FORESCOUT
Active Defense for the Enterprise of Things.

eyeInspect
Formerly SilentDefense

AGENTLESS

Gain a unified, real-time and complete OT asset inventory of connected IP and serial devices.

ACCURATE

Baseline assets and defend your network with thousands of OT-specific threat indicators and powerful machine-learning-based anomaly detection.

EFFECTIVE

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

DEPENDABLE

Gain real-time assurance that security tools and compliance controls are working.

EFFICIENT

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

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

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

- Establish a baseline of admissible network behavior using thousands of ICS/OT-specific threat indicators and queries
- Aggregate thousands of alerts and millions of logs according to their risk level and cause
- Auto-classify and assess devices for policy and regulatory compliance

VISUALIZE

See devices the instant they connect to the network

Continuously monitor as devices come and go

Get real-time asset inventory without business disruption

DETECT

Identify diverse types of IP-enabled and serial OT devices

Baseline devices and device groups

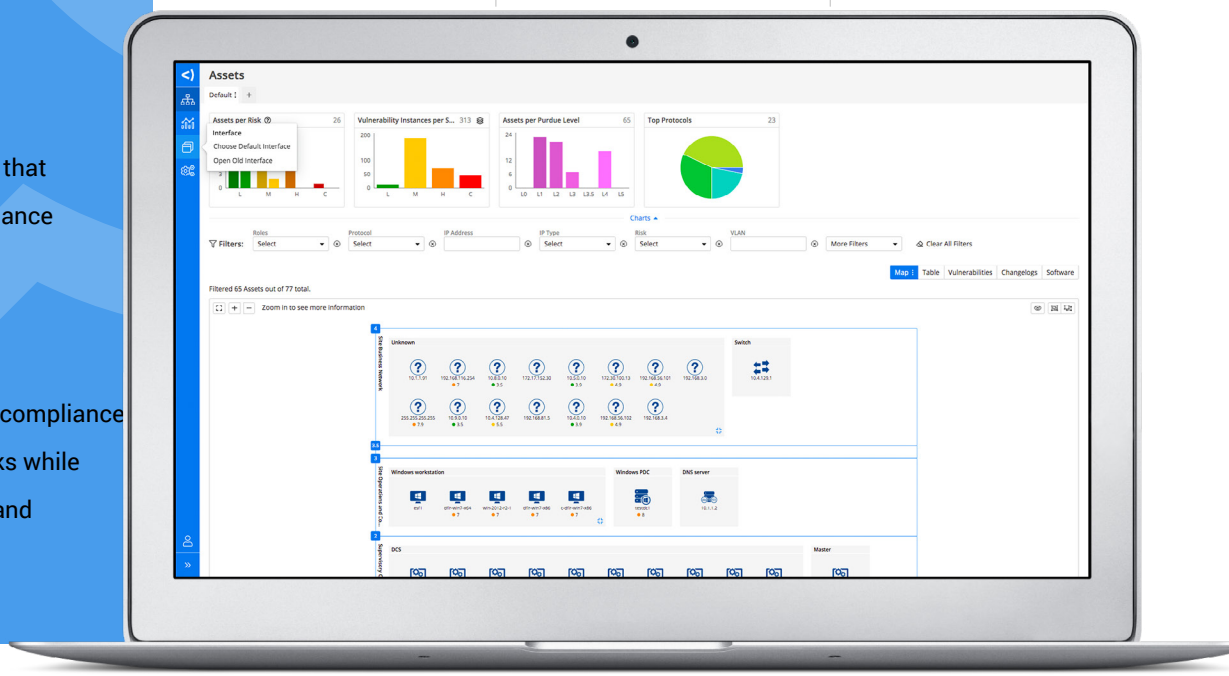
Optimize auto-classification efficacy and continuous monitoring

RESPOND

Automate compliance assessments

Assess risk with intuitive risk scores

Gain situational awareness of cyber and operational risk



VISUALIZE

Visualize thousands of devices on a single screen

- See everything. Eliminate blind spots associated with newly connected and rogue devices
- Obtain a detailed, accurate, real-time asset inventory
- See IP-enabled and serial devices, including HMIs, SCADA, PLCs, controllers, sensors, meters and I/O

DETECT

Detect threats and manage risks intelligently

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

RESPOND

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

- Respond to cyber and operational threats according to clear scores
- Respond to alerts with pre-defined automated workflows, rules and remediation actions
- Respond to compliance changes with asset baseline-defined rules, parameters and reports
- See building management system (BMS) and building automation system (BAS) devices, including HVAC and access control
- See other physical and SDN infrastructure, including switches, routers, VPSs, wireless access points and controllers
- See alerts and logs according to various parameters, including time, devices, network location and alert type

Enterprise Command Center Requirements

Minimum Requirements	
Hardware/Hypervisor	19" rack server or minimum VMware ESXi 5
Processor	12-core (intel®) CPU 64-bit ≥ 2.4GHz
Memory size	32-64 GB
Hard drive	500 GB–1TB thin provisioning
Network interface	Interface for Command Center communication and web application access

Command Center Requirements

	Small Deployment (≤ 5 sensors)	Medium Deployment (≤10 sensors)	Large Depolyment (>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 ≥ 2.4 GHz
Memory size	16 GB	32 GB	64-256 GB
Hard drive	500GB	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 (up to 100 Mbps)	Medium Deployment (up to 500 Mbps)	Large Depolyment (up to 1 Gbps)
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	4-16 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

Minimum Active Sensor Requirements

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

	Stand Alone	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

Forescout extends the value of eyeInspect and the Forescout platform with a suite of products 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 eyeSight, eyeSegment, eyeControl, eyeManage and eyeExtend products.

eyeINSPECT SOLVES FOR:

OT visibility gaps caused by geo-distributed and non-homogeneous 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

Don't just see it. Secure it.

Contact us today to actively defend your Enterprise of Things.

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