FORESCOUT
Active Defense for the Enterprise of Things™

Einfache und störungsfreie Zero-Trust-Segmentierung für OT

Sicherheit für erweiterte OT-Netzwerke mit fortschrittlichem Risikomanagement und dynamischer Segmentierung

Herkömmliche Ansätze zur Absicherung von OT-Geräten (operative Technologie) in OT- und ICS-Netzwerken basieren auf der Trennung industrieller Anlagen von IT-Netzwerken und Remote-Benutzern. Da OT-Unternehmen ihre Infrastruktur mit neuen Technologien wie Cloud SCADA, DCS und MES (Manufacturing Execution Systems) modernisieren, sind die bisherigen, auf Zonen basierenden Strategien nicht mehr in der Lage, die OT-Umgebungen ausreichend zu schützen.

OT-Umgebungen sind mit folgenden Herausforderungen verbunden:

- Risiko lateraler Bewegungen von Malware und böswilligen Akteuren, zonenübergreifende Bedrohungen aus der IT sowie Remote-Benutzer, die die Cyber-physische und OT-Infrastruktur gefährden
- Erkennung und Verhinderung von Malware-Ausbreitung und zonenübergreifenden Bedrohungen für die Cyber-physische und OT-Infrastruktur
- Komplexität der Betriebsabläufe aufgrund mehrerer Anbieter und uneinheitliche Segmentierungskontrollen in erweiterten OT-Umgebungen

Die Lösung von Forescout: Erstklassig bei OT

Wenn Ihnen diese Herausforderungen bekannt vorkommen, ist jetzt der richtige Zeitpunkt für einen genauen Blick die Forescout-Lösung. Sie vereinfacht die Zero-Trust-Segmentierung und optimiert das Risikomanagement für IT-, OT- und ICS-Geräte in Ihrem heterogenen Enterprise of Things (Unternehmen der Dinge, EoT). Die Forescout-Plattform bietet folgende Möglichkeiten:

- **Beschleunigte Zero-Trust-Segmentierung** für IT- und OT-Gruppen
- **Sofortiger Echtzeitüberblick über den Status der IT/OT-Segmentierung** auf jedem Gerät und an jedem Ort in der gesamten Umgebung

> **„Bis 2021 werden 80 % aller industriellen IoT-Projekte [IIoT] spezifische Anforderungen an die OT-Sicherheit stellen, gegenüber 40 % heute.“** [1]
>
> **GARTNER**

> **„IoT- und netzwerkfähige Geräte haben zu neuen Kompromittierungsmöglichkeiten für Netzwerke und Unternehmen geführt. [...] Sicherheitsteams müssen jedes Gerät im Netzwerk permanent isolieren, absichern und kontrollieren.“** [2]
>
> **FORRESTER RESEARCH**

forescout.com/platform/eyeSegment info-dach@forescout.com Telefon (weltweit): +1-408-213-3191

- **Übersicht von Datenflüssen** basierend auf der logischen Taxonomie von Benutzern, Anwendungen, Diensten, Funktionen, Standorten, Geräten und Risikoeinstufung
- **Verringerung der Angriffsfläche und Einhaltung von Konformitätsvorschriften** durch dynamische Segmentierung für IT-, IoT- und OT-Umgebungen
- **Optimierung von IT/OT-Workflows** und Nutzung vorhandener Investitionen mit einer konsistenten Segmentierungsrichtlinie für das gesamte Unternehmensnetzwerk
- **Weniger Konformitätsrisiken sowie geringe Kosten durch die effiziente Verwaltung der netzwerkübergreifenden Zugriffs**, sodass weniger Mitarbeiter benötigt werden

„Fast 20 % aller Unternehmen haben in den vergangenen drei Jahren mindestens einen Angriff über das Internet of Things (IoT) verzeichnet.“ [3]

GARTNER

Optimiertes Risikomanagement und Zero-Trust-Segmentierung für IT/OT-Netzwerke

Die Forescout-Lösung bietet einen umfassenden Überblick über Geräte in OT-Netzwerken und ermöglicht die effektive Problembehebung einer Großzahl an operativen und Cyber-Security-Risiken in Echtzeit. Mit der Lösung können Sie schwierige domänenübergreifende Segmentierungen für die gesamte OT-Umgebung implementieren und mit störungsfreier Bedrohungserkennung und -behebung Risiken mindern.

Forescout eyeSegment unterstützt Sie bei der Konzeption und Implementierung der Zero-Trust-Segmentierung, indem die Datenflüsse automatisch einer logischen Taxonomie für Benutzer, Anwendungen, Dienste, Funktionen, Standorte, Geräte und Risikoeinstufungen im gesamten Unternehmensnetzwerk zugeordnet werden. Dadurch kann OT-Datenverkehr in Echtzeit mit der Baseline abgeglichen werden, ohne dass Agenten oder Umstellungen bei der Infrastruktur notwendig sind. Außerdem können Sie vor der Durchsetzung von Segmentierungsrichtlinien ihre Auswirkungen modellieren.

STEIGERN SIE DEN WERT IHRER SICHERHEITS- UND IT-INVESTITIONEN

- Einheitliche Segmentierungsrichtlinien minimieren die Risiken durch IT/OT-Konvergenz (laterale Bewegung)
- Planung, Monitoring und Reaktion mit detaillierten Segmentierungsrichtlinien minimieren Risiken durch OT-Geräte
- Unterbrechungsfreie und dynamische Segmentierung für sensible OT-Umgebungen durch Nutzung vorhandener Investitionen (Infrastruktur)

Forescout eyeInspect (ehemals SilentDefense) schützt kritische Infrastrukturen mit patentierter Deep Packet Inspection (DPI) und einer umfangreichen Bibliothek ICS-spezifischer Bedrohungsindikatoren. eyeInspect überwacht die Netzwerkkommunikation in Echtzeit und liefert umfangreiche Zusammenhänge zu Netzwerkressourcen, Protokollen und Kommunikationsinhalten. Mit leistungsstarken Funktionen wie der erweiterten Warnmeldungsaggregation und der Asset-Basislinienbestimmung können Sie Bedrohungserkennungs- und Konformitätsaufgaben automatisieren, die die Risiken verringern und die Durchsetzung der OT-Segmentierung unterstützen.

Abbildung 1. Die eyeSegment-Matrix erlaubt die Konzentration auf das Wesentliche, sodass Sie bestimmte Datenverkehrsmuster in Ihrer Umgebung analysieren und untersuchen können. Unabhängig davon, wo Sie in der Matrix-Hierarchie stehen, können Sie umgehend die gewünschten eyeSegment-Richtlinien erstellen, um ein bestimmtes Datenverkehrsmuster zu segmentieren und Ihr Unternehmen zu schützen, während Sie gleichzeitig sicherstellen, dass Produktion und Geschäftsbetrieb störungsfrei erfolgen können.

Die Forescout-Lösung für Netzwerksegmentierung deckt verschiedenste Anwendungsszenarien für OT-Umgebungen ab. In jedem Fall werden durch die Flexibilität der Forescout-Plattform Unterbrechungen des Geschäftsbetriebs minimiert sowie die Betriebskosten für Segmentierungsprojekte gesenkt. Dies sind einige wichtige Anwendungsszenarien:

- Risikominimierung, Gewährleistung der Konformität und Senkung der Betriebskosten für OT-Netzwerke
- Sofortiger Echtzeitüberblick über OT-Umgebungen zum Modellieren unterbrechungsfreier Segmentierungsrichtlinien
- Beschleunigte Zero-Trust-Segmentierung für IT/OT-Umgebungen

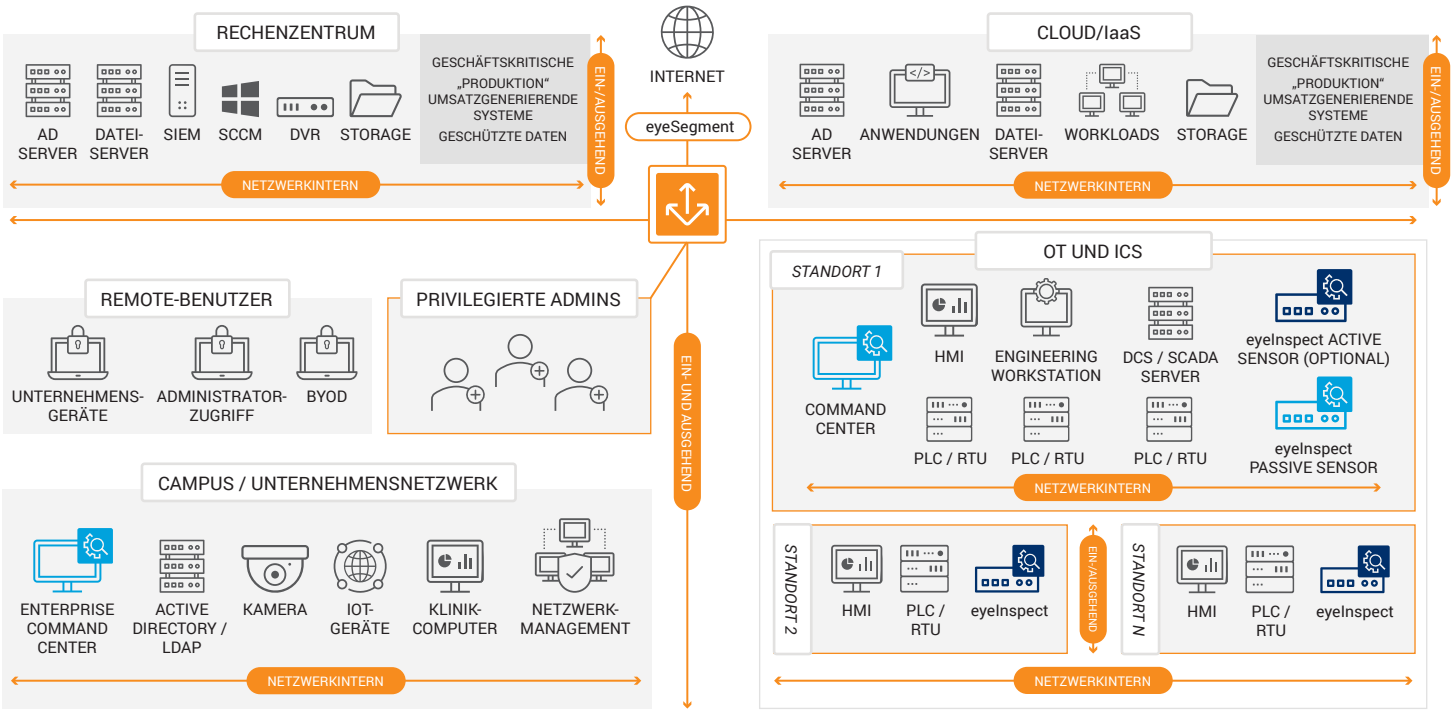

Abbildung 2. Die Forescout-Lösung unterstützt die Behebung von Bedrohungen und bietet einen sofortigen Echtzeitüberblick über Ihren Segmentierungsstatus. Im Beispiel oben verhindert eyeSegment, dass verbundene Geräte zwischen der Gesundheitswesen- und IT/OT-Domäne wechseln können.

1. „Invest Implications: Cool Vendors in Industrial IoT and OT Security" (Investment-Entscheidungen: Interessante Anbieter für Industrial IoT- und OT-Sicherheit), Gartner Research, April 2018
2. „Mitigating Ransomware With Zero Trust" (Abwehr von Ransomware mit Zero Trust), Forrester Research, Inc., 8. Juni 2020
3. „IoT Security Primer: Challenges and Emerging Practices" (Grundlegendes zu IoT-Sicherheit: Herausforderungen und neue Methoden), Gartner, Januar 2020

Nicht nur alles sehen, sondern alles schützen.

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

forescout.com/platform/eyeSegment info-dach@forescout.com Telefon (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

E-Mail: info-dach@forescout.com
Telefon (weltweit): +1-408-213-3191
Support: +1-708-237-6591

Weitere Informationen finden Sie unter Forescout.de