

SILENTDEFENSE™ DATASHEET

SilentDefense is a passive network monitoring and situational awareness platform that provides instant 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 1300 ICS-specific threat indicators to protect asset owners from advanced cyber-attacks, 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

1300+ ICS-Specific Threat Indicators

- 550+ IT/ICS protocol compliance checks
- 300+ controls for networking, operational and cyber security risks and threats
- 300+ vulnerabilities (CVEs) with dynamic updates

Network and Process Anomalies

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

Threat Hunting Framework

- Comprehensive search for indicators of incidents in network traffic and protocol messages
- Continuous full traffic recording for real-time and historical traffic analysis



SDK for Advanced Customizations

- Specification of complex network- and process-specific checks
- Ability to extend protocol support and easily develop custom integrations

Custom Event Logging and Analytics

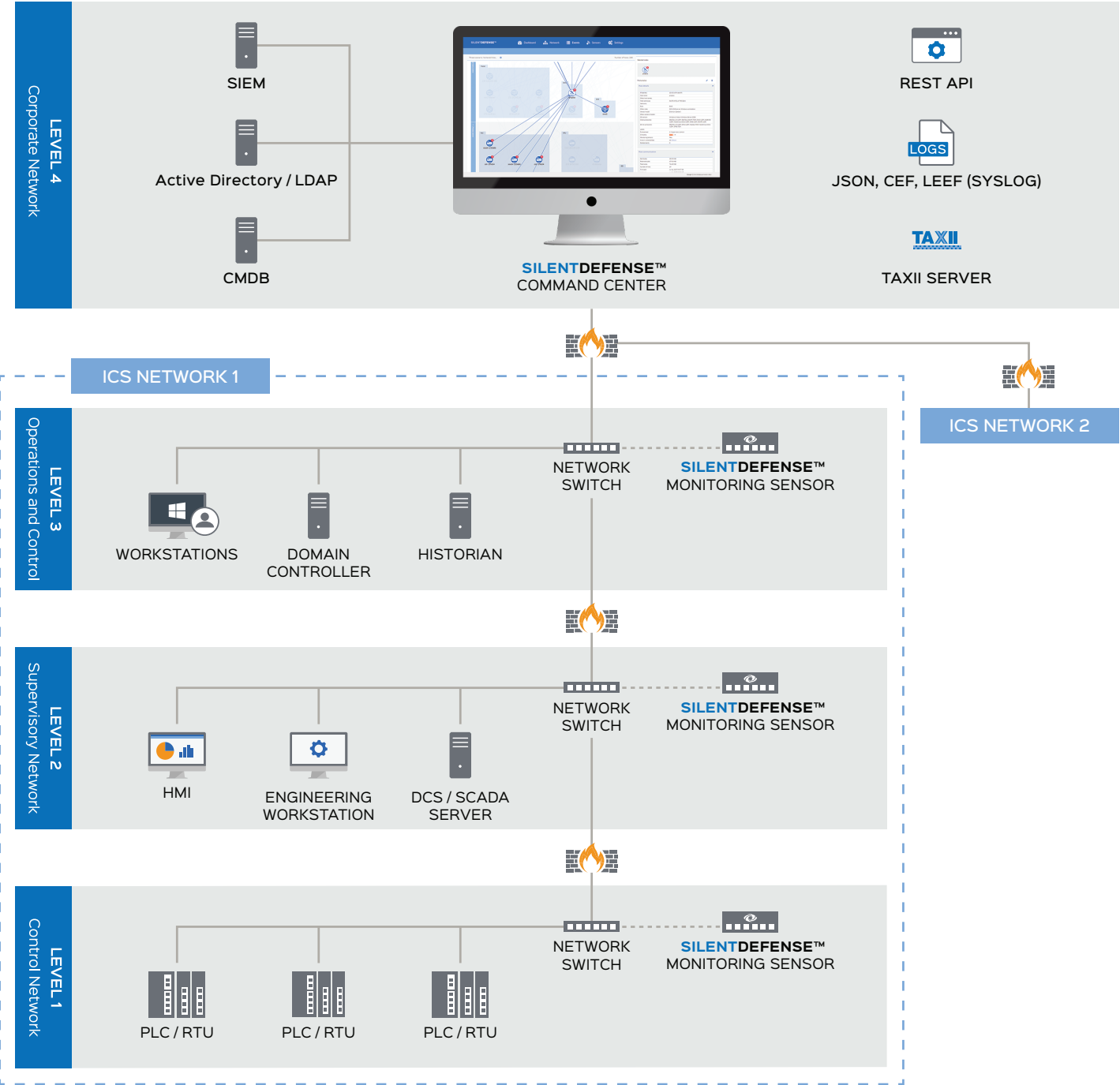
- Logging of remote access and authentication, DNS communications and file operations
- Customizable graphs and widgets to analyze trends and events

Dashboard and Reporting

- Real-time and historical views of network and device activity
- Rich alert details to enable root cause analysis and incident response
- Automated generation of detailed graphical reports

Components and Architecture

SilentDefense allows you to monitor your entire ICS network from a single screen. It is deployed in a matter of hours by connecting Monitoring Sensors to the SPAN/mirroring port of network switches, so that they can forward asset, flows and real-time threat information to the Command Center. SilentDefense natively interfaces with enterprise systems such as SIEM solutions, 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 20 sensors)	Large Deployment (more than 20 sensors)
Model / hypervisor	 		
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 \geq 2.4GHz
Memory size	\geq 12 GB	\geq 16 GB	\geq 32 GB
Hard drive	500 GB - 1 TB		
Management interface	Interface for sensor communication and web application access		

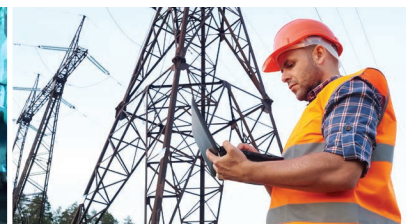
Sensor Requirements

	Small Deployment (up to 20 Mbps)	Medium Deployment (up to 500 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-rail 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 \geq 2.4GHz
Memory size	\geq 4 GB	16 GB	\geq 16 GB
Hard drive	64 GB - 500 GB		
Monitoring interface	Up to 4 monitoring ports	Up to 4 monitoring ports	Up to 8 monitoring ports
Management interface	Server management interface and connection to Command Center		

Protocols

SilentDefense supports analysis and Deep Packet Inspection (DPI) of both IT and OT protocols, as detailed in the table below. Additional protocols are integrated on a continuous basis and at customers' request.

Standard OT protocols	Proprietary OT systems/ protocols	IT protocols	
<ul style="list-style-type: none"> • BACnet • DNP3 • EtherCAT • EtherNet/IP + CIP • Foundation Fieldbus HSE • IEC 60870-5-101/104 • 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) 	<ul style="list-style-type: none"> • CSLib (ABB 800xA) • DMS (ABB AC 800 F) • MMS (ABB AC 800 M) • PN800 (ABB Harmony) • SPLUS (ABB Symphony Plus) • ADS/AMS (Beckhoff) • CygNet SCADA (CygNet) • DeltaV (Emerson) • Ovation (Emerson) • SRTP (GE) • Experion (Honeywell) • ADE (Phoenix Contact) • CIP extensions (Rockwell/AB) • CSP (Rockwell/AB) • COMEX (Schneider Electric Foxboro) • OASyS (Schneider Electric) • Modbus/TCP Unity (Schneider Electric) • Telnet extensions (SEL) • Step7 (Siemens) • S7COMM+/OMS+ (Siemens) • Vnet/IP (Yokogawa) 	<ul style="list-style-type: none"> • AFP • BGP • DHCP • DNS • FTP • HTTP • IMAP • Kerberos • LDAP • LDP • MS-SQL • NTP • NetBIOS • OpenRDA • POP3 • PVSS • Radius • RDP • RFB/VNC • RPC/DCOM • RTSP • SMB / CIFS 	<ul style="list-style-type: none"> • SMTP • SNMP • SSDP • SSH • SSL • SunRPC • Telnet • TFTP



SecurityMatters empowers critical infrastructure and manufacturing organizations with the ability to identify, analyze, and respond to industrial threats and flaws, minimizing troubleshooting costs and unexpected downtime. We leverage ICS-specific knowledge and understanding to provide visibility into critical assets and their activity, and detect operational problems and cyber security threats. Our revolutionary network monitoring platform has been successfully deployed by customers worldwide.

Copyright © 2018 SecurityMatters and respective copyright owners. All rights reserved.
www.secmatters.com | info@secmatters.com

