secunet edge

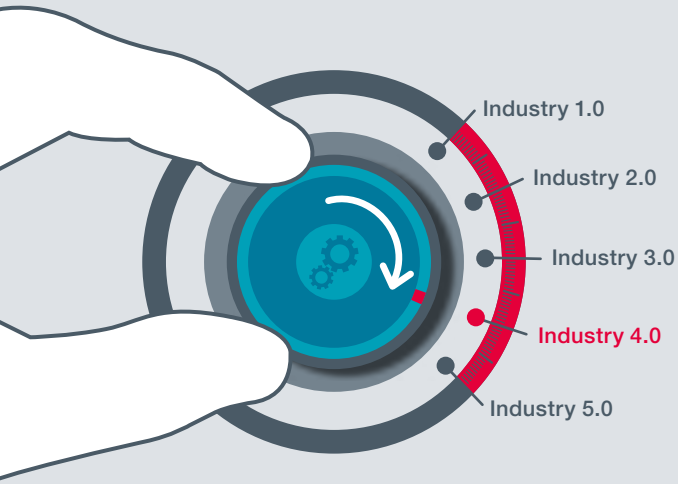
Industry 4.0 –
Protect. Connect. Detect.

secunet

Rethinking Production Reliability – Industry 4.0, IoT & Machine Security

Industry 4.0 connects IT with OT, thereby bringing together two worlds that were previously completely separate. Connected sensors, machines and plants in Industry 4.0 ecosystems increase the complexity and provide new opportunities for cyber criminals to launch attacks. This leads to a higher risk of system failures or even outages.

According to recent surveys and reports, inadequately protected network components and insufficiently secured interfaces to the Internet and the corporate network are considered to be the biggest risks for cyber attacks. Older generations of plants in particular are extremely exposed to malware infections and become an open door for black-mailing via Trojans, ransomware, or attacks via remote access.



secunet edge – Protect. Connect. Detect.
Machines demand comprehensive protection from external influences; yet, at the same time, they need to have a degree of openness to increase the connectivity. secunet edge fulfils exactly this seemingly paradoxical demand.

Like a protective wrapping, secunet edge covers the machine and decouples the machine's life cycle from the IT environment. The product thereby provides IT and OT security without any side effects and without any impact on the machines, systems or manufacturing processes.

At the same time, secunet edge enables a secure and easy connection to internal and external IT services and IoT platforms. By continually monitoring data flows in real-time, embedded sensor functions ensure fast detection of any deviations from regular network traffic (anomalies) and provide additional reliable security.

secunet edge has been designed, developed and patented especially for industrial systems and environments.

Network Security – Protection for Machines and the Network

secunet edge secures machines “at the edge” of the network. Machines are therefore kept separate from the Internet; management of the data flow happens between defined network segments – according to the requirements of each individual level of security.

Highly secure connectivity

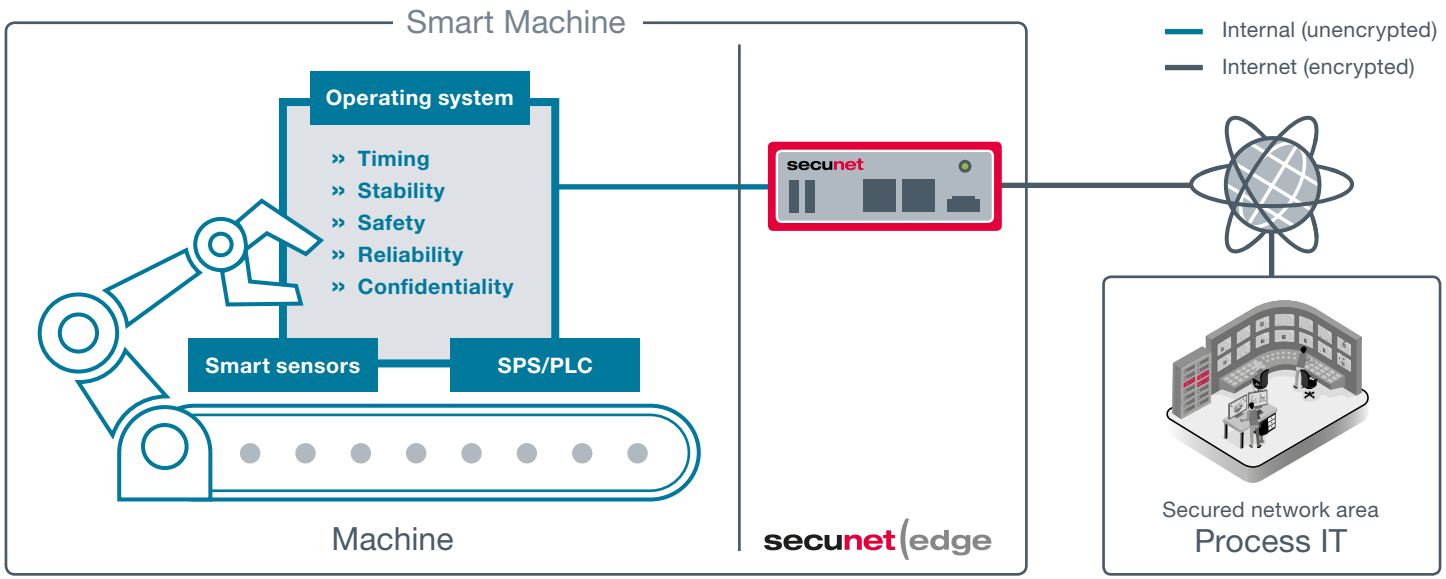
- Secure, controlled and flexible integration of the machine into the network
- Restricted access to the machine and network
- Secure integration within IoT platforms without the need to keep networks permanently open

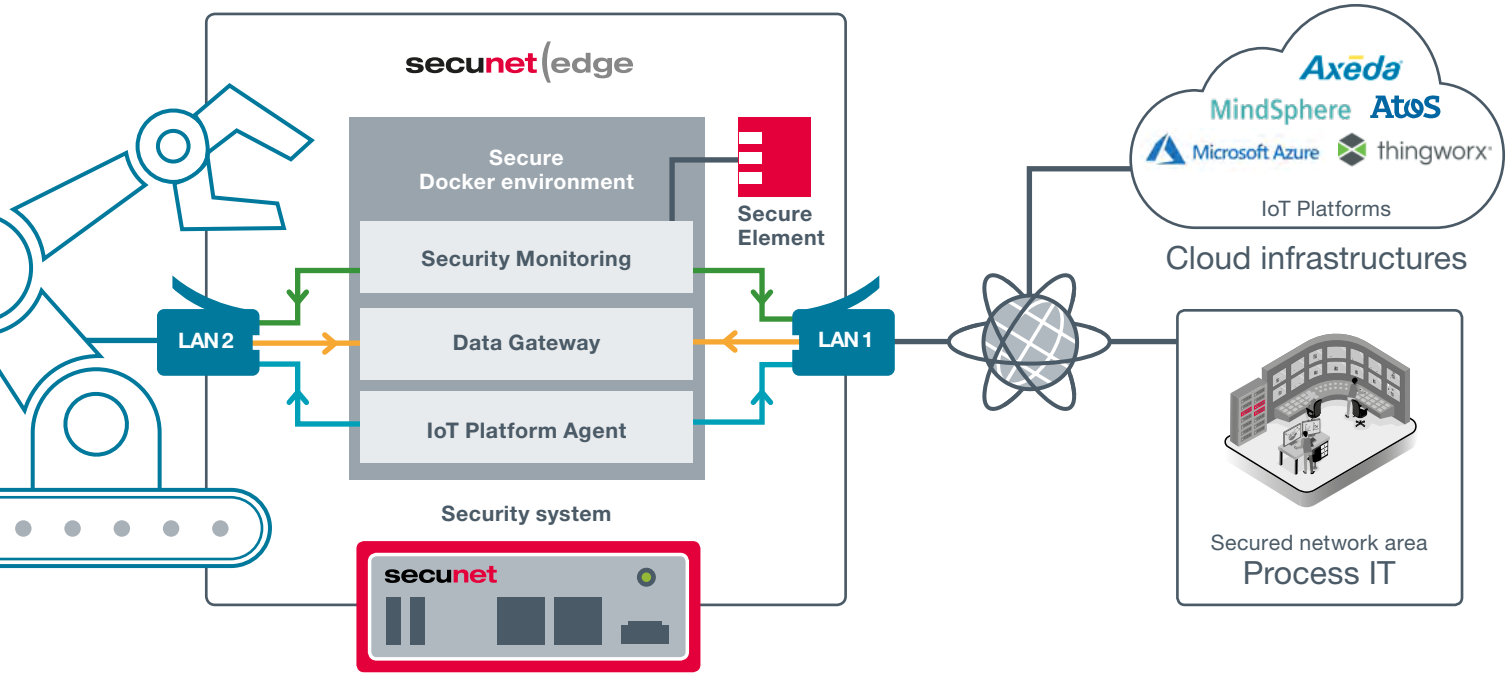
“Stealth factory” approach or micro-segmentation

- **Stealth mode firewall:** machines requiring protection are not visible on the Internet
- **IP firewall mode:** network segmentation

Secure remote access

- Access control for individual types of device
- Case-specific activation





Information Security – Secure Data Processing and Transmission

Thanks to the integrated Docker container, which is secured via a hardened operating system, individual applications can easily be installed and run.

Hardware-based information security

- Embedded Secure Element as a trust anchor for both data security and Docker applications
- Fixed-installation, tamper-proof chip (comparable with smartcard)

secunet security applications as Docker containers

Data gateway – secure processing and encrypted transmission of information

- Directed transfer of the machine's user data to backend or external services
- Protocol translation: from insecure to secure

Security monitoring – real-time monitoring of information flows

- Identification and control of data streams
- Detection of anomalies in data connections

Product Features –
Your Advantages at a Glance

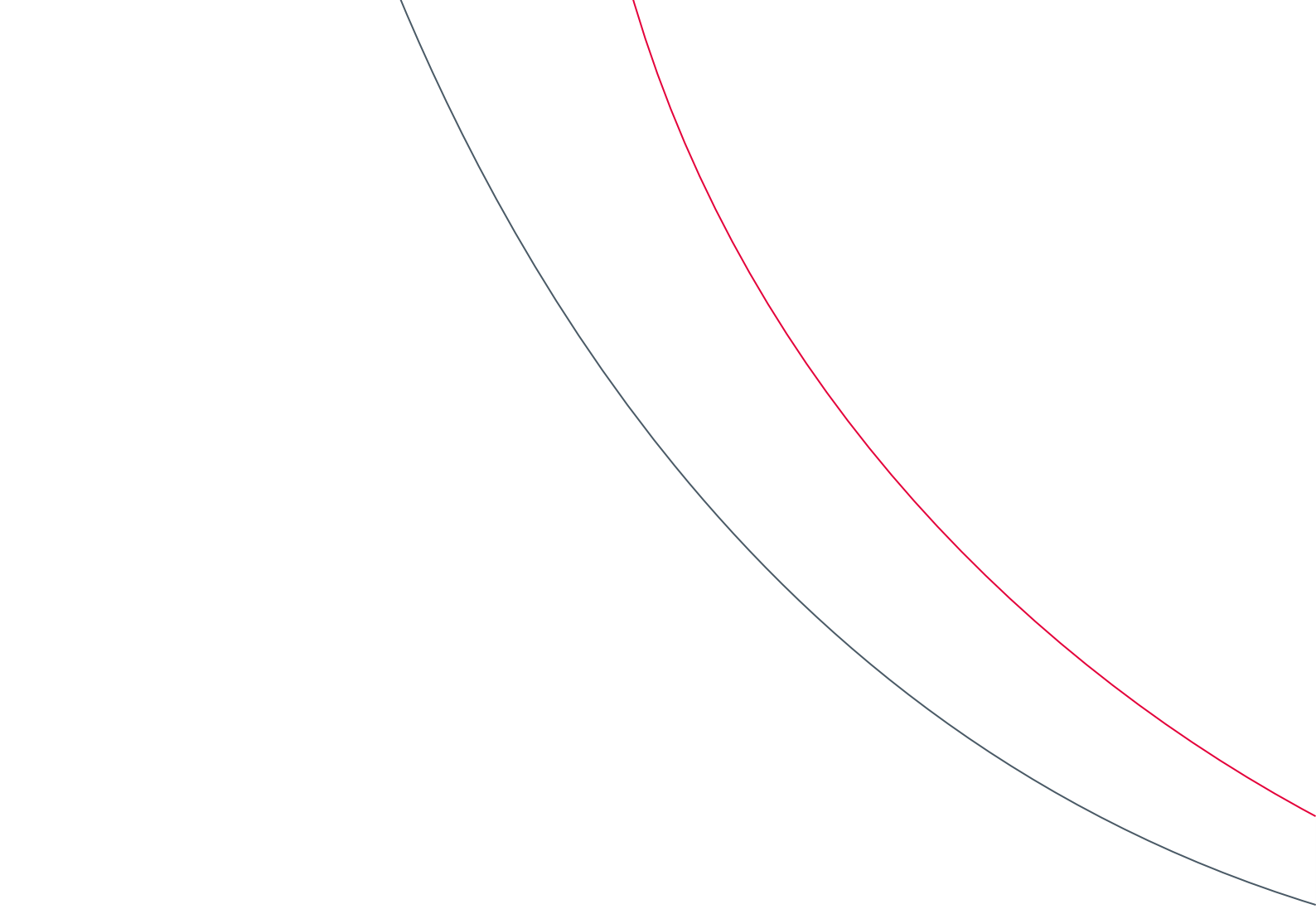
Hardware for industrial use
- Form factor suitable for industrial application
- Industrial long-term availability
- Operational temperature of -40 °C to +85 °C; passively cooled
- Resistant to shock and vibration – IP40
- VESA mount (75x75, 70x70)
- Mounting kits for DIN standard rail and 19" racks
- CE, FCC, EN50155 certified

IT integration
- Can be integrated quickly and easily into existing OT infrastructures
- Interfaces: LAN, Bluetooth, Wi-Fi, 4G, serial COM port

Modular and flexible due to the secure Docker environment
- Future-proof and a secure investment: can be expanded in line with further applications on a modular basis
- Flexible implementation of own business models
- Independent development and operation of Docker applications
- Security applications for Industry 4.0; use cases already available

100% Security made in Germany
- Hardened and minimised operating system
- Hardware-based security: embedded Secure Element (eSE) / CryptoCore® SSD
- Protocol translator
- Anomaly detection / intrusion detection engine

Security standards
- IEC 62443
- ISA99
- ISO 27019
- NIST SP 800-82
- ICS Security Compendium



secunet

secunet Security Networks AG
Kurfuerstenstrasse 58
45138 Essen
Germany
www.secunet.com