FORESCOUT
Active Defense for the Enterprise of Things.

IoT-Sicherheit

Wählen Sie einen flexiblen Zero-Trust-Ansatz zur Absicherung neuartiger Geräte im Enterprise of Things

IoT-Geräte (Internet of Things) bleiben in den Unternehmensnetzwerken häufig verborgen, da sie im Gegensatz zu herkömmlichen Systemen nicht problemlos überwacht werden können und nur selten Software-Agenten unterstützen. Dadurch wachsen die Angriffsfläche und die Risiken für das Unternehmen deutlich, da sie kompromittiert und als Eintrittspunkte in anfällige Netzwerke genutzt werden können. Unternehmen benötigen eine Sicherheitslösung, die jedes IoT-Gerät in heterogenen Netzwerken permanent identifizieren, segmentieren und geltende Vorschriften durchsetzen kann.

IoT-Geräte: Sind sie das Risiko wert?

IoT-Geräte sind wertvolle und häufig kritische Assets in Unternehmen. Sie bieten Vorteile in puncto Produktivität, Produkt- und Service-Qualität und Geschäftsergebnis. 63 % aller Unternehmen rechnen damit, dass sich ihre IoT-Projekte innerhalb von drei Jahren amortisieren.[2] Raffinierte, finanziell gut ausgestattete Kriminelle suchen kontinuierlich nach Bereichen, die sich leicht ausnutzen lassen. Lücken in der IoT-Transparenz und -Sicherheit können zu Ausfallzeiten, Datenkompromittierung, Verlust von geistigem Eigentum und Rufschädigungen führen. Bedenken Sie dazu diese Fakten:

- Laut einer aktuellen Umfrage des Ponemon Institute rechnen fast 90 % der Unternehmen in den nächsten zwei Jahren mit Cyberangriffen oder Datenschutzverletzungen, die durch unsichere IoT-Geräte verursacht werden.[3]
- Bis 2023 wird der durchschnittliche CIO für mehr als dreimal so viele Endgeräte verantwortlich sein, als dies 2018 der Fall war.[4]

DEFINITION VON ZERO TRUST

Das Zero-Trust-Modell von Forrester beschreibt das Konzept und die Architektur für Unternehmenssicherheit. Grundsätzlich geht es bei Zero Trust um die Etablierung von Vertrauen, indem gewährleistet wird, dass ein vertrauenswürdiger Benutzer an einem vertrauenswürdigen Gerät über vertrauenswürdige Zugangsrechte verfügt. Jeder einzelne Benutzer kann dabei nur auf die Unternehmensressourcen zugreifen, die für die Erledigung ihrer entsprechenden Aufgaben benötigt werden. Laut Forrester[1] sind für die Implementierung effektiver Zero-Trust-Richtlinien folgende Schritte erforderlich:

- Umgestaltung des Netzwerks in sichere Zonen
- Stärkung der Datensicherheit mithilfe von Verschleierungstechniken
- Begrenzung der Risiken, welche durch zu weitreichende Zugangsrechte entstehen
- Deutlich verbesserte Erkennung und Behebung von Sicherheitszwischenfällen durch Analyse und Automatisierung

forescout.com/platform/IoT info-dach@forescout.com Tel (weltweit) +1-408-213-3191

Im heutigen Enterprise of Things (EoT), bei dem sich unzählige IT-, IoT- und OT-Geräte (operative Technologie) verbinden und interagieren, benötigen Unternehmen eine Sicherheitslösung, die alle IoT- und andere per IP-Adresse vernetzten Geräte sichtbar und kontrollierbar macht und den Zero-Trust-Ansatz für das Netzwerk umsetzt. Andernfalls könnte jedes Gerät kompromittiert und für böswillige Zwecke missbraucht werden.

Der Zero-Trust-Ansatz von Forescout

Forescout ist der Meinung, dass IoT-Sicherheit auf einem Zero-Trust-Ansatz basieren muss, der vollständige Gerätetransparenz, proaktive Netzwerksegmentierung und Zugriffssteuerung nach dem Least-Privilege-Prinzip für alle digitalen Assets – Geräte, Benutzer, Anwendungen und Workloads – kombiniert. Die Forescout-Plattform ermöglicht die effektive Verwaltung der operativen, Cyber- und Konformitätsrisiken Ihrer gesamten EoT-Umgebung. Dazu bietet sie folgende Möglichkeiten:

- Bereitstellung vollständiger Transparenz zu nicht verwalteten IoT-, OT- und IoMT-Geräten (Internet of Medical Things) sowie allen per IP-Adresse vernetzten Geräten
- Einstufung und Identifizierung von IoT-Geräten mit werksseitig vorgegebenen oder schwachen Anmeldeinformationen sowie Automatisierung von Richtlinienaktionen zur Durchsetzung starker Kennwörter
- Bereitstellung von Echtzeitinformationen zur Kommunikation von IoT-Geräten und zu riskantem Verhalten innerhalb des Netzwerks
- Segmentierung der Geräte in vertrauenswürdige Zonen per Durchsetzung des Least-Privilege-Zugriffs entsprechend der Zero-Trust-Richtlinie
- Automatisierte zentrale Koordinierung der Zero-Trust-Richtlinie für Umgebungen mit Produkten mehrerer Anbieter und mehrerer Netzwerkdomänen
- Aufbrechen von Verwaltungssilos zur Beschleunigung der Behebungsmaßnahmen und optimalen Nutzung Ihrer Investitionen in andere Sicherheitslösungen
- Unterstützung von Anbietern im Gesundheitswesen durch proaktive Erkennung und Verringerung von Schwachstellen und Bedrohungen, detaillierte Durchsetzung von Segmentierungs- und Netzwerkzugriffsrichtlinien, Eindämmung von Bedrohungen für medizinische Geräte und Vereinfachung der Behebungsmaßnahmen – ermöglicht durch eine enge Integration mit Medigate

“Forescout ist der Anbieter für Zero-Trust-Sicherheit für IoT und OT. Die Absicherung von IoT- und OT-Geräten gehört zu den größten Herausforderungen im Unternehmen. Genau dieser Bereich ist der Schwerpunkt von Forescout – und die Möglichkeiten der Plattform dieses Anbieters für IoT/OT-Sicherheit lassen die Mitbewerber weit hinter sich.”

THE FORRESTER WAVE: ZERO TRUST EXTENDED ECOSYSTEM PLATFORM PROVIDERS (PLATTFORMANBIETER FÜR ZERO TRUST EXTENDED-ÖKOSYSTEME), FORRESTER RESEARCH, OKTOBER 2019

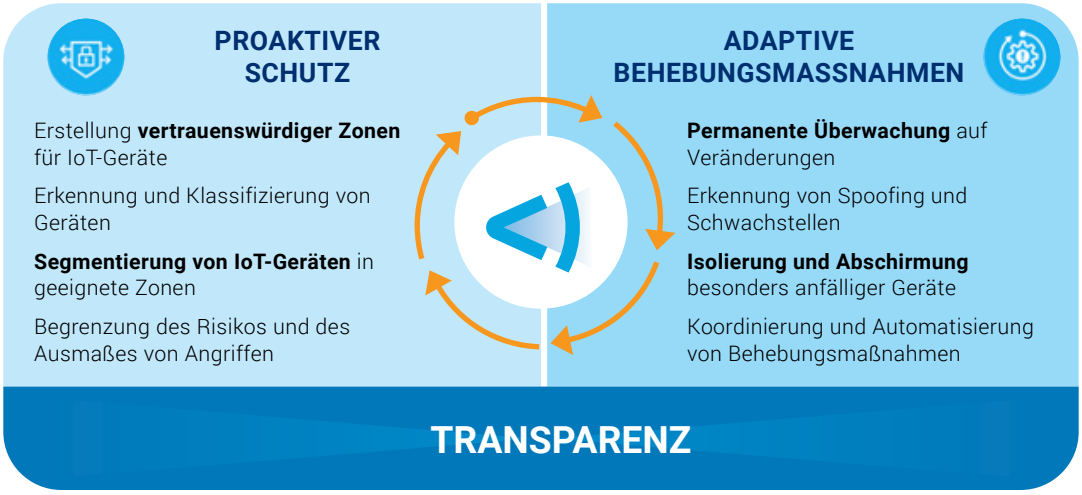

Abbildung 1. Forescout schützt aktiv alle Geräte in Ihrer EoT-Umgebung, indem jedes vernetzte Gerät identifiziert und segmentiert wird und geltende Vorschriften durchgesetzt werden

Erkennung und Klassifizierung aller per IP-Adresse vernetzten Geräte

Sie erhalten vollständige Transparenz sowie Gerätekontext zu allen Endgeräten in Ihrer gesamten heterogenen Umgebung – einschließlich IoT, OT und kritischer Infrastruktur. Die Forescout-Plattform bietet folgende Möglichkeiten:

- Permanente Erkennung aller per IP-Adresse vernetzten physischen und virtuellen Geräte, sobald sich diese mit Ihrem Netzwerk verbinden – hierfür sind keine Agenten erforderlich
- Detaillierte Transparenz zu diesen Geräten dank einer Kombination aus mehr als 20 aktiven und passiven Erkennungs-, Profilerstellungs- und Klassifizierungstechniken
- Nutzung der Forescout Device Cloud, dem weltweit größten Crowdsourcing-Data Lake für Geräteinformationen, als branchenübergreifende zentrale Informationsquelle, einschließlich Fingerprints sowie Verhaltens- und Risikoprofilen zu mehr als 12 Millionen Geräten

Implementierung dynamischer Netzwerksegmentierung und automatisierter Kontrollen

In heutigen heterogenen EoT-Umgebungen müssen Unternehmen, die das Zero-Trust-Modell implementieren, Netzwerksegmentierung umsetzen und Behebungsmaßnahmen auf Vorfälle im gesamten EoT koordinieren können. Forescout bietet folgende Möglichkeiten:

- Korrelation des Zugriffs mit Benutzeridentitäten (Wer macht was, wo, wann und warum?)
- Zuweisung von Geräten zu dynamischen Netzwerksegmenten basierend auf Richtlinien und Echtzeitkontext
- Zuordnung von Datenflüssen zur Erstellung von Segmentierungsrichtlinien und Simulation dieser Richtlinienanwendung, um Arbeitsausfälle zu vermeiden
- Automatisierte Segmentierung zur Verringerung des operativen und Cyber-Risikos

Koordinierung der Sicherheit und Einhaltung von Konformitätsrichtlinien

Die meisten Unternehmen verwenden teure Sicherheitslösungen, die nur für einen Zweck ausgelegt sind und weder Erkenntnisse mit anderen Lösungen austauschen noch die Koordinierung von Behebungsmaßnahmen unterstützen. Mit Forescout können Sie diese Ineffizienz hinter sich lassen. Forescout eyeExtend-Produkte tauschen den Gerätekontext zwischen der Forescout-Plattform und anderen IT- und Sicherheitsprodukten aus, um Workflows und Richtlinieneinhaltung lösungsübergreifend zu automatisieren. Diese Koordinierungsfunktionen bieten folgende Möglichkeiten:

- Steigerung der IoT-Sicherheit und der allgemeinen Gerätekonformität
- Reduzierung der mittleren Erkennungs- und Reaktionszeit
- Steigerung der Rendite mit den vorhandenen Tools
- Automatisierung der Updates für Ihre Verwaltungsdatenbank für Konfigurationsdaten (CMDB) zur Vermeidung zeitaufwändiger und fehleranfälliger manueller Bestandspflege

"Jetzt wissen wir, was sich in unserem Netzwerk befindet, einschließlich IoT-Geräten wie Druckern, VoIP-Telefonen und Sicherheitskameras. Forescout klassifiziert das Gerät und platziert es im entsprechenden VLAN-Segment."

– KEN COMPRES, SENIOR NETWORK SECURITY AND INTEGRATION ENGINEER/CSO, HILLSBOROUGH COMMUNITY

1 Five Steps to a Zero Trust Network (Fünf Schritte zum Zero-Trust-Netzwerk), Roadmap Report, Forrester Research, Oktober 2018

2 A New Roadmap for Third Party IoT Risk Management, Benchmark Study (Eine neue Risikomanagement-Roadmap für Drittanbieter-IoT, eine Benchmark-Untersuchung), Ponemon Institute, Sabine Zimmer, 3. Juni 2020

3 Internet of Things: Unlocking True Business Potential (Das Internet der Dinge: So nutzen Sie das wahre geschäftliche Potenzial), Gartner

4 Gartner Top Strategic IoT Trends and Technologies Through 2023 (Wichtigste strategische IoT-Trends und -Technologien von Gartner bis 2023), September 2018

Sehen Sie Ihre Geräte nicht nur: Schützen Sie sie.

Kontaktieren Sie uns noch heute, damit Sie Ihr Enterprise of Things aktiv verteidigen können.

forescout.com/platform/IoT info-dach@forescout.com Tel (weltweit) +1-408-213-3191

FORESCOUT
Active Defense for the Enterprise of Things.

Forescout Technologies, Inc.
190 W Tasman Dr.
San Jose, CA 95134 USA

info-dach@forescout.com
Tel (Intl) +1-408-213-3191
Support +1-708-237-6591

Weitere Informationen finden Sie unter Forescout.de