FORESCOUT
Active Defense for the Enterprise of Things.

Manufacturing

Cybersecurity and risk management for the Industrial Internet of Things

Recent widespread adoption of cyber-physical systems has led to networks that are highly heterogeneous and flat. As a result, manufacturers are operating with increased risk, paving the way for cyber incidents that can be difficult to control and remediate.

Among the many challenges associated with protecting manufacturing networks, three of the most difficult are:

- Achieving real-time network visibility
- Proactively assessing and managing cyber risks
- Identifying networking and operational issues

Implementing the right OT (operational technology) network monitoring solution can help manufacturing organizations achieve all three of these goals.

> **"By 2021, 70% of OT security will be managed directly by the CIO or CISO, up from 35% today."[1]**
>
> **GARTNER**

The Cyber Resilience Platform for Manufacturers: eyeInspect

Forescout eyeInspect (formerly SilentDefense™) is an OT network monitoring solution that provides complete visibility into industrial networks, while also protecting them from a wide range of threats.

eyeInspect combines patented deep packet inspection (DPI) and anomaly detection technology with a library of thousands of IoCs for advanced cyberattacks, network misconfigurations and operational errors, all of which can help detect both known and unknown threats.

eyeInspect's graphical interface provides real-time network maps, network visualizations and analytics of communications, offering complete visibility into asset communications or hosts changing behaviors. By continuously monitoring and analyzing network communications and comparing them with a baseline of legitimate operations and with "known bad" characteristics defined in our proprietary threat library, eyeInspect identifies and reports cyber and operational threats in real time.

eyeInspect Use Cases for Manufacturing Networks

Achieve real-time network visibility

eyeInspect provides a continuously updated asset inventory for the entire ICS network by passively (or selectively actively) collecting a wide range of OT device information.
Discoverable details include:

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

It also provides full visibility into backplane modules, serial devices and asset configuration changes while logging changes for security analysis and operational forensics. eyeInspect automatically builds a detailed network map with extensive device details, baselines for each asset, communication visualizations, and automatic grouping by network and/or role. Grouping is provided in multiple formats, including Purdue level and communication relationship. eyeInspect's active technology, ICS Patrol, securely and selectively queries specific hosts on the network to extract even more asset details.

Proactively manage cyber risks

Most network monitoring tools force users to look at risk factors independently. eyeInspect is the first solution to automatically assess risk factors and individual data points to provide a security and operational risk score for each asset. The security risk score enables

THREAT INTELLIGENCE WITH eyeInspect

The threat landscape is evolving fast, so security solutions need to be able to quickly incorporate new detection signatures and algorithms. Some of the ways eyeInspect provides actionable threat intelligence include:

- Enables passive, real-time network monitoring and segmentation of OT and IIoT networks
- Provides eyeInspect active sensor, a non-intrusive active technology, that delivers deep asset visibility
- Streamlines IT-OT DevOps and security strategies with rich integrations with ServiceNow
- Optimizes threat analysis and remediation with the Advanced Alert Aggregation
- 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

security analysts to immediately identify assets that have a high probability of being attacked, and for which there is actual evidence that a potential attack is ongoing. Users can drill down into the risk score to understand why that asset is at risk and what can be done about it.

eyeInspect detects known and unknown threats from the earliest stage to the actual exploit using signatures as well as behavioral and patented anomaly detection techniques. A few examples of threats it has detected in the field include:

- L2 servers and field robots communicating and downloading firmware from external servers
- Poor segmentation exposing vulnerable devices to the Internet
- WannaCry-like malware in a factory
- Widespread use of default passwords

eyeInspect's interactive map identifies the source and spread of an incident, and the data provided in its packet captures (PCAPs) supports root cause analysis to expedite response efforts.

Identify networking and operational issues

Occasional networking and operational issues are inevitable, but they needn't result in significant system downtime. The operational risk score mentioned above enables OT engineers to quickly spot assets that require immediate attention, including devices exhibiting signs of misconfiguration or malfunction that could cause unexpected downtime. eyeInspect's Advanced Alert Aggregation feature allows users to correlate threats according to cause and level of urgency. Identified threats include:

- Use of insecure protocols
- Routing/gateway issues
- Data sent in noncompliant formats
- Connectivity issues with field devices
- Failure of critical devices
- Unstable process values
- Incorrect process measurements
- Switch and device misconfigurations

MULTIFACTOR THREAT DETECTION

OT network monitoring tools need to empower users and analysts to detect both known and unknown threats as early as possible, to enable quick response and mitigation actions. eyeInspect combines signatures with behavioral and patented anomaly detection techniques to detect known and unknown threats from the earliest stage (discovery) through the actual exploit, including insecure configurations that may expose critical devices.

eyeInspect can identify and help remediate 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 and misconfiguration
- New and non-responsive assets
- Malformed messages used in exploit attempts
- Unauthorized firmware downloads
- Use of insecure protocols
- Default credentials and insecure authentications
- PLC logic change

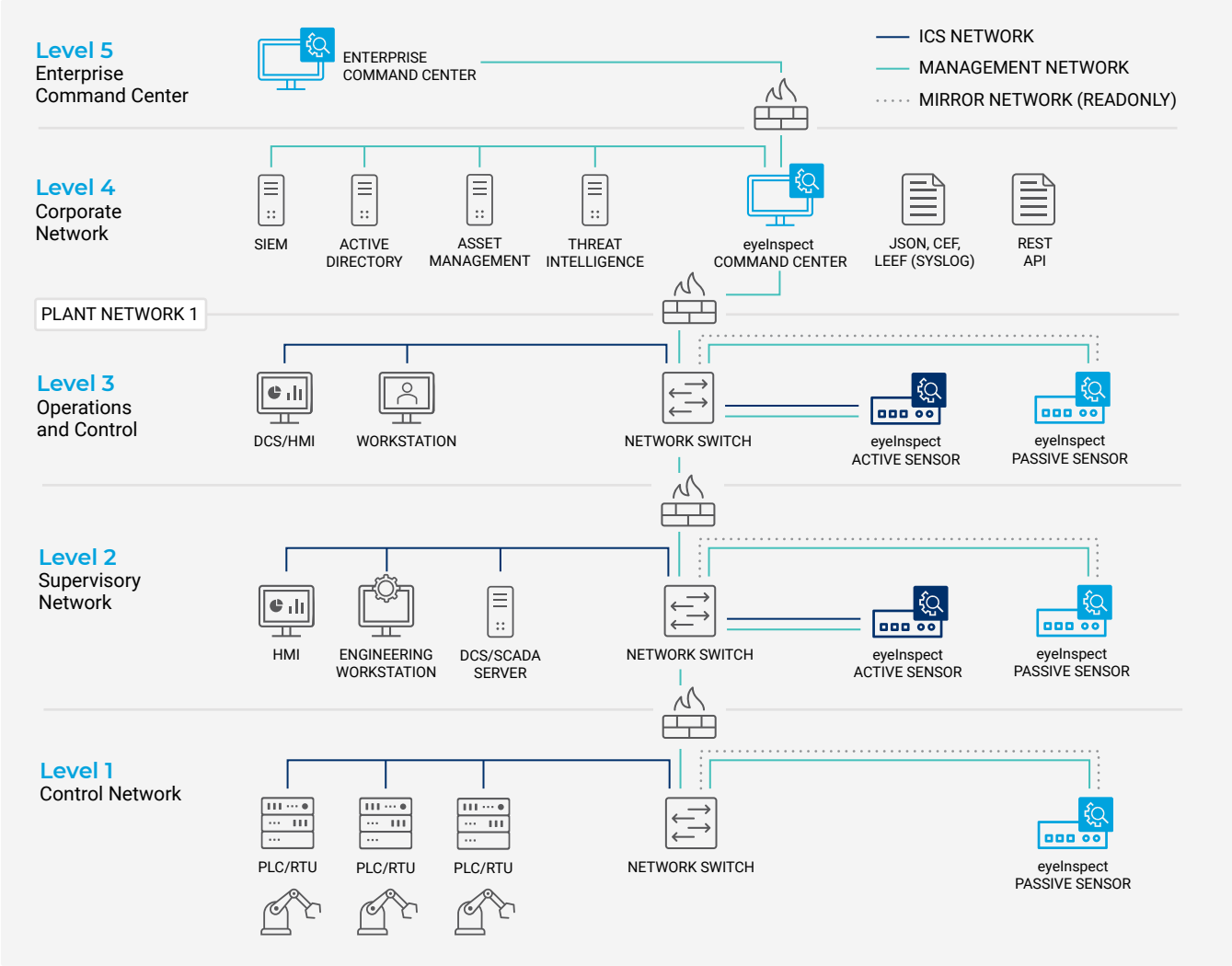

Figure 1: eyeInspect is part of Forescout's unified IT-OT security platform that provides situational awareness and automated control of both cyber and operational risk across the extended enterprise.

Don't just see it. Secure it.

Contact us today to actively defend your Enterprise of Things.

1. *7 Questions SRM Leaders Aren't Asking OT Security Providers During Technology Selection*, Saniye Alaybeyi, https://www.forescout.com/platform/operational-technology/gartner-report-7-questions-for-ot-security-providers/

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