, um eine Vielzahl von Clients in der gesamten kabelgebundenen und kabellosen Infrastruktur zu identifizieren und ein präzises Profil zu erstellen.

[1] HPE Aruba Networking Central – Datenblatt

[2] Erweiterte Funktionen für Transparenz, Netzwerkerkennung und Reaktion sind im neuen HPE Aruba Networking Central mit einer Advanced-Lizenz verfügbar.

[3] Visibility and insight for today's IoT driven networks, HPE

Die KI-basierte Profilerstellung ergänzt andere KI-basierte Tools in HPE Aruba Networking Central, um die Sicherheit zu verbessern. HPE Aruba Networking nutzt beispielsweise AIOps und Modelle für maschinelles Lernen, um APs in Zeiten geringer Aktivität intelligent in den Ruhezustand zu versetzen, wodurch potenzielle Einstiegspunkte für bösartige Aktivitäten eliminiert und Angriffsflächen verkleinert werden.

Diese Leistungsmerkmale werden durch den Einsatz einer 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 wie Kommunikations- und Verhaltensmuster werden analysiert, um dynamisch Cluster ähnlicher Geräte zu bilden. Modelle für maschinelles Lernen können Fingerabdrücke dynamisch aktualisieren und Klassifizierungsempfehlungen abgeben.

Durch die Anwendung von KI und ML auf Daten, die von über 1 Milliarde profilierter Clients gesammelt wurden, kann Client Insights angeschlossene Geräte mit einer Profilierungsgenauigkeit von bis zu 99 % bei bekannten Clients und <5 % bei unbekannten Clients identifizieren.[1]

KI-basierte Verhaltensanalyse

Zu den mit IoT-Geräten verbundenen Gefahren gehört die Neigung, sie einmal zu konfigurieren und danach zu vergessen. Ki-basierte IoT-Erkennungs- und Klassifizierungsfunktionen innerhalb von HPE Aruba Networking Central helfen dabei, IoT-Sicherheitsrisiken durch verbesserte Sichtbarkeit und Identifizierung der mit dem Netzwerk verbundenen Geräte sowie durch kontinuierliche Überwachung auf ungewöhnliches oder unzulässiges Verhalten zu vermeiden.

HPE Aruba Networking Central kann dynamische Geräteattribute analysieren, z. B. Übertragungsmuster und Verhaltensmerkmale wie Verbindungsstatus und Präsenz im Netzwerk, um IoT- und herkömmliche Geräte genau zu kategorisieren und zu identifizieren. Sobald ein IoT-Gerät identifiziert ist, verwendet HPE Aruba Networking Central künstliche Intelligenz, um grundlegende Verhaltensmuster für das Gerät zu erstellen.

Das KI-basierte Erstellen grundlegender Verhaltensmuster auf der Ebene einzelner Geräte erleichtert die Erkennung von Anomalien, die auf eine Kompromittierung und Angriffe hinweisen können.

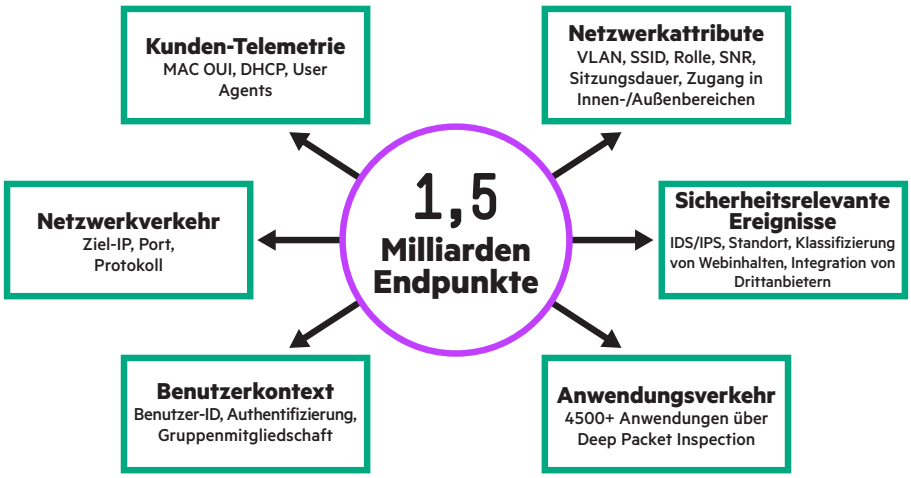

Abbildung 2. Umfassende Inline-Netzwerktelemetrie für HPE Aruba Networking Central

KI-basierte Erkennung von Netzwerkanomalien

Die Erkennung von Anomalien ist bekanntermaßen schwierig. Geringe Schwankungen im Verhalten einzelner Geräte können zu Fehlalarmen führen, was zur Ermüdung durch Warnmeldungen beiträgt und die Erkennung tatsächlicher Sicherheitsprobleme erschwert. Die Betrachtung von Daten in aggregierter Form hingegen kann tatsächliche Anzeichen für Angriffe verschleiern.

[1] AI-powered Network Infrastructure: The answer to IT Efficiency, HPE

Beispiele für die Anomalieerkennung

- **Abnormales Hochladen von Daten**
- **Abnormales Herunterladen von Daten**
- **Kommunikation mit eingeschränkten/unzulässigen Ländern**

Die in HPE Aruba Networking integrierte Anomalieerkennung geht auf diese Bedenken ein und macht es für Netzwerk- und Sicherheitsteams einfacher, potenzielle Kompromittierungen von IoT-Geräten mit hohem Risiko zu erkennen. HPE Aruba Networking Central nutzt seinen branchenführenden Observability Data Lake und wendet KI auf umfassende Gerätetelemetrie an, um anomales Verhalten zu erkennen und Untersuchungen mit Alarmen auszulösen. Netzwerk- und Sicherheitsteams können diesen von einem KI-Modell gesteuerten Ansatz durch die Festlegung von Warnschwellenwerten ergänzen und die Empfindlichkeit der Erkennung an die Präferenzen des Unternehmens anpassen.

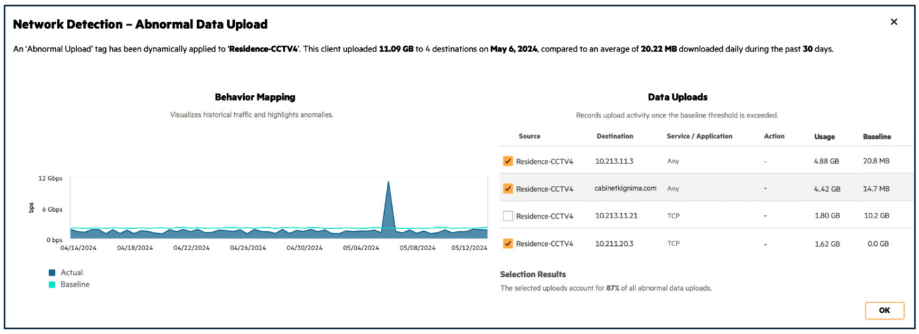

Abbildung 3. Die KI-gestützte Erkennung von Anomalien liefert konkrete Informationen, die den Bediener bei der Entscheidung über die nächste Aktion unterstützen. **Hinweis:** Der Illustration dienende Screenshots, Änderungen vorbehalten.

KI ermöglicht eine präzise Erkennung von Anomalien für eine höhere Genauigkeit und liefert qualitativ hochwertigere Warnungen für Untersuchungen und potenziell weniger Fehlalarme.

Rollen definieren Berechtigungen auf der Grundlage von Stellenprofilen oder Gerätetypen und stellen sicher, dass nur auf relevante Ressourcen zugegriffen werden kann. Rollenbasierte Richtlinien folgen den Benutzern im gesamten Netzwerk und werden einheitlich auf drahtlose, kabelgebundene und Remote-Verbindungen angewendet. Die dynamische Segmentierung von HPE Aruba Networking segmentiert den Datenverkehr auf der Grundlage der jeweiligen Rolle und gewährleistet so den Zugriff mit den geringsten Rechten und passt den Zugriff bei Bedarf an, um die Sicherheit zu gewährleisten.

KI-basierte Richtlinienempfehlungen und Vorschau

Die Änderung von Richtlinien ist oft ein entscheidender Schritt, um potenzielle Angriffe abzufangen. Da Richtlinienänderungen weitreichende und manchmal unbeabsichtigte Folgen haben, sind viele Netzwerk- und Sicherheitsteams der Automatisierung von Richtlinienänderungen gegenüber skeptisch. Das Testen von Strategien in Echtzeit kann jedoch neue Probleme aufwerfen und die Reaktion auf Bedrohungen verlangsamen.

KI-basierte Tools zur Richtlinienoptimierung in HPE Aruba Networking Central helfen Unternehmen, schneller auf Bedrohungen zu reagieren, ohne den Betrieb zu unterbrechen. Netzwerk- und Sicherheitsteams können rollenbasierte Richtlinienempfehlungen überprüfen, die auf den Zero Trust-Sicherheitsprinzipien für Zugriffe mit möglichst geringen Berechtigungen basieren.

Um sicherzustellen, dass die Empfehlungen den Netzwerkbetrieb nicht stören, können die Teams die Auswirkungen ihrer Sicherheitsrichtlinienänderungen vor der Implementierung im Rahmen ihres Durchsetzungs- und Reaktionsworkflows überprüfen. Die KI-basierte Richtlinienvorschau bietet Einblicke in die Auswirkungen auf Netzwerke, Geräte und Anwendungen sowie aussagekräftige Visualisierungen, so dass Teams flexibel entscheiden können, wie sie Richtlinienänderungen handhaben und bewerten. Die Teams können bei Bedarf Änderungen an den empfohlenen Richtlinien vornehmen und diese dann per Mausklick aktualisieren, womit sie dem Kreislauf für die Netzwerkerkennung und -reaktion schließen.

KI-basierte Richtlinienempfehlungen tragen zum Schutz vor Bedrohungen bei, ohne den Netzwerkbetrieb unnötig zu unterbrechen.

Die KI-basierte verhaltensbasierte NDR von HPE Aruba Networking Central erfüllt die im NIST Cybersecurity Framework 2.0 beschriebenen Funktionen Identifizieren, Schützen, Erkennen, Reagieren, Wiederherstellen.

KI und Automatisierung bei der Erkennung und Abwehr von Bedrohungen

Bei Sicherheitsuntersuchungen und -maßnahmen sind Kontextinformationen und Kontrolle von entscheidender Bedeutung, um Netzwerk- und Sicherheitsteams in die Lage zu versetzen, wichtige Entscheidungen über Schutzvorkehrungen zu treffen.

Funktionen für Transparenz, Netzwerkerkennung und Reaktion sind als zustimmungsbasierte Sicherheitslösung in HPE Aruba Networking Central integriert und bieten den Teams die notwendigen Tools und Erkenntnisse für eine fundierte Entscheidungsfindung bei jedem Schritt. Dieser Ansatz beseitigt den Mangel an Transparenz, der mit autonomen Änderungen durch vollautomatische Tools verbunden ist. Am wichtigsten ist jedoch, dass das Urteil von Experten weiterhin entscheidend bleibt, um sicherzustellen, dass bei KI-basierten Sicherheitsentscheidungen ein Mensch involviert ist.

Fazit

Ungesicherte IoT-Geräte im Netzwerk stellen einen blinden Fleck in den Sicherheitsstrategien der meisten Unternehmen dar. IoT-Geräte können für die Initiierung größerer Netzwerkangriffe ausgenutzt werden und tragen somit auch am stärksten zur Vergrößerung der Angriffsflächen bei.

Die in HPE Aruba Networking Central integrierte KI-basierte, auf Verhaltensanalysen aufbauende Closed-Loop-NDR trägt zur Minderung der von IoT-Geräten ausgehenden Risiken bei und bietet verbesserte Sichtbarkeit und Profilerstellung, Beobachtbarkeit, Erkennung von Sicherheitsbedrohungen und richtlinienbasierte Reaktionen. Integrierte Sicherheitslösungen nutzen die Leistung von KI und dem branchenführenden HPE Aruba Networking Central Data Lake, um Unternehmen bei der Stärkung ihrer Cyberabwehr zu unterstützen, mit der sie sich vor neuen Bedrohungen in großem Umfang schützen.

Weitere Informationen

hpe.com/de/de/networking

HPE.com besuchen

Chat mit Vertrieb

© Copyright 2024 Hewlett Packard Enterprise Development LP. Die enthaltenen Informationen können jederzeit ohne vorherige Ankündigung geändert werden. 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.

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.

SO_Scale-IoT-Zero-Trust_A4_RB_111524 a00141780DEE

Hewlett Packard Enterprise