FORESCOUT
Active Defense for the Enterprise of Things™

Cybersicherheit und Risikoverwaltung für OT-Umgebungen

Risiken verringern, Konformitätsrichtlinien automatisieren und Bedrohungsanalysen für ICS- und OT-Umgebungen optimieren

Durch die fortschreitende Konvergenz von IT- (Informationstechnologie) und OT-Netzwerken (operative Technologie) erhöhen sich die Komplexität und die Anfälligkeit zuvor isolierter Netzwerke von Industriesteuerungssystemen (ICS). Parallel dazu kommt es zu einer explosionsartigen Zunahme von industriellen IoT-Geräten (IIoT), die die Transparenzlücke wachsen lässt und die Durchsetzung von Konformität erschwert. Unternehmen benötigen deshalb ein Sicherheitstool, das ihnen detaillierte Transparenz für OT- und ICS-Netzwerke bietet und die effektive Problembehebung von operativen und Cyberrisiken ermöglicht.

> **„Bis 2021 werden 80 % der IIoT-Projekte OT-spezifische Sicherheit-sanforderungen haben.“[1]**
>
> **GARTNER**

Die wichtigsten Herausforderungen in OT-Umgebungen

Da Unternehmen ihre Infrastruktur modernisieren, mit neuen Technologien erweitern und OT- und IT-Netzwerke zusammenführen, müssen sie besonders anfällige OT- und ICS-Systeme in modernen, heterogenen Netzwerkumgebungen unterstützen und schützen. Das führt zu neuen Herausforderungen für die Sicherheits- und IT-Teams, darunter:

- Identifizierung, Klassifizierung und Steuerung aller verbundenen IT-Geräte, IIoT-Systeme und OT-Ressourcen – ob verwaltet oder unverwaltet
- Analyse von Warnmeldungen, Priorisierung von Bedrohungen und zeitnahe Reaktion auf Zwischenfälle mit minimalen Betriebsstörungen
- Gewährleistung der Konformität aller verbundenen Geräte – auch alter OT-Systeme – mit behördlichen Anforderungen und Richtlinien
- Pflege eines genauen, aktuellen Geräteinventars

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

Forescout eyeInspect: Widerstandfähigkeit gegen Cyberbedrohungen und Risiko-verwaltung für die IIoT- und OT-Infrastruktur

Forescout eyeInspect (ehemals SilentDefense™) schützt OT- und ICS-Netzwerke vor verschiedensten Bedrohungen, verfügt über Funktionen für die passive und die aktive Erkennung. So ist die automatische Geräteinventarisierung in Echtzeit möglich und Behebungsmaßnahmen können je nach Grad der Beeinträchtigung gezielt umgesetzt werden.

- Ermöglicht passives Netzwerk-Monitoring und Segmentierung in Echtzeit
- Optimiert die Bedrohungsanalyse und -behebung durch die erweiterte Aggregation von Warnmeldungen
- Bietet umfassende Integrationen mit ServiceNow® und native Schnittstellen für SIEM-Lösungen, Firewalls,
- IT-Ressourcenverwaltung, Sandboxen und Authentifizierungsserver
- Verbessert die Effektivität des SOC und von Analysten, um die Risikoanalyse anhand des Asset-Risiko-Frameworks automatisieren zu können
- Erweitert die außergewöhnlichen Gerätetransparenz-, Klassifizierungs- und Profilerstellungsfunktionen der Forescout-Plattform von der Cloud bis hin zu Edge-Geräten

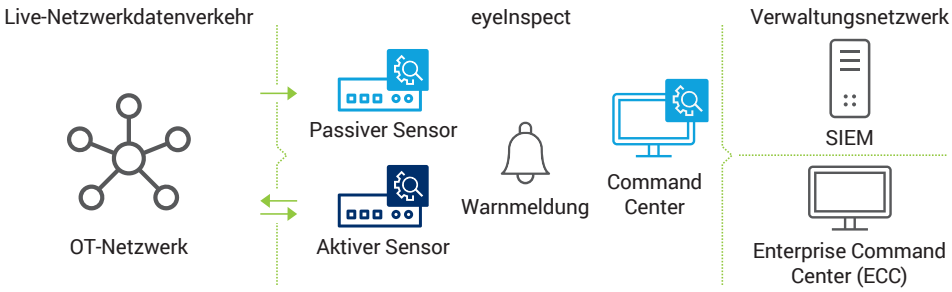

Abbildung 1. Vereinfachtes Modell der eyeInspect-Implementierung

LÜCKENLOSE TRANSPARENZ UND BEDROHUNGSERKENNUNG

Die branchenführenden Funktionen für Gerätetransparenz, -klassifizierung und -profilerstellung der Forescout-Plattform reichen dank eyeInspect sehr viel tiefer in OT- und ICS-Umgebungen hinein. Mit der Lösung können Sie ein umfassendes Spektrum an Cyber- und operativen Risiken identifizieren und effektiv beheben, darunter:

- Cyberangriffe (z. B. DDoS, MITM und Scan-Angriffe)
- Nicht autorisierte Netzwerkverbindungen und -kommunikation
- Verdächtiges Benutzerverhalten und Richtlinienänderungen
- Fehlfunktionen oder Fehlkonfigurationen von Geräten
- Neue und nicht reagierende Geräte
- Gefälschte Nachrichten
- Nicht autorisierte Firmware-Downloads
- Unsichere Protokolle
- Standard-Anmeldedaten und unsichere Authentifizierungen
- Logikänderungen
- Transparenz für IP-fähige und serielle Geräte

Anwendungsszenarien für eyeInspect

Gerätetransparenz und -Monitoring

eyeInspect sorgt für kontinuierliche Gerätetransparenz in allen OT-Netzwerken und an allen Standorten. Die Lösung erstellt automatisch eine detaillierte Netzwerkkarte mit umfassenden Geräteinformationen und automatischer Gruppierung nach Netzwerk/Rolle. Sie wird in verschiedenen Formaten bereitgestellt, beispielsweise durch Purdue Level oder

Kommunikationsverhältnis. Forescout eyeInspect setzt zahlreiche Erkennungsfunktionen ein, darunter:

- Patentierte Deep Packet Inspection von über 150 IT- und OT-Protokollen
- Kontinuierliche, konfigurierbare Richtlinien- und Verhaltensüberwachung
- Automatische Bewertung von Geräteschwachstellen, Gefährdung, Netzwerk- und operativen Problemen
- Optionale nicht-invasive, aktive Komponenten zur selektiven Abfrage bestimmter Hosts

Verwaltung der Gerätekonfiguration
eyeInspect erfasst automatisch verschiedenste OT-Geräteinformationen. Es protokolliert dabei alle Konfigurationsänderungen, damit diese für Sicherheitsanalysen und operative Forensik zur Verfügung stehen. Unter anderem werden folgende Informationen erfasst:

- Netzwerkadresse
- Hostname
- Geräteanbieter und -modell
- Seriennummer
- Betriebssystemversion
- Firmware-Version
- Hardware-Version
- Gerätemodulinformationen

Automatisierte Konformität
Mit dem aktiven eyeInspect-Sensor können die Verantwortlichen auf einfache Art und Weise die Basislinie für Geräte und Gerätegruppen entsprechend den spezifischen Konformitätsrichtlinien bestimmen und Abweichungen automatisch erkennen lassen. Außerdem können Sie eigene Richtlinien definieren, mit denen Sie die für Ihr Unternehmen geltenden Konformitätsrichtlinien wie NERC CIP, ISA99/IEC 62443, NIS und NIST CSF sowie FDA und FIPS einhalten. Die Verantwortlichen können zulässige Nachweise/Berichte der Basislinie für diese Konformitäts-Frameworks generieren.

Netzwerkzugriffssteuerung und -segmentierung
eyeInspect greift auf die ACL- und VLAN-Zuweisungsfunktionen der Forescout-Plattform zurück, sodass die richtlinienbasierte Segmentierung und Zugriffssteuerung auch in OT-Netzwerken möglich ist und die einheitliche, übergreifende Echtzeit-Assetverwaltung für IT-, IoT- und OT-Netzwerke unterstützt wird. Mit eyeInspect verfügen die Verantwortlichen über eine kontextbezogene (d. h. Protokollerfassung/DPI) Zuordnung und Visualisierung von Beziehungen (Kommunikationsmuster) zwischen den Geräten in IT-, OT- und medizinischen Umgebungen. Außerdem ist eine Integration mit anderen vorhandenen Verkehrsflusstelemetrie-Systemen/Produkten (z. B. Medigate, NetFlow, SPAN) möglich.

WIRTSCHAFTLICHE VORTEILE DER WIDERSTANDFÄHIGKEIT GEGEN CYBERBEDROHUNGEN

Forescout eyeInspect kann sich positiv auf das Geschäftsergebnis eines Unternehmens auswirken, weil es die Sicherheit und Widerstandsfähigkeit seiner operativen Systeme erhöht und gleichzeitig die administrative Effizienz, Risikoverwaltung und Konformität erheblich verbessert.

Forescout hat kürzlich beispielsweise untersucht, wie das OT-Netzwerk-Monitoring zu den Finanzergebnissen eines bekannten US-Nahrungsmittelproduzenten beiträgt, bei dem 17 Vollzeitkräfte sich nur auf ICS-Cybersicherheit und -Konformität konzentrieren.[2] Die Untersuchung kam zu folgenden Ergebnissen:

- Jährliche Einsparungen von 820.336 US-Dollar durch reduzierte Arbeitskosten, erhöhte Verwaltungsproduktivität und bessere Threat Hunting-Funktionen in Verbindung mit der Geräte- und Netzwerktransparenz.
- Jährliche Einsparungen von 346.456 US-Dollar aufgrund von verwertbaren aktuellen Bedrohungsmanagement-Informationen, schnelleren Reaktionen auf Vorfälle und des geringeren Risikos für Ausfallzeiten, alles verbunden mit der verbesserten Cyberbedrohungserkennung und -reaktion.
- Jährliche Einsparungen von 158.120 US-Dollar an Konformitätskosten durch Integrationen mit Lösungen für ICS-Sicherheits- und -Geräteverwaltung.

Bedrohungserkennung und Reaktion auf Vorfälle

Mit den Untersuchungs- und Reaktionstools von eyeInspect automatisieren Sie die Erkennung, Eindämmung und Behebung von Bedrohungen, während Dashboards und Widgets die Zusammenarbeit der Benutzer vereinfachen. Umfassende Details zu Warnmeldungen unterstützen die Ursachenanalyse und beschleunigen die effektive und effiziente Reaktion. Im Enterprise Command Center (ECC) können die Benutzer sich Warnmeldungen für alle geografisch verteilten Netzwerke an verschiedenen Standorten genauer ansehen, um einen Vorfall detailliert zu analysieren, einschließlich der beteiligten Geräte und des Kontexts der Warnmeldung.

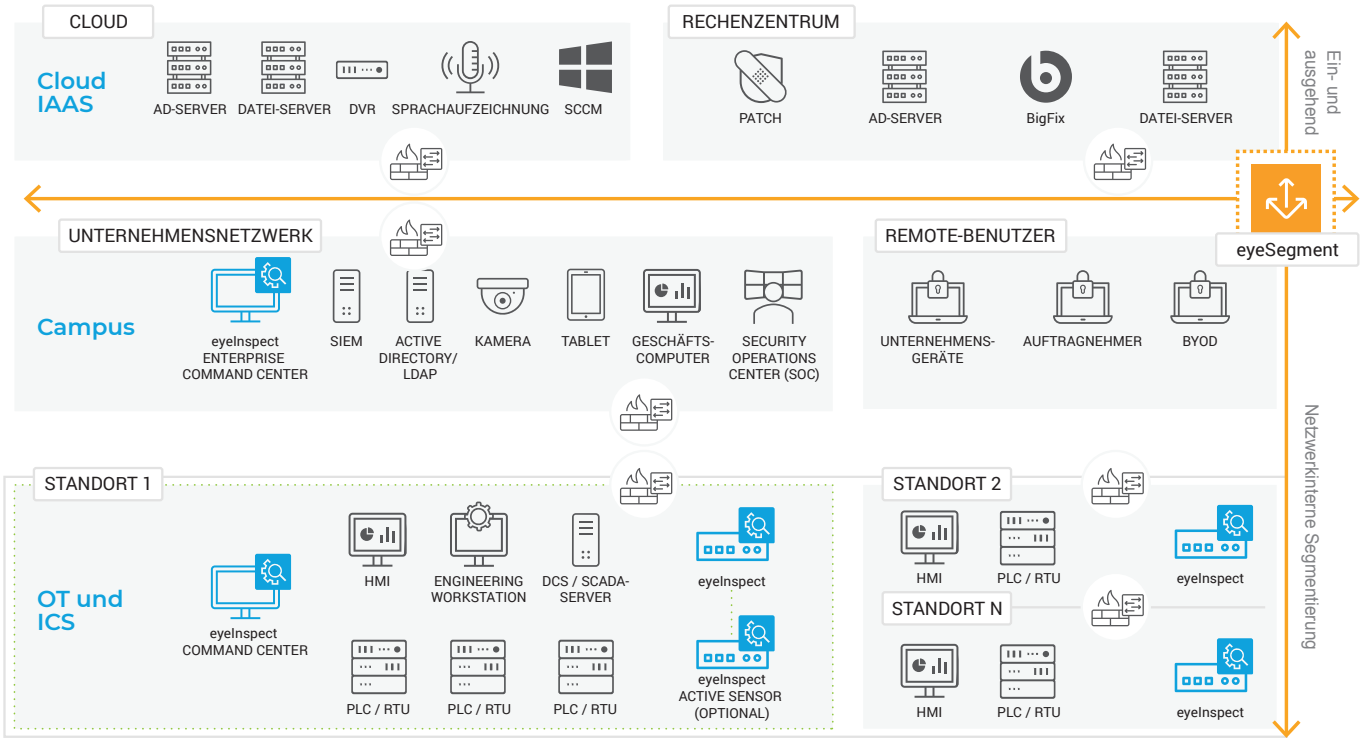

Abbildung 2. eyeInspect ist ein Bestandteil der einheitlichen IT-/OT-Sicherheitsplattform von Forescout, die Situationserkennung und automatische Kontrolle der operativen und Cyberrisiken im gesamten Unternehmensnetzwerk bietet.

Nicht nur alles sehen, sondern alles schützen.

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

1. „7 Questions SRM Leaders Aren't Asking OT Security Providers During Technology Selection" (Sieben Fragen, die SRM-Verantwortliche OT-Sicherheitsanbietern bei der Technologieauswahl nicht stellen), Saniye Alaybeyi, Gartner, 2018, https://www.forescout.com/gartner-report-7-questions-for-OT-security-providers

2. Prognosen auf Grundlage standardisierter Kundendaten. Die tatsächlichen Einsparungen können in Abhängigkeit von verschiedenen Faktoren variieren.

forescout.com/platform/eyeInspect 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