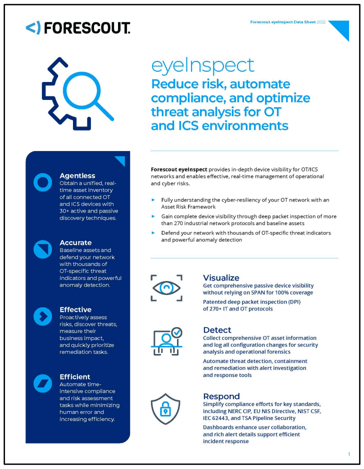


FORESCOUT.

Forescout eyeInspect Data Sheet 2022

eyeInspect

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

**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.

**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

**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

Dashboards enhance user collaboration, and rich alert details support efficient incident response

1

# Forescout eyeInspect Datasheet

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

Thank you for downloading this Forescout datasheet. Carahsoft is the dealer and distributor for Forescout cybersecurity solutions available via GSA Schedule 70, NASA SEWP V, ITES-SW, and other contract vehicles.

To learn how to take the next step toward acquiring Forescout's solutions, please check out the following resources and information:

For additional resources:
carah.io/ForescoutResources

For upcoming events:
carah.io/ForescoutEvents

For additional Forescout solutions:
carah.io/ForescoutProducts

For additional Cybersecurity solutions:
carah.io/Cybersecurity

To set up a meeting:
Forescout@carahsoft.com
833-FSCT-GOV

To purchase, check out the contract vehicles available for procurement:
carah.io/ForescoutContracts

For more information, contact Carahsoft or our reseller partners:
Forescout@carahsoft.com | 833-FSCT-GOV

# eyeInspect

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

**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

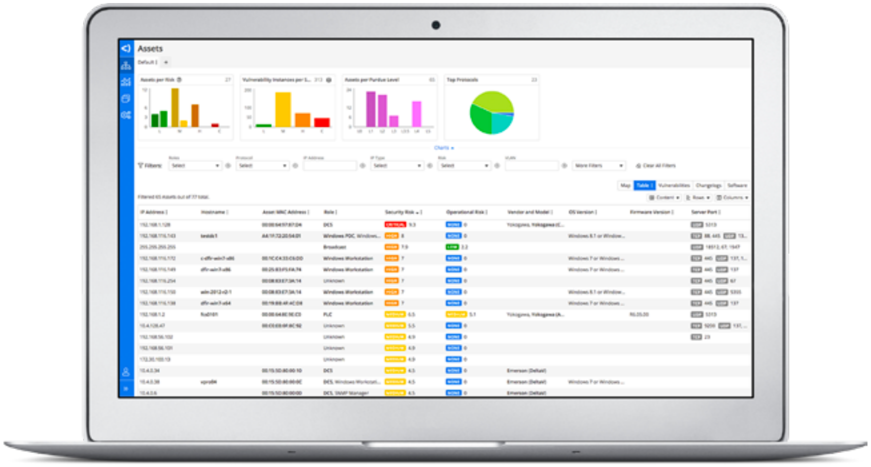
### Respond

Simplify compliance efforts for key standards, including NERC CIP, EU NIS Directive, NIST CSF, IEC 62443, and TSA Pipeline Security

Dashboards enhance user collaboration, and rich alert details support efficient incident response

## 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.



# 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

## Enterprise Command Center Requirements

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

## Command Center Requirements

(*) memory size for eyeSight license only

| | SMALL DEPLOYMENT (≤ 5 sensors) | MEDIUM DEPLOYMENT (≤10 sensors) | LARGE DEPLOYMENT (>10 sensors ≤100) |
|---|---|---|---|
| Hypervisor | Minimum VMware ESXi5 | | |
| Form Factor | 19” rack server or virtual appliance | | |
| Processor | 4-core CPU 64-bit | 4/6-core (Intel) CPU 64-bit | 12-core (Intel) CPU 64-bit |
| Memory Size | 16(*)-64 GB | 32(*)-64 GB | 64-256 GB |
| Hard Drive | 500 GB | 1 TB | >1 TB |
| | (Based on data retention of 90 days) | | |
| Network Interface | Interface for sensor communication and web application access | | |

## Passive Sensor Requirements

| | SMALL DEPLOYMENT (≤ 5 sensors) | MEDIUM DEPLOYMENT (≤10 sensors) | LARGE DEPLOYMENT (>10 sensors ≤100) |
|---|---|---|---|
| Example Hardware Model | Foxguard® IADIN-FS1 | Dell® Embedded PC 5000 | Dell® PowerEdge R640 |
| Deployment Description | Deployments in small networks and harsh environments | Deployments in medium-sized networks, harsh environments | Deployments in large networks and data center installations |
| Form Factor | Small-sized industrial PC/DIN rail-fitting | Medium-sized industrial PC | 19” 1U rack server |
| Processor | 2- or 4-core (Intel) CPU 64-bit | 4 or 6-core (Intel) CPU 64-bit with 8 GT/s | 6-core (Intel) CPU 64-bit ≥ 2.4GHz |
| Memory Size | 8-16 GB | 16-32 GB | 64-256 GB |
| Hard Drive | 64 GB – 500 GB in industrial PCs (wide-temperature SSDs should be used) | | |
| Monitoring Interface | Up to 4 monitoring ports | Up to 8 monitoring ports | Up to 8 monitoring ports |

## Command Center Requirements

**INTEGRATED WITH PASSIVE SENSOR**

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

| | STANDALONE | VIRTUAL |
|---|---|---|
| **Processor** | 2-4 core CPU | 4 vCPU |
| **Memory Size** | 4 GB RAM | 4 GB RAM |
| **Network Interface** | ≥ 1 | ≥ 1 |

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.

**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