secunet medical connect

Trustworthy and securely networked medical devices

sie.at

secunet.com

Networked medical devices? – the foundation for modern medicine!

Networked medical equipment offers new possibilities and opportunities, but also poses various risks and challenges.

Systems that assist with treatments, AI-based analyses for early detection of diseases and operations with globally distributed players are target scenarios in modern medicine. Based on digital transformation, they enable state-of-the-art treatment, diagnosis and care methods.

One thing is clear: Such digitisation concepts require an unhindered flow of information plus secure and trustworthy communication between medical devices in digital infrastructures.

Challenges in medical device networking

Operating medical devices in a networked digital world is a challenging task: data-driven use cases are complex, regulatory requirements must be met and IT security aspects must be constantly addressed for critical medical equipment and sensitive data.

Every networking point creates new threat vectors for cyberattacks on medical devices and networks. The risk of system failures increases. The consequences can be far-reaching.

Regulations impose and require an IT security level for medical devices, networks and applications to be set up and maintained in line with needs.

Complex retrospective approval procedures for medical devices hamper innovation and prevent adaptations for their integration into digital care and management processes.

The long life-cycles of medical devices create a void between the installed information technology and the current state of the art, so that the systems increasingly exhibit weaknesses over time, thus giving rise to operational risks.

Medical devices are used in **heterogeneous environments** and sometimes have outdated interfaces that complicate uniform networking and do not provide the necessary level of security.

Medical devices are increasingly targeted by attackers. Recent studies show that

- medical devices have an average of **6.2 vulnerabilities**.
- medical equipment is increasingly at risk from **cyberattacks**.
- 60 % of medical devices in the field are **end-of-life** and no longer maintained.

Frost & Sullivan, Medical Device and Network Security – Coming to terms with the Internet of Medical Things (IoMT), 2019
HHS Cyber Security Program, 2021 Forecast: The Next Year of Healthcare Cybersecurity, 2020

Application-oriented concepts in four domains

In order to create needs-based networks for medical devices and to integrate them into digitisation projects, it is necessary to address requirements and measures in four different domains. Consequently, skills from different specialist disciplines have to be combined.

Compute

Processing and transfer of data in medical spheres of activity

- Secure execution of applications at the point of origin (close to the medical device)
- Protected communication with internal and external digital services

Protect

IT security at all levels: from hardware to application

- Protection of the medical device, applications and data according to need
- Continuous maintenance of the IT security level according to the current state of technology

Connect

Connection of systems to the IT infrastructure

- Flexible adaptation to heterogeneous architectures of operator infrastructures
- Consideration of legacy interface standards (retrofitting of legacy systems in the field)
- Inclusion of modern transmission technologies and concepts of information technology

Compliant

Compliance with various regulations and requirements

- Regulatory requirements (MDR, IVDR, FDA) are met
- Operator requirements (KRITIS B3S, ISO 80001) are taken into account

Should the domains be implemented directly in medical equipment?

You can add appropriate software and hardware components to the medical devices to cater for the requirements of the individual domains. However, this leads to a close linkage between individual solutions and the respective medical device, which inevitably drives up the development times and costs of the devices, and will eventually lead to the emergence of monolithic and poorly manageable overall systems. In order to prevent such a dilemma, the best solution would be a modular overall system in which various connectivity and security components are connected according to need, upstream of the medical system itself.

Yet this holistic solution approach that covers the requirements of individual domains requires more than the cascading of specialised components on the medical device. These are frequently strong in one domain. Merging them in the overall solution is a complex and cost-intensive task – it is hardly feasible to organise the various manufacturers, life cycles and modes of operation along with the integration and operating conditions of the products.

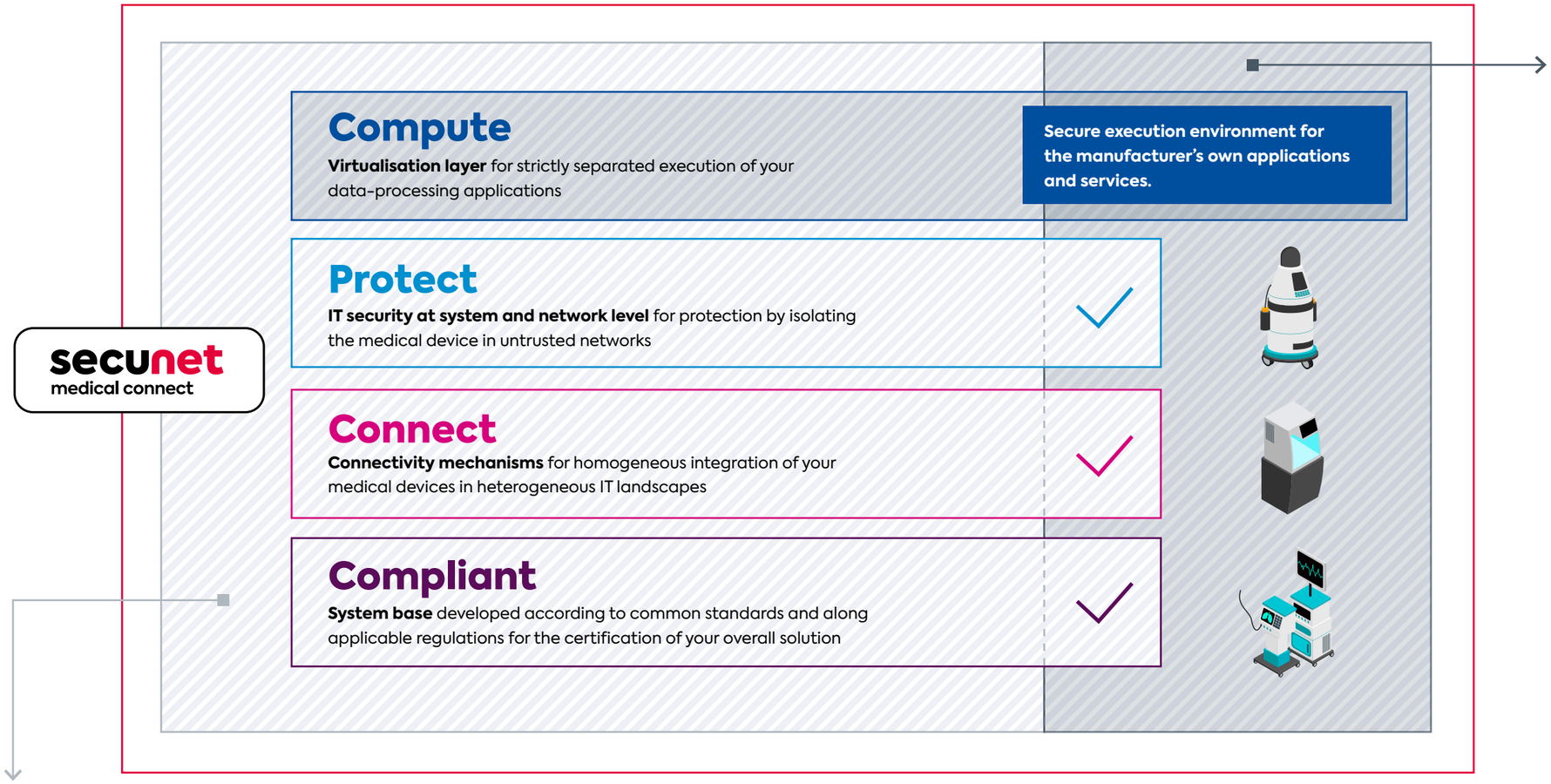
	Compute Integration in digital services	**Protect** IT security of medical equipment	**Connect** Interfaces to infrastructures	**Compliant** Compliant with regulations
IT security solutions	✗	✓	✗	✗
Connectivity solutions	✗	✗	✓	✗
Industrial PCs	✓	✗	✓	✗
secunet medical connect	✓	✓	✓	✓

The **secunet medical connect** security gateway takes into account requirements from all domains and consolidates relevant specifications and concepts from the fields of medical technology, information technology and IT security.

Solution concept for networking medical equipment

The combination of relevant technologies from different disciplines on one security gateway enables the secure and flexible connection of medical technology to the fast-moving IT world. By integrating **secunet medical connect** into your concept, you can dedicate your full attention to the development of your medical equipment and services. We handle the system basis and properties of the individual domains for secure networking of medical equipment.

secunet medical connect always provides the same secure foundation for various digitisation concepts. Required modules and functions are used, depending on the application.



Manufacturer

Your advantage from a flexible security platform

- Focus on your medical devices and specialist applications
- Implementation of your digital processes through integration of your medical device
- Secure bidirectional communication between your medical device and digital services
- Your medical device is constantly protected through agile update cycles
- Assistance in meeting legal requirements
- Harmonisation of digitisation concepts for your various medical devices on a system basis
- Flexible networking of your existing and future medical devices
- Reduction of your efforts and costs in conceptualisation and operation through a uniform system basis
- Investment protection through successive implementation of your use cases

secunet & S.I.E

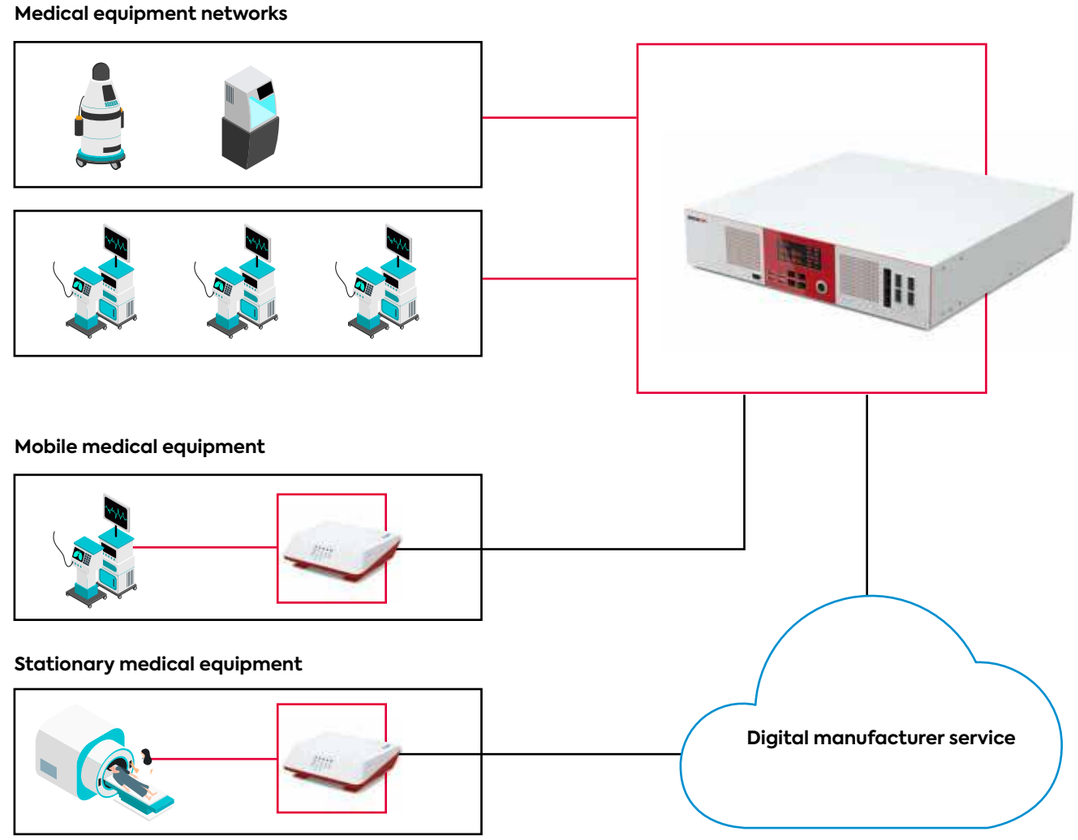
Our organisational excellence and expertise

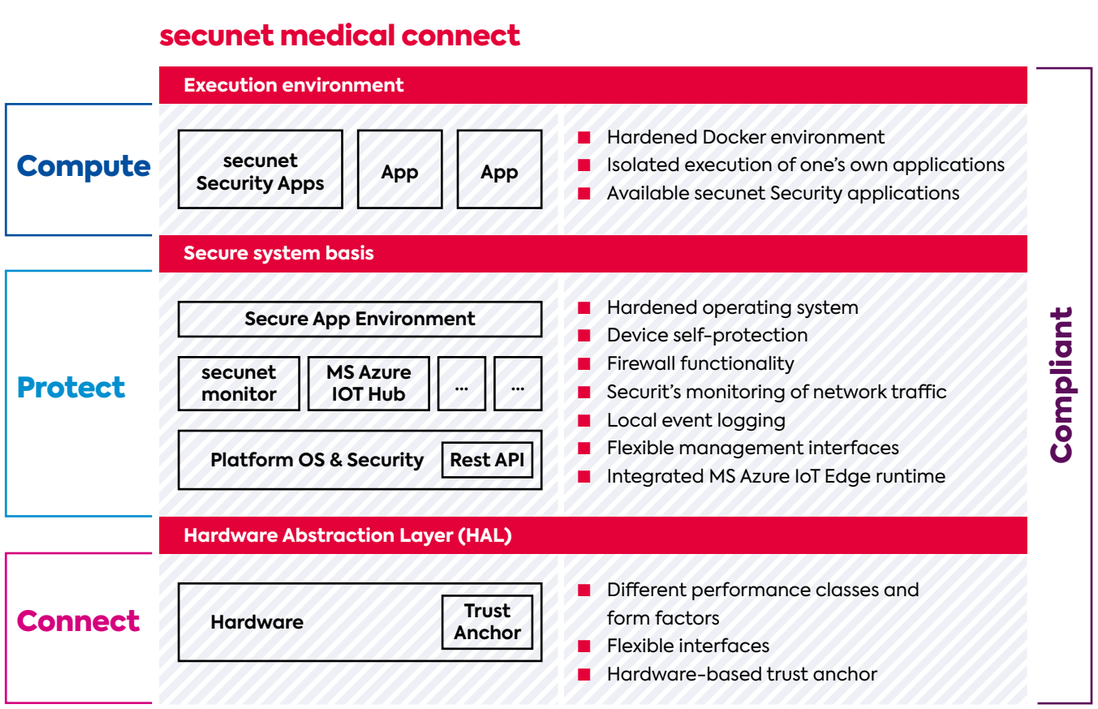
- Hardware and software development
- IT security solutions
- Certifications & approvals
- Concept and prototype
- Lifecycle management
- Supply chain management

Holistic solution concepts through strong partnerships
The implementation of digitisation projects through networked medical devices requires combined expert knowledge on the four levels: Connect, Protect, Compute and Compliant. This is the only way to avoid both isolated solutions and considerable additional work. The approach: a seamless link between security and medical equipment.

The future for trust-worthy digitisation projects

The **secunet medical connect** product family is based on secure gateway technology that combines modern IT security and information technology solution concepts in a single platform.



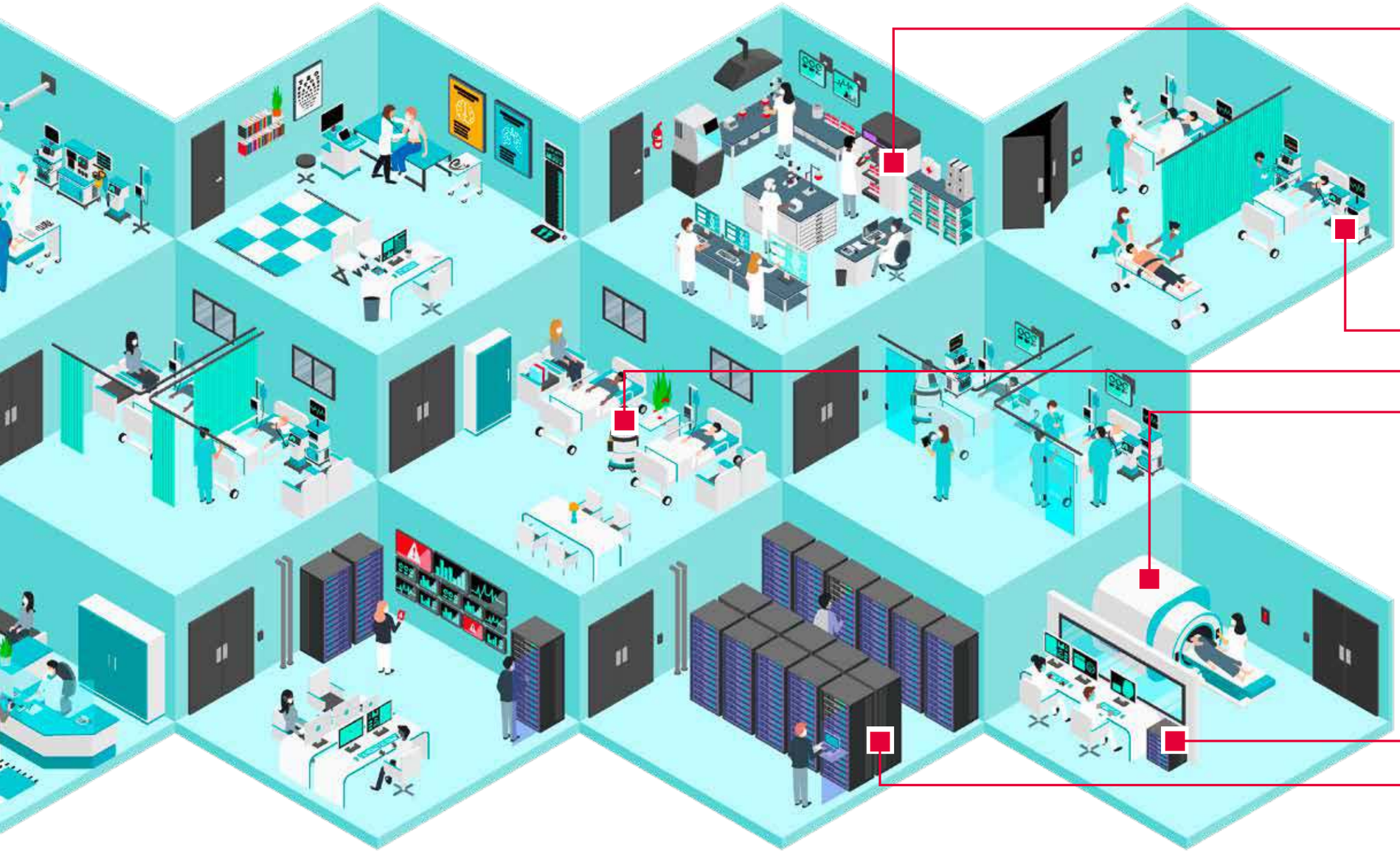


As an individually applicable gateway technology, **secunet medical connect** is our solution approach which serves different application scenarios and performance requirements in various hardware versions.

One platform, different applications, individual spheres of activity

secunet medical connect can act as a security gateway in various forms – adapted to the application scenarios within the operator's IT infrastructure. The individual variants can also be operated independently or in combination. For example, data can be collected directly on the medical device (**Juno** or **Carna**), processed and then made available to data-driven and more computationally intensive services on the central authority (**Athene**).

The different versions of the **secunet medical connect** platform are based on one and the same hardened system basis. Numerous integrated IT security mechanisms enable the compliant networking of medical devices according to current regulations and best practices.



secunet medical connect Juno
Gatekeeper for rule-compliant networking of medical devices

secunet medical connect Carna
Medical applications on near-patient medical devices

secunet medical connect Athene
Data integration and processing for heterogeneous data sources in a central location

Medical device protection and secure connection to remote services

secunet medical connect Juno helps you protect your medical devices in compliance with rules as defined by the operator, while at the same time enabling you to provide your management and maintenance-relevant applications via the hardened execution environment (e.g. for remote maintenance). As a manufacturer, you benefit from the platform's integrated IT security mechanisms: Placed between the medical device and the rest of the network, Juno acts as a security gateway to isolate medical devices from the rest of the IT infrastructure, thus protecting them against unauthorised access.

Secure medical device networking
Restriction and monitoring of communication flows into the connected operator network

Secure integration of medical devices in digital services
Securely and flexibly integrate your own applications for remote maintenance

Rule-compliant medical device networking
Implement IT security requirements (from MDR, FDA, B3S KRITIS, ISO 80001) during operation

Corrective security measures for rule-compliant operation

Secure remote access, asset management and update processes

Retrofit medical devices with a low level of IT security

Data intermediary between different security zones

Symbiosis with medical equipment

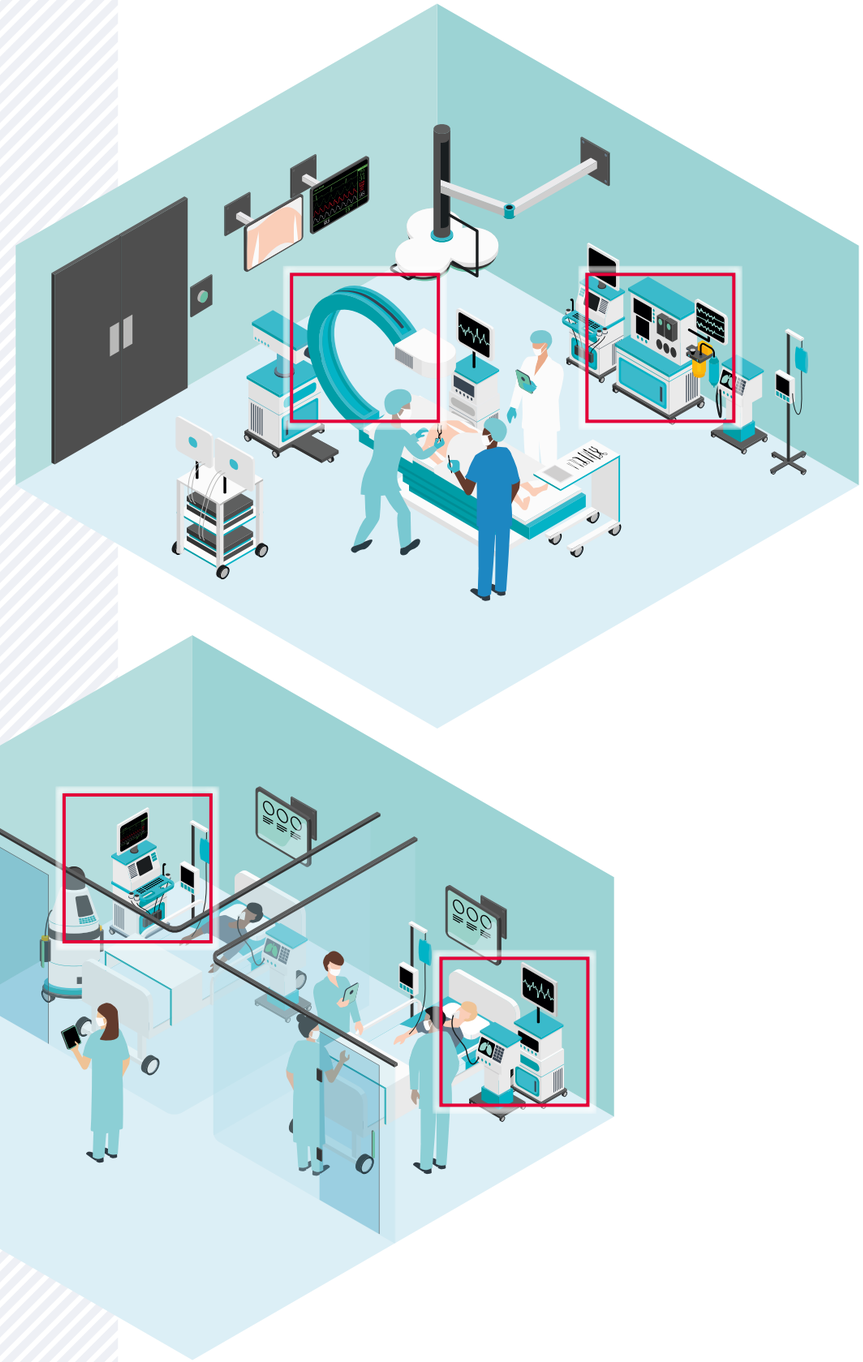
In addition to rule-compliant networking of medical devices, **secunet medical connect Carna** enables secure execution of applications that affect medical work processes. This enables medically relevant data to be securely processed by the connected medical device and made available to other services in the digital infrastructure. **Carna** can be operated directly near the patient and in direct interaction with medical equipment.

Medical grade. Gateway for medical devices and medical processes
Carrying out medical applications near the patient

Rule-compliant (MDR, FDA) medical device networking
Compliance with the IT security requirements of the system

Flexible connection of medical devices to the infrastructure
Support for wired and wireless transmission technologies

Connection of medical devices to modern infrastructures
Support for old interface standards (e.g. RS-232) for networking legacy systems with modern IT infrastructures



- Protective layer on the medical device, even for mobile devices
- Diverse safeguards for medical equipment
- Bidirectional communication with cloud infrastructures
- Edge computing for data processing on the medical device

Data integration at the edge of the network

When implemented as the central authority of trust in the operator network, **secunet medical connect** Athene coordinates the communication flows of entire network segments “at the edge”. As a transition point to the internal infrastructure and to the cloud, the Security Gateway provides a secure execution environment at a central location.

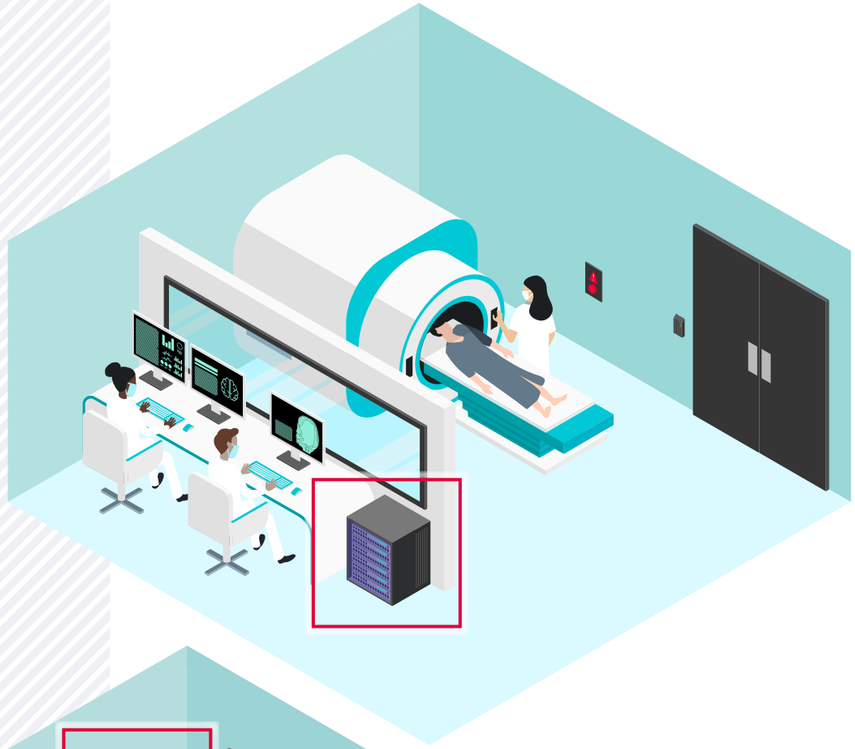
Different versions precisely serve different performance requirements of diverse use cases with individual demands on the hardware (e.g. AI applications).

Central authority for heterogeneous data sources
Consolidation of data originating from various sources at a central location and transfer to other services

Execution of AI applications
High performance for resource-intensive and compute-intensive processes

Trustworthy transition from the medical to classic IT network
Isolation of medical devices from the other IT infrastructure and secure locking of data

Rule-compliant medical device networking
Compliance with the IT security requirements of the system (from MDR, FDA, B3S KRITIS, ISO 80001)



Combined medical equipment clusters

Secure access point for external services & cloud applications

Data consolidation and data integration platform

AI-based medical applications “at the edge”

secunet medical connect product family

Juno

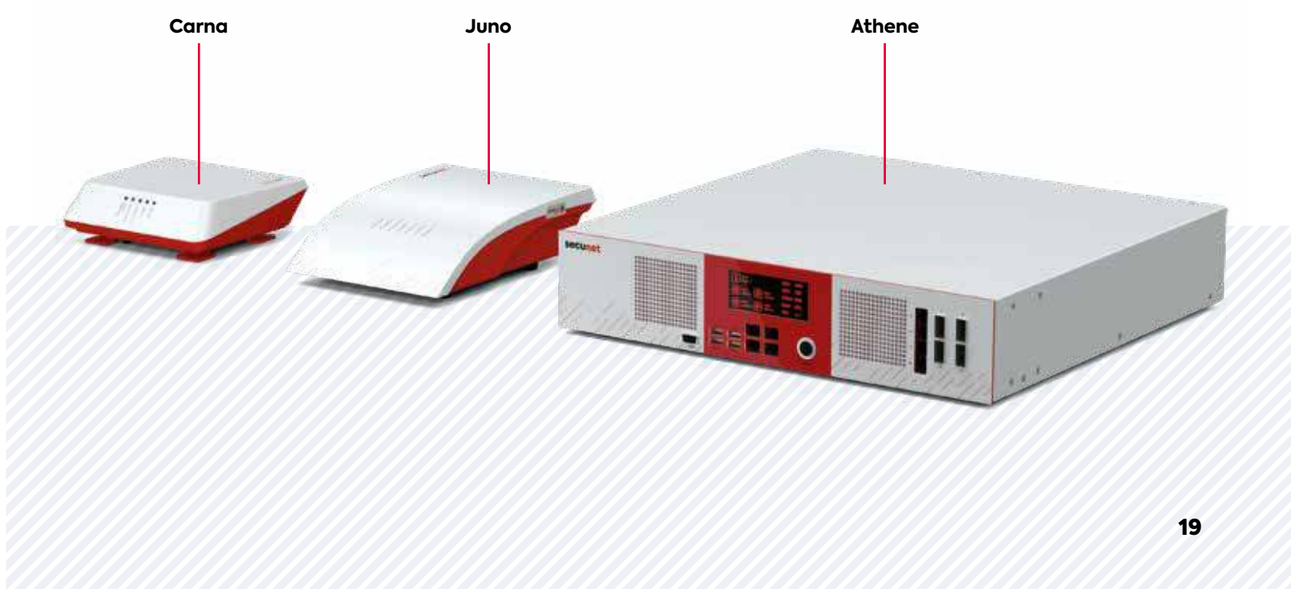
Areas of application	Integration of medical devices into digital management and maintenance processes
Classification	IT equipment
Operating environment	In the vicinity of the medical device (> 1.5 m from the patient)
Performance features	■ Quad Core CPU (Speed 1.1 GHz, Burst 2.5 GHz, TDP6W) ■ 8 GB LPDDR3 RAM (1866 MT/s) ■ 16 GB M.2 PCIe mass storage ■ Interfaces (1× USB 2.0, 2× 1 Gbit-Ethernet) ■ Temperature range +5 °C – +40 °C
Dimensions	approx. 70 mm × 180 mm × 250 mm
Availability	Serial product

Carna

Areas of application	Integration of medical devices into medical, administrative and maintenance-relevant processes
Classification	Medical grade. The hardware–software appliance is suitable for certification as a medical device
Operating environment	Near the patient, on the medical device
Performance features	■ Atom® ×6425E Quad Core 2.0 GHz ■ 8 GB LPDDR4× RAM (3733 MT/s) ■ 64 GBeMMC5.1 flash mass storage device ■ Interfaces (1× USB 3.1 Type C, 2× USB 3.1 Type A, 2× 1 RJ45 Gbit-Ethernet) ■ Temperature range 0 °C – +60 °C
Dimensions	approx. 41 mm × 176 mm × 132 mm
Availability	Pre-series/final specification

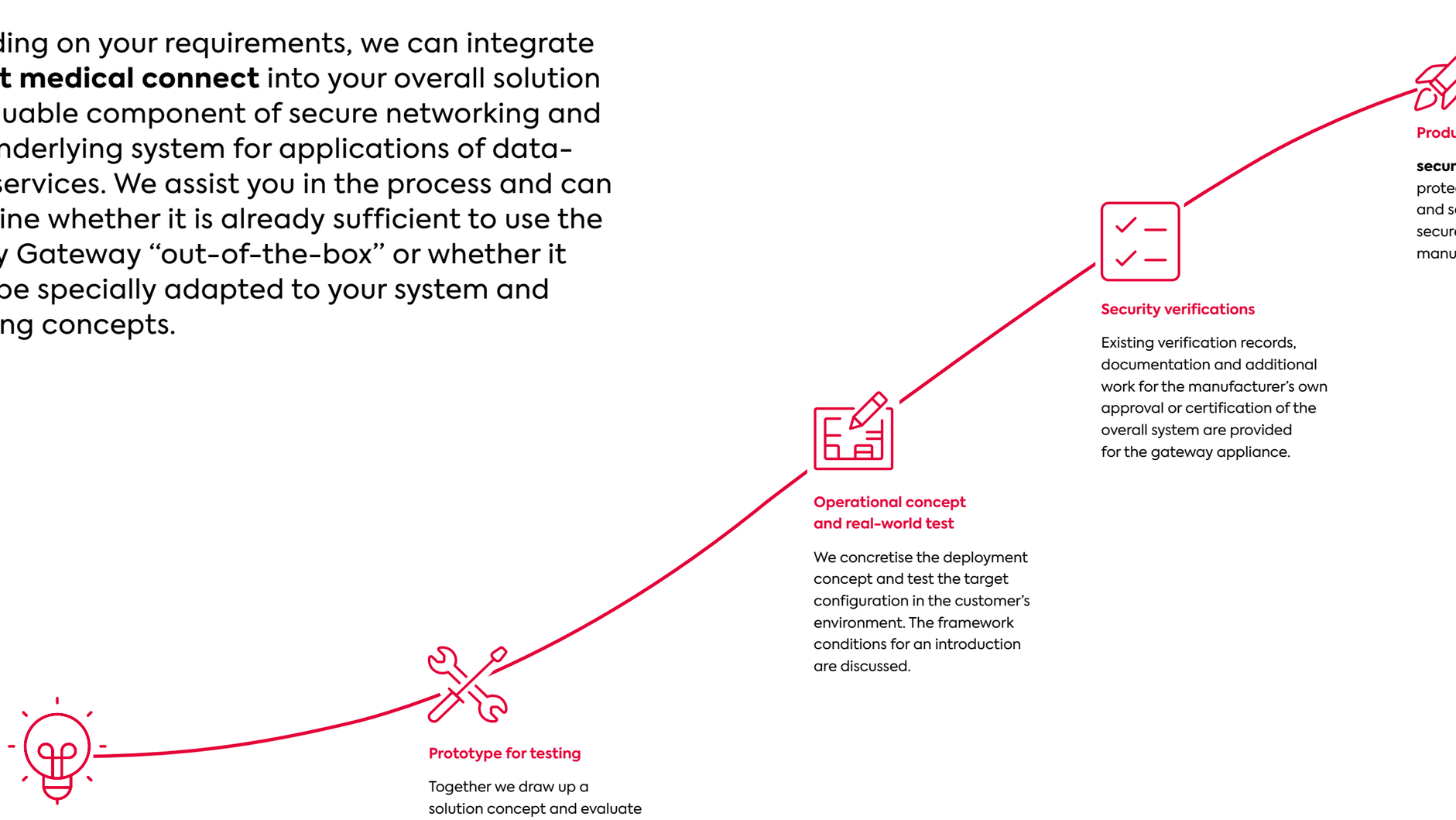
Athene

Areas of application	Central component for managing and securing devices and running applications
Classification	IT equipment
Operating environment	Central in the data-processing centre or in the department network
Characteristics for different performance requirements	**Connect variant** ■ Focus on the segmentation of networks ■ High data transmission rates **High Performance variant** ■ Implementation of computationally intensive tasks ■ Integration of graphics cards for high performance ■ AI applications
Dimensions	2 HE 19" Server approx. 89 mm × 483 mm
Availability	Pre-series/final specification



Our vision of the road to success

Depending on your requirements, we can integrate **secunet medical connect** into your overall solution as a valuable component of secure networking and as an underlying system for applications of data-driven services. We assist you in the process and can determine whether it is already sufficient to use the Security Gateway “out-of-the-box” or whether it should be specially adapted to your system and operating concepts.



Use case and advantages in use

Develop your specific use cases together with our hardware and software experts. Together we define the requirements for the technology derived from regulations.

Prototype for testing

Together we draw up a solution concept and evaluate technical feasibility and security requirements.

Operational concept and real-world test

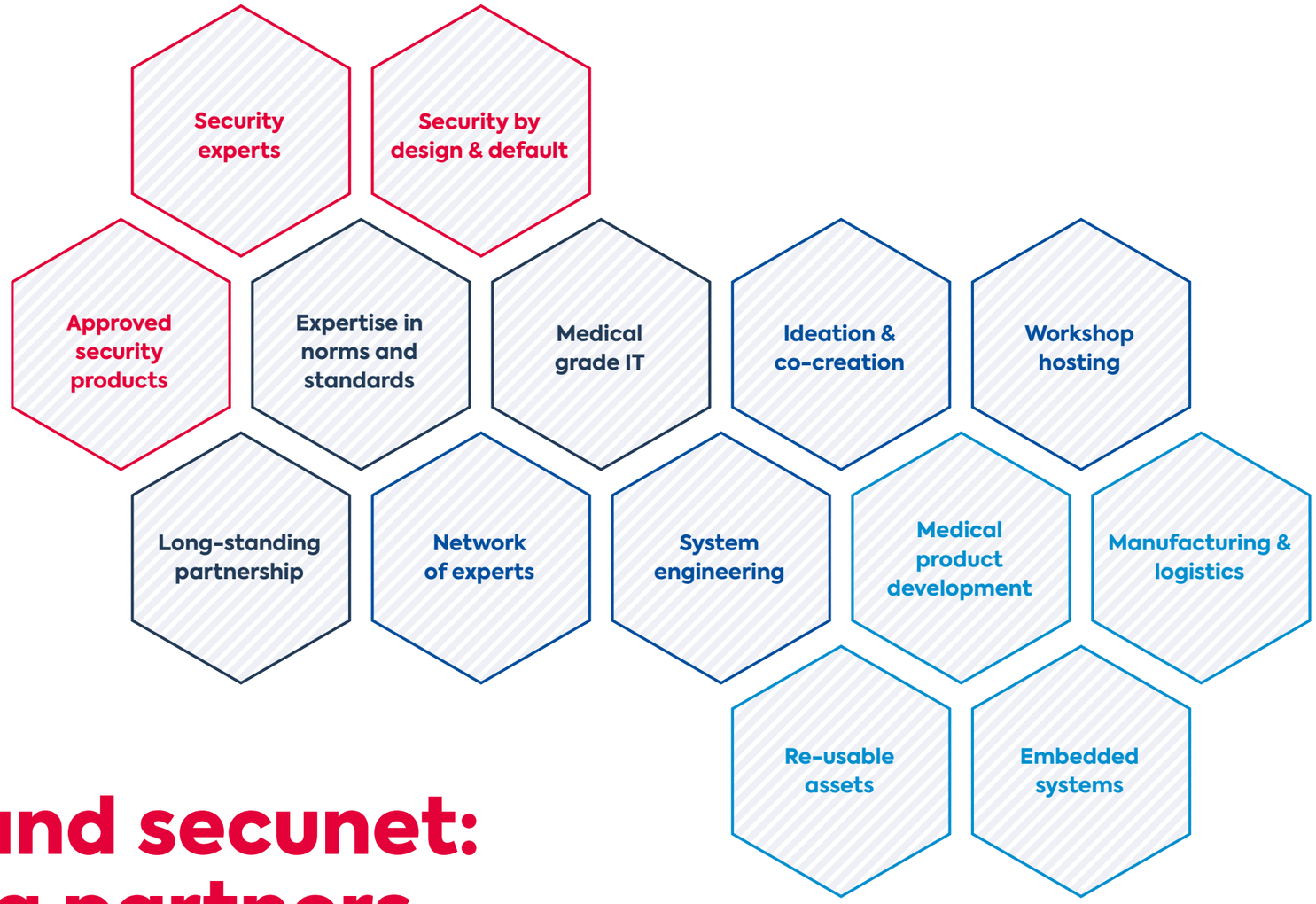
We concretise the deployment concept and test the target configuration in the customer’s environment. The framework conditions for an introduction are discussed.

Security verifications

Existing verification records, documentation and additional work for the manufacturer’s own approval or certification of the overall system are provided for the gateway appliance.

Productive implementation

secunet medical connect protects the medical equipment and serves as a platform for secure integration into the manufacturer’s digital services.



S.I.E and secunet: strong partners by your side

Sustainably successful innovations and products can only be achieved if they are useful and user-oriented. The **secunet medical connect** security platform requires expert knowledge from the hardware to the application level. For this purpose, national and international norms and standards must be catered for so that the customer can use a flexibly integrable gateway for his medical equipment and data-driven services.

We are strong partners with decades of experience, providing product services from our respective specialist domains to ensure your success.

secunet ist Sicherheitspartner der Bundesrepublik Deutschland

eurobits

Allianz für Cyber-Sicherheit

ECS

bitkom

TeleTrusT
Pioneers in IT security.

ECO SYSTEM
ENTSCHEIDERFABRIK

medical cluster

MTC
MEDICAL TECHNOLOGY CLUSTER

Forum MedTech Pharma

secunet

secunet is Germany's leading cyber-security enterprise. In an increasingly networked world, secunet provides a combination of products and consulting services for resilient digital infrastructure and maximum protection for data, applications and digital identities. secunet specialises in fields where special security requirements prevail – among them cloud applications, IIoT, eGovernment and eHealth. With secunet's security solutions, businesses can comply with the strictest security standards in their digitalisation projects, enabling them to make progress in their digital transformation.

Over 700 experts help boost the digital integrity of governments, businesses and society. Its customers include German government ministries, more than 20 DAX-listed corporations as well as other national and international organisations. The company was founded in 1997. It is listed in the Prime Standard segment of the Frankfurt Stock Exchange and achieved a turnover of around 286 million euros in 2020.

secunet is an IT security partner of the Federal Republic of Germany and a partner of the Alliance for Cyber Security. The secunet Division eHealth provides security for digital processes in healthcare and helps optimise the security and comfort of information technologies. In doing so, secunet also provides support for medical and organisational activities in healthcare while observing and meeting statutory requirements at all times.

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

System Industrie Electronic GmbH

The S.I.E (System Industrie Electronic GmbH) is one of the market-leading development and manufacturing specialists for embedded systems and cyber-physical systems in challenging regulatory environments (medical, industrial, cyber security).

As a full-service provider, the company assists its customers throughout the entire product life cycle, starting with creative ideation and consulting processes, through development and production, to quality and life-cycle services. The focus and common ambition of S.I.E., its customers and the entire partner network is to always provide sustainable and real added value to people, notwithstanding all the digital DNA.

Especially with medical equipment, which has to meet strict requirements on safety, security and the handling of sensitive data, the success of digitalisation depends on coordination between specialists in a wide variety of fields.

From user-oriented user experience topics, hardware and software development of corresponding embedded systems and industrial design, to data management and security: S.I.E. organises and implements services related to product creation, development and manufacturing for its partners.

S.I.E
System Industrie Electronic GmbH
Millennium Park 12
AT-6890 Lustenau
T +43 5577 89900
info@sie.at
sie.at