FORESCOUT

SilentDefense™ Datasheet

SilentDefense is a non-intrusive network monitoring and situational awareness platform that provides in-depth visibility and cyber resilience for industrial control systems (ICS) and SCADA networks.

SilentDefense protects ICS/SCADA networks from a wide range of threats. It combines patented anomaly detection and deep packet inspection (DPI) with a library of over 2,100+ ICS-specific behavioral checks and a continuously growing library of 3,000+ IoCs to protect asset owners from advanced cyberattacks, network misconfigurations, and operational errors.

SilentDefense natively interfaces with enterprise systems such as SIEM, firewalls, IT asset management, malware analysis, authentication servers and third-party platforms.

Asset Inventory and Network Map

- Automatic asset, communication and vulnerability inventory with full device fingerprinting
- Interactive visualizations of threats and risks
- Host properties, activity and configuration change log
- Optional active component driven by the passive system to collect information such as open ports, services, applications and patches

Network and Process Monitoring

- Patented DPI for IT & OT protocols, monitoring protocol correctness and process values
- Self-configuring network and process whitelists
- Automatic assignment of alerts to cases

SDK for Advanced Customizations

- Easy development of complex network- and process-specific checks
- Quick support for new protocols and custom integrations

Logging & Investigation

- Logging and behavioral analysis of remote authentications, DNS communications and file operations
- Multi-factor file dissection: effectively extracting and analyzing files using rule-based analysis

Threat Hunting Framework

- Comprehensive search for indicators of incidents in network traffic and protocol messages
- Automatic threat intelligence ingestion and back-in-time threat detection
- 2,100+ threat indicators like protocol compliance checks, CVEs, and proprietary behavioral checks for cyberattacks, network issues, and operational errors

Dashboard and Reporting

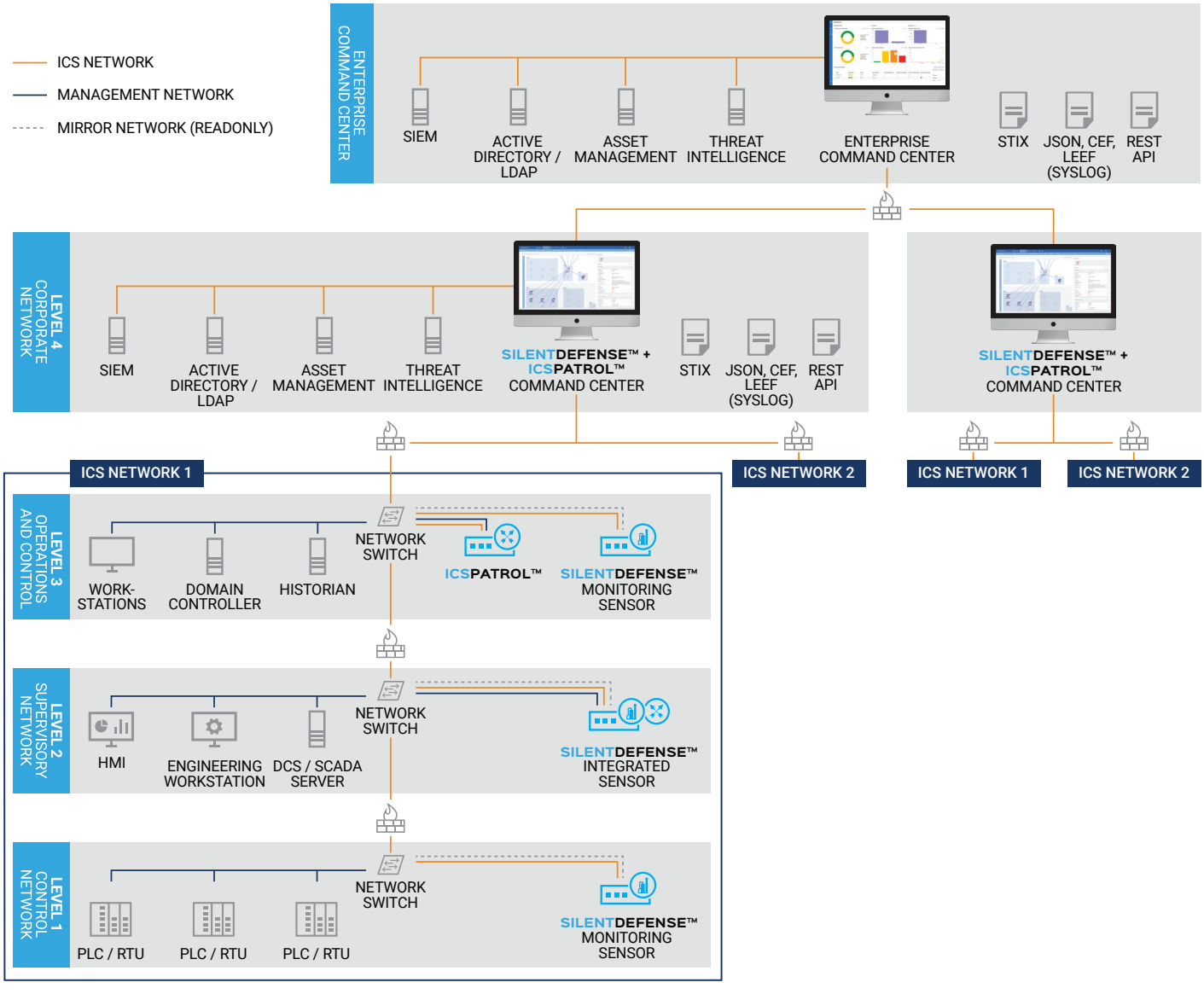
- Dashboards and widgets for easy collaboration among users on asset and threat visibility, including alert trends, asset charts etc.
- Rich alert details to enable root cause analysis and incident response
- Automated generation of editable graphical reports

Components and Architecture

SilentDefense provides in-depth device visibility and cyber resilience for OT/ICS networks. By connecting to the SPAN/mirroring port of a network switch, it passively establishes a complete asset inventory and network baseline of normal communications. SilentDefense immediately alerts if there is a deviation, enabling real-time operational and cyber risk management.

An optional active component driven by the passive system, ICS Patrol™, allows discovery of assets in a given network, or network segment, for more comprehensive asset inventory / device fingerprinting.

At the top level, the Enterprise Command Center (ECC) aggregates the information coming from multiple SilentDefense Command Centers into a single dashboard for monitoring global system health, assets, vulnerabilities and threats.



Available Configurations

Enterprise Command Center Requirements

	Standard Deployment
Model / hypervisor	 vmware
Form factor	19” rack server or virtual appliance
Processor	12-core (Intel) CPU 64 bits ≥ 2.4GHz
Memory size	≥ 32-64 GB
Hard drive	500 GB - 1 TB

Command Center Requirements

	Small Deployment (up to 5 sensors)	Medium Deployment (up to 10 sensors)	Large Deployment (more than 10 sensors)
Model / hypervisor	 vmware		
Form factor	19” rack server or virtual appliance		
Processor	4-core (Intel) CPU 64 bits	4/6-core (Intel) CPU 64 bits	12-core (Intel) CPU 64 bits ≥ 2.4GHz
Memory size	16-32 GB	32-64 GB	64-256 GB
Hard drive	500 GB - 1 TB		

Passive Sensor Requirements

	Small Deployment (up to 40 Mbps)	Medium Deployment (up to 200 Mbps)	Large Deployment (up to 1 Gbps)
Example hardware model			
Deployment description	Deployments in small networks and harsh environments	Deployments in medium-sized networks and harsh environments	Deployments in large networks and data center installation
Form factor	Small size industrial PC / DIN-rall fitting	Medium-size industrial PC	19” 1U rack server
Processor	2- or 4- core (Intel) CPU 64 bits	6-core (Intel) CPU 64 bits	6-core (Intel) CPU 64 bits ≥ 2.4GHz
Memory size	4-16 GB	16-32 GB	32-64 GB
Hard drive	64 GB - 500 GB		
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		Stand Alone	Virtual
It can be integrated directly on any passive sensor for small, medium and large deployment.	Processor	2-4 core CPU	4 vCPU
	Memory size	4 GB RAM	4 GB RAM
	Network interface	≥ 1	≥ 1

Configurations shown as examples. Refer to a sales representative for details and specific requests like increased number of monitoring ports.

Protocols

Standard OT Protocols

- BACnet
- CC-Link (Field, FieldBasic, Control)
- DLMS/COSEM
- DNP3
- EtherCAT
- EtherNet/IP + CIP
- Foundation Fieldbus HSE
- 60870-5-104 / 101
- ICCP TASE.2
- IEC 61850 (MMS, GOOSE, SV)
- IEEE C37.118 (Synchrophasor)
- Modbus ASCII
- Modbus RTU
- Modbus/TCP
- OPC-DA
- OPC-AE
- PROFINET (RPC, RTC, RTA, DCP and PTCP)
- SLMP

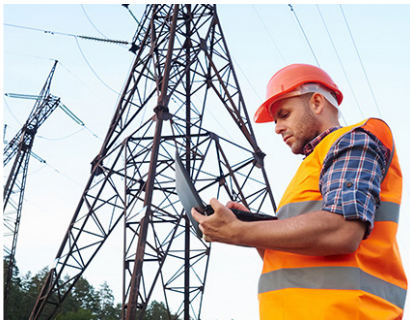
Proprietary OT Systems/Protocols

- CNCP (ABB)
- CSLib (ABB 800xA)
- DMS (ABB AC 800 F)
- MMS (ABB AC 800 M)
- PN800 (ABB Harmony)
- RNRP (ABB)
- SPLUS (ABB Symphony Plus)
- ADS/AMS (Beckhoff)
- BSAP & BSAP IP (Bristol Babcock)
- CDP (Cisco)
- CygNet SCADA (CygNet)
- DeltaV (Emerson)
- Ovation (Emerson)
- ROC (Emerson/Fischer)
- SRTP (GE)
- SES 92 (GRE)
- Experion (Honeywell)
- FOX (Honeywell Niagara / Tridium)
- LonTalk (LonWorks)
- Melsoft (Mitsubishi Electric)
- ADE (Phoenix Contact)
- CIP extensions (Rockwell/AB)
- CSP (Rockwell/AB)
- Citect (Schneider Electric)
- COMEX (Schneider Electric Foxboro)
- Modbus/TCP Unity (Schneider Electric)
- OASyS (Schneider Electric)
- Triconex Tristation (Schneider Electric)
- Fast Message Protocol (SEL)
- Telnet extensions (SEL)
- Sinec H1 (Siemens)
- Step7 (Siemens)
- S7COMM+/OMS+ (Siemens)
- CAMS(Yokogawa)
- Centum DCS (Yokogawa)
- HART nested devices (Yokogawa)
- ISaGRAF IXL (Yokogawa ProSafe and others)
- Vnet/IP (Yokogawa)
- VNet IP WAN(Yokogawa)
- CodeSys (Wago, ABB, and others)

IT Protocols

- AFP
- BGP
- HSRP (Cisco)
- DHCP
- DNS
- DTP
- FTP
- HTTP
- ISAKMP
- IMAP
- Kerberos
- LDAP
- LDP
- LLDP
- MS-SQL
- MQTT
- NMF
- NTP
- NetBIOS
- NetSupport
- OpenRDA
- Oracle TNS
- POP3
- PVSS
- Radius
- RDP
- RFB/VNC
- RIP
- RPC/DCOM
- RTCP
- RTP
- RTSP
- SMB /CIFS
- SMTP
- SNMP
- SSDP
- SSH
- SSL
- STP
- SunRPC
- Telnet
- TFTP



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