Forescout eyeInspect provides in-depth device visibility for OT/ICS networks and enables effective, real-time management of operational and cyber risks.

- Fully understanding the cyber-resiliency of your OT network with an Asset Risk Framework
- Gain complete device visibility through deep packet inspection of more than 270 industrial network protocols and baseline assets
- Defend your network with thousands of OT-specific threat indicators and powerful anomaly detection

**Agentless**
Obtain a unified, real-time asset inventory of all connected OT and ICS devices with 30+ active and passive discovery techniques.

**Accurate**
Baseline assets and defend your network with thousands of OT-specific threat indicators and powerful anomaly detection.

**Effective**
Proactively assess risks, discover threats, measure their business impact, and quickly prioritize remediation tasks.

**Efficient**
Automate time-intensive compliance and risk assessment tasks while minimizing human error and increasing efficiency.

**Visualize**
Get comprehensive passive device visibility without relying on SPAN for 100% coverage
Patented deep packet inspection (DPI) of 270+ IT and OT protocols

**Detect**
Collect comprehensive OT asset information and log all configuration changes for security analysis and operational forensics
Automate threat detection, containment and remediation with alert investigation and response tools

**Respond**
Simplify compliance efforts for key standards, including NERC CIP, EU NIS Directive, NIST CSF, IEC 62443, and TSA Pipeline Security
Dashboard enhance user collaboration, and rich alert details support efficient incident response
Forescout eyeinspect Data Sheet

Visualize

Visualize thousands of devices in a single view

- Passively obtain an accurate, real-time asset inventory without disrupting operations.
- See IP-enabled and serial connected assets, including HMIs, SCADA, PLCs, building management systems (BMS) and building automation systems (BAS).
- Prioritize alerts and view logs according to various parameters, including time, devices, network location and alert type.

Detect

Detect threats and manage risks intelligently

- Detect known and unknown cyberthreats using thousands of ICS/OT-specific threat checks and indicators of compromise (IOC).
- Detect cyber and operational risks and prioritize them according to the level of urgency and potential impact on the business.
- Detect noncompliant assets and policies throughout the network.
- Detect changes to the network in real-time, including new devices, changes to infrastructure, and irregular operational activity.

Respond

Respond with the world’s most intelligent and scalable OT security solution

- Leverage intuitive risk scores to respond to cyber and operational threats which simplifies response decisions
- Automated workflows, rules, and remediation actions enable real-time response to threats as they emerge
- Respond to compliance changes with asset baseline-defined rules, parameters, and reports

eyeInspect Solves For:

- **OT visibility gaps** caused by geo-distributed and heterogenous device networks.
- **Defense and vulnerability challenges** when patches go unaddressed, or applications are left exposed.
- **Operational and cyber risk** due to alert overload and improper remediation task prioritization.
- **Incomplete threat intelligence** hindering the execution of defensible policies.
- **Compliance tasks** that are resource-intensive and expose your organization to risk of serious fines.

eyeInspect Solves For:

- OT visibility gaps caused by geo-distributed and heterogenous device networks.
- Defense and vulnerability challenges when patches go unaddressed, or applications are left exposed.
- Operational and cyber risk due to alert overload and improper remediation task prioritization.
- Incomplete threat intelligence hindering the execution of defensible policies.
- Compliance tasks that are resource-intensive and expose your organization to risk of serious fines.

eyeInspect Solves For:

- OT visibility gaps caused by geo-distributed and heterogenous device networks.
- Defense and vulnerability challenges when patches go unaddressed, or applications are left exposed.
- Operational and cyber risk due to alert overload and improper remediation task prioritization.
- Incomplete threat intelligence hindering the execution of defensible policies.
- Compliance tasks that are resource-intensive and expose your organization to risk of serious fines.
## Enterprise Command Center Requirements

<table>
<thead>
<tr>
<th>Hardware/Hypervisor</th>
<th>PRODUCT DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>19” rack server or minimum VMware ESXi 5</td>
<td></td>
</tr>
<tr>
<td>Processor</td>
<td>4-core (Intel®) CPU 64-bit ≥ 2.4GHz</td>
</tr>
<tr>
<td>Memory Size</td>
<td>16-32 GB</td>
</tr>
<tr>
<td>Hard Drive</td>
<td>&gt; 250 GB</td>
</tr>
<tr>
<td>Network Interface</td>
<td>Interface for Command Center communication and web application access</td>
</tr>
</tbody>
</table>

## Command Center Requirements

<table>
<thead>
<tr>
<th>SMALL DEPLOYMENT (≤ 5 sensors)</th>
<th>MEDIUM DEPLOYMENT (≤10 sensors)</th>
<th>LARGE DEPLOYMENT (&gt;10 sensors ≤100)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hypervisor</td>
<td>Minimum VMware ESXi5</td>
<td></td>
</tr>
<tr>
<td>Form Factor</td>
<td>19” rack server or virtual appliance</td>
<td></td>
</tr>
<tr>
<td>Processor</td>
<td>4-core CPU 64-bit</td>
<td></td>
</tr>
<tr>
<td>Memory Size</td>
<td>16(*)-64 GB</td>
<td></td>
</tr>
<tr>
<td>Hard Drive</td>
<td>500 GB</td>
<td></td>
</tr>
<tr>
<td>Network Interface</td>
<td>Interface for sensor communication and web application access (Based on data retention of 90 days)</td>
<td></td>
</tr>
</tbody>
</table>

## Passive Sensor Requirements

<table>
<thead>
<tr>
<th>SMALL DEPLOYMENT (≤ 5 sensors)</th>
<th>MEDIUM DEPLOYMENT (≤10 sensors)</th>
<th>LARGE DEPLOYMENT (&gt;10 sensors ≤100)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example Hardware Model</td>
<td>Foxguard® IADIN-FS1</td>
<td>Dell® Embedded PC 5000</td>
</tr>
<tr>
<td>Deployment Description</td>
<td>Deployments in small networks and harsh environments</td>
<td></td>
</tr>
<tr>
<td>Form Factor</td>
<td>Small-sized industrial PC/DIN rail-fitting</td>
<td></td>
</tr>
<tr>
<td>Processor</td>
<td>2- or 4-core (Intel) CPU 64-bit</td>
<td></td>
</tr>
<tr>
<td>Memory Size</td>
<td>8-16 GB</td>
<td></td>
</tr>
<tr>
<td>Hard Drive</td>
<td>64 GB – 500 GB in industrial PCs (wide-temperature SSDs should be used)</td>
<td></td>
</tr>
<tr>
<td>Monitoring Interface</td>
<td>Up to 4 monitoring ports</td>
<td></td>
</tr>
</tbody>
</table>

(*) memory size for eyeSight license only
Command Center Requirements

<table>
<thead>
<tr>
<th>INTEGRATED WITH PASSIVE SENSOR</th>
<th>STANDALONE</th>
<th>VIRTUAL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processor</td>
<td>2-4 core CPU</td>
<td>4 vCPU</td>
</tr>
<tr>
<td>Memory Size</td>
<td>4 GB RAM</td>
<td>4 GB RAM</td>
</tr>
<tr>
<td>Network Interface</td>
<td>≥ 1</td>
<td>≥ 1</td>
</tr>
</tbody>
</table>

eyInspect can be integrated directly on any passive sensor for small, medium and large deployments.

For more hardware requirement information, go to: https://www.forescout.com/company/resources/command-center-and-sensor-hardware-guidelines/

Protocols

For a complete list of all standard OT, IT and proprietary OT systems protocols, please visit this link: https://www.forescout.com/company/resources/eyeinspect-protocols/

Orchestrate, Segment, and Control

The Forescout Continuum platform extends the value of eyeInspect with a suite of capabilities to design and implement policies and automated actions for asset management, device compliance, network access, network segmentation and incident response.

Visit www.forescout.com/platform/ to learn about Forescout’s Continuum platform.