FORESCOUT

Solution Brief

Operational Technology

Securing Vulnerable ICS and OT Networks

Use continuous asset visibility to unify cyber and operational risk management across IT and OT environments

Driven by the need to stay competitive, organizations are converging information technology (IT) 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 IoT devices has compounded the visibility gap, leaving industrial networks that power critical infrastructure systems vulnerable to hacking and other cyberthreats.

By 2021

80%

of IIoT projects will have OT-specific security requirements [1]

— *Gartner*

The Challenge

The risk of cyberattacks on OT networks is unprecedented as aging ICS systems converge with IoT-infused business and industrial networks of all kinds. Asset owners and cybersecurity stakeholders are increasingly facing revenue loss from unplanned downtime, uncertain breach containment, increasing security operations workloads and potential noncompliance. These risks are further increased by the widespread lack of comprehensive asset visibility across OT and ICS environments.

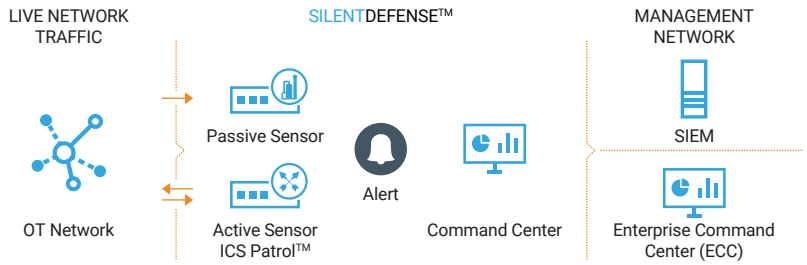
Forescout SilentDefense

- Enables passive, real-time network monitoring of OT and ICS networks.
- Provides non-intrusive active technology, ICS Patrol, to deliver deeper asset visibility.
- Saves time, improves SOC and analyst effectiveness and automates risk analysis with the Asset Risk Framework.
- Displays key operational status of multi-site OT and ICS networks on a single pane of glass with the Enterprise Command Center (ECC).
- Increases threat discovery capabilities and reduces the mean time to respond (MTTR) to cyberphysical threats.
- Extends the exceptional device visibility, classification and profiling capabilities of the Forescout platform from campus to OT.

Forescout SilentDefense™: Instant Cyber Resilience for OT Infrastructure

SilentDefense provides in-depth device visibility for OT/ICS networks and enables effective, real-time management of a full range of operational and cyber risks. SilentDefense protects critical infrastructure from a wide range of threats with patented deep packet inspection (DPI) and anomaly detection technology, combined with a vast library of ICS-specific threat indicators. The Asset Risk Framework, an impact-based risk analysis tool, aggregates relevant risk factors and weighs them based on the impact that corruption of a device may have to determine current risk posture and provides two intuitive risk scores. The Security Risk Score enables security analysts to immediately identify assets with a high probability of being attacked, while the Operational Risk Score enables OT engineers to quickly spot assets that need immediate attention.

SilentDefense lets you monitor your entire ICS network from a single screen. It deploys in hours by connecting 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 where 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 platform.



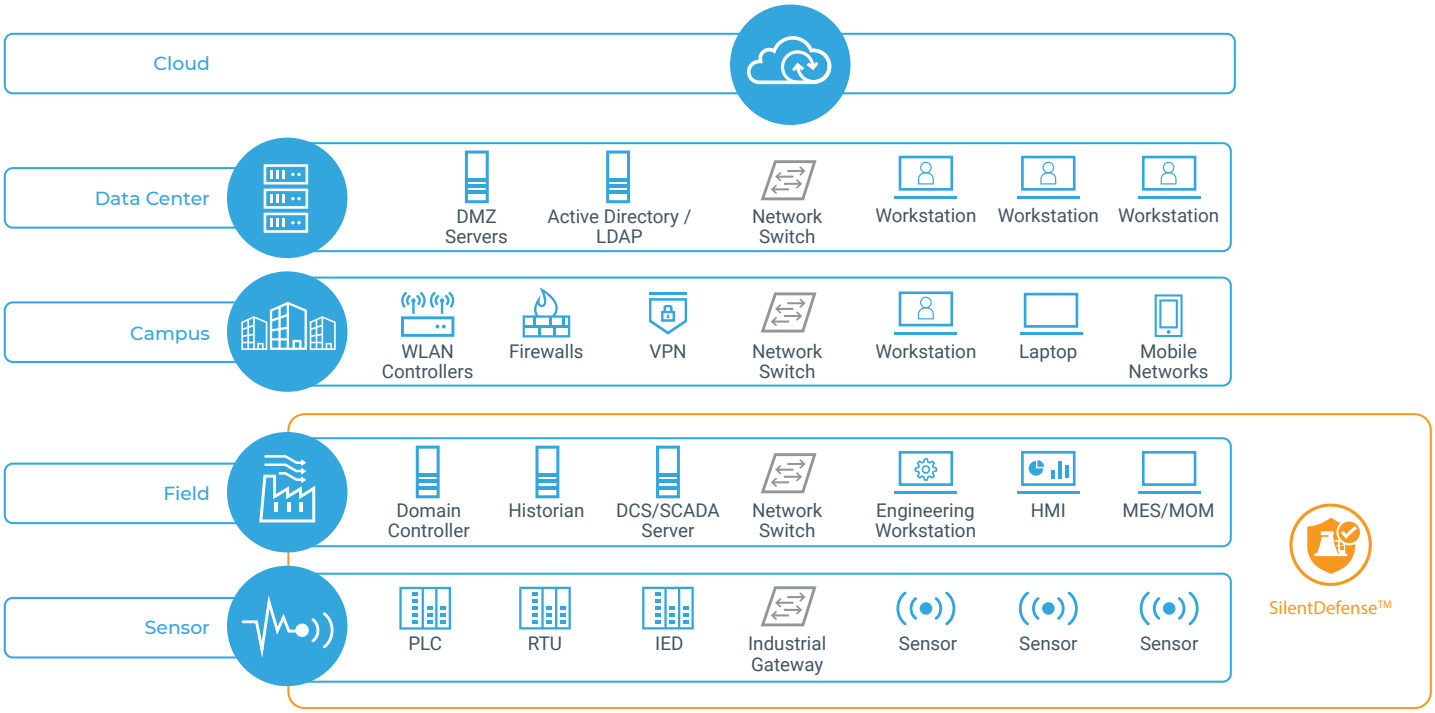
Basic SilentDefense Deployment Model

The optional selective scanning technology, ICS Patrol™, extends asset visibility even deeper into OT environments by selectively querying specific hosts to better identify and dissect asset information, files, vulnerabilities, compliance violations and threats. The optional Enterprise Command Center (ECC) provides global asset visibility and risk management for geo-distributed networks. Security stakeholders can analyze any incident in detail, including devices involved and context of the alert. The ECC solves real problems related to IT-OT convergence by transmitting relevant data from the field level up to the enterprise level.

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 the identification and effective remediation of a full range of both cyber and operational threats, including, but not limited to the following:

- Cyber attacks (DDoS, MITM & Scanning, etc.)
- Unauthorized network connections, communications
- Suspicious user behavior / policy changes
- Device malfunction misconfiguration
- New and non-responsive assets
- Corrupted messages
- Unauthorized firmware downloads
- Insecure protocols
- Default credentials and insecure authentications
- Logic changes



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 continuous asset visibility across OT networks and sites.

SilentDefense provides continuous asset visibility across OT networks and sites. It automatically builds a detailed network map with rich asset details and automatic grouping by network and/or role, provided in multiple formats such as Purdue level and communication relationship. SilentDefense uses a wide range of discovery capabilities that include:

- Patented deep packet inspection of 130+ IT and OT protocols.
- Continuous, configurable policy and behavior monitoring.
- Automatic assessment of device vulnerabilities, threat exposure, networking issues and operational problems.
- Optional, non-intrusive active component to selectively query specific hosts.

Optional, active component ICS Patrol can selectively query specific hosts for deeper asset information.

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

SilentDefense includes powerful dashboards, analytics and out-of-the-box reporting tools that simplify compliance with key standards.

Risk Management and Compliance

Proactively identify vulnerable OT assets to prioritize mitigation strategies with the Asset Risk Framework, the first centrally available 'impact-based' risk tool for ICS/OT networks. It saves time, improves SOC and analyst effectiveness and reduces risk by automating security and operational risk analysis. SilentDefense includes powerful dashboards, analytics and out-of-the-box reporting tools that simplify compliance with key standards, including NERC CIP, NIST, ISA99/IEC 62443 and FDA. The non-intrusive active capabilities of ICS Patrol also help ease compliance with NERC CIP requirements, including Access Control Management, Security Patch Management and Configuration Change Management.

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 as per IEC 62443.

The Enterprise Command Center (ECC) lets users zoom in on alerts from any of their multi-site or geo-distributed networks to analyze an incident in detail.

Threat Detection & 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. The Enterprise Command Center (ECC) lets users zoom in on alerts from any of their multi-site or geo-distributed networks to analyze an incident in detail, including devices involved and context of the alert.

Bottom-Line Benefits of OT Cyber Resilience

Forescout SilentDefense can positively impact an organization's bottom line 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 OT network monitoring to the financial performance of an asset owner using an example U.S. food production company with 17 FTEs focused on ICS cybersecurity and compliance.[2] 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 7 Questions SRM Leaders Ar en't Asking OT Security Providers During Technology Selection, Saniye Alaybe yi, Gartner, 2018, https://www.forescout.com/gartner-report-7-questions-for-OT-security-providers

2 Projections based on standardized customer data, actual savings may vary depending on multiple factors

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