Cybersecurity and Risk Management for OT

Reduce risk, automate compliance and optimize threat analysis for ICS and OT environments

The ongoing convergence of information technology (IT) and operational technology (OT) networks is increasing the complexity and vulnerability of previously isolated industrial control system (ICS) networks. This is taking place alongside the explosive growth of Industrial IoT (IIoT) devices, which has created a significant visibility gap and made compliance enforcement more difficult. Organizations need a security tool that can provide in-depth visibility into OT and ICS networks and enable effective, real-time management of operational and cyber risks.

> **By 2025, 75% of OT security solutions will be interoperable with IT security solutions and delivered via multifunction platforms.[1]**
>
> GARTNER

Key Challenges in OT Environments

As organizations upgrade infrastructure, incorporate new technologies, and bring together OT and IT networks, highly vulnerable OT and ICS systems must be maintained and protected within modern, heterogeneous network environments. As a result, challenges are emerging for security and operations teams, including:

- Identifying, classifying and controlling all connected IT devices, IIoT systems and OT assets – managed and unmanaged
- Analyzing alerts, prioritizing threats and responding to incidents in a timely manner with minimal business disruption
- Making sure all connected devices – even legacy OT systems – comply with regulatory requirements and policies
- Maintaining an accurate, up-to-date asset inventory

Forescout eyeInspect: Cyber Resilience and Risk Management for IIoT and OT Infrastructure

Forescout eyeInspect (formerly SilentDefense™) protects OT and ICS networks from a wide range of threats, provides both passive and active discovery capabilities that create an automatic, real-time asset inventory and enables targeted remediation actions based on potential business impact.

- Enables passive, real-time network monitoring and segmentation
- Optimizes threat analysis and remediation with the Advanced Alert Aggregation
- Offers rich integrations with ServiceNow® and natively interfaces with SIEM solutions, firewalls, IT asset management, sandboxes and authentication servers
- Improves SOC and analyst effectiveness to automate risk analysis with the Asset Risk Framework
- Extends the exceptional device visibility, classification and profiling capabilities of the Forescout platform from cloud to edge devices

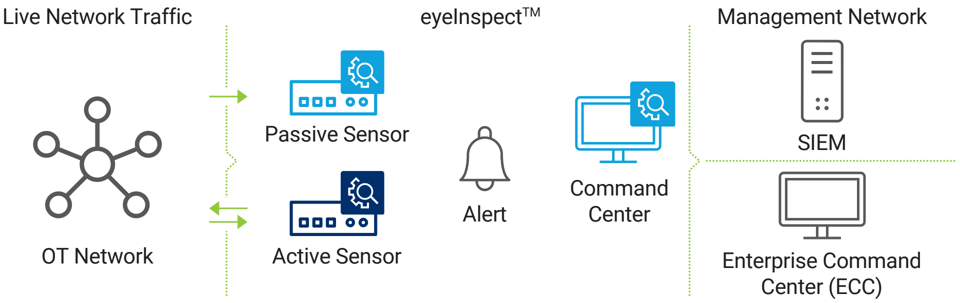

Figure 1: Basic eyeInspect deployment model

eyeInspect Use Cases

Asset visibility and monitoring

eyeInspect provides continuous asset visibility across OT networks and sites. It automatically builds a detailed network map with rich asset details and automatic grouping by network/role, provided in multiple formats such as Purdue level and communication relationship. eyeInspect uses a wide range of discovery capabilities that include:

COMPLETE VISIBILITY AND THREAT DETECTION

eyeInspect extends the industry-leading device visibility, classification and profiling capabilities of the Forescout platform far deeper into OT and ICS environments. It enables the identification and effective remediation of a full range of both cyber and operational threats, including:

- Cyberattacks (DDoS, MITM & scanning, etc.)
- Unauthorized network connections, communications
- Suspicious user behavior/policy changes
- Device malfunction or misconfiguration
- New and non-responsive assets
- Corrupted messages
- Unauthorized firmware downloads
- Insecure protocols
- Default credentials and insecure authentications
- Logic changes
- Visibility to IP-enabled and serial devices

- Patented deep packet inspection of 150+ IT and OT protocols
- Continuous, configurable policy and behavior monitoring
- Automatic assessment of device vulnerabilities, threat exposure, networking issues and operational problems
- Optional, non-intrusive active component to selectively query specific hosts

Asset configuration management

eyeInspect automatically collects a wide range of OT asset information, logging all configuration changes for security analysis and operational forensics. Discoverable details include:

- Network address
- Host name
- Vendor and model of the asset
- Serial number
- OS version
- Firmware version
- Hardware version
- Device modules information

Automated compliance

With eyeInspect active sensor, asset owners can easily baseline assets and asset groups according to specific compliance policies to automatically detect deviations from the established baseline. These baselines allow you to define custom baseline policies according to organizational need, or according to compliance guidelines such as NERC CIP, ISA99/IEC 62443, NIS and NIST CSF, as well as FDA and FIPS. Asset owners can generate admissible proofs/reports of the baseline for these compliance frameworks.

Network access control and segmentation

eyeInspect leverages the ACL and VLAN assignment capabilities of the Forescout platform, bringing policy-based segmentation and access control to operational networks to support unified and real-time asset management across IT, IoT and OT. With eyeInspect, asset owners have context-aware (i.e., protocol awareness/DPI) mapping and visualization of relationships (communication patterns) between assets across IT, OT and healthcare environments, and can integrate with other existing traffic flow telemetry system/products (Medigate, NetFlow, SPAN, etc.)

BOTTOM-LINE BENEFITS OF OT CYBER RESILIENCE

Forescout eyeInspect can positively impact an organization's bottom line by improving the security and resilience of its operational systems while dramatically enhancing administrative efficiency, risk management and compliance.

For example, Forescout recently studied the contribution of OT network monitoring to the financial performance of a prominent U.S. food production company with 17 FTEs focused on ICS cybersecurity and compliance.2 The study found:

- Annual savings of $820,336 in reduced labor costs, increased management productivity and improved threat-hunting capabilities associated with asset and network visibility.
- Annual savings of $346,456 related to actionable threat-management updates, faster incident response and reduced downtime risk, all associated with improved cyberthreat detection and response capabilities.
- Annual savings of $158,120 in compliance costs associated with built-in integrations with ICS security and asset management solutions.

Threat detection and incident response

Automate threat detection, containment and remediation with eyeInspect's alert investigation and response tools. Dashboards and widgets enhance user collaboration. Rich alert detail supports root cause analysis and expedites effective, efficient response. The Enterprise Command Center (ECC) lets users zoom in on alerts from any of their multisite or geo-distributed networks to analyze an incident in detail, including devices involved and context of the alert.

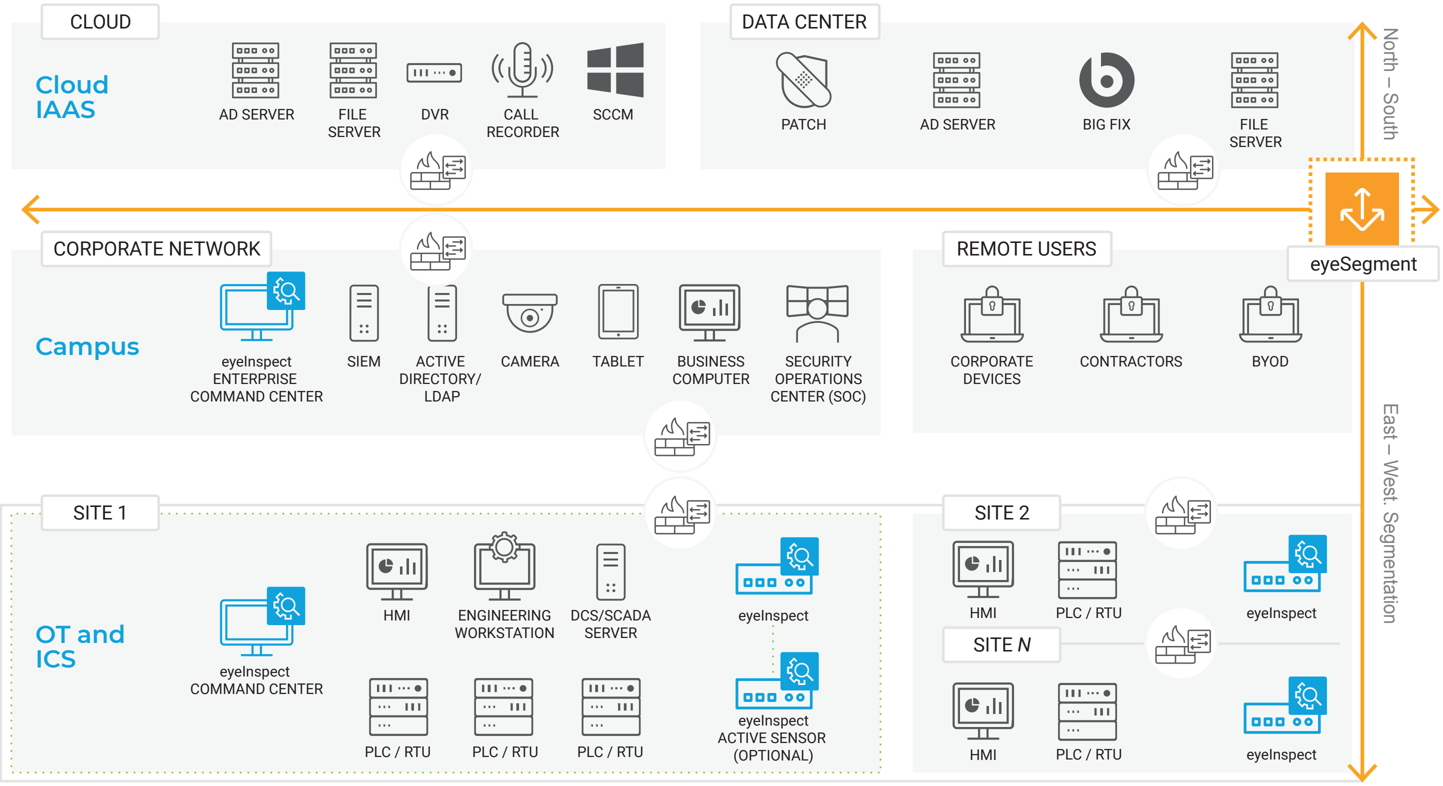

Figure 2: eyeInspect is part of Forescout's unified IT-OT security platform that provides situational awareness and automated control of both cyber and operational risk across the extended enterprise.

Don't just see it. Secure it.™

Contact us today to actively defend your Enterprise of Things.

[1] Gartner Market Guide for Operational Technology Security, January 13, 2021

[2] Projections based on standardized customer data. Actual savings may vary depending on multiple factors.

forescout.com/platform/eyeInspect salesdev@forescout.com toll free 1-866-377-8771

FORESCOUT
Active Defense for the Enterprise of Things™

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

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

Learn more at Forescout.com