FORESCOUT

Solution Brief

ICS Patrol

Going Selectively Active for Comprehensive OT Visibility

A passively driven, active component for extended ICS device visibility and network intelligence

79%

of organizations with a SCADA/ICS network have suffered a breach in the past 24 months [1]

— Forrester

The Challenge

Operational technology (OT) cybersecurity stakeholders and ICS asset owners may have blind spots within their operation that a completely passive ICS cybersecurity solution cannot solve. Incomplete asset information and device visibility resulting from dormant and legacy ICS devices can leave networks exposed to elevated risk. Moreover, regulatory compliance tasks are resource intensive and prone to potential human error. OT asset owners demand detailed and contextual device data for enriched security posture analysis and a better means of supporting compliance efforts.

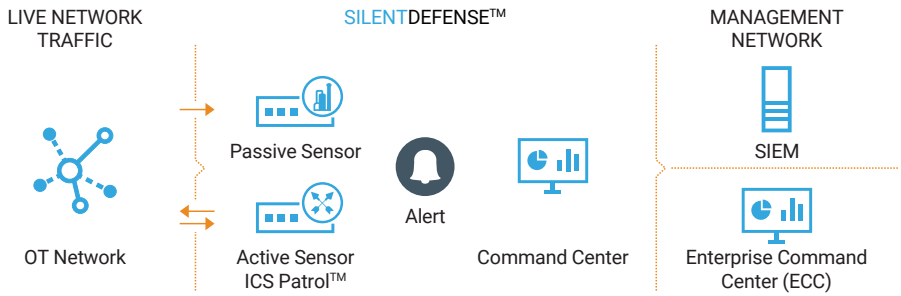
Passive Monitoring Capabilities		Active Monitoring Capabilities		SilentDefense™ with ICS Patrol™
• Vendor agnostic • Plug and play capable • Non-intrusive threat detection • Advanced network monitoring	+	• Extended device visibility • Detailed fingerprinting • Compliance task automation	=	• Identify and monitor dormant devices • Automate compliance and reporting tasks • Enrich device data for extended security posture analysis
PASSIVE		ACTIVE		BETTER TOGETHER

SilentDefense ICS Patrol

- Provides detailed asset inventory and device fingerprinting information such as installed patches, installed applications or open ports and services.
- Improves situational awareness of OT and ICS networks by providing detailed device operating status of dormant devices.
- Extracts asset information from PLCs without the need for a passive sensor.
- Supports compliance and regulatory tasks with the automated gathering of relevant network data and performance indicators.
- Safeguards sensitive equipment by using ICS Patrol's OT-specific scanning policies.

ICS Patrol: The Best of Both Worlds

When combined with the completely passive SilentDefense sensor, ICS Patrol merges passive anomaly detection with active cybersecurity capabilities to non-intrusively extend ICS network visibility and operating intelligence. Provided as a separate, optional component in the form of a modular add on to SilentDefense, ICS Patrol is carefully driven by the passive system and selectively queries specific hosts based on one or more asset inventory characteristics. It can also actively query PLCs from popular OT vendors without the passive sensor. This enriches alert details with valuable contextual data of devices that otherwise may have been not visible. This added layer of visibility provides a more detailed asset inventory, comprehensive vulnerability and risk assessment, improved threat hunting capabilities and more efficient compliance with regulatory and internal standards.



Basic SilentDefense and ICS Patrol Deployment Model

ICS Patrol Use Cases

Network Discovery and Device Fingerprinting

ICS Patrol securely and selectively queries specific hosts on the ICS network to enhance asset visibility and provide more comprehensive inventories that include, but are not limited to, host status, OS version, manufacturer, software and applications, serial numbers, network user behavior and installed patches. It can also actively query PLCs from popular OT vendors without the passive sensor for an even more detailed asset inventory.

Comprehensive Risk and Vulnerability Assessment

A non-intrusive, automated process of collecting asset information allows cybersecurity stakeholders to evaluate risks and potential vulnerabilities in even greater detail. ICS Patrol enriches alert details with valuable contextual data that otherwise may have been not visible with a passive solution alone.

Easier Standards and Regulatory Compliance

ICS Patrol can selectively export all information collected by the active sensor to easily build periodical documentation of network status, helping to reduce operating costs and lower the risk of compliance violation fines under standards like NERC CIP and the NIS Directive.

1 Forrester Research 2018 – "Protecting Industrial Control Systems And Critical Infrastructure From Attack"

Experience ICS Patrol for yourself

SCHEDULE A DEMO

FORESCOUT

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