secunet edge

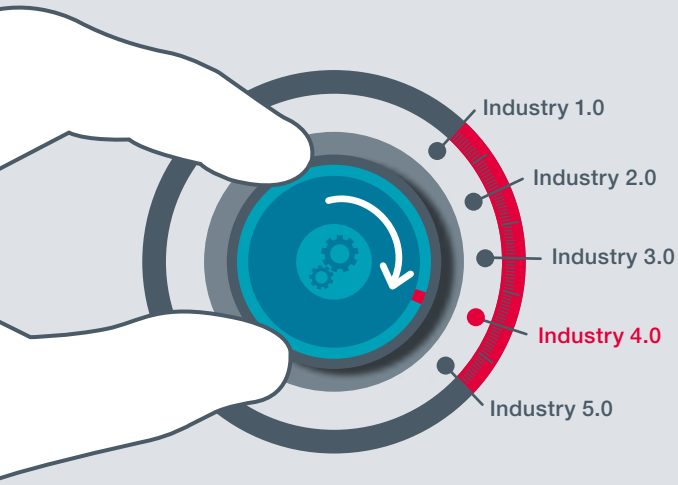
Industry 4.0 –
Protect. Connect. Detect.

secunet

Produktionssicherheit neu denken – Industry 4.0, IoT & Machine Security

Industrie 4.0 verbindet IT mit OT und verschmilzt damit zuvor getrennte Welten miteinander. Vernetzte Sensoren, Maschinen und Anlagen in der Industrie 4.0 erhöhen die Komplexität, schaffen neue Angriffsflächen für Cyber-Kriminelle und steigern damit die Gefahr von Systemfehlern oder gar -ausfällen.

Aktuellen Umfragen und Berichten zufolge, bestehen die derzeit größten Gefahren in unzureichend geschützten Netzwerkkomponenten, ungenügend gesicherten Schnittstellen zum Internet sowie zum Unternehmensnetzwerk. Gerade ältere Anlagengenerationen sind damit anfällig für Infektionen durch Schadsoftware und bilden darüber hinaus ein beliebtes Einfallstor für Erpressungen mittels Trojanern und Ransomware oder für Einbrüche über Fernzugriffe.



secunet edge – Protect. Connect. Detect.
Maschinen erfordern einen umfassenden Schutz vor äußeren Einflüssen, gleichzeitig jedoch eine Öffnung zur Erhöhung der Konnektivität. secunet edge erfüllt genau diesen paradox erscheinenden Anspruch. Wie eine Schutzhülle legt sich secunet edge um die Maschine und entkoppelt ihren Lebenszyklus von dem der IT-Umgebung. Somit bietet das Produkt IT- und OT-Sicherheit ohne Nebenwirkungen und ohne Auswirkungen auf Maschinen, Systeme oder Produktionsprozesse.

Gleichzeitig ermöglicht secunet edge die sichere und problemlose Anbindung an interne sowie externe IT-Dienste und IoT-Plattformen. Integrierte Sensorfunktionen garantieren durch die kontinuierliche Überwachung der Informationsflüsse in Echtzeit eine schnelle Anomalie-Erkennung und damit eine zuverlässige Sicherheit.

secunet edge wurde speziell für industrielle Systeme und Umgebungen konzipiert, entwickelt und patentiert.

Netzwerksicherheit – Schutz für Maschine und Netz

secunet edge sichert Maschinen am Rande des Netzwerks – „at the edge“ – ab. Maschinen sind dadurch vom Internet isoliert. Die Steuerung der Datenflüsse erfolgt zwischen definierten Segmenten – so wie es der Schutzbedarf der Zonen verlangt.

Hochsichere Konnektivität

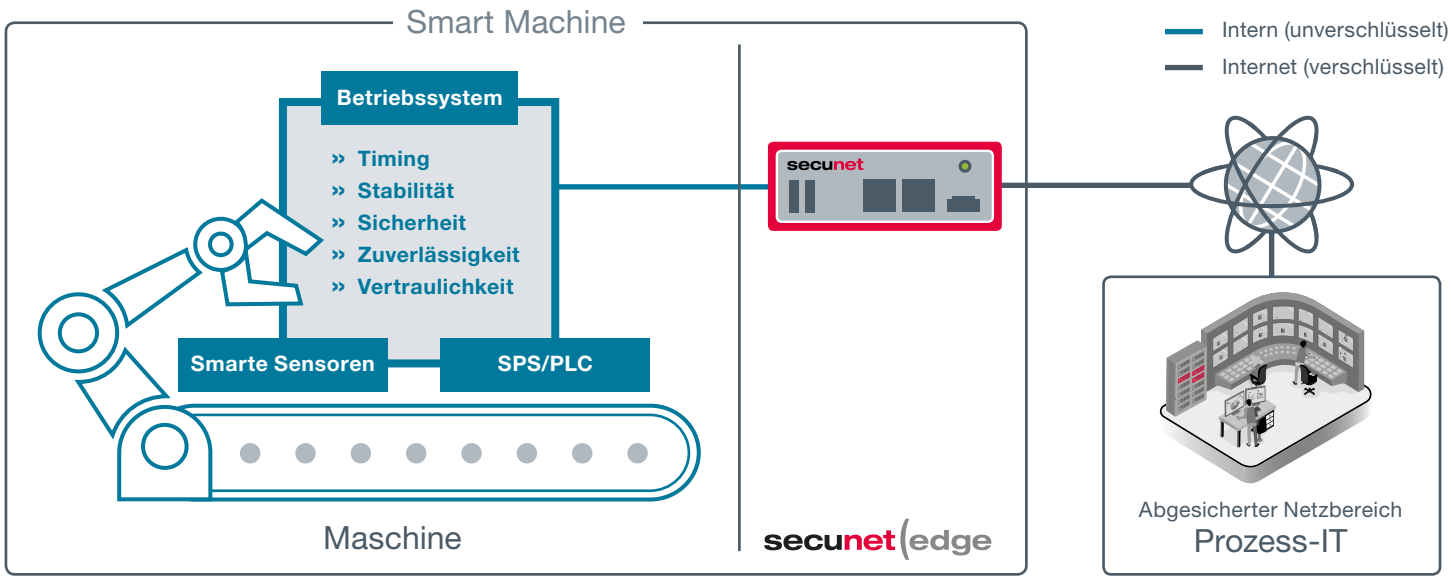
- Sichere, kontrollierte und flexible Integration der Maschine in das Netzwerk
- Regulierter Zugriff auf Maschine und Netzwerk
- Sichere Integration in IoT Plattformen ohne Netzwerke dauerhaft öffnen zu müssen

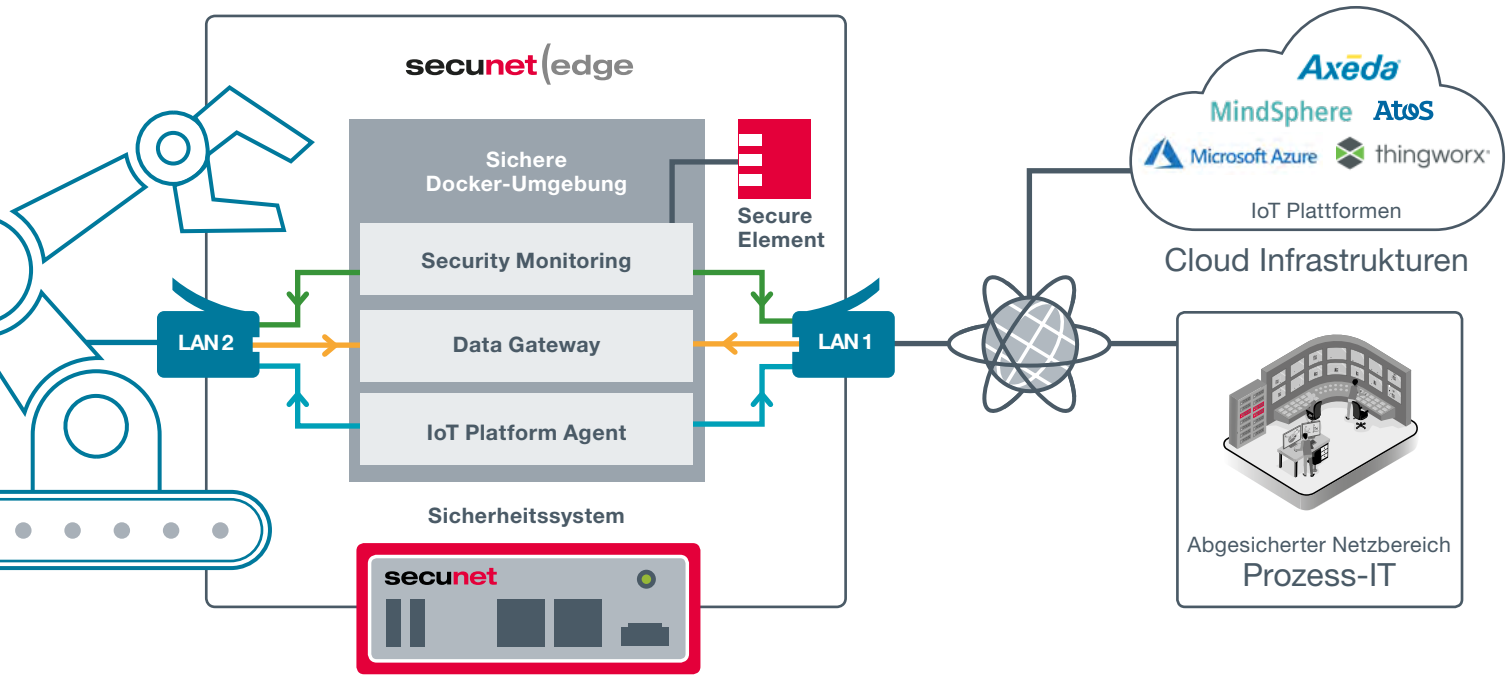
Stealth Factory-Ansatz oder Mikro-Segementierung

- **Stealth Mode Firewall:** Zu schützende Maschinen sind für das Internet unsichtbar
- **IP Firewall Mode:** Segmentierung des Netzwerks

Sichere Fernzugriffe

- Regelbare Zugriffssteuerung auf Geräteklassen
- Anlassbezogene Freischaltung





Informationssicherheit – Sichere Verarbeitung und Übertragung von Daten

Dank der integrierten und durch ein gehärtetes Betriebssystem gesicherten Docker Container können individuelle Anwendungen einfach installiert und betrieben werden.

Hardware-basierte Informationssicherheit

- Secure Element als Vertrauensanker für Docker-Anwendungen und Datensicherheit
- Fest verbauter und manipulationssicherer Chip (vergleichbar mit Smartcard)

secunet Sicherheitsanwendungen als Docker Container

Data Gateway – Sichere Verarbeitung und verschlüsselte Übertragung von Informationen

- Gerichteter Transfer von Nutzdaten der Maschine zu Backend- oder externen Diensten
- Protokollübersetzung: von unsicher zu sicher

Security Monitoring – Echtzeitüberwachung von Informationsflüssen

- Erkennen und Kontrollieren von Datenströmen
- Erkennen von Anomalien in Datenverbindungen

Produktmerkmale –
Ihre Vorteile auf einen Blick

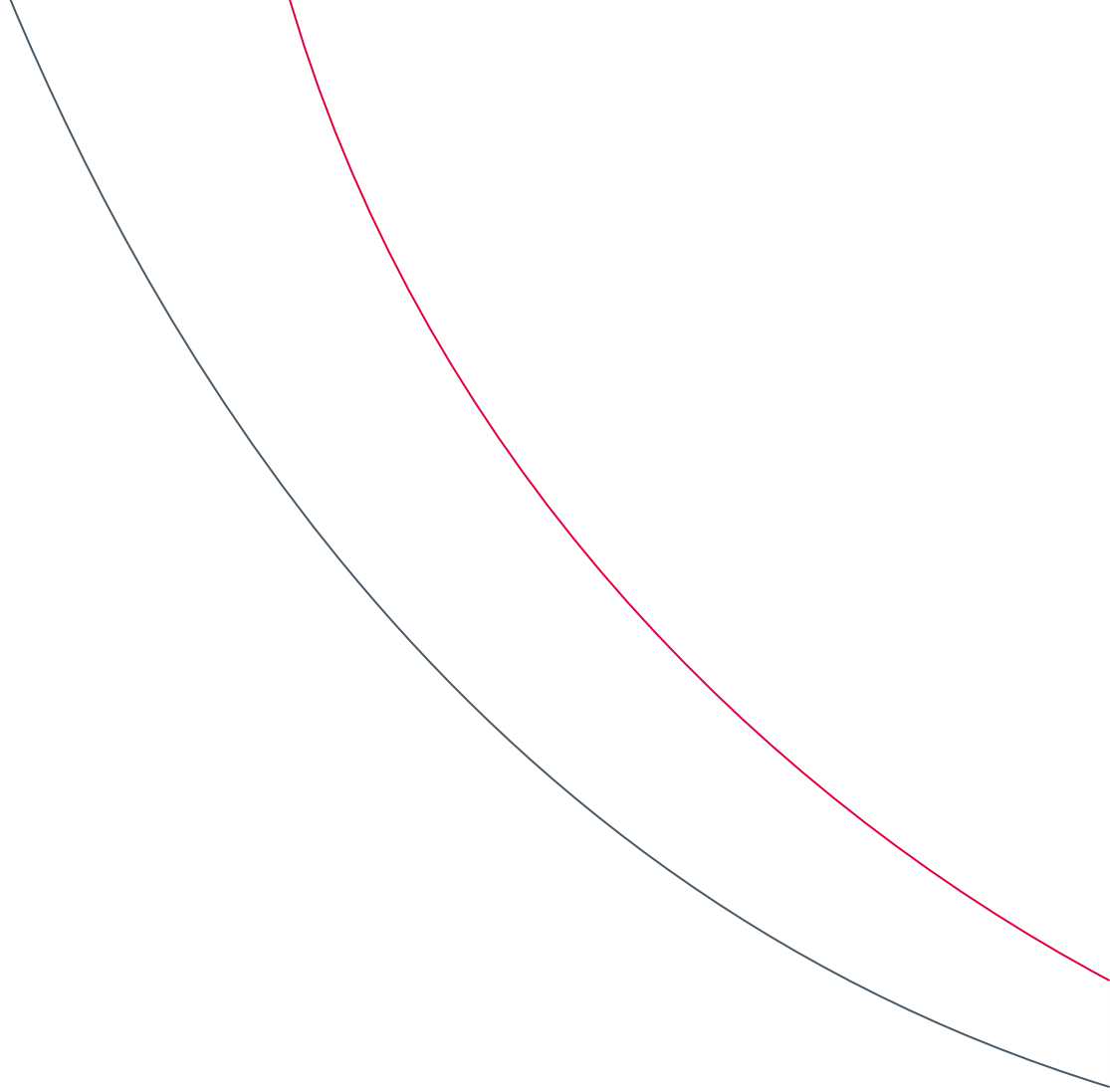
Hardware für den industriellen Einsatz
- Industrial fit form factor
- Industrielle Langzeitverfügbarkeit
- -40 °C bis +85 °C, passiv gekühlt
- IP 40 / schock- und vibrationsresistent
- VESA-Mount (75x75, 70x70)
- Mounting-Kits für DIN-Rail und 19"
- CE, FCC, EN50155 zertifiziert

IT Integration
- Einfache und schnelle Integration in bestehende OT-Infrastrukturen
- Schnittstellen: LAN, Bluetooth, Wi-Fi, 4G, serieller COM-Port

Modular und flexibel Dank sicherer Docker-Umgebung
- Zukunfts- und investitionssicher: modular erweiterbar um weitere Anwendungen
- Flexible Umsetzung eigener Geschäftsmodelle
- Eigenständiges Entwickeln und Betreiben von Docker-Anwendungen
- Sicherheitsanwendungen für Industrie 4.0-Anwendungsfälle bereits verfügbar

100% Security Made in Germany
- Gehärtetes und minimalisiertes Betriebssystem
- Hardware-basierte Sicherheit: Secure Element (eSE) / Krypto-SSD
- Protokoll Translator
- Anomalie-Erkennung / Intrusion Detection Engine

Sicherheitsstandards
- IEC 62443
- ISA99
- ISO 27019
- NIST SP 800-82
- ICS Security Kompendium



secunet

secunet Security Networks AG
Kurfürstenstraße 58
45138 Essen

www.secunet.com