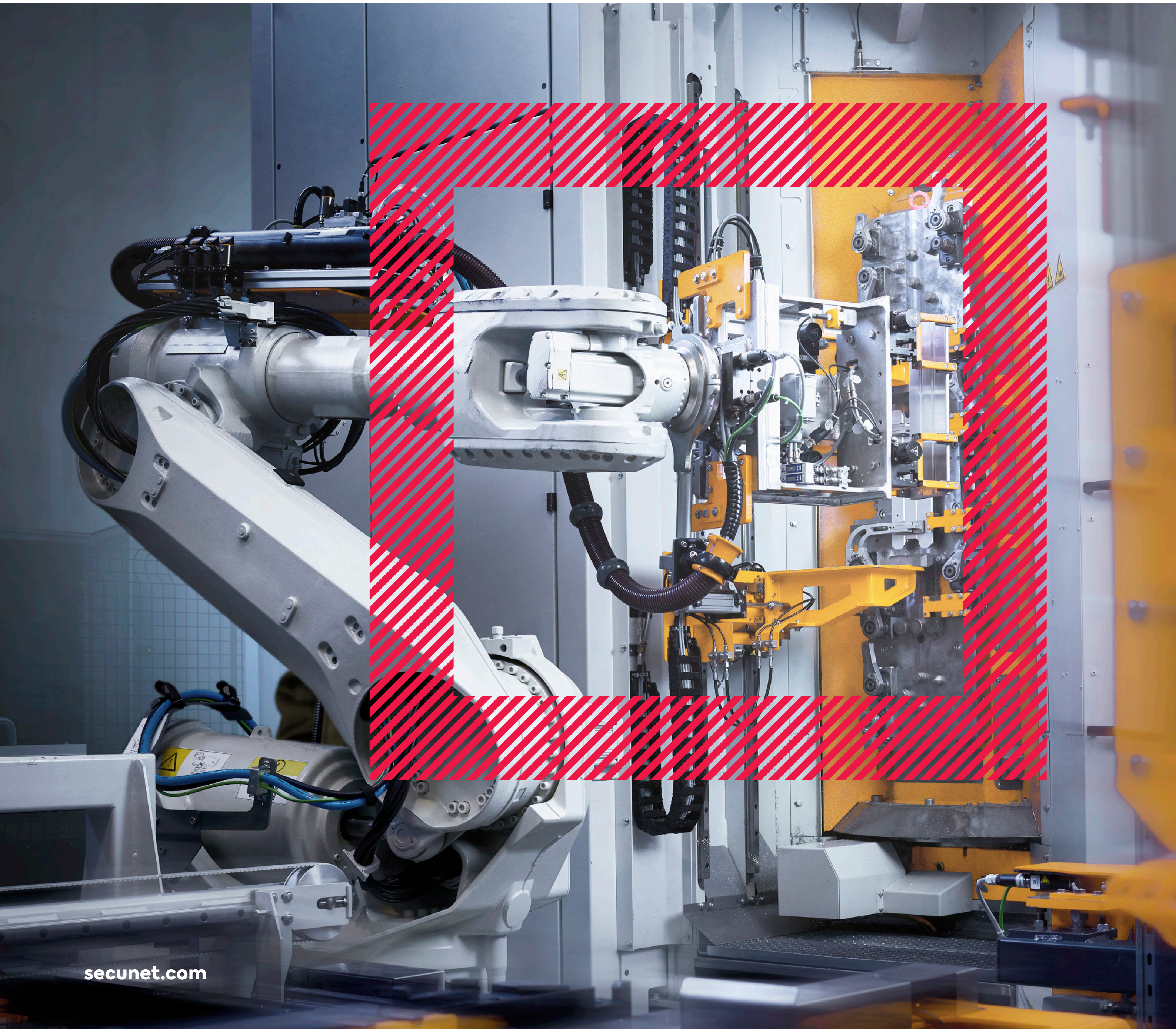
secunet
edge

Rethinking production security

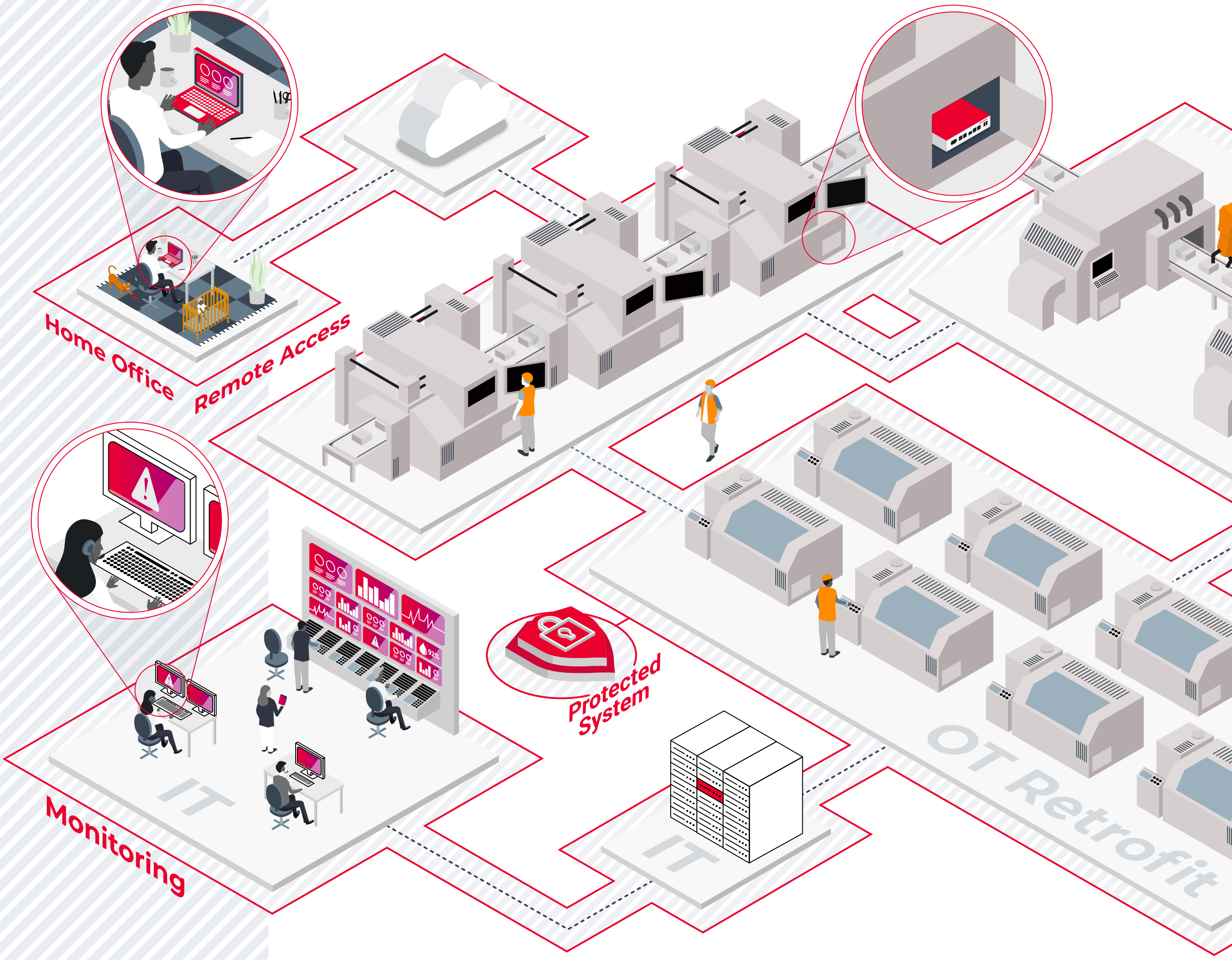
Connect. Protect. Compute.



secunet.com

Industry 4.0, IIoT & machine security

Industry 4.0 combines IT with OT. Merging worlds that were previously separate requires new security mechanisms.

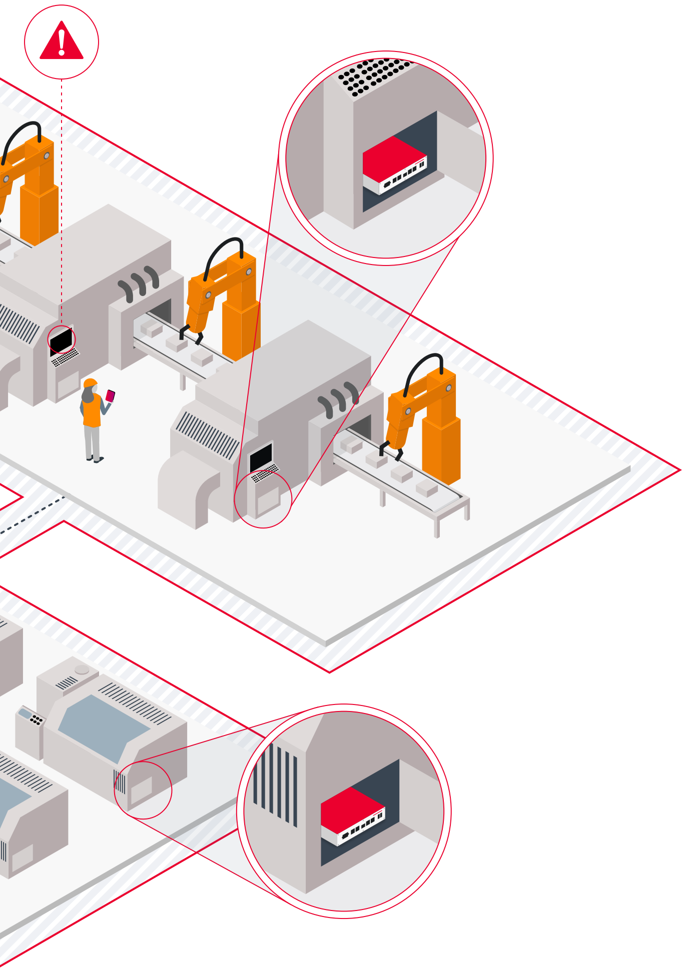


Sample application in the production environment

Shielding, monitoring, remote access, application platform and much more for industrial production.

Networked sensors, machines and systems in Industry 4.0 increase complexity and create new targets of attack for cyber criminals, increasing the risk of system faults or even failures.

This makes older generations of systems particularly prone to attacks and malware. They also offer a gateway for extortion attempts via Trojans and ransomware or for unauthorized remote access.



According to the IDC study "Cybersecurity in DACH 2022", **72%** of companies in the DACH region have been affected by ransomware. In fact, **40%** have seen an increase in cyberattacks in the past twelve months. Looking ahead, half of those surveyed (**50%**) expect the number of attacks to continue to rise. If a ransomware attack occurred, only **50%** of companies would be able to successfully fend it off.

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

Three features in one device

As older machines become increasingly networked, they require comprehensive protection from external factors while also being open to enable increased connectivity. secunet edge fulfills exactly this apparently paradoxical requirement, wrapping itself around the machine like a protective cover and decoupling its life cycle from that of the IT environment. Thus, the product offers IT and OT security without side effects and without impacting machines, systems or production processes.

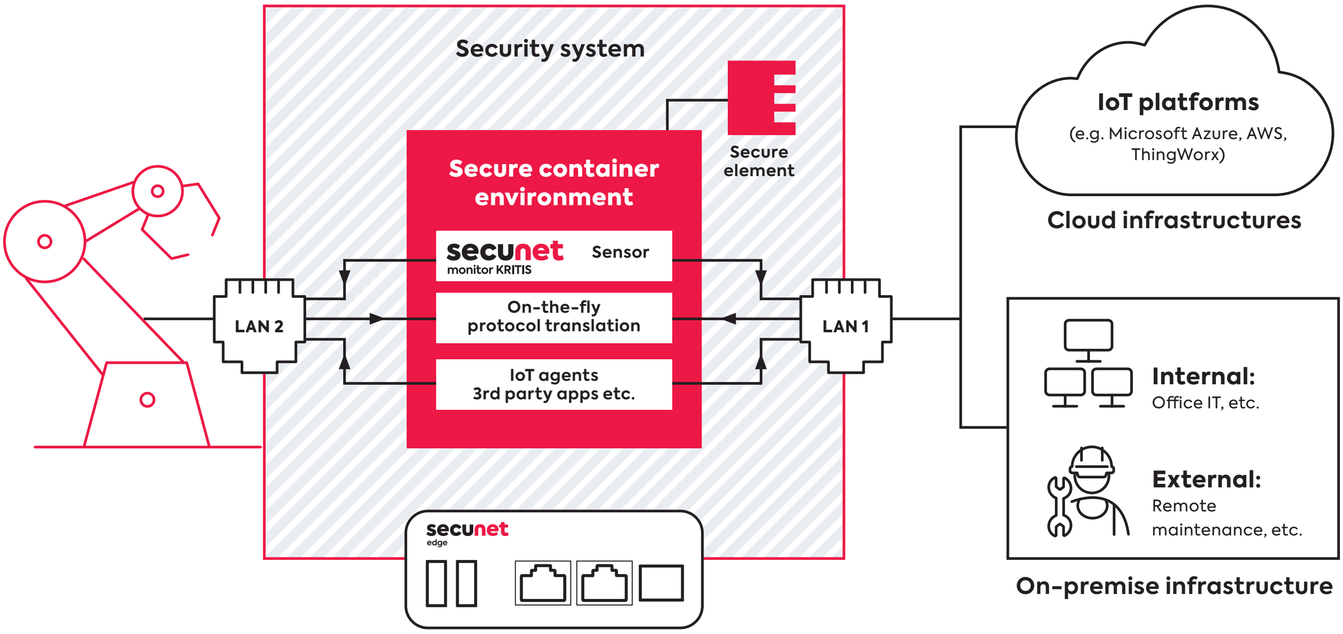
	Connect	Protect	Compute
Cloud gateway functionality	✗		
Securing external access		✗	
Retrofitting thanks to protocol translations	✗	✗	✗
Patented stealth mode: IP-less connectivity with retailed availability of inline management and container management remain	✗	✗	
Built-in firewall		✗	
Expandable thanks to Docker environment with secunet and customer-owned containers		✗	✗

IT/OT security

Connect.

Secure connectivity: Connection to internal and external services.

Ensuring secure communication of facilities with the corporate network and within production networks, as well as securing the basic connectivity of systems to structures, processes, cloud and IoT services.



Multi-functional

Flexible and modular

- Designed for OT and machine-level use
- Flexible for individual customer requirements
- Easy to integrate into corporate structures
- Local analysis and pre-processing of machine-generated data

Easy and secure integration of machines

- Secure, controlled and flexible integration of machines into networks
- Communication to and from the machines can be controlled
- Bridging the gap between legacy machines and state-of-the-art IT infrastructure

Managed by IT

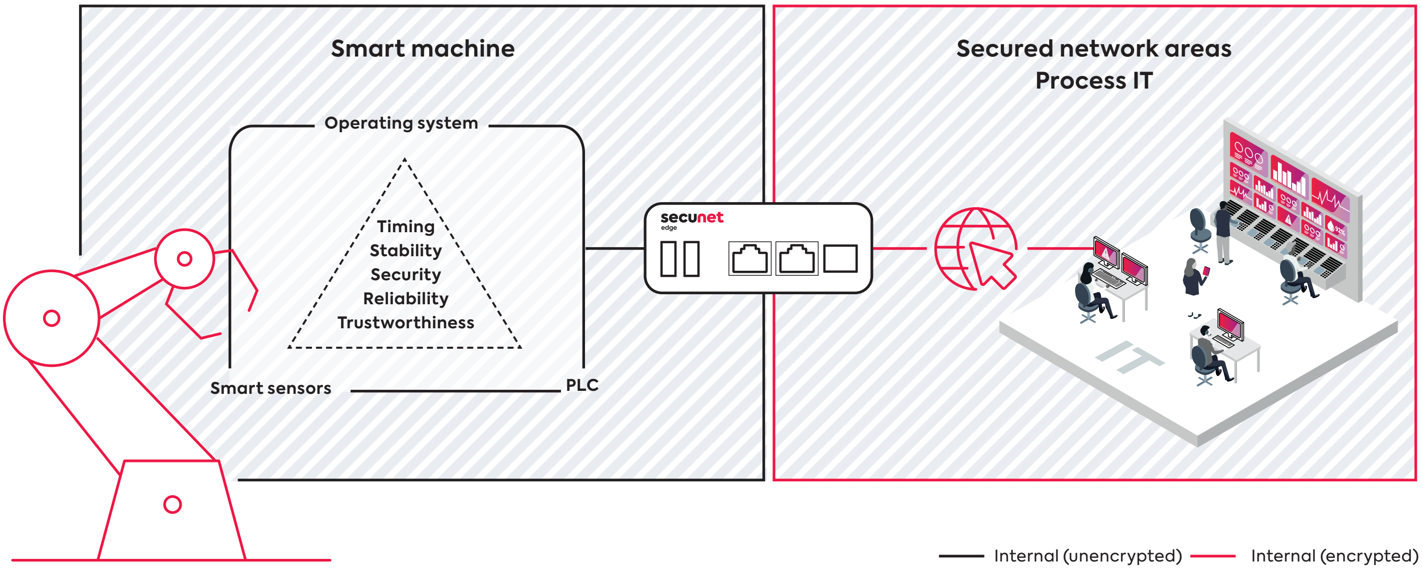
- Interfaces to SNMPv3, NAC, SIEM
- In-line management, no separate IT management network required

Network security

Protect.

Protection for machines and networks.

Machines are insulated from the network. The data flows are controlled between defined segments – as required by the protection requirements of the zones.



Secure edge platform

Security

- Certified embedded Secure Element (CC L3 EAL5)
- Industrial firewall also for app containers
- Patented on-the-fly protocol translation

Stealth factory approach or micro-segmentation

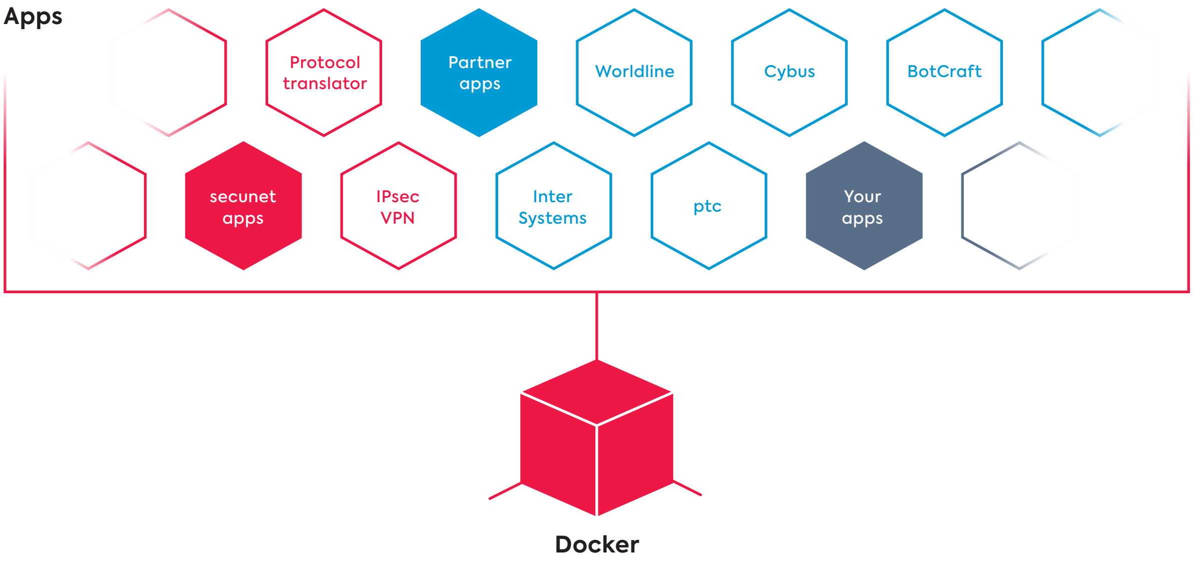
- **Stealth mode firewall:** Machines are protected by an invisible firewall
- **On-the-fly protocol:** Translation with no modification to the machines
- **Patented stealth mode process:** The secunet edge remains hidden from attackers and can still be administered
- **IP firewall mode:** Insulation of a machine through fine-grained network segmentation and on-the-fly protocol translation

Flexibility and future-proofing

Compute.

High-performance and secure edge computing platform based on flexible container environment

The integrated container runtime, which is secured by a hardened operating system, makes it easy to install and operate individual applications and containers, including your own.



Edge computing

- Intel Unified IoT Edge Framework-compliant
- Microsoft Azure IoT Edge-certified
- OCI-compliant container environment

Partners and customers

- Designed for app container development
- APIs for interaction with secunet edge firmware
- Microsoft VS Code Azure IoT CI-CD support
- Compatible with major IoT platforms such as Microsoft Azure, AWS or PTC

Containers provided by secunet (excerpt)

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

<-> / -> = translation in both/one direction(s)
<|> = Connector to separate new protocols from old ones

An overview of our containers can be found at:
https://www.secunet.com/en/solutions/edge

Benefits to you at a glance

Highly secure connectivity

- Secure, controlled and flexible integration of the machine into the network
- Regulated access to machine and network
- Secure integration into IoT platforms without having to permanently open networks

On-the-fly protocol translation in stealth mode (excerpt)

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

Stealth factory approach or micro-segmentation

- **Stealth mode firewall:** The machine to be protected is invisible in the network
- **IP firewall mode:** Segmentation of the network

Open, hardened container environment

- Based on Docker Moby
- APIs for interaction with integrated secunet edge firmware
- Integration of your own containers
- Compatible with major IoT platforms such as Microsoft Azure, AWS or PTC
- **Future-proof and investment-proof:** Modular expansion possible to include additional applications
- Flexible implementation of own business models

Security

100% security made in Germany

- Hardened and minimised Linux operating system
- Hardware-based security: Embedded Secure Element (eSE) / secunet CryptoCore SSD BSI CC L3 EAL5 certified
- Microsoft Azure IoT Edge runtime natively implemented in firmware
- Hardware made in Germany by Beckhoff Automation

secunet security applications as containers

- Data gateway – secure processing and encrypted transmission of information
- Directed transfer of user data from the machine to backend or external services
- Protocol translation: From insecure to secure and vice versa

secunet edge OS

- Hardened operating system
- Monthly CVE reports
- Immediate remediation of critical zero-day exploits
- Growing range of functions based on customer feedback

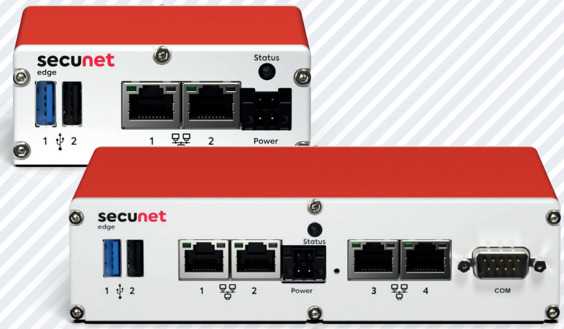
Features

Hardware for industrial use

- Industrial-grade IP40 metal housing
- Long-term industrial availability
- -25°C to +85°C, passively cooled
- Shock- and vibration-resistant
- VESA mount (75x75, 70x70)
- Mounting kits for DIN rail and 19“ rack
- Approved by CE and FCC

IT integration

- Easy and fast integration into existing OT infrastructures
- Interfaces: LAN, serial COM port, USB 2.0 and 3.0



secunet edge in cooperation with

BECKHOFF

intel IoT Solutions Alliance

Infineon Security Partner Preferred

WORLDLINE

Microsoft Azure Certified

aws

secunet – protecting digital infrastructures

secunet is Germany's leading cybersecurity company. In an increasingly connected world, the company's combination of products and consulting assures resilient digital infrastructures and the utmost protection for data, applications and digital identities. secunet specializes in areas with unique security requirements – such as cloud, IIoT, eGovernment and eHealth. With security solutions from secunet, companies can maintain the highest security standards in digitisation projects and advance their digital transformation.

Over 1,000 experts strengthen the digital sovereignty of governments, businesses and society. secunet's customers include federal ministries, more than 20 DAX-listed corporations as well as other national and international organisations. The company was established in 1997, is listed at the German Stock Exchange and generated revenues of around 393 million euros in 2023.

secunet is an IT security partner to the Federal Republic of Germany and a partner of the German Alliance for Cyber Security.

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

Would you like more information?
Find out more at:
www.secunet.com/en/solutions/edge

Broschüre_secunet edge_Production safety_EN_04/2024 Subject to change