FORESCOUT

Securing Vulnerable ICS and OT Networks

Use pervasive asset visibility to unify cyber and operational risk management across IT, OT and ICS environments

Driven by the need to stay competitive, organizations are converging information technology and **operational technology (OT)** networks, which is increasing the complexity and vulnerability of previously isolated **industrial control system (ICS)** networks.

This digital evolution coupled with the explosive growth of agentless IoT devices has compounded the visibility gap, leaving industrial networks that power interconnected cities, industries and transportation systems vulnerable to hacking and other cyberthreats.

The Challenge

The risk of cyberattacks on OT systems is unprecedented as aging ICS systems converge with IoT-infused business and industrial networks of all kinds. Owners are increasingly at risk of control loss, unplanned downtime, revenue loss, threat propagation into IT networks, data loss, increasing administrative workloads and potential noncompliance. These risks are further increased by the widespread lack of comprehensive asset visibility across OT and ICS environments. As a result:

- 4 out of 10 ICS security practitioners lack sufficient visibility into their ICS networks [1]
- 70% of organizations suffer from some level of ignorance about their ICS assets [2]
- 79% of organizations with a SCADA/ICS network have suffered a breach in the past 24 months [3]

Forescout SilentDefense™: Instant Visibility and Cyber Resilience for OT Infrastructure

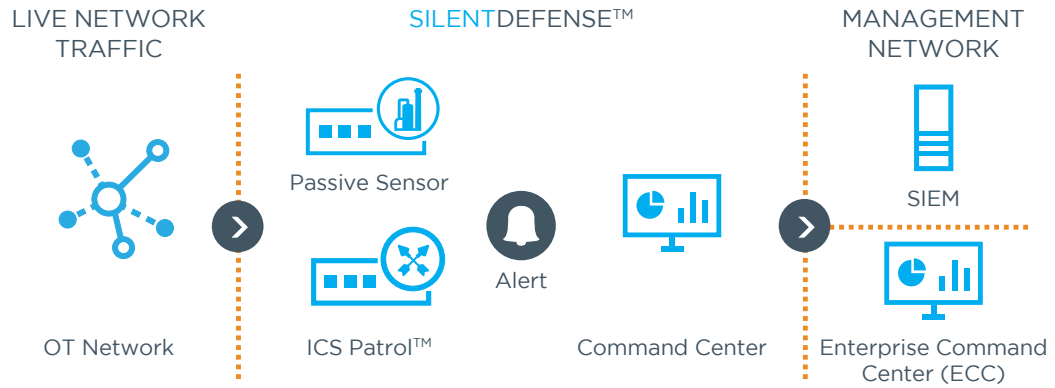
SilentDefense is a nonintrusive network monitoring and situational awareness solution that provides instant visibility and cyber resilience for OT and ICS networks. SilentDefense protects operational infrastructure from a wide range of threats with patented deep packet inspection (DPI) and anomaly detection technology, combined with a library of over 1,600 ICS-specific threat indicators for advanced cyberattacks, network misconfigurations and operational errors.

Forescout SilentDefense

- Is a nonintrusive network monitoring and situational awareness platform
- Provides instant visibility and cyber resilience for industrial control systems (ICS) and OT networks
- Allows you to monitor your ICS network from a single screen
- Deploys in hours
- Extends the exceptional device visibility, classification and profiling capabilities of the Forescout platform from campus, cloud and data center environments deep into OT and ICS environments

SilentDefense allows you to monitor your ICS network from a single screen. It deploys in hours by connecting SilentDefense passive monitoring sensors to the SPAN/mirroring ports of network switches. Asset information and alerts about potential threats are then delivered to a central management platform (the Command Center) in real time. From there, they can be escalated appropriately within the organizational ecosystem. In fact, SilentDefense natively interfaces with SIEM solutions, firewalls, IT asset management, sandboxes, authentication servers and other enterprise security systems, including the Forescout device visibility and control platform. Optionally, you can deploy additional nonintrusive active functionality with ICS Patrol™.

SilentDefense with ICS Patrol™ extends visibility and proactive threat-hunting capabilities beyond what would be possible with an agentless solution alone, without impact to network operations.

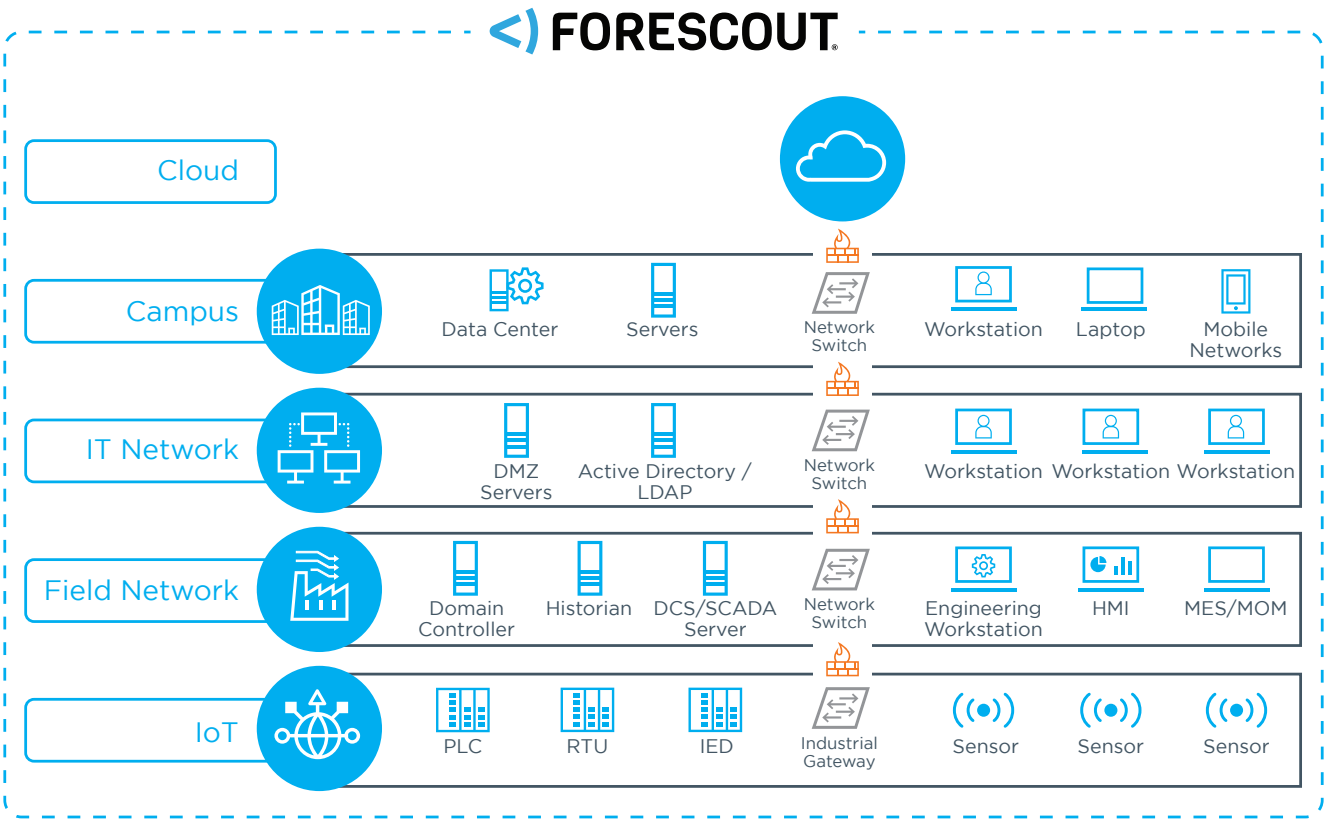


Simplified SilentDefense Deployment Model

Complete IT/OT Visibility

SilentDefense extends the industry-leading device visibility, classification and profiling capabilities of the Forescout platform far deeper into OT and ICS environments. It enables effective management of a full range of both cyber and operational risks, including:

- System shutdown
- Network connectivity issues
- System failure
- Device malfunction/misconfiguration
- Insecure protocols
- Default credentials
- Human safety
- SLA violations
- Data theft
- Regulatory fines



SilentDefense 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.

SilentDefense Use Cases

Asset visibility and monitoring

SilentDefense provides pervasive asset visibility across operational networks and sites. It automatically maps networks and inventories connected devices using a wide range of discovery capabilities that include:

- Patented deep packet inspection of 100+ IT/OT protocols
- Continuous, configurable policy and behavior monitoring
- Automatic assessment of device vulnerabilities, threat exposure, networking issues and operational problems

Asset configuration management

SilentDefense automatically collects a wide range of OT asset information, logging all configuration changes for security analysis and operational forensics. Discoverable details include:

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

Risk management and compliance

Proactively identify vulnerable OT assets with multifactor risk scoring and mitigation prioritization. SilentDefense includes powerful dashboards, analytics and reporting tools that simplify compliance across key standards, including NERC-CIP, NIST, ISA99/IEC 62443 and FDA. Its powerful, out-of-the-box reporting helps organizations comply with standards and required tasks.

Network access control and segmentation

SilentDefense leverages the ACL and VLAN assignment capabilities of the Forescout platform, bringing policy-based segmentation and access control to operational networks. It also offers plug-and-play integration with leading firewall vendors through Forescout Extended Modules as per IEC 62443.

Incident response

Automate threat detection, containment and remediation with SilentDefense's alert investigation and response tools. Dashboards and widgets enhance user collaboration. Rich alert detail supports root cause analysis and expedites effective, efficient response.

Bottom-Line Benefits of OT Asset Visibility

Forescout SilentDefense can directly impact the bottom-line profitability of an organization by improving the security and resilience of its operational systems while dramatically enhancing administrative efficiency, risk management and compliance. For example, Forescout recently studied the contribution of pervasive OT asset visibility and network monitoring to the financial performance of an asset owner using the example of a U.S. food production company with 17 FTEs focused on ICS cybersecurity and compliance.[4] The study found:

- Annual savings of $820,336 in reduced labor costs, increased management productivity and improved threat-hunting capabilities associated with asset and network visibility
- Annual savings of $346,456 related to actionable threat-management updates, faster incident response and reduced downtime risk, all associated with improved cyberthreat detection and response capabilities
- Annual savings of $158,120 in compliance costs associated with built-in integrations with ICS security and asset-management solutions.

[1] *SANS Survey, Securing Industrial Control Systems—2017*
[2] *Cyber Security for Industry 4.0: SecurityMatters Presenting Latest Cyber Resilience Solutions at ICS Europe*
[3] *SecurityMatters blog article, Unprecedented ICS Visibility and Control for a Proactive Cybersecurity Strategy, Oct. 2018*
[4] *Projections based on standardized SecurityMatters customer data*

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
Fax +1-408-371-2284