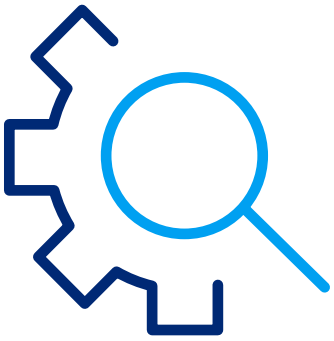
FORESCOUT



eyeInspect

Risiken in OT- und ICS-Umgebungen reduzieren, Compliance automatisieren und Bedrohungsanalysen optimieren

Agentenlos
Konsolidierte Echtzeit-Inventarisierung aller verbundenen OT- und ICS-Geräte mit 30+ aktiven und passiven Erkennungstechniken.

Präzise
Bestimmung einer Asset-Baseline und Schutz des Netzwerks mithilfe tausender OT-spezifischer Bedrohungsindikatoren und leistungsstarker Anomalieerkennung.

Effektiv
Proaktive Bewertung der Risiken, Erkennung von Bedrohungen, Ermittlung ihrer geschäftlichen Auswirkungen und schnelle Priorisierung von Abhilfemaßnahmen.

Effizient
Automatisierung zeitaufwändiger Aufgaben rund um Compliance und Risikobewertung, Minimierung menschlicher Fehler und gesteigerte Effizienz.

Forescout eyeInspect bietet einen detaillierten Überblick über alle Geräte in OT-/ICS-Netzwerken und ermöglicht die effektive Behebung von operativen und Cyberrisiken in Echtzeit.

- Framework für Asset-Risiken zur umfassenden Bestimmung der Cyber-Resilienz Ihres OT-Netzwerks
- Vollständige Gerätetransparenz dank DPI (Deep Packet Inspection)-Filterung von mehr als 270 industriellen Netzwerkprotokollen und Baseline-Assets
- Schutz des Netzwerks mithilfe tausender OT-spezifischer Bedrohungsindikatoren und leistungsstarker Anomalieerkennung

Visualisieren

Umfassende Gerätetransparenz durch SPAN-Ports und vielfältige andere passive Techniken, um 100%ige Abdeckung zu gewährleisten

Patentierte DPI (Deep Packet Inspection)-Analysen an 270+ IT- und OT-Protokollen

Erkennen

Erfassung umfassender Informationen zu den OT-Assets; Protokollierung aller Konfigurationsänderungen für Sicherheitsanalysen und forensische Untersuchungen

Automatisierte Erkennung, Eindämmung und Beseitigung von Bedrohungen mit Tools zur Untersuchung und Behandlung von Warnmeldungen

Reagieren

Vereinfachte Einhaltung wichtiger Standards wie NERC CIP, EU NIS-Richtlinie, NIST CSF, IEC 62443 und TSA Pipeline Security

Dashboards für effizientere Kooperation und ausführliche Details zu Alarmen für eine wirksame Reaktion auf Vorfälle

eyeInspect ist die Lösung für:

- **Mangelnde OT-Transparenz** aufgrund geografisch verteilter und heterogener Gerätenetzwerke
- **Abwehrlücken und Schwachstellenrisiken,** wenn Patches nicht installiert werden oder Anwendungen Bedrohungen ausgesetzt sind.
- **Operative und Cyberrisiken** durch Überflutung mit Warnmeldungen und schlechte Priorisierung von Abhilfemaßnahmen
- **Unvollständige Informationen zu Bedrohungen,** wodurch die Ausführung von Schutzrichtlinien verhindert wird.
- **Compliance-Aufgaben,** die mit großem Aufwand und hohem Bußgeldrisiko verbunden sind.

Visualisieren

Tausende von Geräten in einer einzigen Ansicht visualisieren

- Präzise Echtzeit-Erfassung des Asset-Inventars mit passiven Techniken ohne Betriebsunterbrechungen
- Anzeige IP-fähiger und serieller Geräte, einschließlich HMIs, SCADA, SPS, Gebäudemanagement- (BMS) und Gebäudeautomationssystemen (BAS)
- Priorisierung von Warnmeldungen und Anzeige von Protokollen nach verschiedenen Parametern, einschließlich Zeit, Geräten, Netzwerkstandort und Alarmtyp

Erkennen

Erkennung von Bedrohungen und intelligentes Risikomanagement

- Erkennung bekannter und unbekannter Cyberbedrohungen mithilfe tausender ICS-/OT-spezifischer Prüfungen und Indikatoren für Kompromittierungen (IOCs)
- Erkennung von Cyber- und operativen Risiken; Priorisierung nach ihrer Dringlichkeit und ihren potenziellen Auswirkungen auf das Geschäft
- Erkennung von Compliance-Verstößen bei Geräten und Richtlinien im gesamten Netzwerk
- Echtzeit-Erkennung von Änderungen am Netzwerk, einschließlich neuer Geräte, Änderungen an der Infrastruktur und auffälliger betrieblicher Aktivitäten

Reagieren

Schnell reagieren mit der weltweit intelligentesten und skalierbarsten OT-Sicherheitslösung

- Intuitiv verständliche Risikobewertungen, die Entscheidungshilfen bei der Reaktion auf Cyber- und operative Bedrohungen bieten
- Automatisierte Workflows, Regeln und Korrekturmaßnahmen für Echtzeit-Reaktionen auf neu auftretende Bedrohungen
- Reaktion auf Compliance-Änderungen mithilfe von Regeln, Parametern und Berichten, die den definierten Asset-Baselines entsprechen

Enterprise Command Center – Anforderungen

	PRODUKTBESCHREIBUNG
Hardware/Hypervisor	19-Zoll-Rack-Server oder mindestens VMware ESXi 5
Prozessor	4-Kern-CPU (Intel®) 64-bit ≥ 2.4GHz
Speichergröße	16-32 GB
Festplatte	> 250 GB
Netzwerkschnittstelle	Schnittstelle für Command Center-Kommunikation und Webanwendungszugriff

Command Center – Anforderungen

(*) Größe des Arbeitsspeichers gilt nur für die eyeSight-Lizenz

	Kleine Implementierung (≤ 5 Sensoren)	Mittlere Implementierung (≤10 Sensoren)	Große Implementierung (>10 Sensoren ≤100)
Hypervisor	Mindestens VMware ESXi5		
Formfaktor	19-Zoll-Rack-Server oder virtuelle Appliance		
Prozessor	4-Kern CPU 64-bit	4/6-Kern (Intel) CPU 64-bit	12-Kern (Intel) CPU 64-bit
Speichergröße	16(*)-64 GB	32(*)-64 GB	64-256 GB
Festplatte	500 GB	1 TB	>1 TB
	(Bei 90 Tagen Datenaufbewahrung)		
Netzwerkschnittstelle	Schnittstelle für Sensorkommunikation und Webanwendungszugriff		

Passiver Sensor – Anforderungen

	Kleine Implementierung (≤ 5 Sensoren)	Mittlere Implementierung (≤10 Sensoren)	Große Implementierung (>10 Sensoren ≤100)
Beispiel-Hardware-Modell	Foxguard® IADIN-FS1	Dell® Embedded PC 5000	Dell® PowerEdge R640
Beschreibung der Implementierung	Implementierungen in kleinen Netzwerken und bei rauen Umgebungsbedingungen	Implementierungen in mittel-großen Netzwerken, bei rauen Umgebungsbedingungen	Implementierungen in großen Netzwerken und Installationen im Rechenzentrum
Formfaktor	Kleiner Industrie-PC/ DIN-Schienenmontage	Mittelgroßer Industrie-PC	19-Zoll-1U-Rack-Server
Prozessor	2- oder 4-Kern CPU (Intel) 64-bit	4 oder 6-Kern-CPU (Intel) 64-bit mit 8 GT/s	6-Kern-CPU (Intel) 64-bit ≥ 2.4GHz
Speichergröße	8-16 GB	16-32 GB	64-256 GB
Festplatte	64-500 GB für Industrie-PCs (es sollten SSDs mit großem Temperaturbereich verwendet werden)		
Monitoring-Schnittstelle	Bis zu 4 Monitoring-Ports	Bis zu 8 Monitoring-Ports	Bis zu 8 Monitoring-Ports

Aktiver Sensor –Anforderungen

INTEGRIERT IN PASSIVEM SENSOR
eyeInspect kann direkt auf jedem passiven Sensor für kleine, mittelgroße und große Implementierungen integriert werden.

	Eigenständig	Virtuell
Prozessor	2-4-Kern-CPU	4 vCPU
Speichergröße	4 GB RAM	4 GB RAM
Netzwerkschnittstelle	≥ 1	≥ 1

Weitere Informationen zu den Hardware-Anforderungen finden Sie hier: https://www.forescout.com/company/resources/command-center-and-sensor-hardware-guidelines/

Protokolle

Eine vollständige Liste aller standardmäßigen OT-, IT- sowie proprietären OT-Systemprotokolle finden Sie unter diesem Link: https://www.forescout.com/company/resources/eyeinspect-protocols/

Orchestrieren, segmentieren, kontrollieren

Die Plattform von Forescout steigert den Nutzen von eyeInspect mit einer Produkt-Suite zur Erstellung und Implementierung von Richtlinien und automatisierten Maßnahmen für Asset Management, Gerätekonformität, Netzwerkzugriffe, Netzwerksegmentierung und Reaktion auf Vorfälle.

Um mehr über die Plattform von Forescout zu erfahren, besuchen Sie bitte www.forescout.com/platform/

FORESCOUT

Forescout Technologies, Inc.

Gebührenfrei (US) 1-866-377-8771
Tel (intl) +1-408-213-3191
Support +1-708-237-6591

Erfahren Sie mehr auf Forescout.com