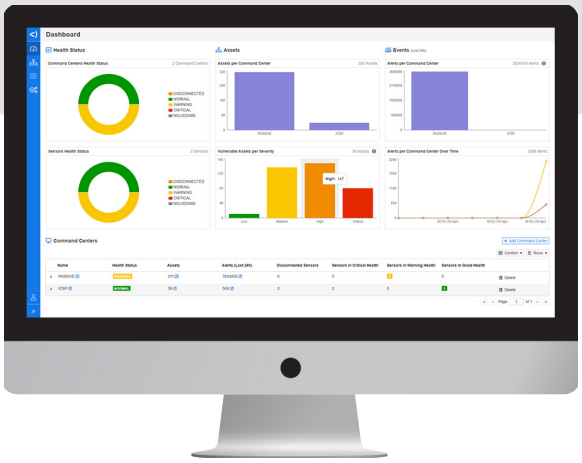
FORESCOUT

SilentDefense™ Datenblatt

SilentDefense ist eine nicht-invasive, situationssensitive Netzwerküberwachungsplattform, die eine tiefgehende Transparenz und Internetsicherheit für industrielle Steuerungssysteme (ICS) und SCADA-Netzwerke gewährleistet.

SilentDefense schützt ICS/SCADA-Netzwerke vor zahlreichen Bedrohungen. Es kombiniert eine patentierte Anomalie-Erkennung und Deep Packet Inspection (DPI) mit einer Bibliothek aus über 2.100 ICS-spezifischen Prüfungen ungewöhnlichen Verhaltens und einer ständig wachsenden Bibliothek von über 3.000 IoCs, um Anlagen vor hochentwickelten Cyberangriffen, fehlkonfigurierten Netzwerken und Fehlfunktionen zu schützen.

SilentDefense arbeitet direkt mit Enterprise-Systemen wie SIEM, Firewalls, IT-Assetmanagement- und Malware-Analyse-Systemen, Authentifizierungsservern und Drittplattformen zusammen.



Inventar- und Netzwerkübersicht

- Automatische Übersicht zu allen Geräten, Verbindungen und Gefahren inklusive ausführlicher Geräteinformationen
- Interaktive Visualisierung aller Angriffe und Risiken
- Change Log alle Geräteeigenschaften, Aktivitäten und Konfigurationsänderungen
- Optionale aktive Komponente (vom passiven System gesteuert), um Informationen wie offene Ports, Dienste, Anwendungen und Patches zu erfassen

Netzwerk- und Prozess-Monitoring

- Patentierte DPI für IT- & OT-Protokolle, Einhaltung der Kommunikationsprotokolle und ausgetauschten Daten
- Selbstkonfigurierendes Netzwerk und Prozess-Whitelists
- Automatische Zuordnung von Warnungen zu Vorfällen

SDK für erweiterte Anpassungen

- Einfache Entwicklung komplexer Netzwerk- und Prozess-spezifischer Prüfungen
- Schnelle Hilfe bei neuen Protokollen und Kundenanpassungen

Protokollierung & Analyse

- Protokollierung und Verhaltensanalyse von Remote-Authentifizierungen, DNS-Kommunikation und Dateioperationen
- Multi-Faktor-Dateizerlegung: Effektive Extraktion und Analyse von Dateien mit regelbasierter Analyse

Funktionen zur Gefahrensuche

- Ausgefeilte Suche nach Gefahrenindikatoren im Netzwerkverkehr und Log-Dateien
- Automatische Aufzeichnung von Bedrohungsdaten und Back-in-time-Bedrohungserkennung
- Über 2.100 Bedrohungsindikatoren wie Protokoll-Compliance-Checks, CVEs und Prüfungen auf ungewöhnliches Verhalten für Cyberangriffe, Netzwerkprobleme und Fehlfunktionen

Dashboard und Berichte

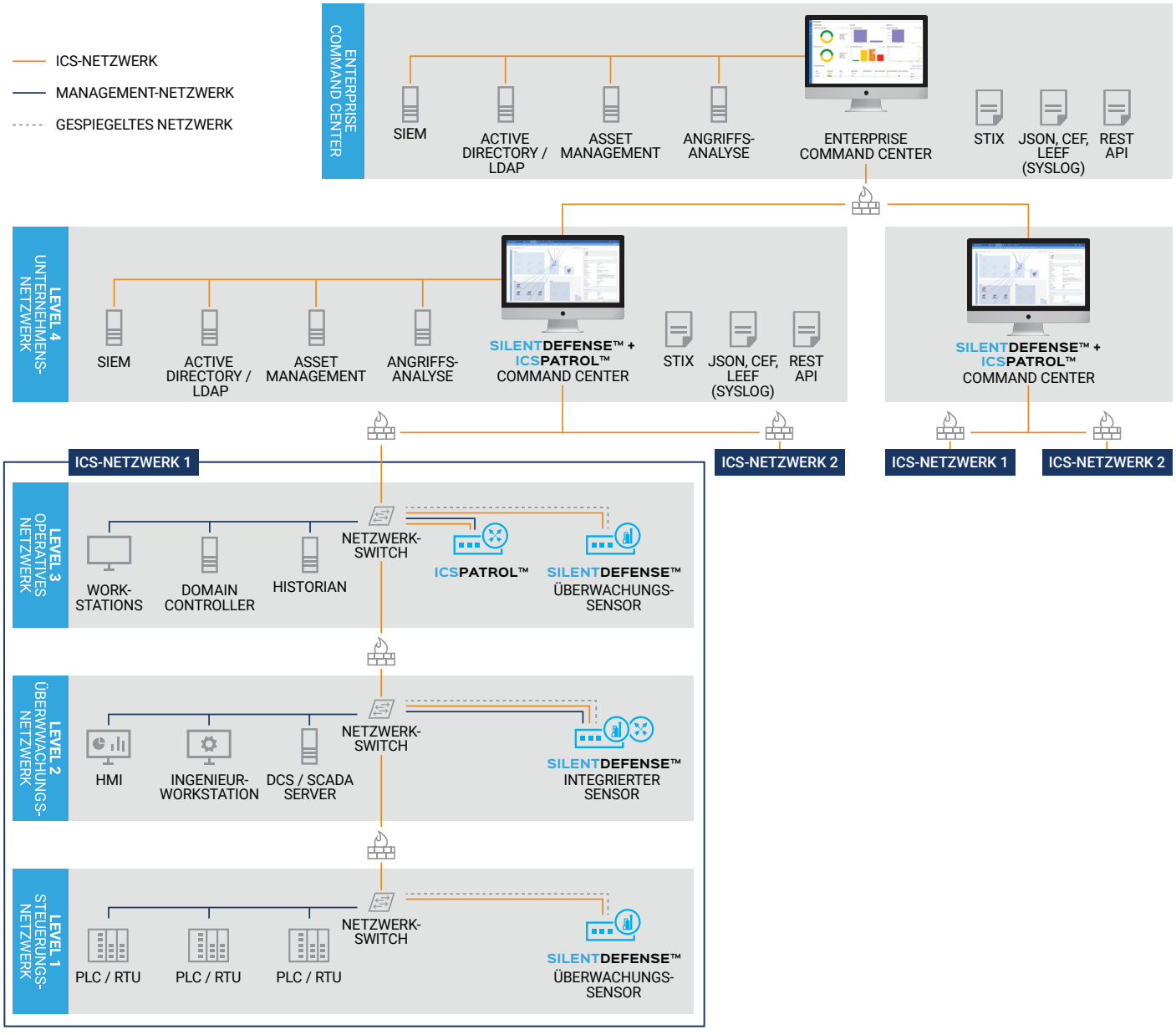
- Dashboards und Module zur Übersicht von Geräten und Bedrohung inklusive Gerätediagrammen und Trends sowie zur einfachen Zusammenarbeit von Benutzern
- Umfangreiche Warndetails zur Ursachenanalyse und die Reaktion auf Vorfälle
- Automatisierte Erstellung editierbarer grafischer Berichte

Architektur und Komponenten

SilentDefense sorgt für umfassende Transparenz und Internet-Sicherheit in OT- und ICS-Netzwerken. Über die Verbindung eines SPAN/Mirror-Ports eines Netzwerk-Switches erstellt es passiv eine Komplettübersicht aller Geräte und der normalen Kommunikation im Netzwerk. SilentDefense warnt sofort bei Abweichungen und ermöglicht so in Echtzeit ein operatives Angriffs- und Risikomanagement.

Das optionale aktive Modul ICS Patrol™ kann – unter der Kontrolle des passiven Systems – für eine weitergehende Erfassung von Geräten und Geräteinformationen das Netzwerk oder Netzwerksegmente analysieren.

Auf oberster Ebene führt das Enterprise Command Center (ECC) die Informationen diverser SilentDefense-Instanzen auf einem einfachen Dashboard zusammen, um einen vollständigen Überblick über Zustand, Geräte, Angriffe und Schwachstellen zu gewährleisten.



Verfügbare Konfigurationen

Enterprise-Command-Center-Anforderungen

	Standard-Installation
Modell / Hypervisor	 vmware
Formfaktor	19” Rack-Server oder Virtual Appliance
Prozessor	12-Core (Intel) CPU 64 Bit ≥ 2.4 GHz
Hauptspeicher	≥ 32-64 GB
Festplatte	500 GB - 1 TB

Command-Center-Anforderungen

	Kleine Installation (bis 5 Sensoren)	Mittlere Installation (bis 10 Sensoren)	Große Installation (mehr als 10 Sensoren)
Modell / Hypervisor	 vmware		
Formfaktor	19” Rack Server oder Virtual Appliance		
Prozessor	4-Core (Intel) CPU 64 Bit	4/6-Core (Intel) CPU 64 Bit	12-Core (Intel) CPU 64 Bit ≥ 2.4 GHz
Hauptspeicher	16-32 GB	32-64 GB	64-256 GB
Festplatte	500 GB - 1 TB		

Passiv-Sensor-Anforderungen

	Kleine Installation (bis 40 Mbps)	Mittlere Installation (bis 200 Mbps)	Große Installation (bis 1 Gbps)
Beispiel-Hardware			
Umgebung	Einsatz in kleinen Netzwerken und rauen Umgebungen	Einsatz in mittelgroßen Netzwerken und rauen Umgebungen	Einsatz in großen Netzwerken und im Rechenzentrum
Formfaktor	Kleiner Industrie-PC DIN-gerechte Montage	Mittelgroßer Industrie-PC	19-Zoll-1H-Rack-Rerver
Prozessor	2- oder 4-Core (Intel) CPU 64 Bit	6-Core (Intel) CPU 64 Bit	6-Core (Intel) CPU 64 Bit ≥ 2.4 GHz
Hauptspeicher	4-16 GB	16-32 GB	32-64 GB
Festplatte	64 GB - 500 GB		
Überwachungsschnittstellen	Bis zu 4 Schnittstellen	Bis zu 8 Schnittstellen	Bis zu 8 Schnittstellen

Mindestanforderungen für Aktive Sensoren

In passiven Sensor integriert
Kann direkt in jeden passiven Sensor für kleine, mittlere oder große Installationen integriert werden.

	Physisch	Virtuell
Prozessor	2-4 core CPU	4 vCPU
Hauptspeicher	4 GB RAM	4 GB RAM
Netzwerkschnittstellen	≥ 1	≥ 1

Die Konfigurationen sind Beispiele. Wenden Sie sich an einen Vertriebsmitarbeiter für spezifische Anfragen und Details, wie eine höhere Anzahl von Überwachungsschnittstellen.

Protokolle

Standard-OT-Protokolle

- 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

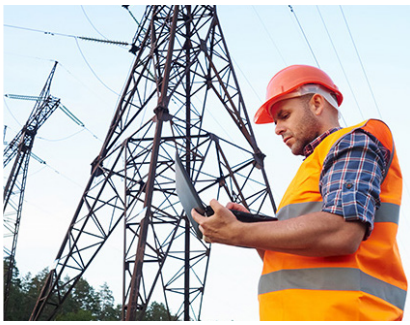
Proprietäre OT-Systeme und -Protokolle

- 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-Protokolle

- 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

Erfahren Sie mehr unter Forescout.com