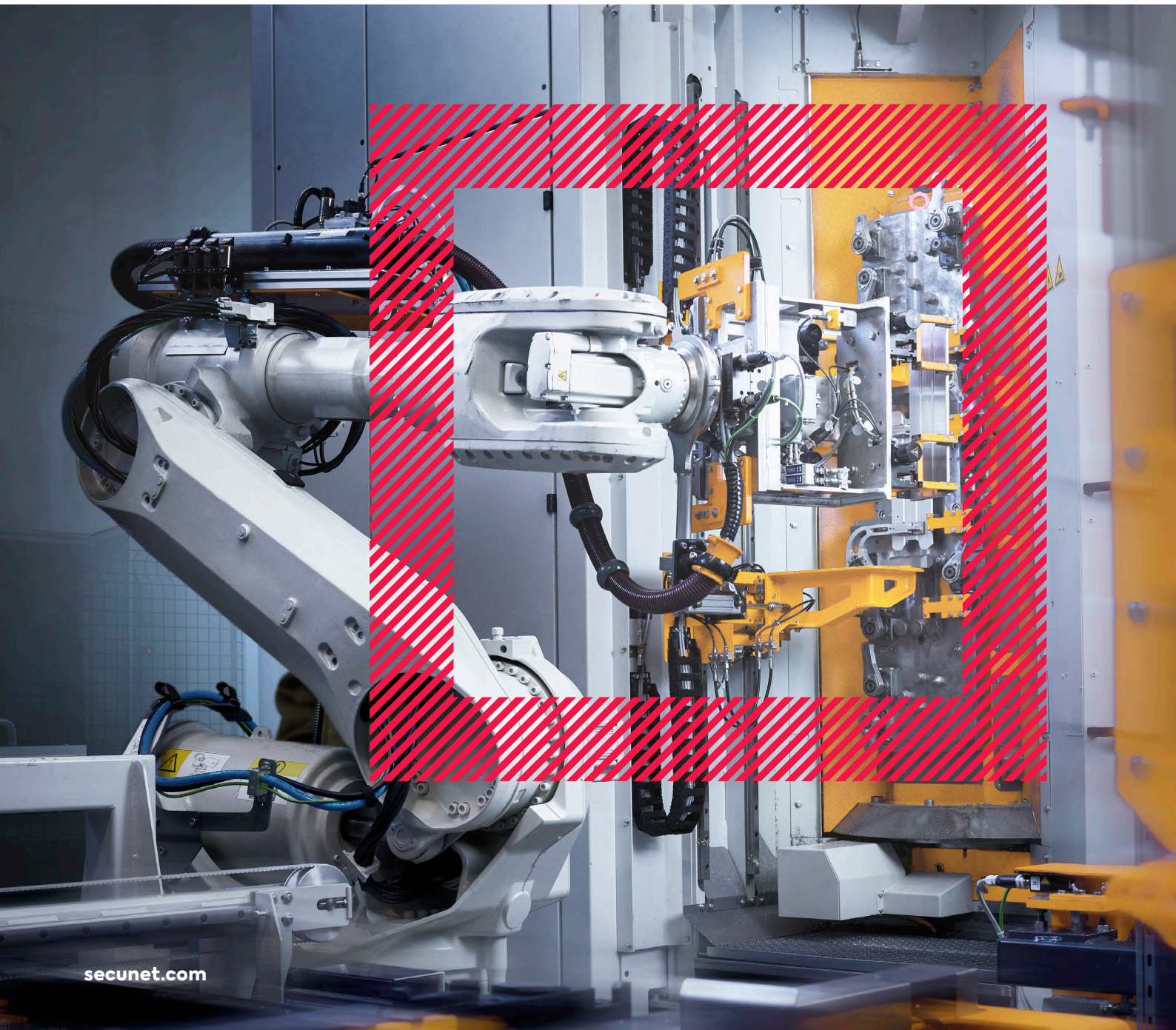


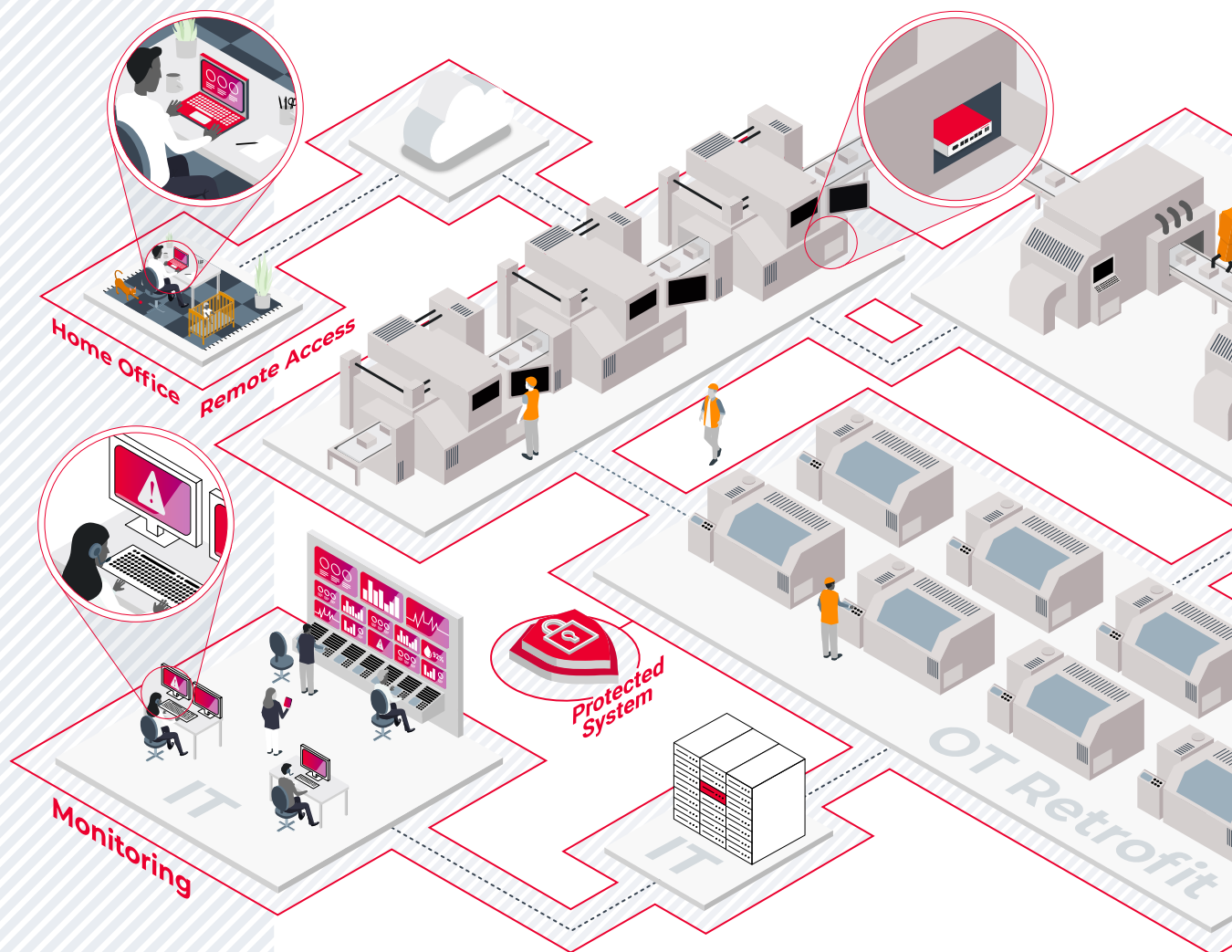
# Produktionssicherheit neu denken

Connect. Protect. Compute.



# Industrie 4.0, IIoT & Maschinen-Sicherheit

Industrie 4.0 verbindet IT mit OT.  
Somit verschmelzen zuvor getrennte  
Welten miteinander was neue Sicher-  
heitsmechanismen erfordert.

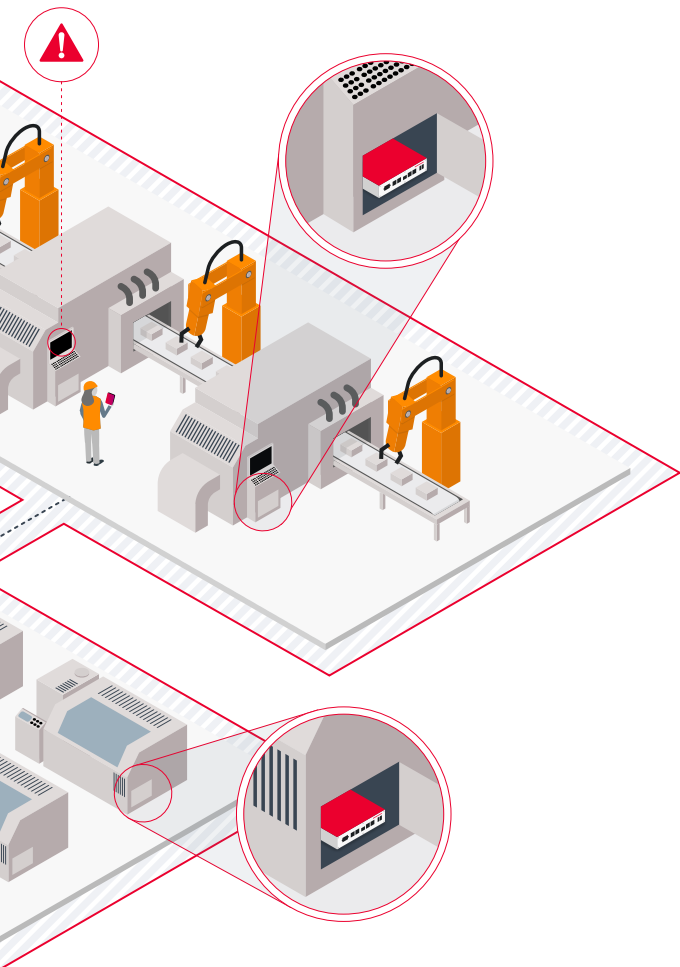


## Anwendungsbeispiel im Produktionsumfeld

Abschirmung, Überwachung, Fernzugriff, Anwen-  
dungsplattform und vieles mehr für die industrielle  
Produktion.

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.

Gerade ältere Anlagengenerationen sind damit anfällig für Angriffe und Schadsoftware. Sie bilden darüber hinaus ein Einfallstor für Erpressungen mittels Trojanern und Ransomware oder für unerlaubte Fernzugriffe.



Laut IDC Studie „Cybersecurity in DACH 2022“ waren **72 %** der Unternehmen in der DACH-Region von Ransomware betroffen. **40 %** haben in den vergangenen zwölf Monaten sogar einen Anstieg von Cyberangriffen verzeichnet. Mit Blick auf die Zukunft geht die Hälfte der Befragten (**50 %**) davon aus, dass die Zahl der Angriffe noch weiter steigen wird. Kam es zu einer Ransomware-Attacke, konnten lediglich **50 %** der Unternehmen diese erfolgreich abwehren.

## secunet edge – 3 in 1 Connect. Protect. Compute.

### Drei Leistungen in einem Gerät

Durch die zunehmende Vernetzung auch von alten Maschinen, erfordern diese 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.



	connect	protect	compute
Cloud-Gateway-funktionalität	×		
Absicherung externer Zugriffe		×	
Retrofitting dank Protokoll-übersetzungen	×	×	×
Patentierter Stealth-Mode: IP-Less Konnektivität, trotzdem bleiben Inlinemanagement und Containermanagement verfügbar	×	×	
Integrierte Firewall		×	
erweiterbar dank Docker-Umgebung mit secunet- und kundeneigenen Containern		×	×

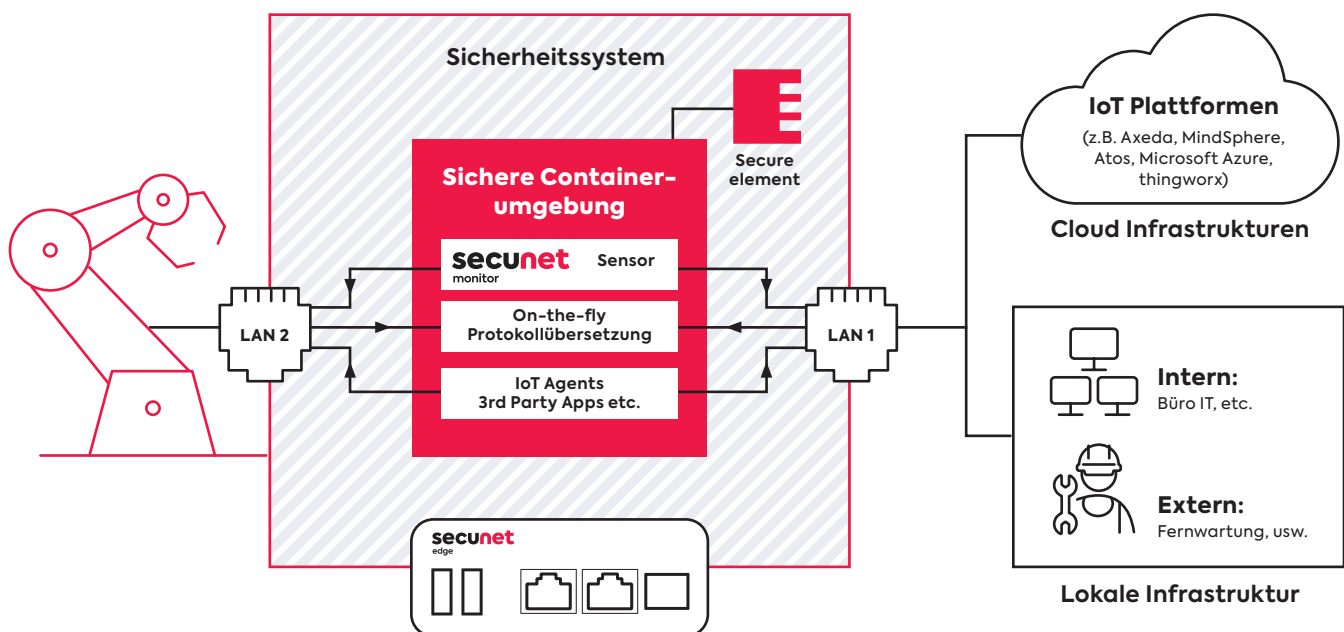
# IT/OT Sicherheit



## Connect.

**Sichere Konnektivität: Verbindung zu internen und externen Diensten.**

Die sichere Kommunikation von Anlagen mit dem Unternehmensnetzwerk, innerhalb von Produktionsnetzen sowie die grundsätzliche sichere Anbindung (Connectivity) von Systemen an Strukturen, Prozesse, Cloud- und IoT-Diensten.



### Multi-Funktional

#### Flexibel und modular

- Entwickelt für OT und maschinennahen Einsatz
- Flexibel für individuelle Kundenanforderungen
- Einfach zu integrieren in Unternehmensstrukturen
- Lokale Analyse und Vorverarbeitung von maschinengenerierten Daten

#### Maschinen einfach und sicher integrieren

- Sichere, kontrollierte und flexible Integration von Maschinen in Netzwerke
- Kommunikation von und zu den Maschinen kann kontrolliert werden
- Brücke zwischen legacy Maschinen zur state-of-the-art IT Infrastruktur

#### Verwaltet durch IT

- Schnittstellen zu SNMPv3, NAC, SIEM
- In-line Management, kein separates IT Management Netzwerk erforderlich

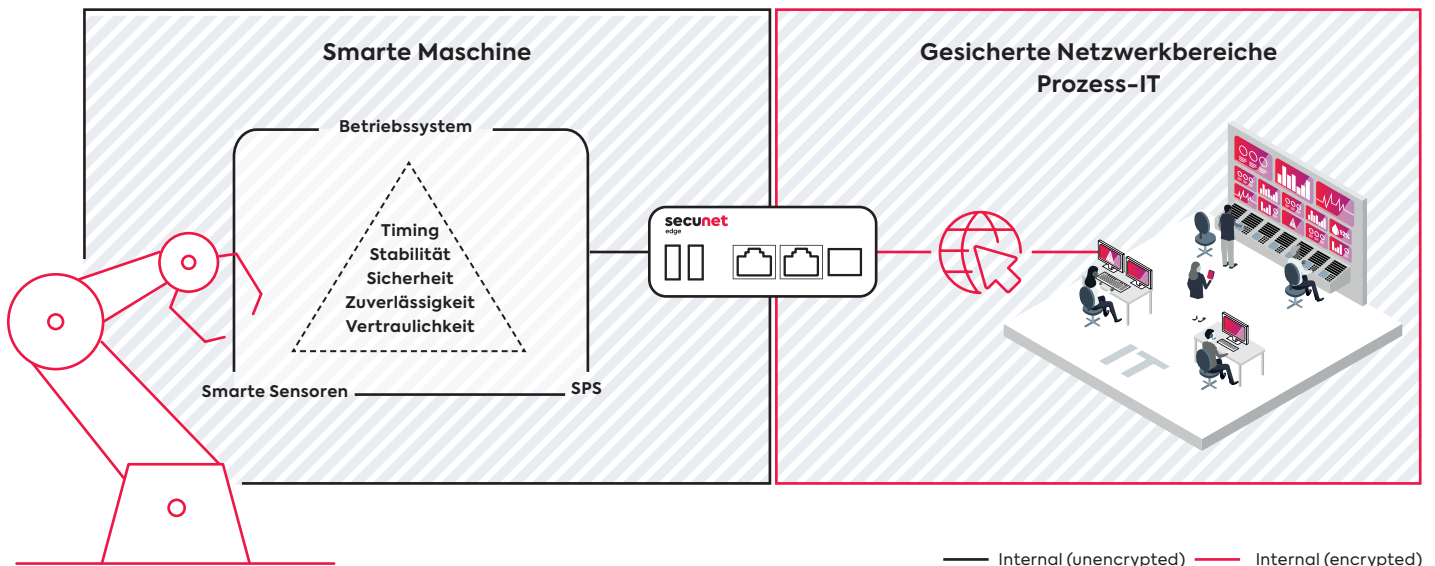
# Netzwerksicherheit



## Protect.

Schutz für Maschinen und Netzwerke.

Maschinen sind vom Netzwerk isoliert. Die Steuerung der Datenflüsse erfolgt zwischen definierten Segmenten – so wie es der Schutzbedarf der Zonen verlangt.



### Secure Edge Platform

#### Sicherheit

- Zertifiziertes embedded Secure Element (CC L3 EAL5)
- Industrial Firewall auch für App-Container
- Patentierte on-the-fly Protokollübersetzung

### Stealth-Factory-Ansatz oder

#### Mikro-Segmentierung

- **Stealth mode firewall:** Maschinen werden geschützt durch eine unsichtbare Firewall
- **On-the-fly Protokoll:** Übersetzung ohne Änderung an den Maschinen
- **Patentiertes Stealth Mode Verfahren:** die secunet edge bleibt vor Angreifern verborgen und trotzdem administrierbar
- **IP firewall mode:** Isolation einer Maschine durch fein-granularer Netzwerksegmentierung und on-the-fly Protokoll Übersetzung

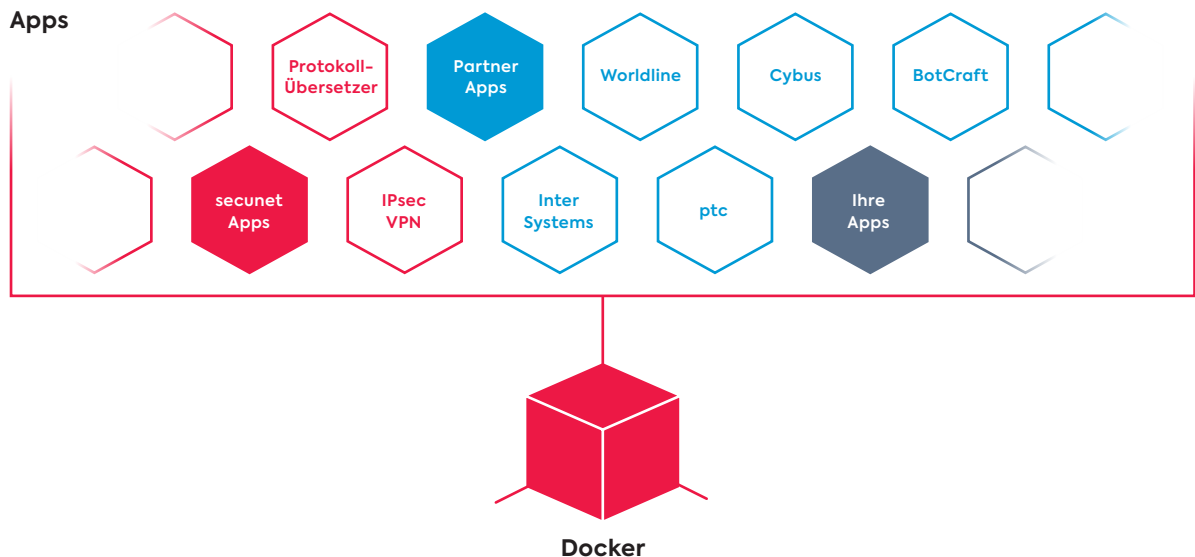
# Flexibilität und Zukunftssicherheit



## Compute.

Leistungsstarke und sichere Edge Computing Plattform basierend auf flexibler Containerumgebung

Durch die integrierte Container Runtime, die durch ein gehärtetes Betriebssystem gesichert ist, lassen sich einzelne Anwendungen und Container, auch ihre eigenen, einfach installieren und betreiben.



### Edge computing

- Intel Unified IoT Edge Framework compliant
- Microsoft Azure IoT Edge zertifiziert
- OCI compliant Container-Umgebung

### Partner und Kunden

- Designed für Entwicklung von App-Container
- APIs für Interaktion mit secunet edge Firmware
- Microsoft VS Code Azure IoT CI-CD-Support
- Kompatibel mit den wichtigsten IoT Plattformen

### Von secunet bereitgestellte Container (Auszug)

- SFTP/FTPS <-> SMB/FTP
- SMBv3 <-> SMBv1, SMBv2
- ssh <-> Telnet
- https <-> http/https
- ssh -> RS-232
- RDP/VNC <|> RDP/VNC/SSH

<-> / -> = Übersetzung in beide / eine Richtung(en)  
<|> = Connector um neue Protokolle von alten zu trennen

Eine Übersicht unserer Container finden Sie unter:  
[www.secunet.com/loesungen/edge](http://www.secunet.com/loesungen/edge)



## Ihre Vorteile auf einen Blick

### 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

### On-the-fly Protokoll Übersetzung im Stealth Mode (Auszug)

- SMBv3 <-> SMBv1, SMBv2
- sftp/ftps <-> smb/ftp
- ssh <-> telnet

### Stealth Factory-Ansatz oder Mikro-Segmentierung

- **Stealth Mode Firewall:** Die zu schützende Maschine ist im Netzwerk unsichtbar
- **IP Firewall Mode:** Segmentierung des Netzwerks

### Offene, gehärtete Containerumgebung

- Basierend auf Docker Moby
- APIs für Interaktion mit integrierter secunet edge Firmware
- Integration von eigenen Containern
- Kompatibel mit den wichtigsten IoT Plattformen wie z.B. Microsoft Azure, AWS oder PTC
- **Zukunfts- und investitionssicher:** modular erweiterbar um weitere Anwendungen
- Flexible Umsetzung eigener Geschäftsmodelle

## Sicherheitsmerkmale

### 100% Security Made in Germany

- Gehärtetes und minimalisiertes Linux Betriebssystem
- Hardwarebasierte Sicherheit: embedded Secure Element (eSE) / secunet CryptoCore SSD BSI CC L3 EAL5 zertifiziert
- Microsoft Azure IoT Edge runtime nativ in Firmware implementiert
- Hardware made in Germany by Beckhoff Automation

### secunet Sicherheitsanwendungen als 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 und umgekehrt

### secunet edge OS

- gehärtetes Betriebssystem
- monatliche CVE Reports
- umgehende Behebung von kritischen zero day exploits
- Wachsender Funktionsumfang auf Kundenfeedback Basis

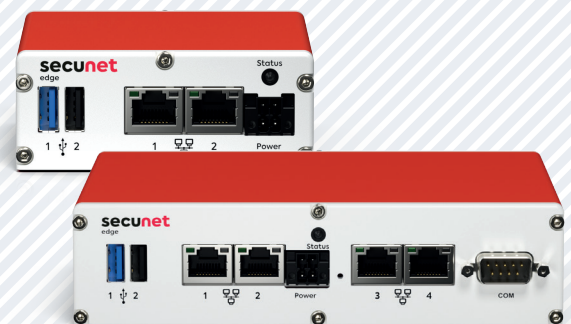
## Produktmerkmale

### Hardware für den industriellen Einsatz

- Industrietaugliches IP40 Metallgehäuse
- Industrielle Langzeitverfügbarkeit
- -25 °C bis +85 °C, passiv gekühlt
- schock- und vibrationsresistent
- VESA-Mount (75x75, 70x70)
- Mounting-Kits für DIN-Rail und 19" Rack
- Zugelassen nach CE und FCC

### IT Integration

- Einfache und schnelle Integration in bestehende OT-Infrastrukturen
- Schnittstellen: LAN, serieller COM-Port, USB 2.0 und 3.0



### secunet edge in Kooperation mit

**BECKHOFF**



IoT Solutions Alliance



**WORLDLINE**



## **secunet – Schutz für digitale Infrastrukturen**

secunet ist Deutschlands führendes Cybersecurity-Unternehmen. In einer zunehmend vernetzten Welt sorgt das Unternehmen mit der Kombination aus Produkten und Beratung für widerstandsfähige, digitale Infrastrukturen und den höchstmöglichen Schutz für Daten, Anwendungen und digitale Identitäten. secunet ist dabei spezialisiert auf Bereiche, in denen es besondere Anforderungen an die Sicherheit gibt – wie z. B. Cloud, IIoT, eGovernment und eHealth. Mit den Sicherheitslösungen von secunet können Unternehmen höchste Sicherheitsstandards in Digitalisierungsprojekten einhalten und damit ihre digitale Transformation vorantreiben.

Über 1000 Expert\*innen stärken die digitale Souveränität von Regierungen, Unternehmen und der Gesellschaft. Zu den Kunden zählen die Bundesministerien, mehr als 20 DAX-Konzerne sowie weitere nationale und internationale Organisationen. Das Unternehmen wurde 1997 gegründet. Es ist im SDAX gelistet und erzielte 2022 einen Umsatz von rund 347 Mio. Euro.

secunet ist IT-Sicherheitspartner der Bundesrepublik Deutschland und Partner der Allianz für Cyber-Sicherheit.

### **secunet Security Networks AG**

Kurfürstenstraße 58 · 45138 Essen  
T +49 201 5454-0 · F +49 201 5454-1000  
info@secunet.com · secunet.com

**Sie wünschen weitere Informationen?  
Erfahren Sie mehr unter  
[www.secunet.com/loesungen/edge](http://www.secunet.com/loesungen/edge)**