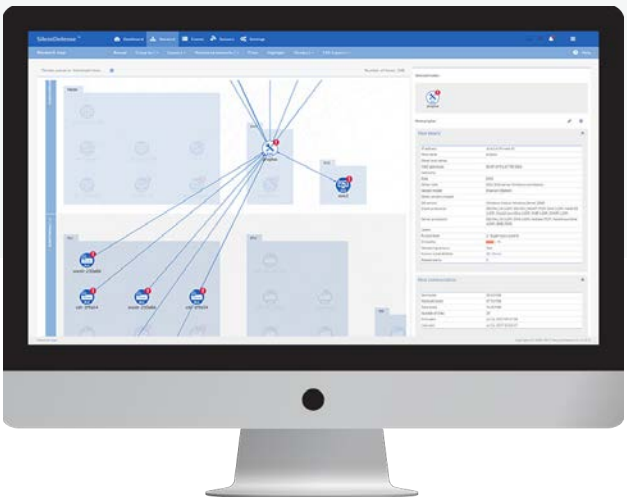
FORESCOUT

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 the widest range of threats. It combines patented deep packet inspection (DPI) technology with a library of over 1,600 ICS-specific threat indicators to protect asset owners from advanced cyberattacks, network misconfigurations, and operational errors.



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
- Advanced vulnerability management

Network and Process Monitoring

- Full patented DPI for IT & OT protocols, monitoring down to process values
- Self-configuring network and process whitelists
- Automatic assignment of alerts to cases

SDK for Advanced Customizations

- Complex network- and process-specific checks
- Ability to extend protocol support and easily develop custom integrations

Logging & Investigation

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

Threat Hunting Framework

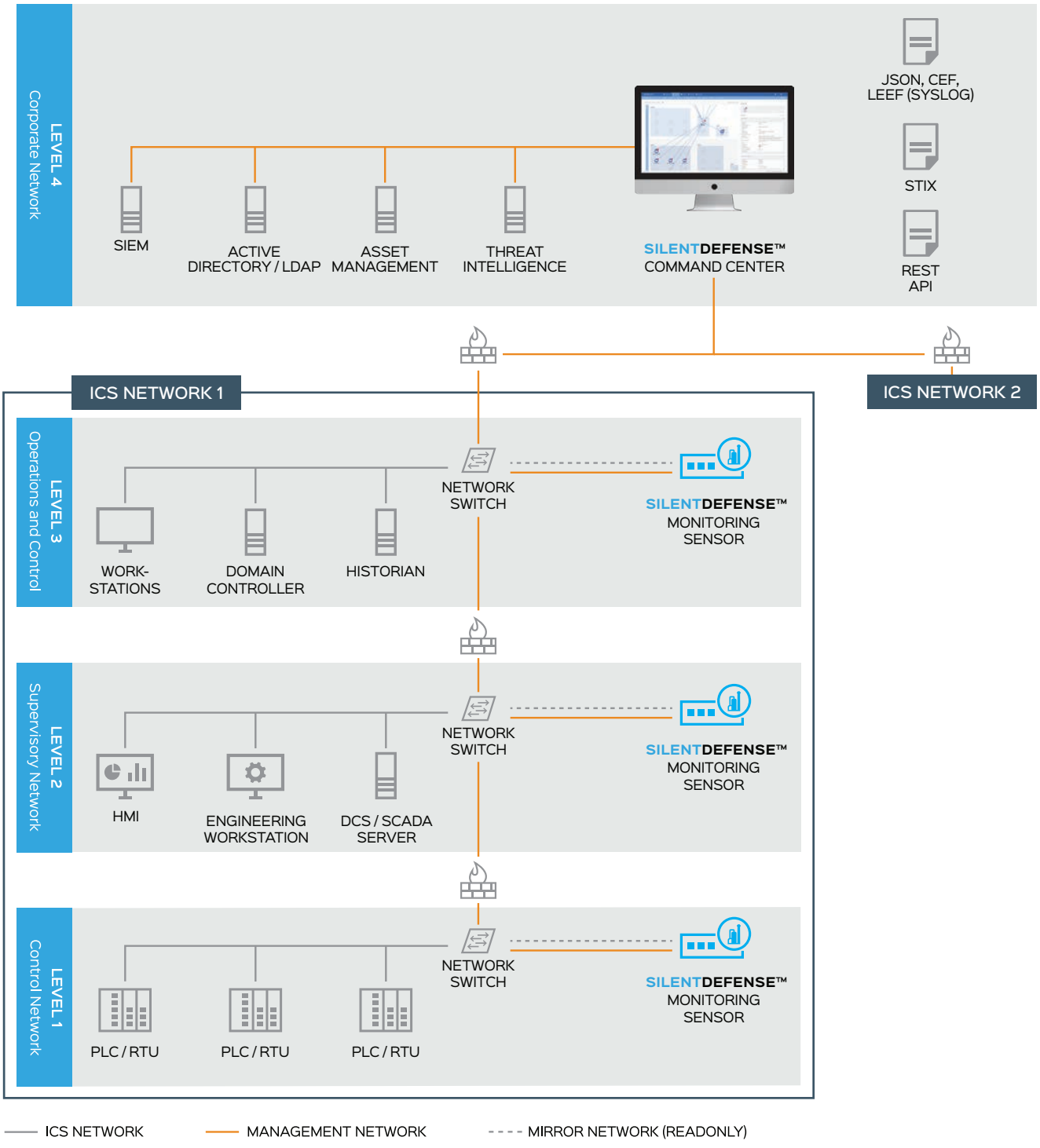
- Comprehensive search for indicators of incidents in network traffic and protocol messages
- Automatic threat intelligence ingestion and back-in-time threat detection
- 1,600+ threat indicators like protocol compliance checks, CVEs, and proprietary behavioral checks for cyberattacks, network issues, and operational errors

Analysis & Reporting

- Dashboards and widgets for asset and threat visibility, including: alert trends, asset charts and easy collaboration among users
- 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 and immediately alerts if there is a deviation, enabling real-time operational and cyber risk management. SilentDefense natively interfaces with enterprise systems such as SIEM solutions, firewalls, IT asset management, Sandboxes, authentication servers and third-party platforms.



Available Configurations

SilentDefense Command Center and Monitoring Sensors can be provided in different configurations:

- For deployments in production environments, the Command Center can be installed on a rack server or VMware ESXi hypervisors, whereas Monitoring Sensors are installed on dedicated hardware.
- For lab environments, assessments and demonstrations, the Command Center and one Monitoring Sensor can be provided, either physically or virtually, in a bundled configuration.

Command Centers are also offered in High Availability configuration.
New hardware platform can be certified on customer request.

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	6-core (Intel) CPU 64 bits	6-core (Intel) CPU 64 bits ≥ 2.4GHz
Memory size	≥ 12 GB	≥ 16 GB	≥ 32 GB
Hard drive	500 GB - 1 TB		

Sensor Requirements

	Small Deployment ≤20 Mbps (in some cases up to 40 Mbps)	Medium Deployment (up to 800 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 GB	16 GB	≥ 16 GB
Hard drive	64 GB - 500 GB		
Monitoring interface	Up to 4 monitoring ports	Up to 8 monitoring ports	Up to 8 monitoring ports

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), DNP3, EtherCAT, EtherNet/IP + CIP, Foundation Fieldbus HSE, 60870-5-104, 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

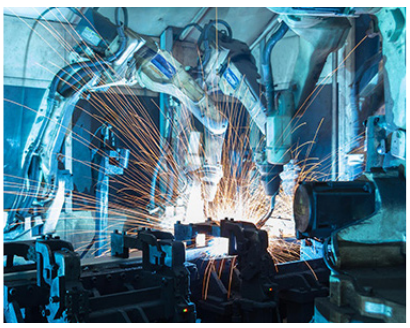
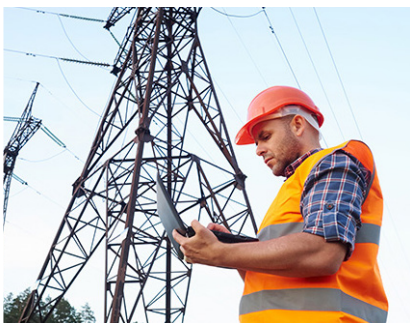
CSLib (ABB 800xA), DMS (ABB AC 800 F), MMS (ABB AC 800 M), PN800 (ABB Harmony), SPLUS (ABB Symphony Plus), ADS/AMS (Beckhoff), BSAP & BSAP IP (Bristol Babcock), CDP (Cisco), CygNet SCADA (CygNet), DeltaV (Emerson), Ovation (Emerson), SRTP (GE), Experion (Honeywell), FOX (Honeywell Niagara / Tridium), 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), Step7 (Siemens), S7COMM+/OMS+ (Siemens), Centum DCS (Yokogawa), ISaGRAF IXL (Yokogawa ProSafe and others), Vnet/IP (Yokogawa), CodeSys (Wago, ABB, and others)

IT Protocols

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

Additional protocols are continuously integrated. Refer to a sales representative for details and specific requests.



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