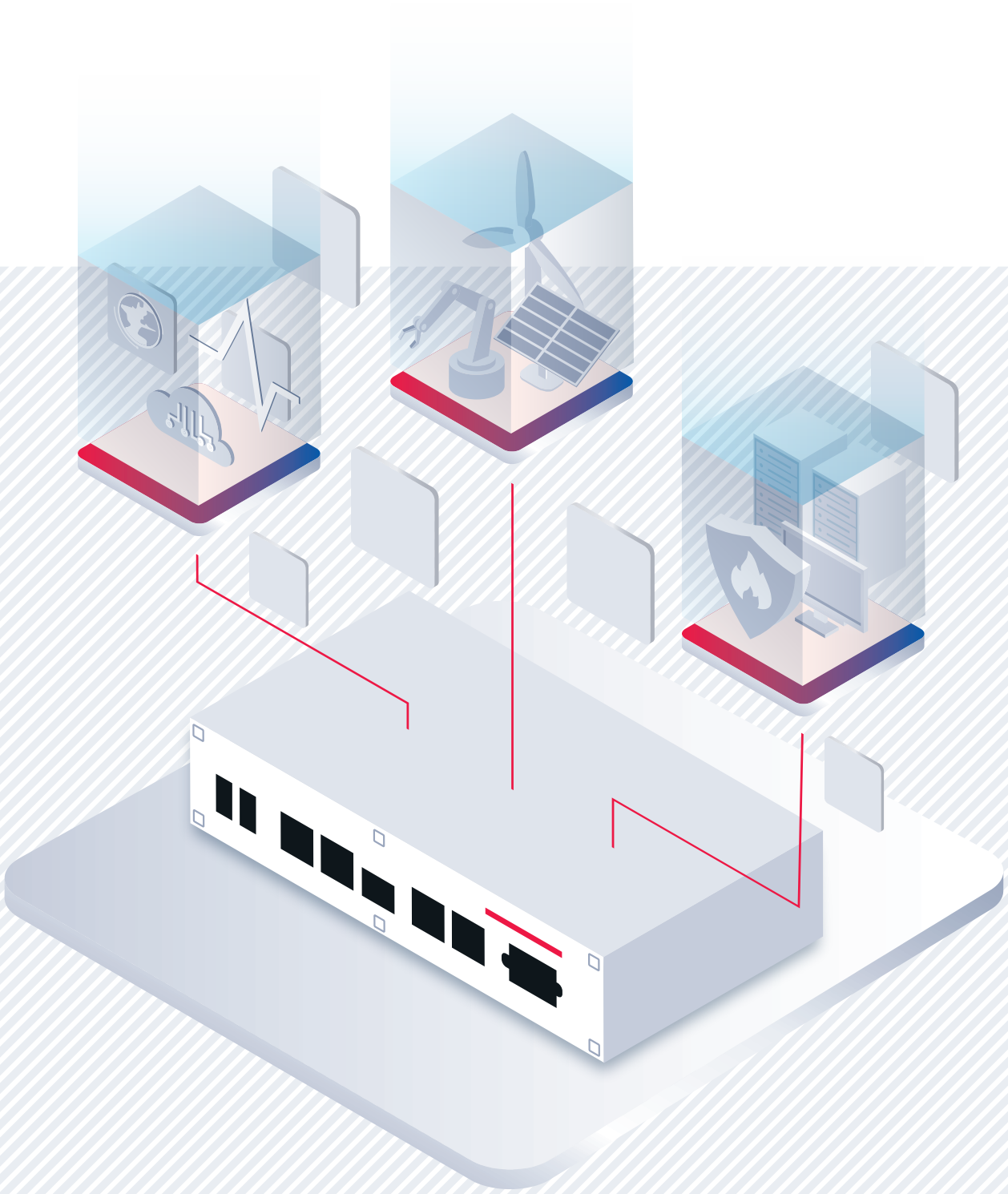
secunet
edge

Factbook



secunet.com

Content

Edge Computing

Best with a complete solution

In edge computing, data and data processing by applications, and possibly also data storage, are shifted away from central nodes toward the edge of networks. It is a major advantage of edge computing that by shifting data processing to the periphery, limited bandwidth and resources are relieved and response times are accelerated. This is particularly relevant in an industrial environment.
Edge computing is thus an integral part of digitalization - whether in its basic form as data processing near to applications or machines, as part of Industry 4.0 or in the Industrial Internet of Things (IIoT).

Edge computing is also essential for "catch-up" digitalization in existing infrastructures (so-called brownfield with often older legacy systems) as well as for digitalizing environments or individual systems that are not sufficiently secure by themselves – but can be made secure by means of suitable enhancements.

Edge computing also allows for combinations of a wide range of use cases - for example a local aggregation of data from an outdated system prior to transfer to the cloud.

In order to best benefit from these developments and to make use of synergies, edge computing should be implemented as a comprehensive solution. The overall solution secunet edge is cost-efficient, convenient and premiumsecure and can be used as a platform for several applications – as shown in the following practical examples:

Cost efficiency and convenience through scaling: In a automation technology reference project, new network segments must be constantly configured. In the past, this used to take several weeks. Now, this been reduced to less than an hour. To achieve the timesavings, individual secunet edge appliances hold a centrally maintained configuration for a highly scalable import into the corresponding network segments.

Scaling and security: In another reference project, a large number of machines had to be connected to a central data exchange. In combination with a secunet partner solution for machine connectivity (deployed as an application on secunet edge), we were able to implement this as a "plug-and-play" solution. In addition to the highly scalable implementation, there is also an additional gain in security because the barely protected machines are now connected via secure secunet edge appliances that act as a firewall, include a secure remote access application and enable monitoring for attacks and anomalies.

Security down to every corner: In a third reference project, secunet edge appliances are used as distributed sensors for a comprehensive network security monitoring. By looking into the respective network areas, the company's security situation report now also covers over a hundred systems "in the field" that were previously invisible.

More in the document:
Introduction to the Overall Solution

Applications for Edge Computing:

- Data processing near to applications or machines
- Connecting (older) machines and protocols
- Retrospective protection of systems
- Monitoring of facilities
- (Secure) remote maintenance and administration
- Network segmentation

secunet_edge_factbook_EN_04/2022

Introduction to the Overall Solution

Secure platform with flexible applications

Digitalized and networked plants, machines, actuators and sensors create great business potential. At the same time, they create attack vectors for malware and targeted attacks - the risk of malfunctions or failures increases. Any expansion of functionality and connectivity must therefore be accompanied by a comprehensive protection against digital threats.

secunet edge addresses these challenges of edge computing as a comprehensive solution with a platform and applications. The platform is made up of a software and a hardware part. The software comprises a hardened operating system with a secure application environment. The hardware of the platform consists of Industrial PCs (IPCs) with built-in security components. secunet offers software and hardware as appliances. Suitable applications are available both from secunet and from partners.

All components of the overall solution have been developed, refined and tested by secunet on the basis of our extensive and long-standing experience and with a special focus on security and trustworthiness (following "Security by Design" for in-house developments and "Security by Default" for adaptations of third-party products).

Widely used, mature and reliably maintained basic components such as an Intel x86 processor, Debian Linux and a fully Docker-compatible virtualization environment ensure maximum compatibility with existing IT and OT infrastructures.

secunet edge is, what an edge solution should be - but also:

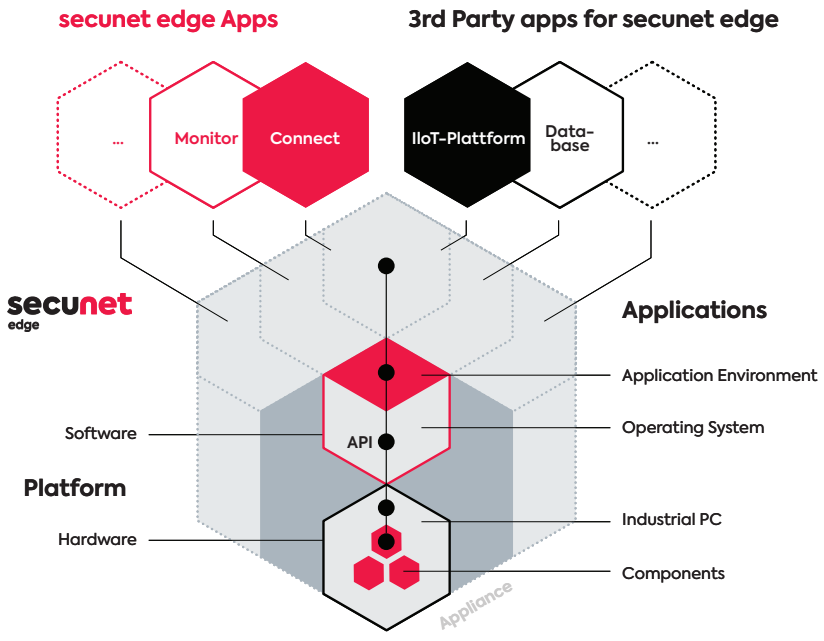
cost-efficient
convenient
premiumsecure

secunet and our parent company Giesecke+Devrient (G+D) secure:

- Sovereign communications
- Critical and systemically relevant infrastructures
- Financial & healthcare systems
- Defence
- Industry

You too can rely on our expertise.

More in the documents:
Secure Edge Platform
Connect (Application for secunet edge)
Monitor (Application for secunet edge)
Remote (Application for secunet edge)



secunet_edge_factbook_EN_04/2022

Secure Edge Platform

Trusted hardware and software

secunet edge offers a stable platform and reliable applications for security in edge computing, in Industry 4.0 and for the Industrial Internet of Things (IIoT).

The secunet edge platform consists of hardware designed for industrial use and a hardened operating system with a flexible environment for applications. Designed as an appliance that combines hardware and software, secunet edge ensures maximum system stability, compatibility and security as well as long time reliability.

Please also ask for the suitable edge applications of our partners and secunet!

Secure hardware – Industry proven

Our secunet edge Industrial PCs are developed together with our partner Beckhoff Automation GmbH & Co KG and made in Germany. The result is a solution tailored to industrial requirements with the reliability, sustainability and quality known from the industrial hardware market leader Beckhoff. High-performance Intel technology further ensures extensive compatibility with established solutions.

BECKHOFF intel Infineon

Capital-optimized life cycles and cost efficiency through less replacement. Convenience through compatible Intel technology platform (avoiding architectural breaks). Premium physical security outside and inside the hardware.

For more on the added value see also:
Value Proposition

Solid cryptography

secunet edge is the first edge hardware that integrates the patented CryptoCore SSD with a dedicated and flexible embedded secure element (eSE) from Infineon as opposed to a static trusted platform module (TPM). The security anchor operates with a smart card operating system developed by Giesecke & Devrient (G+D). The eSE and its software is adapted from the high-security sector and with FIPS 140-2 Level 3 or BSI Common Criteria EAL 5 certified according to the highest security standards.

Less risk of incidents due to optimally protected keys and less effort for replacement.

In the comprehensive concept of the integrated secunet CryptoCore SSD hard drive, local storage is secured directly via hardware encryption.

Out-of-the-box hard disk encryption protects sensitive data “by default” and reduces the configuration effort compared to extra solutions.

The secure element and its cryptographic functions can be conveniently used from application containers via a standard interface.

Cryptography becomes much more convenient and cost-effective to use - with higher security, because it is not self-built but already implemented by experts.

secunet edge Line-Up

secunet edge	secunet edge extended	secunet edge high performance
		
2× LAN with Intel Chipset i210 1× USB 2.0, 1× USB 3.0	4× LAN with Intel Chipset i210 1× USB 2.0, 1× USB 3.0 RS232	6× LAN with Intel i210 4× USB 3.1
Intel ATOM E3827	Intel ATOM E3827	Intel Core i5 8365UE
2 GB DDR3L RAM	2/4 GB DDR3L RAM	16 GB DDR4L RAM
16/64 GB secunet CryptoCore SSD*	16/64 GB secunet CryptoCore SSD*	64 GB secunet CryptoCore SSD*
Dimensions W×H×D: 85.6×33.8×83.3 (mm)	Dimensions W×H×D: 162.6×40.6×121.6 (mm)	Dimensions W×H×D: 162.6×64.5×123 (mm)

*with Embedded Secure Element SCE7 (FIPS 140-2 L3 or BSI CC L3 EAL5 certified)

Secure operating system

The secunet edge platform operating system is based on the long-term support releases of Debian Linux, which is recognised for professional use. The OS has been further hardened using experience from the high-security sector. secunet also closely follows the Civil Infrastructure Platform Project of the Linux Foundation.

Less attack surface than non-hardened standard and less effort compared to own hardening.

Flexible and secure application environment

The secunet edge application environment runs on the hardened operating system of the secunet edge platform. Your advantage: maximum flexibility with highest security. The application environment consists of a user-friendly web interface, a hardened container environment and comprehensive application interfaces.

Web-Interface

Instead of complex configuration at command line level, important functions of the platform and the secure application environment can be used from a comfortable user interface - for single instances or extensive installations (see also "Central Management").

Quick and correct configuration and maintenance after a short training period, comfortable operation and lower maintenance costs.

Hardened environment

On the secunet edge platform, applications ("apps") are executed in a hardened container environment or, if required, as "add-ons" closer to the hardware. By using containers, applications can be rolled out, exchanged, reused and better maintained in a scalable manner.

Compatible with agile approaches and response times, efficient in development and maintenance as well as reduced effort for maintenance and updates.

Interface (API)

Instead of costly development kits and laborious training, container apps can use functions of the platform via a standardized interface (REST API).

Reduced integration efforts, less room for costly errors through standardized functionality and less effort for development. Convenient use of the platform functions including security components.

Scalable deployment

A secunet edge device is rarely used alone – in industrial environments, sometimes even hundreds or thousands of instances are used. Therefore, our platform is designed for scale.

Auto-provisioning saves money – especially in the roll-out phase of a new solution – reduces the risk of individual errors and is much more convenient than individual provisioning.

Central management

The core component for scaling is the central management that administers appliances and orchestrates applications. secunet edge offers the following options:

- Microsoft Azure IoT: Use Microsoft's established platform for central management and direct connection to cloud applications. secunet edge is Microsoft Azure IoT Edge certified.

Microsoft Azure Certified

- PTC Thingworx Cloud & On-Premise: secunet edge brings direct support for PTC's Industrial IoT platform. Thingworx is available both in the cloud (e.g. in Microsoft Azure) and on-premise.
- secunet edge Central Management: Central management is also possible without a public cloud and IoT platform. Our management application turns any secunet edge device into a management appliance.

Less administration effort when operating many instances.
Reduced risk of human error through automation. Flexible and convenient use through remote maintenance without the need of being on site – with all security advantages of the platform.

Auto provisioning

With Microsoft Azure IoT, distributed secunet edge devices can be provisioned quickly and automatically.

Well thought-out concept

Customers value secunet and our partners as a guarantee for reliability and stability. Accordingly, the Edge platform offers long-term support (hardware and software) for ten years. The security concept of the platform ranges from the overall concept to the details and includes, for example, encrypted and thus secure time synchronisation. edge is continually being developed as a core component for Critical Infrastructures (KRITIS) and infrastructures in the public interest. We aim to certify secunet edge with a corresponding security label (as soon such a label is available from a regulatory point of view).

With secunet hardware and software, you are in good company: in addition to security authorities and other public clients, the defence sector and the automotive industry, secunet is also a trustworthy supplier for KRITIS and manufacturing companies in many sectors and industries.

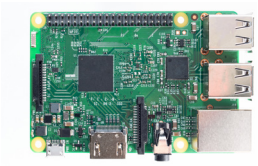
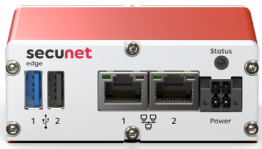
Many years of experience and mature components from the high security sector are incorporated and integrated by default – more security for the same investment.

Trust the well thought-out concept of secunet edge. Further information on hardware and software as well as on the certifications of our platform can be found in the document:
Technical information

Edge-Computing/Industry 4.0/IIoT from the security partner of the Federal Republic of Germany.

Comparison

Generic Edge Device and secunet edge

Component	Generic or self-built	secunet edge
		
Recommended fields of application	Learning, development, prototypes, demon-stratordemonstration	Development, prototypes, demonstration and in production
Cryptography	No hardware component or purely static Trusted Platform Module (TPM) and as well as functions usually only implemented in software	Expert implemented, dedicated and flexible embedded secure element (eSE) with cryptog-raphy and key storage on the hardware level
Operating system	Standard or community distribution or self-made with integration and compatibility via own effort	Operating system hardened by secunet with long-term support based on Debian Linux
Updates	Own effort	Kept track of, maintained and provided by secunet with guaranteed compatibility
Configuration	Command line	Web-Interface or REST API
Scalable management	No default integration with management platforms or connection to be integrated by the user	Existing integrations with IoT platforms and independent solution by secunet available
Technology Platform	Mostly ARM-based	Intel x86 for industrial use and compatib
Hardware components	Self-assembled individual components with independently implemented tests	Comprehensive system developed and main-tained from a single source, tested (climate chamber, electrostatic discharge, burn-in tests, etc.) and ready for immediate use
Hard disk encryption	None or software based with individual setup	Already implemented on the hardware level via CryptoCore SSD
Life cycle	No specified life cycle or oriented towards the DIY market	Industrial life cycle of at least 10 years
Origin	Standard components	Trusted sourcing and validation
Production	Made in Somewhere	Made in Germany
Certification	Varies and mostly basic certificates, recertifi-cation necessary depending on configuration	Extensive pre-certifications including special fields of applicationas well as continuously updated by secunet

Value Proposition

From vision to value

Our vision

The best overall solution for digitalization and networking in Edge Computing, Industry 4.0 and for the Industrial Internet of Things (IIoT).

Our mission

We provide a secure edge platform that enables various applications for Industry 4.0, Industrial Internet of Things (IIoT) and Edge Computing and creates added value for our customers – especially by reducing information security risks such as data theft, manipulation and failures.

Our value proposition

Don't go on an adventure with uncertain outcomes – invest in a well-capitalized and sustainable solution for your digitalization projects. From concept to operation in familiar life cycles – secunet edge is the user-friendly backbone for Industry 4.0 and beyond. We ensure security and trust in information technology – you build, secure and optimize your success.

secunet edge can do what an edge solution must be able to do – but also:

cost-efficient, convenient and **premiumsecure.**

cost-efficient

- **One platform for several solutions** instead of many systems for only one solution each
- **Long life cycles** instead of replacing, scrapping, and relearning every few years
- **Reduced risk of damages** by avoiding breakdowns
- **Less effort for replacement & maintenance** due to long-term stability
- **Less training and manageable requirements** for operators and administrators
- **Complex security already reliably implemented** instead of costly in-house developments

convenient

- **Scalable use** through central management
- **Containers** for applications instead of integration efforts
- All important functions availablevia an **API**
- **Choice** of **individual configuration** or **central management** as **on-premise, via (I)IoT platforms** or with **Microsoft Azure**
- **Mature and reliable** through many years of productive use
- **Flat learning curve** through user-friendliness and comprehensive documentation

premiumsecure

- **Security by Design** of applications down to the hardware component level
- **Security by Default** according to established standards
- **Secure applications** from reliable ecosystem partners and from secunet
- **Solid cryptography** from the market leader
- **Certified** for safety and industry-specific requirements
- Future **KRITIS core component**
- Comprehensive solution from the **security partner of the Federal Republic of Germany**

secunet_edge_factbook_EN_04/2022

Connect

Application for secunet edge

The secure communication of machines with the corporate network, within production networks as well as the basic secure connectivity of systems to structures, processes, cloud and IoT services is an essential part of digitalization.

Connect is available as an application for secunet edge appliances and enables secure connectivity.

Usability

All functions of the application can be configured as well as used efficiently and conveniently via the specially developed user interface. Learning more complex mechanisms - such as using a command line - is not necessary.

Ease of use not only saves time, but also allows employees with less experience or skills to establish secure connectivity.

Protocol translation

By translating obsolete or insecure interfaces and protocols, security is added after the fact (e.g. SMB to SFTP). This is done "on-the-fly", i.e. without intermediate storage of data on the secunet edge appliance.

Existing functions of insufficiently secure systems can still be used conveniently and without the need for costly modifications.

Cloud- and IoT-Gateway

The use of cloud services and IoT platforms is an important part of IT and digitalization strategies. secunet edge provides hardened agents for common providers to ensure a fast and secure connection.

Public or private cloud connections are already included or can be efficiently implemented via interfaces.

Connectivity with secunet edge

Connect for secunet edge is the solution for a **cost-efficient, convenient** and **premiumsecure** connectivity of systems and facilities. The application is delivered as a container to secunet edge appliances.

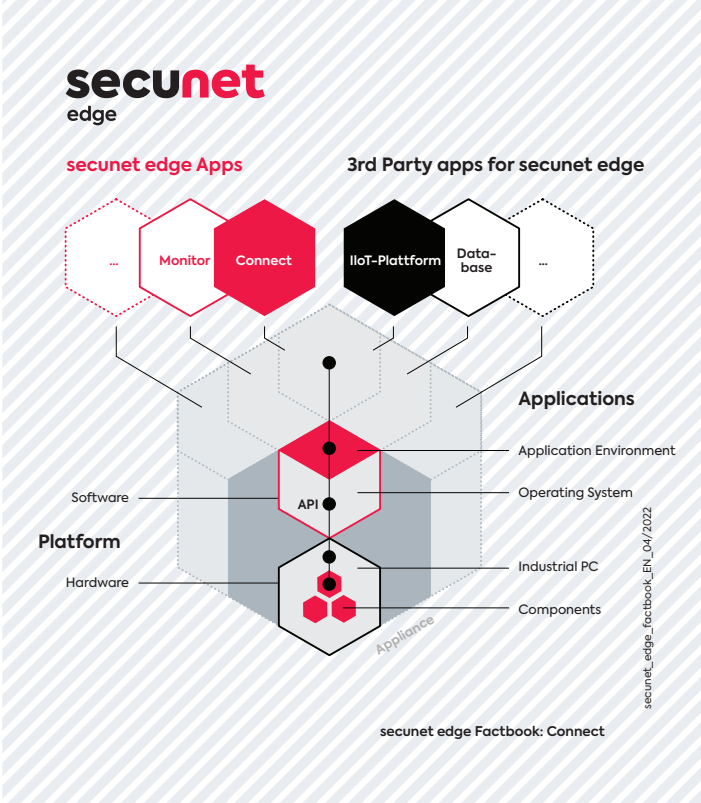
secunet edge comprehensive solution

secunet edge offers a stable platform and reliable application solutions for security in Edge Computing, in Industry 4.0 and for the Industrial Internet of Things (IIoT). The secunet edge platform consists of hardware with security components designed for industrial use and a hardened operating system with a flexible environment for application solutions.

Hardware and software platform are available as a ready-to-use appliance.

secunet edge enables you to make use the opportunities of digitalization and reduce the associated risks at the same time.

secunet edge's flexible architectureis further well prepared for other applications such as predictive maintenance or data aggregation at the edge.



Remote

Application for secunet edge

Remote

For maintenance and the configuration of machines, technicians often have to be on site. This is associated with high travel costs and longer reaction times, especially for external service providers and geographically distributed plants.

Remote for secunet edge is the solution for a **cost-efficient, convenient** and **premiumsecure** connectivity of systems and facilities. The application is delivered as a container to secunet edge appliances.

Remote is available as an application for secunet edge appliances and enables secure remote maintenance.

Remote maintenance with Edge Computing

For some time now, digital technologies have made remote access to machines possible. The advantages are quickly apparent: less time is requiredwhich leads to lower costs. In addition, response times are shortened, which reduces process failures and creates opportunities through more agile adjustments. Unfortunately, it turns out that many systems do not meet the technical requirements for efficient and secure remote maintenance.

Edge computing is an integral part of digitalization, because it uses technology that can be embedded in existing, "older" infrastructures. The Edge Computing component provides the necessary computing power and storage capacity as well as suitable interfaces and functions. Edge devices can therefore be understood as "retrofit kits" in the context of digitalization measures.

However, some users of edge computing bring serious security problems into their organizations when they upgrade. Suddenly, not only their own technicians or trusted service providers have access to systems, but also unauthorized external parties via weak points. If, for example, production is then infected with ransomware, high damages can result.

Remote maintenance with secunet edge

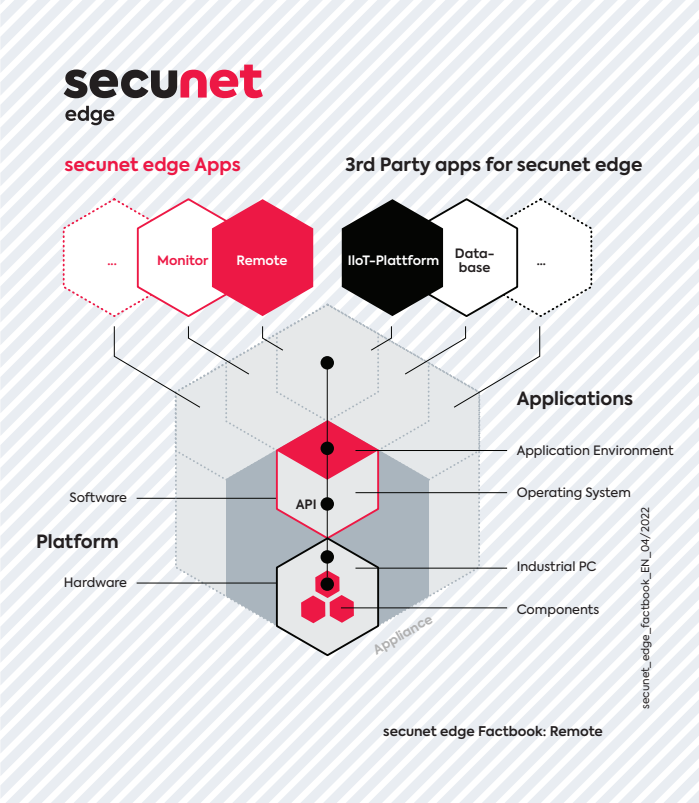
With "Stealth Machine - Stealth Factory", systems connected via secunet edge are mostly invisible to attackers. In addition, unlike many other solutions, VPN network coupling is not absolutely necessary.

secunet edge comprehensive solution

secunet edge offers a stable platform and reliable application solutions for security in Edge Computing, in Industry 4.0 and for the Industrial Internet of Things (IIoT). The secunet edge platform consists of hardware with security components designed for industrial use and a hardened operating system with a flexible environment for application solutions. Hardware and software platform are available as a ready-to-use appliance.

secunet edge enables you to make use the opportunities of digitalization and reduce the associated risks at the same time.

secunet edge's flexible architecture is further well prepared for other applications such as predictive maintenance or data aggregation at the edge.



Monitor

Application for secunet edge

Monitor

Employing network monitoring enables you to monitor the security and quality of your networks and thus obtain an up-to-date situation report. Distributed sensors are an integral part of this monitoring, especially for connecting remote locations and systems as well as for "looking behind" firewalls and other abstracting network components.

Monitor is available as an application for secunet edge appliances and enables reliable monitoring.

The application requires the network security monitoring solution secunet monitor (avilable on-premise or as-a-service).

Asset discovery & network topologies

Ideally, the systems and their topology within networks should be known. However, real transparency only comes about through continuous discovery and recording of the actual conditions.

Completely passive sensor technology can be quickly integrated into existing infrastructures, does not affect operation and cannot cause any interference itself.

Attack Detection

The passive sensor detects known attack patterns - e.g. hidden tunnels within legitimate protocols like DNS or ICMP. By integrating suitable indicators (Threat Intelligence), signature-based attacks or attempted attacks in the network can also be detected and fended off.

This functionality has increased system requirements (possible with secunet edge high performance - available from early 2021 - or via a server appliance).

Premium protection against known attacks and a chance to detect advanced threats.

Vulnerability & Compliance Detection

Distributed sensors in the network also enable passive detection of weak spots such as obsolete operating systems or insecure protocols, as well as compliance deviations such as risky network transitions between production and office networks. Unwanted or disallowed communication is also detected.

Comfortable and efficient comparison of plan and reality based on actual conditions

Anomaly detection

By observing network traffic and through machine learning, the usual behavior within networks is determined. Deviations from the learned normal state (including service issues and attacks) are thus directly noticeable as anomalies.

A chance to detect unknown attacks and problems that otherwise cannot be detected - especially not before it is already too late.

secunet_edge_factbook_EN_04/2022

Investigations

Using the local storage of a secunet edge, security-relevant data and even the entire network traffic (depending on bandwidths and data volume) can permanently be stored in a ring buffer. This data can be invaluable in the (forensic) investigation of incidents.

The recording of data on the outer arms of the infrastructure provides helpful details for efficient incident handling and storage close to the origin. Furthermore, it saves scarce bandwidth when connecting remote systems.

Transparency & Documentation

Via the respective secunet monitor central system, extensive possibilities for interaction, documentation and for manual and automatic reports are available. This way, you always have an overview and can track changes.

Configurable reports enable a comfortable and automated reporting suited to the target audience.

Network monitoring with secunet edge

secunet edge monitor is the solution for cost-efficient, convenient and premiumsecure network monitoring. The application is delivered as an add-on to secunet edge appliances.

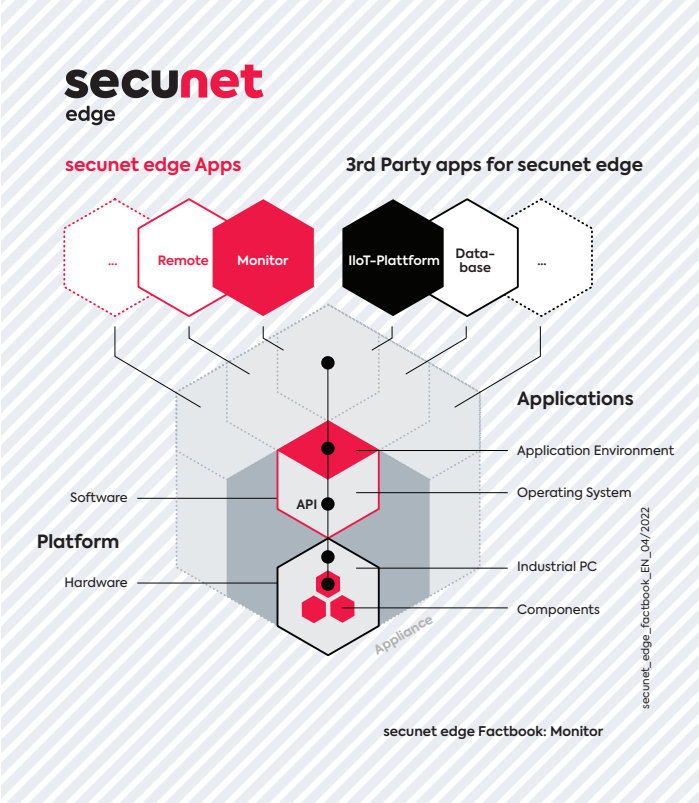
secunet edge comprehensive solution

secunet edge offers a stable platform and reliable application solutions for security in Edge Computing, in Industry 4.0 and for the Industrial Internet of Things (IIoT). The secunet edge platform consists of hardware with security components designed for industrial use and a hardened operating system with a flexible environment for application solutions.

Hardware and software platform are available as a ready-to-use appliance.

secunet edge enables you to make use the opportunities of digitalization and reduce the associated risks at the same time.

secunet edge's flexible architectureis further well prepared for other applications such as predictive maintenance or data aggregation at the edge.



Multiple possibilities.

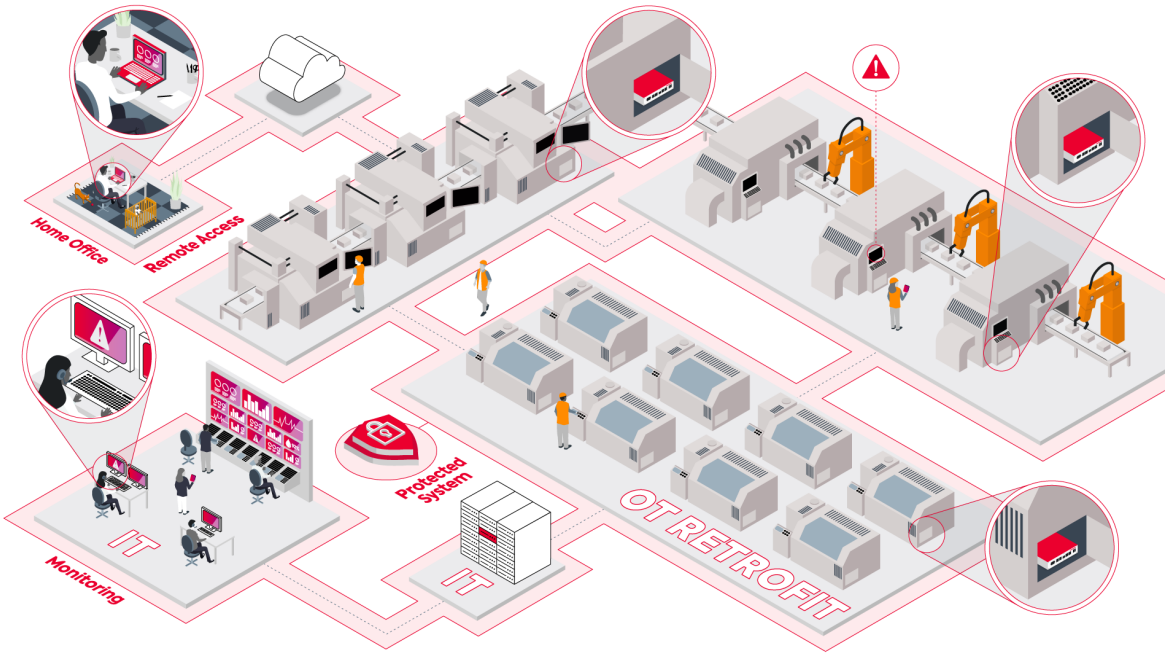
secunet edge use cases

Thanks to the flexible structure of the overall solution, many areas of application are possible, including those that may only take off in the near future – for example, autonomization by means of machine learning. secunet edge is flexible in terms of the breadth of application areas and can at the same time be specifically aligned to concrete industry use cases – as the following practical examples show:

Production

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

secunet edge enables or extends your capabilities at the boundary between the digital world and the physical world and increases the security of your production processes. As an overall solution, it combines many use cases in a stable and trustworthy infrastructure.

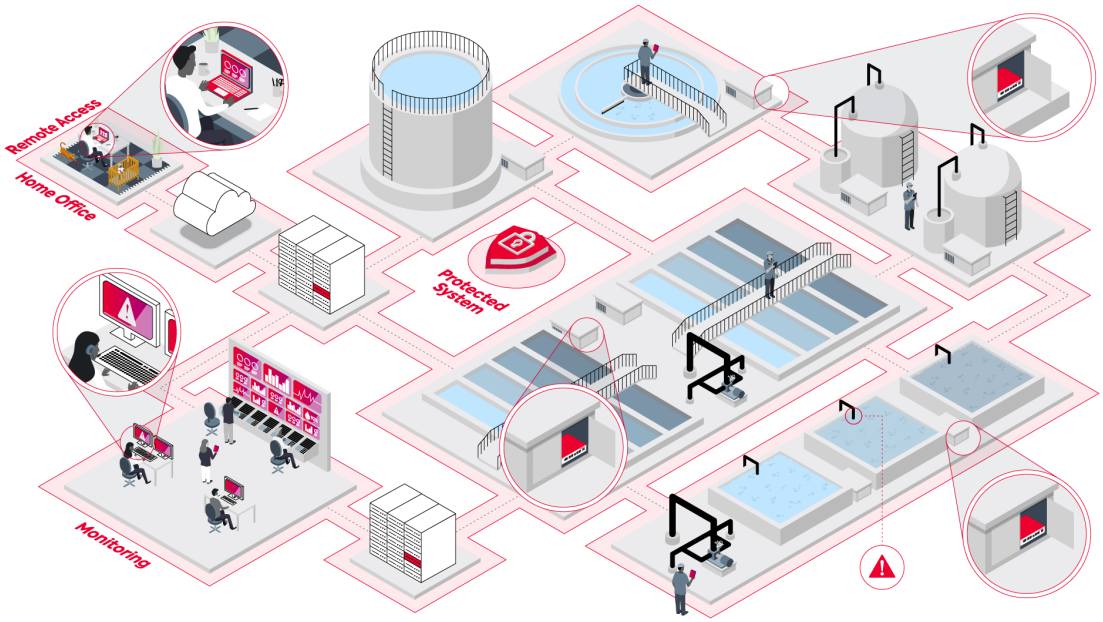


secunet_edge_factbook_EN_04/2022

Water Supply

Screening of water supply & waste-water treatment systems & use of advanced applications.

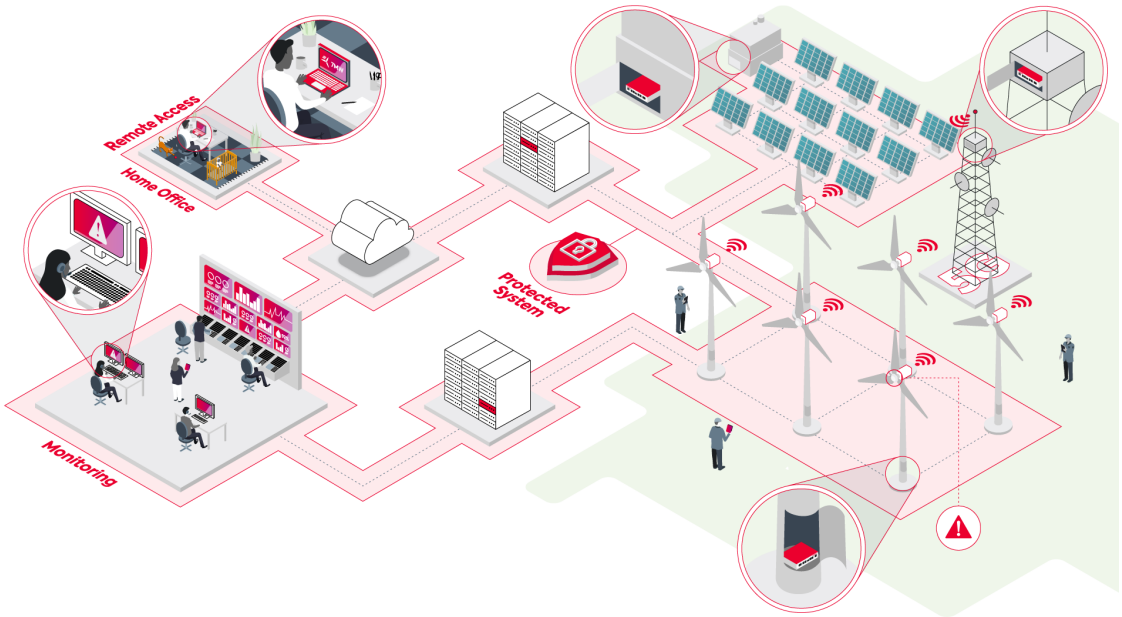
secunet edge also retrofits systems in critical infrastructures such as fresh water supply or wastewater treatment plants. In addition to providing a protective umbrella and a cloak of invisibility for risky systems, the platform can also be used for modern applications - for example, to increase energy efficiency.



Energy Supply

Secure remote access and pro-active monitoring in distributed power supply.

secunet edge enables secure remote access and protected remote administration for distributed and networked power generation plants, substations or other plants „in the field“. With the same infrastructure, security states and quality aspects can also be monitored proactively.



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 specialises 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 700 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 in the Prime Standard segment of the Frankfurt Stock Exchange and generated revenues of 285.6 million euros in 2020 (preliminary business results as at January 22nd, 2021).

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