secunet medical connect

Vertrauensvoll und sicher vernetzte Medizingeräte

sie.at

secunet.com

Vernetzte Medizingeräte? – Basis für moderne Medizin!

Vernetzte Medizintechnik offeriert neue Möglichkeiten und Chancen, birgt aber auch Risiken und Herausforderungen.

Systeme, die bei Behandlungen unterstützen, KI-basierte Analysen zur frühzeitigen Krankheitserkennung oder Operationen mit weltweit verteilten Akteuren sind Zielbilder in der modernen Medizin. Auf Basis der digitalen Transformation ermöglichen sie hochmoderne Behandlungs-, Diagnose- und Versorgungsmethoden.

Klar ist: Für solche Digitalisierungskonzepte sind ein ungehinderter Informationsfluss und eine sichere und vertrauensvolle Kommunikation von Medizingeräten in digitalen Infrastrukturen grundlegend.

Herausforderungen bei der Vernetzung von Medizingeräten

Medizingeräte in einer vernetzten digitalen Welt zu betreiben, ist herausfordernd: datengetriebene Anwendungsfälle sind komplex, dazu müssen gesetzliche Vorgaben erfüllt und fortwährend auf Aspekte der IT-Sicherheit der kritischen Medizintechnik und sensiblen Daten eingegangen werden.

Mit jedem Vernetzungspunkt entstehen **neue Angriffsflächen** für Cyberangriffe auf Medizingeräte und Netzwerke. Die Gefahr von Systemausfällen steigt. Die Folgen können weitreichend sein.

Regularien verpflichten und verlangen den Aufbau sowie die Aufrechterhaltung eines bedarfsgerechten IT-Sicherheitsniveaus für Medizingeräte, Netzwerke und Anwendungen.

Aufwändige nachträgliche Zulassungsverfahren für Medizingeräte hemmen Innovationen und verhindern Anpassungen für deren Integration in digitale Versorgungs- und Verwaltungsprozesse.

Lange Lebenszyklen von Medizingeräten verursachen eine Lücke zwischen verbauter Informationstechnik und dem aktuellen Stand der Technik, sodass die Systeme über Zeit mehr und mehr Schwachstellen aufweisen und Risiken im Betrieb entstehen.

Medizingeräte werden in **heterogenen Umgebungen** eingesetzt und verfügen zum Teil über veraltete Schnittstellen, die eine einheitliche Vernetzung erschweren und nicht das nötige Maß an Sicherheit bieten.

Medizingeräte werden zunehmend Ziel von Angreifern. Aktuellen Studien zufolge

- weisen medizintechnische Geräte durchschnittlich **6,2 Schwachstellen** auf.
- ist Medizintechnik immer stärker durch **Cyberangriffe** bedroht.
- sind 60 % der medizintechnischen Geräte im Feld **End of Life** und werden nicht mehr gewartet.

Frost & Sullivan, Medical Device and Network Security – Coming to terms with the Internet of Medical Things (IoMT), 2019

HHS Cyber Security Programm, 2021 Forecast: The Next Year of Healthcare Cybersecurity, 2020

Anwendungsorientierte Konzepte in vier Domänen

Um Medizingeräte bedarfsgerecht zu vernetzen und in Digitalisierungsvorhaben zu integrieren, sind Anforderungen und Maßnahmen in vier verschiedenen Domänen zu berücksichtigen. Daraus resultiert, dass Kompetenzen aus unterschiedlichen Fachdisziplinen vereint werden müssen.

Compute

Verarbeitung und Transfer von Daten in medizinischen Wirkungskreisen

- Sichere Ausführung von Anwendungen am Ort der Entstehung (nah am Medizingerät)
- Geschützter Austausch mit internen und externen digitalen Diensten

Protect

IT-Sicherheit auf allen Ebenen: von der Hardware bis zur Anwendung

- Bedarfsgerechter Schutz des Medizingeräts sowie der Anwendungen und Daten
- Stete Aufrechterhaltung des IT-Sicherheitsniveaus nach aktuellem Stand der Technik

Connect

Anbindung von Systemen an die IT-Infrastruktur

- Flexible Anpassung an heterogene Architekturen von Betreiber-Infrastrukturen
- Berücksichtigung alter Schnittstellenstandards (Retrofitting von Altsystemen im Feld)
- Einbezug moderner Übertragungstechnologien und Konzepte der Informationstechnik

Compliant

Konformität zu verschiedenen Regularien und Anforderungen

- Erfüllung von regulatorischen Anforderungen (MDR, IVDR, FDA)
- Berücksichtigung der Betreiber-Anforderungen (KRITIS B3S, ISO 80001)

Sollten die Domänen direkt in der Medizintechnik umgesetzt werden?

Sie können die Medizingeräte um entsprechende Software- und Hardwarekomponenten erweitern, um die Anforderungen an die einzelnen Domänen zu bedienen. Dies führt jedoch zu einer engen Koppelung von individuellen Lösungen mit dem jeweiligen Medizingerät, was unweigerlich die Entwicklungszeiten und -kosten der Geräte in die Höhe treibt und zur Entstehung von monolithischen und schlecht handhabbaren Gesamtsystemen führen wird. Um einem solchen Dilemma vorzubeugen, bietet sich ein modulares Gesamtsystem an, in dem der eigentlichen medizinischen Anlage je nach Bedarf verschiedene Konnektivitäts- und Sicherheitskomponenten vorgeschaltet sind.

Für diesen ganzheitlichen Lösungsansatz, der die Anforderungen einzelner Domänen abdeckt, braucht es allerdings mehr als die Kaskadierung spezialisierter Komponenten am Medizingerät. Diese sind häufig stark in einer Domäne. Sie in der Gesamtlösung zu vereinen, ist jedoch komplex und kostenintensiv; die Organisation der verschiedenen Hersteller, Lebenszyklen und Funktionsweisen sowie Integrations- und Betriebsbedingungen der Produkte ist kaum umsetzbar.

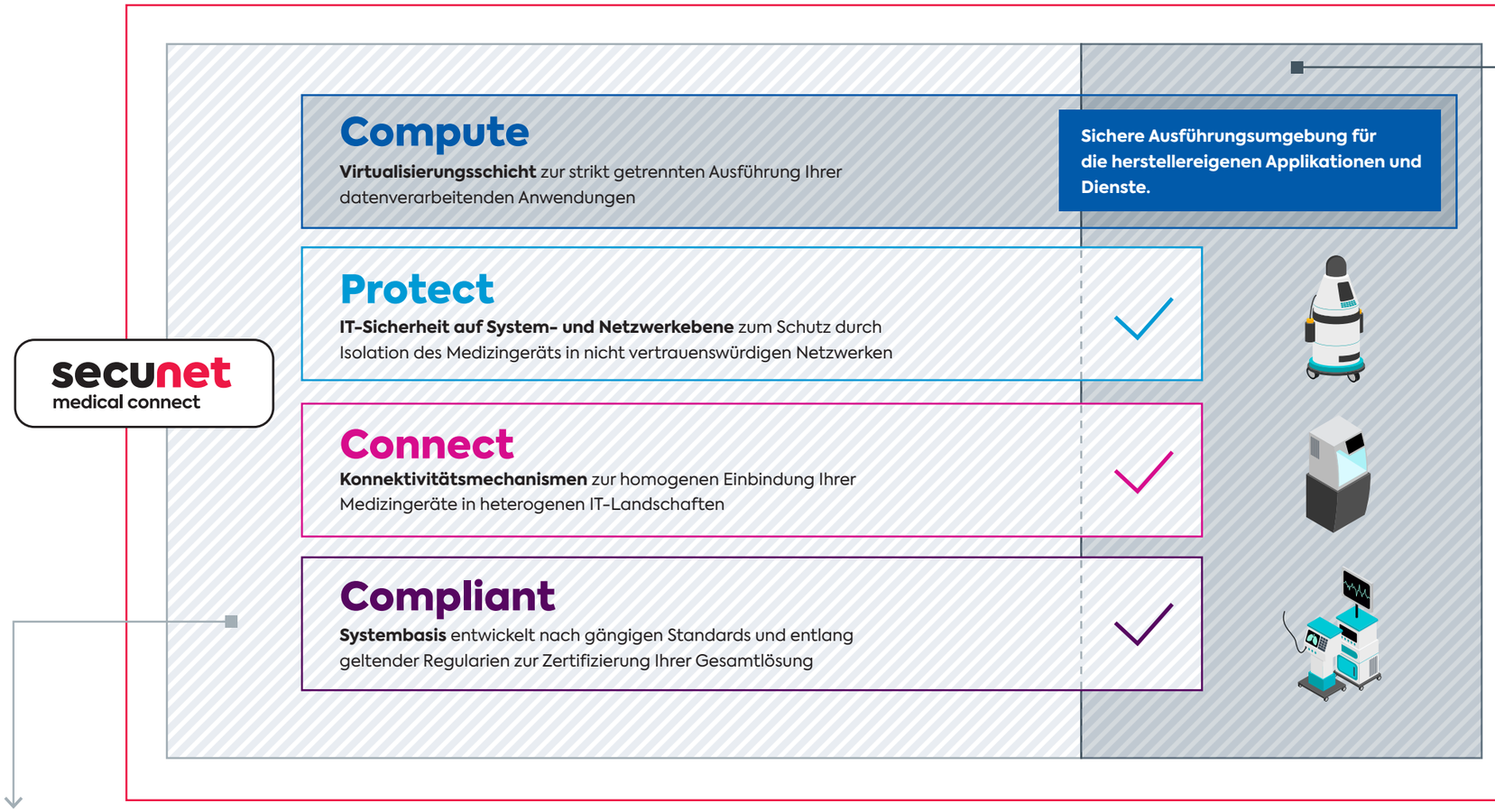
	Compute Integration in digitale Dienste	**Protect** IT-Sicherheit der Medizintechnik	**Connect** Schnittstellen zu Infrastrukturen	**Compliant** Konform zu Regularien
IT-Sicherheitslösungen	✗	✓	✗	✗
Konnektivitätslösungen	✗	✗	✓	✗
Industrie-PCs	✓	✗	✓	✗
secunet medical connect	✓	✓	✓	✓

Das Security Gateway **secunet medical connect** berücksichtigt Anforderungen aller Domänen und konsolidiert relevante Vorgaben und Konzepte aus den Bereichen der Medizintechnik, Informationstechnologie und IT-Sicherheit.

Lösungskonzept zur Vernetzung von Medizintechnik

Die Bündelung relevanter Technologien unterschiedlicher Fachdisziplinen auf einem Security Gateway ermöglicht die sichere und flexible Anbindung von Medizintechnik an die schnelllebige IT-Welt. Durch die Integration von **secunet medical connect** in Ihr Konzept können Sie sich voll und ganz auf die Entwicklung Ihrer Medizintechnik und Dienste konzentrieren. Wir kümmern uns um die Systembasis und Eigenschaften der einzelnen Domänen für eine sichere Vernetzung der Medizintechnik.

secunet medical connect stellt die stets gleiche sichere Ausgangsbasis für verschiedene Digitalisierungskonzepte. Je nach Anwendungsfall werden benötigte Module und Funktionen verwendet.



Hersteller

Ihr Nutzen einer flexiblen Sicherheitsplattform

- Konzentration auf Ihre Medizingeräte und fachlichen Anwendungen
- Umsetzung Ihrer digitalen Prozesse durch Integration Ihres Medizingeräts
- Sichere bidirektionale Kommunikation Ihres Medizingerätes mit digitalen Diensten
- Steter Schutz Ihres Medizingerätes durch agile Update-Zyklen
- Unterstützung bei der Erfüllung gesetzlicher Vorschriften
- Harmonisierung von Digitalisierungskonzepten Ihrer unterschiedlichen Medizingeräte auf einer Systembasis
- Flexible Vernetzung Ihrer bestehenden und zukünftigen Medizingeräte
- Reduktion Ihrer Aufwände und Kosten bei Konzept und Betrieb durch eine einheitliche Systembasis
- Investitionsschutz durch sukzessive Umsetzung Ihrer Anwendungsfälle

secunet & S.I.E

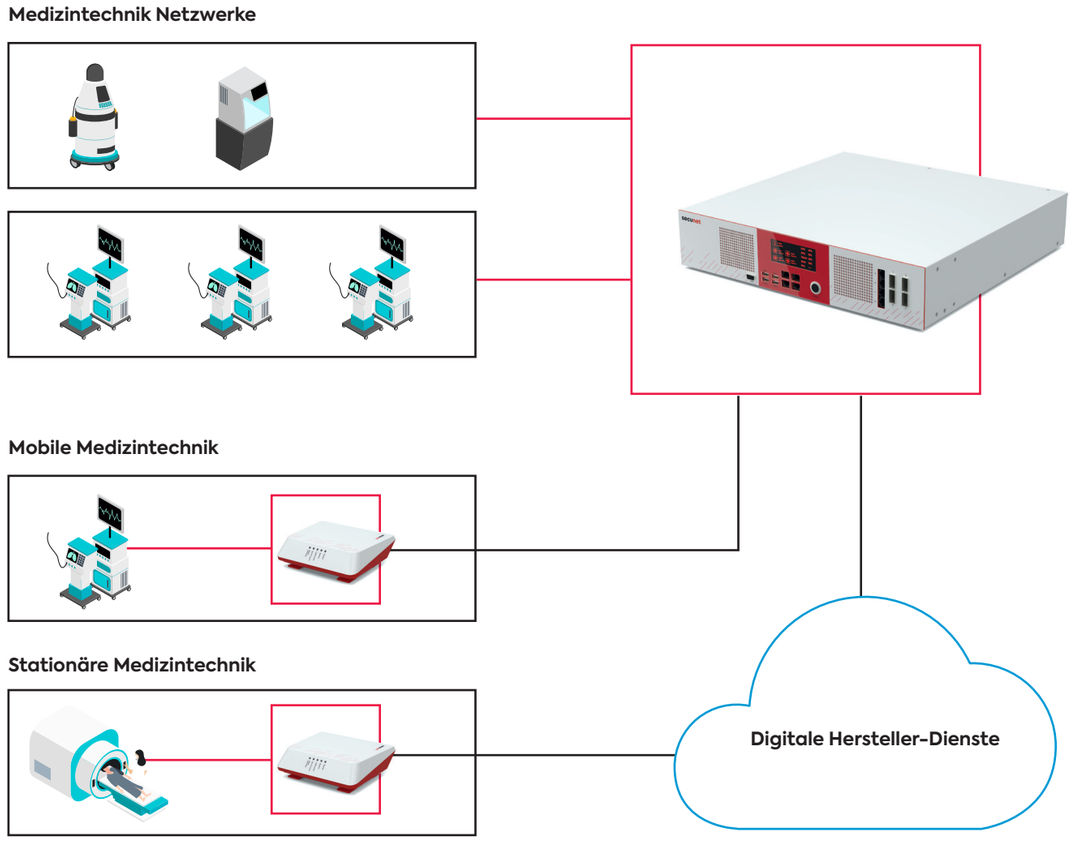
Unsere Organisationsstärke und Expertise

- HW- & SW-Entwicklung
- IT-Sicherheitslösungen
- Zertifizierungen & Zulassungen
- Konzept und Prototyp
- Lifecycle-Management
- Supply Chain Management

Ganzheitliche Lösungskonzepte durch starke Partnerschaften
Die Umsetzung von Digitalisierungsvorhaben durch vernetzte Medizingeräte erfordert eine Bündelung von Expertenwissen auf den vier Ebenen Connect, Protect, Compute und Compliant. Nur so können Sie sowohl Insellösungen als auch erheblichen Mehraufwand vermeiden. Der Ansatz: ein enger Schulterschluss von Sicherheit und Medizintechnik.

Die Zukunft für vertrauenswürdige Digitalisierungs-vorhaben

Die **secunet medical connect** Produktfamilie basiert auf einer sicheren Gateway-Technologie, die moderne Lösungskonzepte der IT-Sicherheit und Informationstechnik in einer Plattform bündelt.



secunet medical connect

Compute

Ausführungsumgebung

secunet Security Apps | App | App

- Gehärtete Docker-Umgebung
- Isolierte Ausführung eigener Anwendungen
- Verfügbare secunet Security Anwendungen

Protect

Sichere Systembasis

Secure App Environment

secunet monitor | MS Azure IOT Hub | ... | ...

Platform OS & Security | Rest API

- Gehärtetes Betriebssystem
- Selbstschutz des Geräts
- Firewall-Funktionalität
- Security Monitoring des Netzwerkverkehrs
- Protokollierung lokaler Ereignisse
- Flexible Management-Schnittstellen
- Integrierte MS Azure IoT Edge Runtime

Connect

Hardware-Abstraction-Layer (HAL)

Hardware | Trust Anker

- Verschiedene Leistungsklassen und Formfaktoren
- Flexible Schnittstellen
- Hardwarebasierter Vertrauensanker

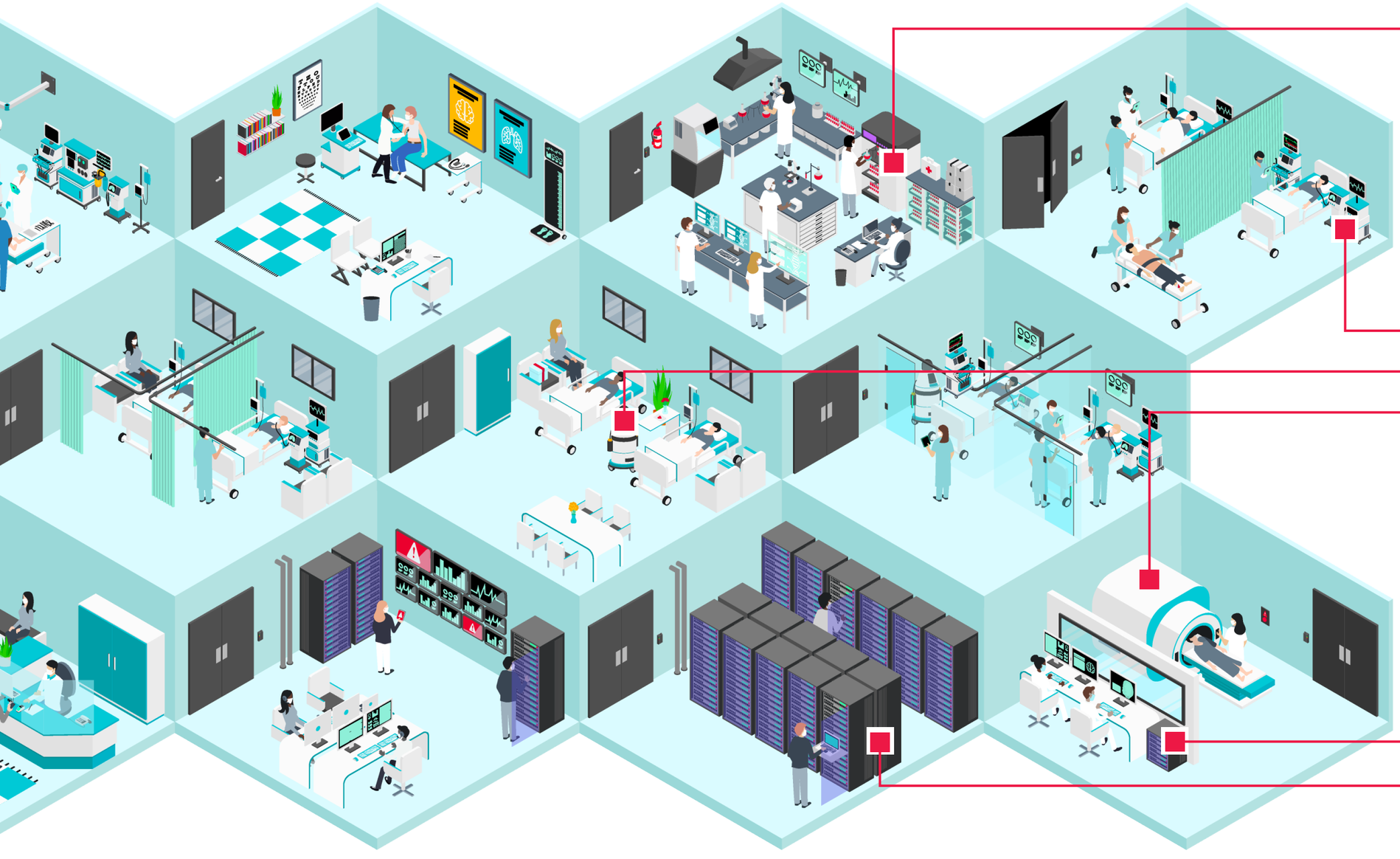
Compliant

Als individuell einsetzbare Gateway-Technologie bedient unser Lösungsansatz **secunet medical connect** in verschiedenen Hardware-Ausprägungen unterschiedliche Einsatzszenarien und Leistungsanforderungen.

Eine Plattform, verschiedene Anwendungen, individuelle Wirkungskreise

secunet medical connect kann – angepasst an die Einsatzszenarien innerhalb der IT-Infrastruktur des Betreibers – in verschiedenen Ausprägungen als Security Gateway wirken. Auch lassen sich die einzelnen Varianten eigenständig oder in Kombination betreiben. Beispielsweise können Daten direkt am Medizingerät erhoben (**Juno** oder **Carna**), aufbereitet und anschließend datengetriebenen und rechenintensiveren Diensten auf der zentralen Instanz (**Athene**) zur Verfügung gestellt werden.

Die verschiedenen Ausprägungen der **secunet medical connect** Plattform basieren auf ein und derselben gehärteten Systembasis. Zahlreiche integrierte IT-Sicherheitsmechanismen ermöglichen die konforme Vernetzung von Medizingeräten nach gängigen Regularien und Best Practices.



secunet medical connect Juno
Gatekeeper für die regelkonforme Vernetzung von Medizingeräten

secunet medical connect Carna
Medizinische Anwendungen an Medizingeräten in Patientennähe

secunet medical connect Athene
Datenintegration und -verarbeitung für heterogene Datenquellen an zentraler Stelle

Schutz der Medizin-geräte und sichere Anbindung an Remote-Dienste

Mit **secunet medical connect Juno** schützen Sie Ihre Medizingeräte regelkonform im Sinne des Betreibers und bieten gleichzeitig Ihre verwaltungs- und wartungsrelevanten Anwendungen über die gehärtete Ausführungsumgebung an (z. B. zur Fernwartung). Als Hersteller profitieren Sie von den integrierten IT-Sicherheitsmechanismen der Plattform: Platziert zwischen dem medizintechnischen Gerät und dem weiteren Netzwerk, isoliert **Juno** als Security Gateway die Medizingeräte von der restlichen IT-Infrastruktur und schützt so vor unautorisiertem Zugriff.

Medizingeräte sicher vernetzen
Restriktion und Überwachung der Kommunikationsflüsse in das angeschlossene Betreibernetzwerk

Medizingeräte sicher in digitale Dienste integrieren
Eigene Anwendungen für die Fernwartung sicher und flexibel einbinden

Medizingeräte regelkonform vernetzen
Anforderungen an die IT-Sicherheit (aus MDR, FDA, B3S KRITIS, ISO 80001) im Betrieb umsetzen

Korrektive Sicherheitsmaßnahmen für einen regelkonformen Betrieb

Sicherer Fernzugriff, Asset Management und Update-Prozesse

Retrofit von Medizingeräten mit geringem IT-Sicherheitsniveau

Data-Intermediär zwischen unterschiedlichen Sicherheitszonen

Symbiose mit der Medizintechnik

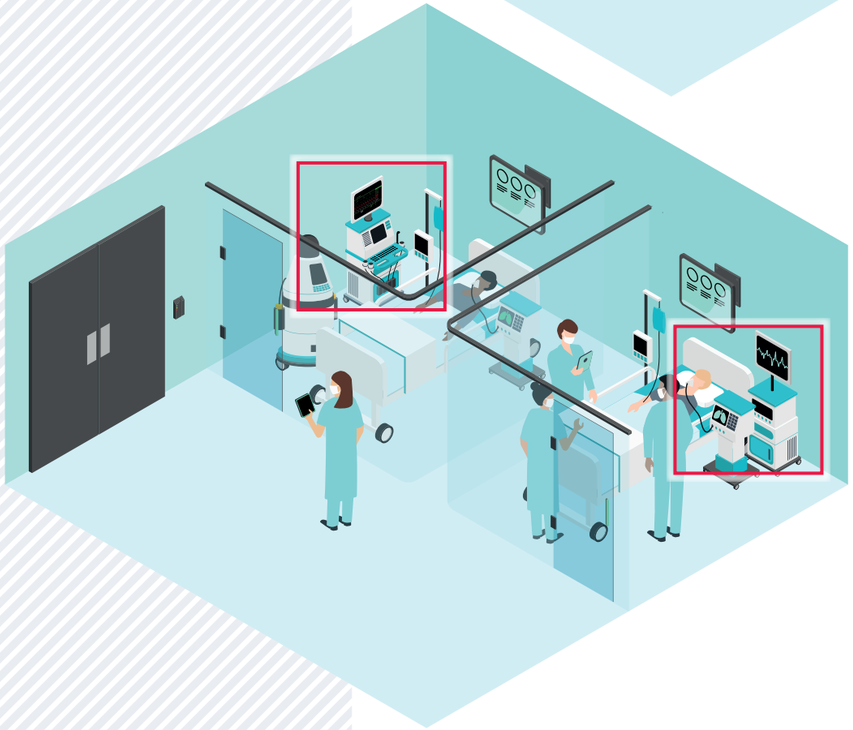
Neben der regelkonformen Vernetzung von Medizingeräten ermöglicht **secunet medical connect Carna** die sichere Ausführung von Anwendungen, die in medizinische Arbeitsprozesse eingreifen. So können medizinisch relevante Daten vom angeschlossenen Medizingerät sicher verarbeitet und anderen Diensten in der digitalen Infrastruktur zugänglich gemacht werden. **Carna** kann direkt in Patientennähe und im unmittelbaren Zusammenspiel mit der Medizintechnik betrieben werden.

Medical Grade. Gateway für Medizinprodukte und medizinische Prozesse
Ausführung von medizinischen Anwendungen in Patientennähe

Medizingeräte regelkonform (MDR, FDA) vernetzen
Erfüllung der Anforderungen an die IT-Sicherheit des Systems

Medizingeräte flexibel mit der Infrastruktur verbinden
Unterstützung kabelgebundener und kabelloser Übertragungstechnologien

Medizingeräte an moderne Infrastrukturen anbinden
Unterstützung alter Schnittstellenstandards (z. B. RS-232) zur Vernetzung von Altsystemen mit modernen IT-Infrastrukturen



Schutzschicht am Medizingerät, auch für mobile Geräte

Vielfältige Schutzmaßnahmen für die Medizintechnik

Bidirektionale Kommunikation mit Cloud-Infrastrukturen

Edge Computing für Datenverarbeitung am Medizingerät

Datenintegration am Rande des Netzwerks

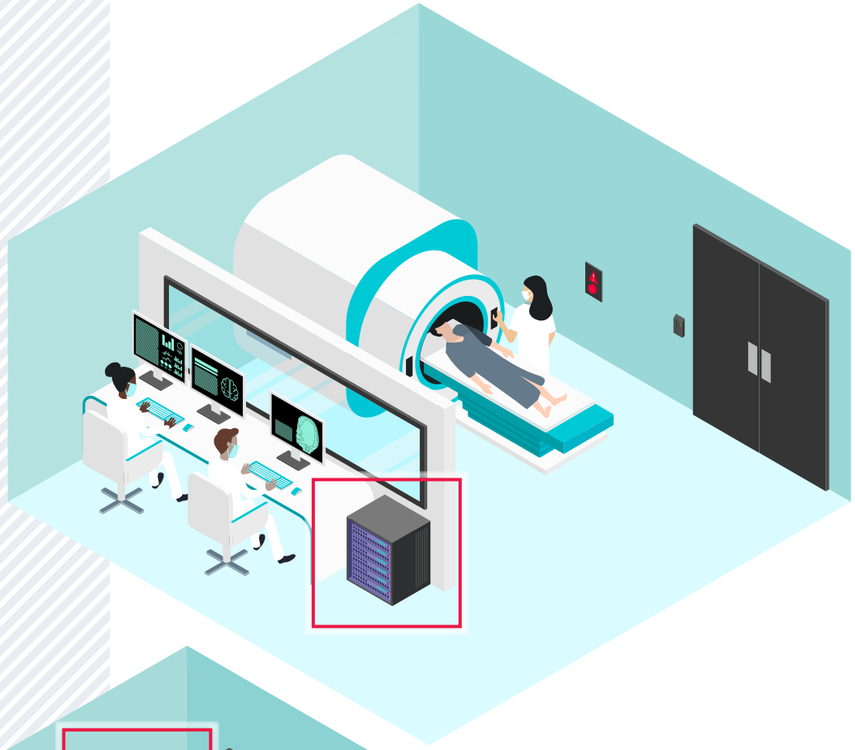
Als zentrale Vertrauensinstanz im Betreiber-Netzwerk konzertiert **secunet medical connect Athene** die Kommunikationsflüsse ganzer Netzwerksegmente „at the edge“. Als Übergangspunkt zur internen Infrastruktur sowie zur Cloud bietet das Security Gateway eine sichere Ausführungsumgebung an zentraler Stelle. Verschiedene Ausprägungen bedienen passgenau unterschiedliche Leistungsanforderungen diverser Anwendungsfälle mit individuellen Ansprüchen an die Hardware (z.B. KI-Anwendungen).

Zentrale Instanz für heterogene Datenquellen
Konsolidierung von Daten aus verschiedenen Quellen an zentraler Stelle und Transfer an weitere Dienste

Ausführung von KI-Anwendungen
Hohe Performanz für ressourcen- und rechenintensive Prozesse

Vertrauenswürdiger Übergang vom medizinischen ins klassische IT-Netz
Isolation medizinischer Geräte von der restlichen IT-Infrastruktur und sicheres Schleusen von Daten

Medizingeräte regelkonform vernetzen
Erfüllung der Anforderungen an die IT-Sicherheit (aus MDR, FDA, B3S KRITIS, ISO 80001)



Bündelung von Medizintechnik-Clustern

Sicherer Zugangspunkt für externe Dienste & Cloud-Anwendungen

Datenkonsolidierung und -integrationsplattform

KI-basierte medizinische Anwendungen „at the edge“

secunet medical connect Produktfamilie

Juno

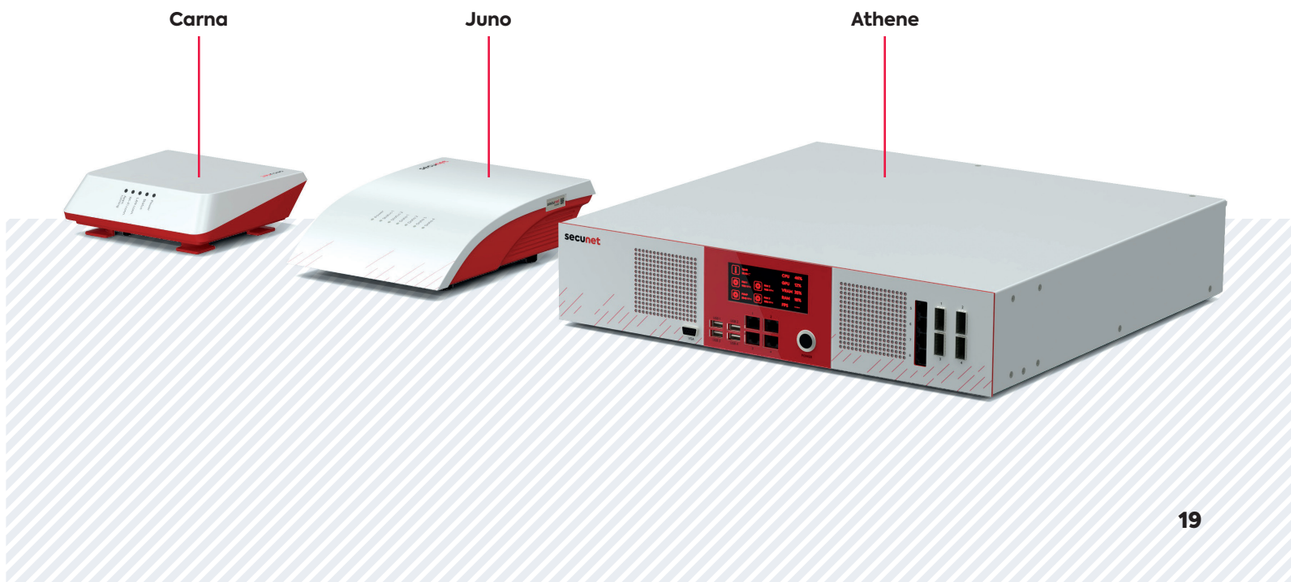
Anwendungsbereiche	Integration von Medizingeräten in digitale Verwaltungs- und Wartungsprozesse
Klassifizierung	IT-Equipment
Betriebsumgebung	Im Umfeld des Medizingeräts (> 1,5m vom Patienten)
Leistungsmerkmale	■ 4 Core CPU (Speed 1.1 GHz, Burst 2.5 GHz, TDP 6 W) ■ 8 GB LPDDR3 RAM (1866 MT/s) ■ 16 GB M.2 PCIe Massenspeicher ■ Interfaces (1× USB 2.0, 2× 1 Gbit-Ethernet) ■ Temperaturbereich +5 °C – +40 °C
Abmessung	ca. 70 mm × 180 mm × 250 mm
Verfügbarkeit	Serienprodukt

Carna

Anwendungsbereiche	Integration von Medizingeräten in medizinische sowie verwaltungs- und wartungsrelevante Prozesse
Klassifizierung	Medical Grade. Die Hardware-Software-Appliance ist geeignet für eine Zertifizierung als Medizinprodukt
Betriebsumgebung	In Patientennähe, am Medizingerät
Leistungsmerkmale	■ Atom® ×6425E Quad Core 2.0 GHz ■ 8 GB LPDDR4× RAM (3733 MT/s) ■ 64 GB eMMC 5.1 Flash Massenspeicher ■ Interfaces (1× USB 3.1 Type C, 2× USB 3.1 Type A, 2× 1 RJ45 Gbit-Ethernet) ■ Temperaturbereich 0 °C – +60 °C
Abmessung	ca. 41 mm × 176 mm × 132 mm
Verfügbarkeit	Vorserie / Finale Spezifikation

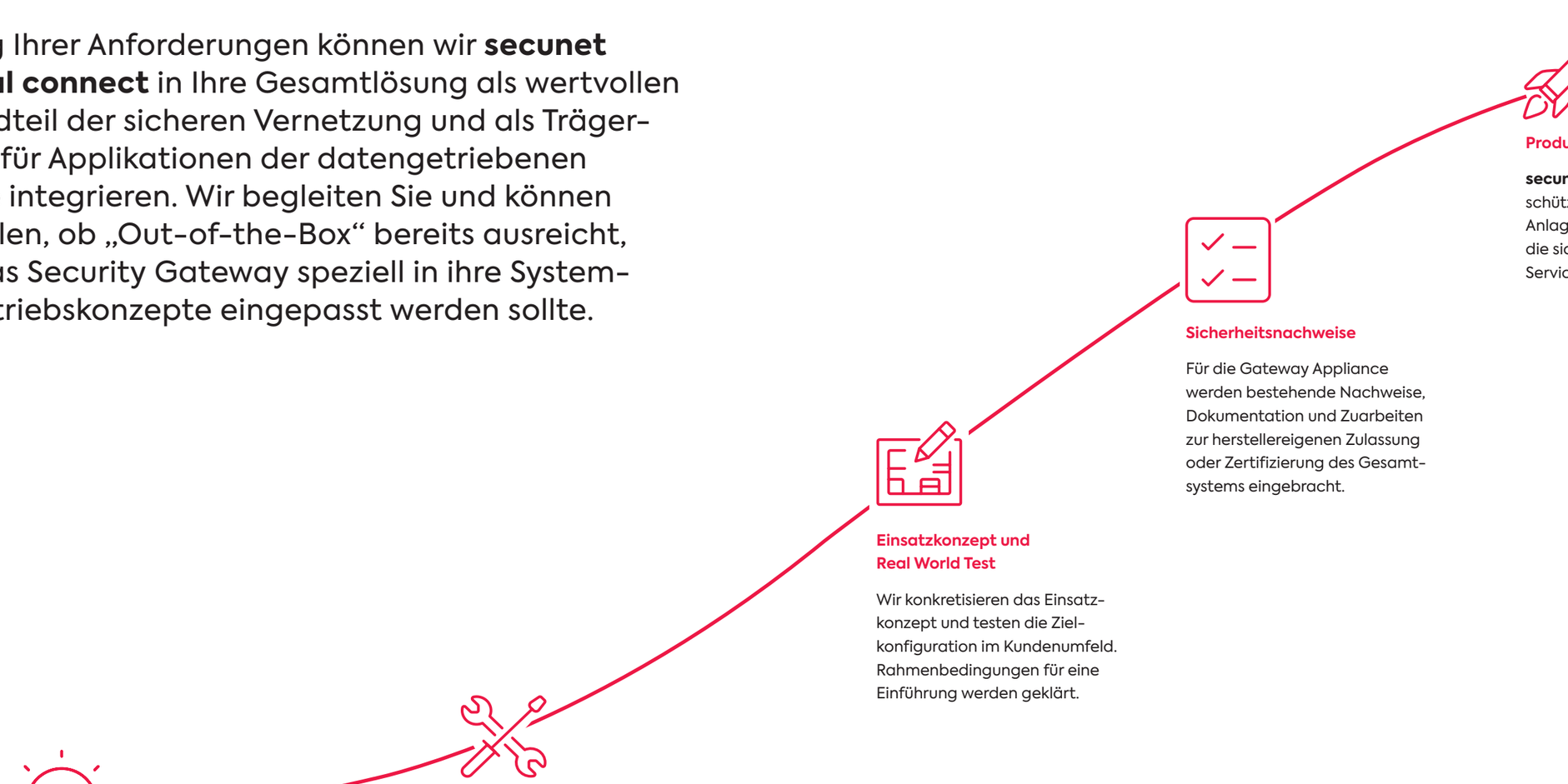
Athene

Anwendungsbereiche	Zentrale Komponente zum Verwalten und Absichern von Geräten und zur Ausführung von Anwendungen
Klassifizierung	IT-Equipment
Betriebsumgebung	Zentral im Rechenzentrum oder im Fachbereichsnetzwerk
Ausprägungen für unterschiedliche Leistungsanforderungen	**Variante Connect** ■ Fokus auf die Segmentierung von Netzen ■ Hohe Datenübertragungsraten **Variante High Performance** ■ Umsetzung von rechenintensiven Aufgaben ■ Integration von Grafikkarten für High Performance ■ KI-Anwendungen
Abmessung	2 HE 19“ Server ca. 89 mm × 483 mm
Verfügbarkeit	Vorserie / Finale Spezifikation



Unser Verständnis vom Erfolgsweg

Entlang Ihrer Anforderungen können wir **secunet medical connect** in Ihre Gesamtlösung als wertvollen Bestandteil der sicheren Vernetzung und als Trägersystem für Applikationen der datengetriebenen Dienste integrieren. Wir begleiten Sie und können feststellen, ob „Out-of-the-Box“ bereits ausreicht, oder das Security Gateway speziell in ihre System- und Betriebskonzepte eingepasst werden sollte.



Use Case und Vorteile im Einsatz

Entwickeln Sie gemeinsam mit unseren Hard- und Software-Experten Ihre spezifischen Anwendungsfälle. Gemeinsam definieren wir die aus Regularien resultierenden Anforderungen an die Technik.

Prototyp für Verprobung

Gemeinsam stellen wir ein Lösungskonzept auf und evaluieren technische Machbarkeit sowie Sicherheitsvorgaben.

Einsatzkonzept und Real World Test

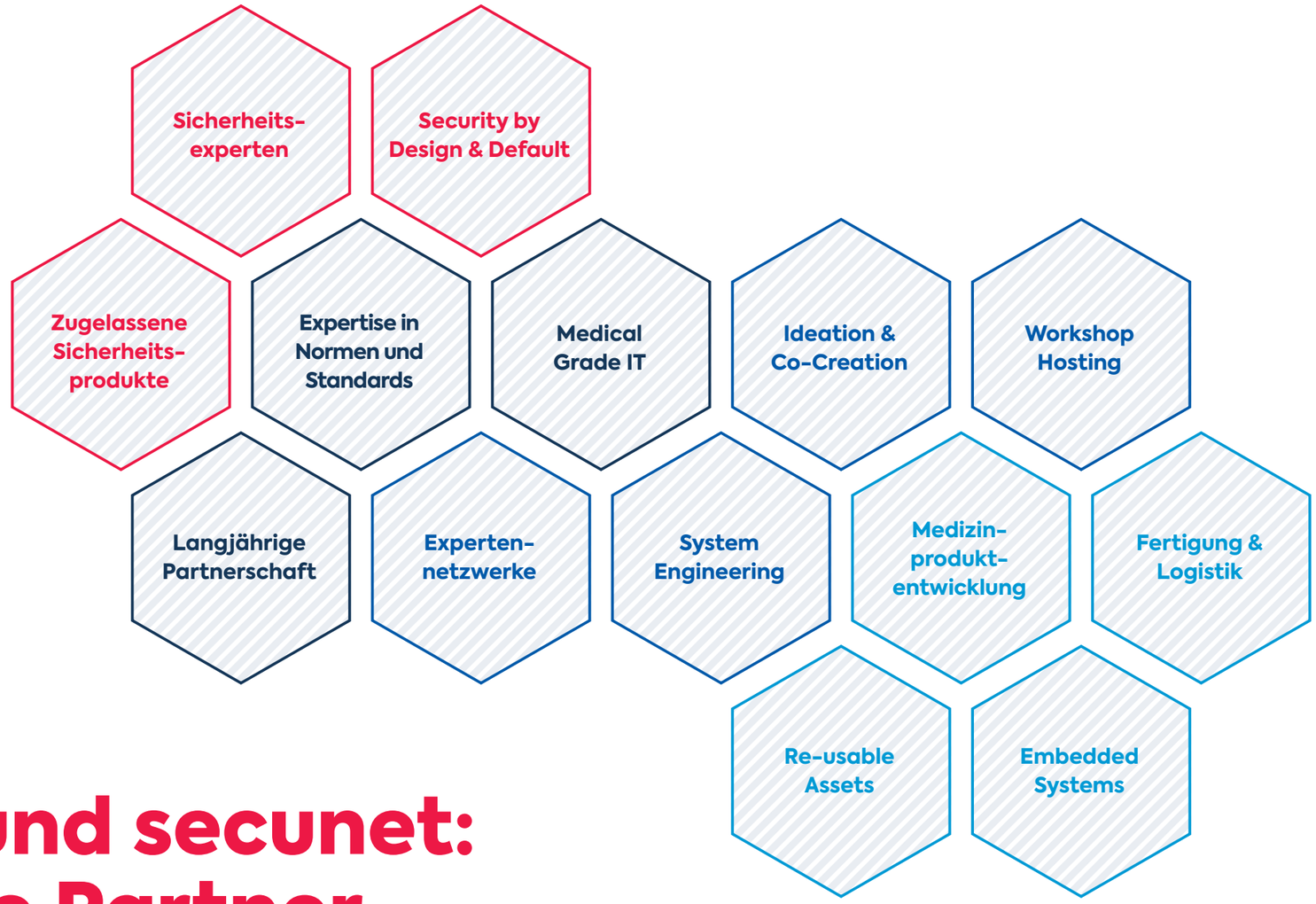
Wir konkretisieren das Einsatzkonzept und testen die Zielkonfiguration im Kundenumfeld. Rahmenbedingungen für eine Einführung werden geklärt.

Sicherheitsnachweise

Für die Gateway Appliance werden bestehende Nachweise, Dokumentation und Zuarbeiten zur herstellereigenen Zulassung oder Zertifizierung des Gesamtsystems eingebracht.

Produktiveinsatz

secunet medical connect schützt die medizintechnische Anlage und dient als Plattform für die sichere Einbindung in digitale Services des Herstellers.



S.I.E und secunet: starke Partner an Ihrer Seite

Nachhaltig erfolgreiche Innovationen und Produkte sind nur nutzen- und nutzerzentriert realisierbar. Die Sicherheitsplattform **secunet medical connect** erfordert dabei Expertenwissen vom Hardware- bis zum Applikations-Level. Dazu müssen nationale wie internationale Standards und Normen bedient werden, damit der Kunde ein flexibel integrierbares Gateway für seine Medizintechnik und datengetriebenen Dienste nutzen kann.

Als starke Partner mit jahrzehntelanger Erfahrung Produktservices aus unseren jeweiligen Fachdomänen für Ihren Erfolg.

secunet ist Sicherheitspartner der Bundesrepublik Deutschland

eurobits

Allianz für Cyber-Sicherheit

ECS European Cyber Security Organisation

bitkom

TeleTrusT Pioneers in IT security.

ECO System Entscheiderfabrik

medical cluster

MTC Medical Technology Cluster

Forum MedTech Pharma

secunet

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 700 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 Segment Prime Standard der Frankfurter Wertpapierbörse gelistet und erzielte 2020 einen Umsatz von rund 286 Mio. Euro.

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

Die secunet Division eHealth sichert digitale Prozesse im Gesundheitswesen ab und optimiert die sichere und komfortable Nutzung von Informationstechnologien. Damit unterstützt secunet medizinische und organisatorische Tätigkeiten im Gesundheitswesen und berücksichtigt bzw. erfüllt dabei stets die gesetzlichen Anforderungen.

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

System Industrie Electronic GmbH

Die S.I.E (System Industrie Electronic GmbH) ist einer der marktführenden Entwicklungs- und Fertigungsspezialisten für Embedded Systeme und Cyber-Physische Systeme in regulativ herausfordernden Umfeldern (Medizin, Industrie, Cyber Security).

Als Full-Service-Anbieter begleitet das Unternehmen seine Kunden dabei über den gesamten Produktlebenszyklus, beginnend bei kreativen Ideations- und Beratungsprozessen, über die Entwicklung und Produktion, bis hin zu Qualitäts- und Life-Cycle-Services. Fokus und gemeinsame Ambition der S.I.E, ihrer Kunden und des gesamten Partnernetzwerks sind trotz aller digitaler DNA dabei stets nachhaltige und echte Mehrwerte für den Menschen.

Insbesondere in der Medizintechnik mit ihren hohen Anforderungen an Safety und Security sowie ihren sensiblen Daten, ist – für erfolgreiche Digitalisierung – ein abgestimmtes Zusammenspiel von Spezialisten verschiedenster Fachbereiche notwendig.

Von anwenderorientierten User Experience-Themen, Hard- und Softwareentwicklung entsprechender Embedded Systeme und Industriedesign, bis hin zu Datenmanagement und -sicherheit: S.I.E übernimmt die Organisation und Umsetzung relevanter Services rund um die Produktkonzeption, Entwicklung und Fertigung für seine Partner.

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