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 2,400+ ICS-specific behavioral checks and a continuously growing library of 3,500+ 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, PLC information, services, applications and patches
- Impact-based security and operational risk scoring framework

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
- 2,400+ 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

<table>
<thead>
<tr>
<th></th>
<th>Minimum Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardware / hypervisor</td>
<td>19” rack server or minimum VMware ESXi 5</td>
</tr>
<tr>
<td>Processor</td>
<td>12-core (Intel®) CPU 64 bits ≥ 2.4GHz or better</td>
</tr>
<tr>
<td>Memory size</td>
<td>32-64 GB</td>
</tr>
<tr>
<td>Hard drive</td>
<td>500 GB – 1 TB thin provisioning</td>
</tr>
<tr>
<td>Network interface #1</td>
<td>Interface for Command Center communication and web app.</td>
</tr>
</tbody>
</table>

#### Command Center Requirements

<table>
<thead>
<tr>
<th></th>
<th>Small Deployment (≤5 sensors)</th>
<th>Medium Deployment (≤10 sensors)</th>
<th>Large Deployment (&gt;10 sensors ≤100)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hypervisor</td>
<td>minimum VMware ESXi 5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Form factor</td>
<td>19” rack server or virtual appliance</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Processor</td>
<td>4-core CPU 64 bits</td>
<td>4/6-core (Intel) CPU 64 bits</td>
<td>12-core (Intel) CPU 64 bits ≥ 2.4GHz</td>
</tr>
<tr>
<td>Memory size</td>
<td>16 GB</td>
<td>32 GB</td>
<td>64-256 GB</td>
</tr>
<tr>
<td>Hard drive</td>
<td>500 GB</td>
<td>1TB</td>
<td>&gt;1 TB</td>
</tr>
<tr>
<td>Network interface #1</td>
<td>Interface for sensor communication and web app.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Passive Sensor Requirements

<table>
<thead>
<tr>
<th></th>
<th>Small Deployment (up to 100 Mbps)</th>
<th>Medium Deployment (up to 200 Mbps)</th>
<th>Large Deployment (up to 1 Gbps)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example hardware model</td>
<td>Foxguard® IADIN-FS1</td>
<td>Dell® Embedded PC 5000</td>
<td>Dell PowerEdge R640</td>
</tr>
<tr>
<td>Deployment description</td>
<td>Deployments in small network and harsh environments</td>
<td>Deployments in mediumsized networks, harsh environments</td>
<td>Deployments in large networks and data center installation</td>
</tr>
<tr>
<td>Form factor</td>
<td>Small size industrial PC / DIN-rail fitting</td>
<td>Medium-size industrial PC 4 or 6-core</td>
<td>19” 1U rack server</td>
</tr>
<tr>
<td>Processor</td>
<td>2- or 4- core (Intel) CPU 64 bits</td>
<td>(Intel) CPU 64 bits with 8 GT/s</td>
<td>6-core (Intel) CPU 64 bits ≥ 2.4GHz</td>
</tr>
<tr>
<td>Memory size</td>
<td>4-16 GB</td>
<td>16-32 GB</td>
<td>32-64 GB</td>
</tr>
<tr>
<td>Hard drive</td>
<td>64 GB – 500 GB In industrial PCs (wide-temperature) SSDs should be used.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Monitoring interface</td>
<td>Up to 4 monitoring ports</td>
<td>Up to 8 monitoring ports</td>
<td>Up to 8 monitoring ports</td>
</tr>
</tbody>
</table>

#### Minimum Active Sensor Requirements

<table>
<thead>
<tr>
<th>Integrated with Passive Sensor</th>
<th>Stand Alone</th>
<th>Virtual</th>
</tr>
</thead>
<tbody>
<tr>
<td>It can be integrated directly on any passive sensor for small, medium and large deployment.</td>
<td>Processor</td>
<td>2-4 core CPU</td>
</tr>
<tr>
<td></td>
<td>Memory size</td>
<td>4 GB RAM</td>
</tr>
<tr>
<td></td>
<td>Network interface</td>
<td>≥ 1</td>
</tr>
</tbody>
</table>

Configurations shown as examples. Refer to a sales representative for details and specific requests like increased number of monitoring ports. Visit [www.forescout.com/platform/specifications/](http://www.forescout.com/platform/specifications/) for appliance specifications.
### 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-AE
- OPC-DA
- OPC-UA
- PROFINET (RPC, RTC, RTA, DCP and PTCP)
- SLMP

#### Proprietary OT Systems/Protocols
- CNCP (ABB)
- IAC/MMS (ABB)
- CSLib (ABB 800xA)
- DMS (ABB AC 800 F)
- PN800 (ABB Harmony)
- RNRP (ABB)
- SPLUS (ABB Symphony Plus)
- ADS/AMS (Beckhoff)
- BSAP & BSAP IP (Bristol Babcock)
- CygNet SCADA (CygNet)
- DeltaV (Emerson)
- Ovation (Emerson)
- ROC (Emerson/Fischer)
- MarkVI/Vie (GE)
- SRTP (GE)
- SES 92 (GRE)
- Experion (Honeywell)
- FOX (Honeywell Niagara / Tridium)
- NetI0 (Kongsberg)
- LonTalk (LonWorks)
- Melsoft (Mitsubishi Electric)
- ADE (Phoenix Contact)
- CIP extensions (Rockwell/AB)

#### IT Protocols
- AFP
- BGP
- CDP (Cisco)
- HSRP (Cisco)
- DHCP
- DNS
- DTP
- FTP
- HTTP
- ISAKMP
- CDP (Cisco)
- Kerberos
- LDAP
- LDP
- LLDP
- MS-SQL
- MQTT
- NMF
- NTP
- NetBIOS
- .NET Remoting
- NetSupport
- OpenRDA
- Oracle TNS
- POP3
- PYSS
- Radius
- RDP
- RFB/VNC
- RIP
- RPC/DCOM
- RTCP
- RTP
- RTSP
- SMB /CIFS
- SNMP
- SSDP
- SSH
- SSL
- STP
- Sentinel LDK
- SunRPC
- Telnet
- TFTP
- WS-Discovery

*Additional protocols are continuously integrated. Ask a sales representative for details.*