SOLUTION BRIEF

Forescout eyeInspect for Microsoft Sentinel®

Complete OT Visibility and Threat Intelligence for Industrial Environments

FORESCOUT

Built for OT.
Designed for Action.
Connected to Microsoft.

Forescout 4D Platform™

Delivers risk exposure management, network security, compliance, and threat detection and response across IT, OT, IoT, and building automation systems, through a unified platform that integrates seamlessly with your existing ecosystem.

Forescout eyeInspect

Delivers deep visibility and real-time insights for the industrial systems that keep your business running. Identifies assets across all Purdue levels, detects misconfigurations, process anomalies, and threats, and feeds high-fidelity OT data directly into Microsoft Sentinel.

Forescout eyeInspect for Microsoft Sentinel®

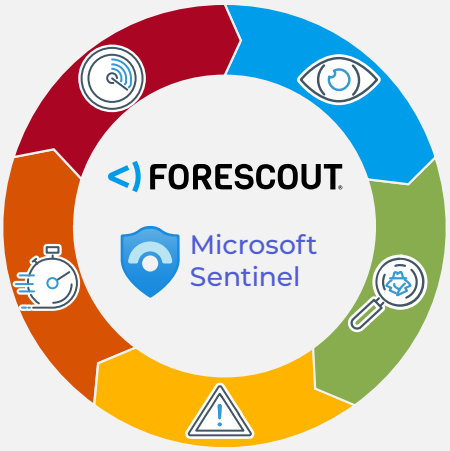
Complete OT Visibility and Threat Intelligence for Industrial Environments

Extend Microsoft Sentinel into Operational Networks to gain full visibility, unlock security insights, and respond faster to threats.

Microsoft Sentinel delivers powerful analytics and correlation across enterprise data, but industrial networks present an extra layer of complexity. OT systems are notoriously hard to monitor, most can't run agents, don't generate logs, and often aren't connected to anything beyond the plant floor. That's where Forescout eyeInspect steps in. Purpose-built for operational environments, it delivers deep, real-time visibility across all device types and every level of the Purdue model. From sensors and PLCs to SCADA systems, networking equipment, HMIs, and industrial servers. It gives Sentinel the visibility and context it needs to discover assets, detect threats, and identify process-related anomalies before they impact operations or business resilience. A perfect match—two platforms, one operational view.

Challenges

- Gaining real-time visibility into unmanaged, legacy, or non-Windows devices across IT, IoT, OT, and building automation systems.
- Identifying both cyber and operational threats in real time before they impact business resilience.
- Correlating signals across IT and OT to detect abnormal behaviour and early warning signs.
- Tracking changes, misconfigurations, or activity that could increase risk exposure or compromise compliance.



Joint Value Proposition

Forescout: Automatically discovers and classifies all connected assets, IT, IoT, OT and BAS in real time, no agent or changes needed.

Forescout: Detects security and operational threats using deep packet inspection across all major industrial protocols.

Forescout: Identifies misconfigurations, unauthorized changes, and abnormal behaviour that increase risk or impact compliance.

Sentinel: Automatically correlates eyeInspect asset and alert data with enterprise signals to uncover threats and attack paths.

Sentinel: Triggers playbooks to perform remediation actions across different 3rd systems, including the Forescout 4D Platform™.

Highlights

Complete asset visibility across unmanaged IT, IoT, OT, and building automation systems.

Real-time context sharing to enrich detection and accelerate investigation.

Focused incident response through smarter correlation and actionable risk insights.

Automated response execution that closes the loop from detection to action.

Use Cases

Real-time Asset Visibility and Attack Surface Analysis:

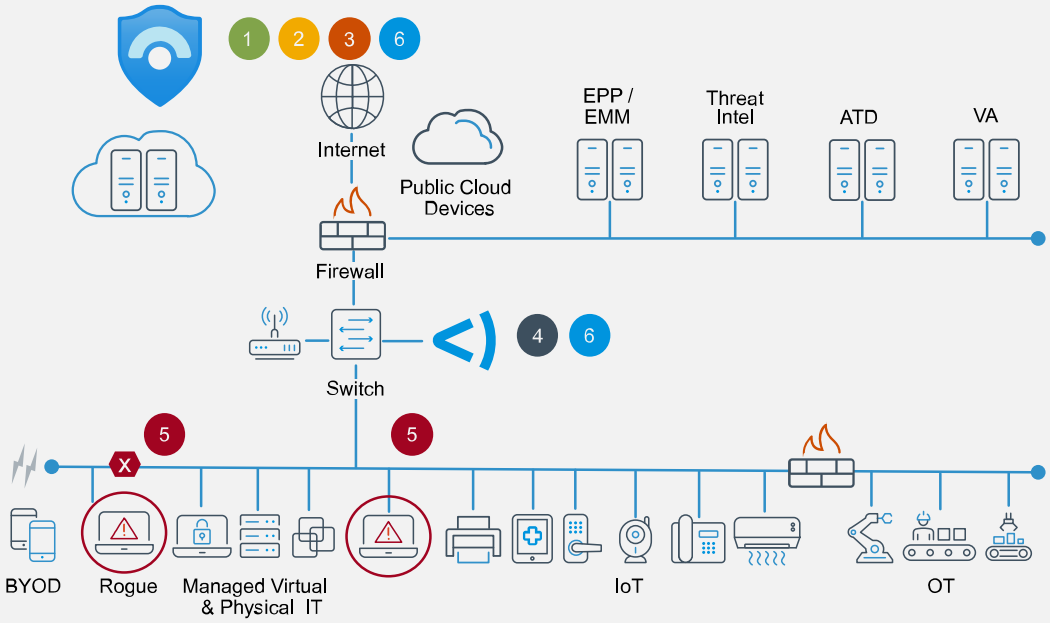
Continuously identify and profile all devices across IT, IoT, OT, and BAS—capturing properties, communications, and exposure in real time.

Industrial Threat Detection:

Detect cyber threats targeting industrial systems through deep inspection of OT network traffic, including unauthorized commands, scans, or lateral movement.

Change and Configuration Monitoring:

Identify unauthorized logic changes, configuration drift, and deviations from expected behaviour that increase operational or compliance risk.



1. **Forescout detects a new device on the production plant:** A contractor laptop connects through a network switch. It's flagged as unknown and non-compliant, missing required controls.
2. **Alert and asset context sent to Microsoft Sentinel:** Forescout shares device details, including configuration, security status, and event details.
3. **Sentinel generates a high-severity incident:** A custom rule identifies policy violations and creates an incident for a non-compliant transient device.
4. **Sentinel triggers a LogicApp to initiate response:** The playbook runs automatically and instructs the Forescout 4D Platform™ to contain the device.
5. **Forescout isolates the device at the switch level:** The laptop is moved to a quarantine VLAN, blocked from all IT and OT resources but granted access to a remediation portal.
6. **Forescout confirms and records the action in Sentinel:** Containment is logged and tracked for auditing.

FORESCOUT

Forescout Technologies, Inc.

Toll-Free (US) 1-866-377-8771
Tel (Intl) +1-408-213-3191
Support +1-708-237-6591

Learn more at Forescout.com