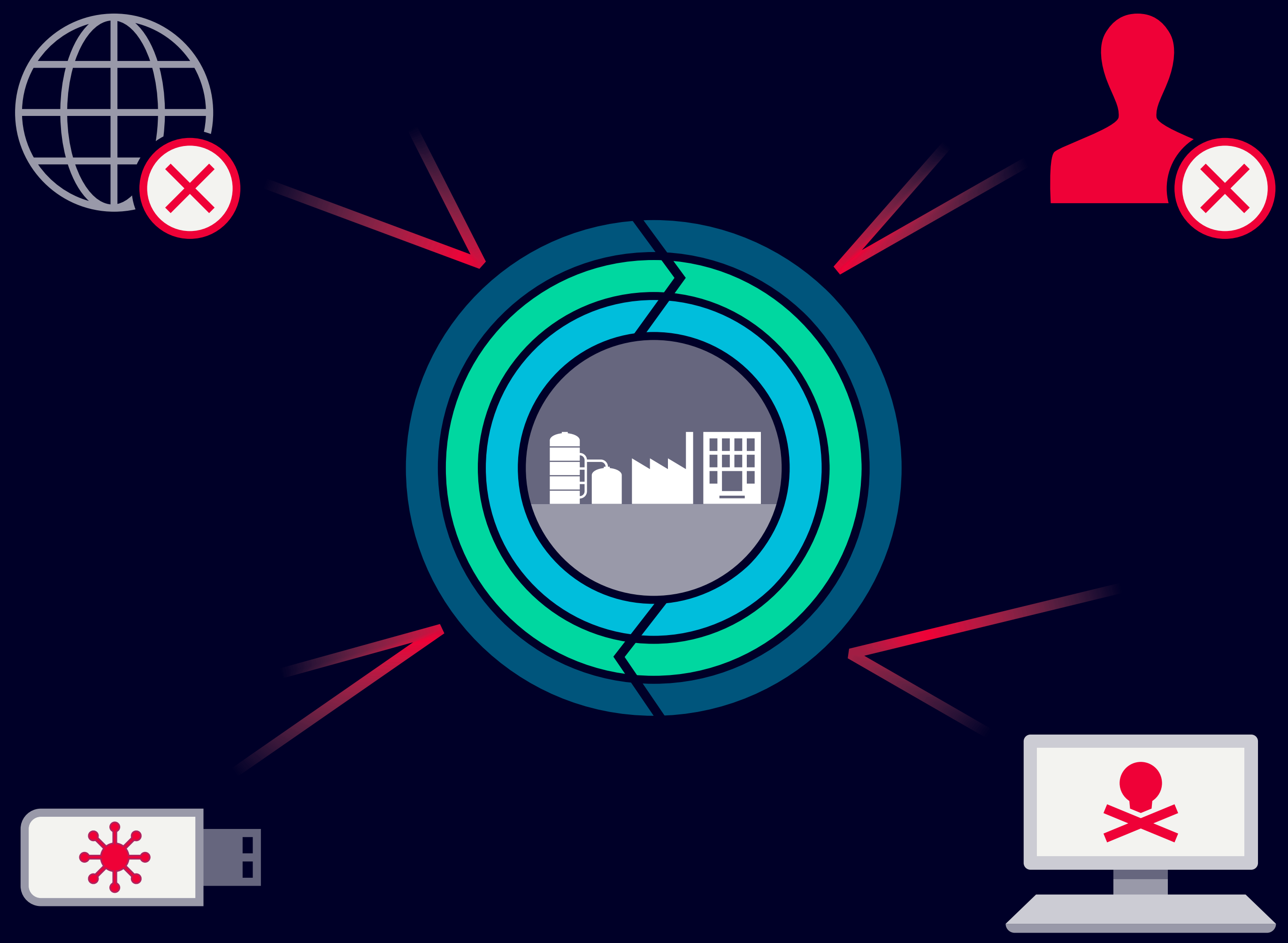
SIEMENS

# Protected in every aspect

## Cybersecurity for Industry as an essential component of Digital Enterprise

siemens.com/cybersecurity-industry

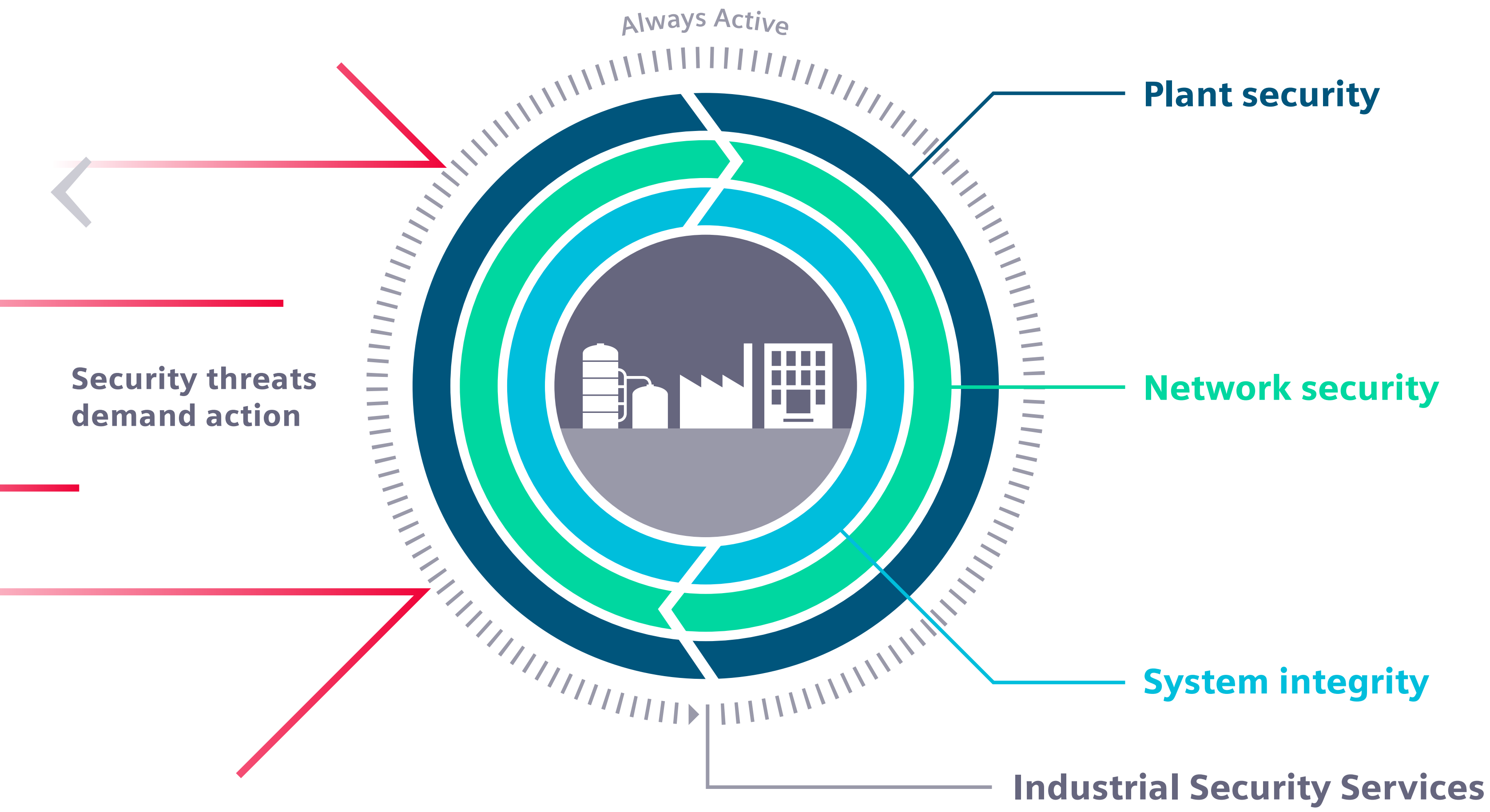
# Defense in depth



To protect industrial plants from internal and external cyber attacks, all levels must be protected simultaneously – from the plant management level to the field level and from access control to secure data communication.

With ”defense in depth“, Siemens provides a multi-layered security concept the ensures comprehensive and extensive protection for industrial facilities. It’s based on plant security, network security, and system integrity as it is recommended by IEC 62443.

# Defense in depth ...



## Plant security

Protects physical access of persons to critical components. It starts with conventional building access and extends to securing of sensitive areas by means of key cards. In addition, plant security comprises the integration of processes and guidelines as well as continuous monitoring of the security status of production facilities.

## Network security

Protection of the automation network against unauthorized access, especially at connection points to other networks (office or Internet). Network segmentation is providing additional security. Data transmission can be protected by using a VPN, e.g. for worldwide remote access to distant plants via Internet or mobile networks.

## System integrity

Securing system integrity means to protect automation systems and controllers like SIMATIC S7 controllers, control systems like SIMATIC PCS 7 and PCS neo, SCADA and HMI systems against unauthorized access or to protect the know-how contained therein. It also comprises user authentication and their access rights as well as system hardening against attacks.

## Industrial Security Services

Our experts in automation, digitalization and cybersecurity are the reliable partner for your secure digital transformation. They follow an end-to-end approach, starting with the evaluation of your security status over the implementation of security measures up to continuous monitoring and security management.

# Charter of Trust

Cybersecurity is an essential factor for the success of the digital economy. If we expect people to support the digital transformation, the security of data and networked systems must be guaranteed.

As pioneers in the field of digitalization, we are well aware of our responsibility. That is why we and our partners in government, industry and civil society are committed to the development of binding rules and standards that will create a new basis for trust and fair competition.

That is why Siemens and its partners in industry, government and civil society are working to establish the "Charter of Trust" – a charter that pursues three important goals:

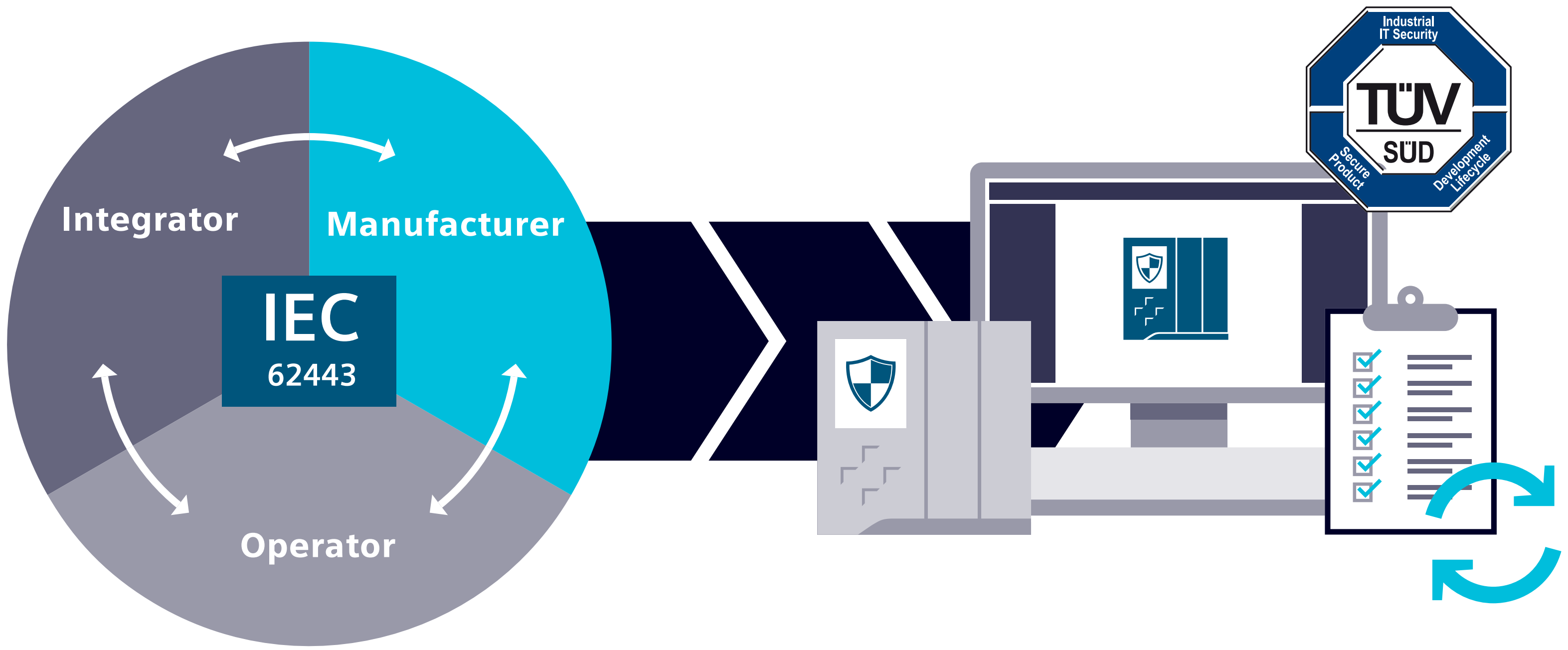
- Protect the data of individuals and companies
- Protect people, businesses and infrastructure from damage
- Establish a reliable foundation that supports and fosters the growth of trust in a networked digital world

## Basic principles

1. **Ownership of cyber and IT security**
2. **Responsibility throughout the digital supply chain**
3. **Security by default**
4. **User-centricity**
5. **Innovation and co-creation**
6. **Make cybersecurity a mandatory element of educational and training programs**
7. **Certify critical infrastructures and IoT solutions**
8. **Increase transparency and reaction speed**
9. **Regulatory framework**
10. **Advance joint initiatives**

# Plant security

Plant security starts with conventional building access and extends to securing of sensitive areas by means of key cards. Tailored industry security services include processes and guidelines for comprehensive plant protection. These range from risk analysis and the implementation and monitoring of suitable measures to regular updates.



**Integrators, operators and manufacturers require insights into IT security measures in order to design and operate automation processes and automation systems.**

## Access control

Managed access control is an essential factor when it comes to safeguarding critical company areas. Siemens Building Technologies offers an extensive portfolio of products, solutions and services for the protection of critical infrastructure. The range extends from access solutions and video monitoring systems to command and control platforms.

## Standards

Although there are hundreds of IT security standards, only a few have proven themselves useful for the protection of industrial systems. Building on our many years of experience, we advise you on the selection and implementation of appropriate standards.

In particular, IEC 62443/ISA99 is a well-proven international standard for the industrial automation environment.

## Defining guidelines

We support you in defining appropriate guidelines for your own application, and take all the relevant rules and standards into consideration. For example, the handling of removable storage devices must be clearly regulated. These precise guidelines help to ensure a high level of security for all concerned, without placing any constraints on productivity. In this way, Industrial Security becomes a central management task.

## Security monitoring

With continuous analysis and correlation of logs as well as comparison with our databases we detect and classify potential threats. In case of a security threat we notify you immediately and give a constant overview of the current security status of the plant through monthly status reports.

# Network security

One of the key challenges for consistent communication is simply to establish adequate protection of the easily accessible open systems. The focus here is on availability and the protection of automation networks against unauthorized access. This includes monitoring all interfaces like the ones between office and automation networks or remote maintenance access to the Internet. Automation networks and systems as well as industrial communication can be secured through network access protection, network segmentation (e.g. with "demilitarized zones", DMZ) and encrypted communication with Industrial Security Appliances, Industrial Routers, and security communications processors for SIMATIC S7 controllers.

## Excellent components for network security

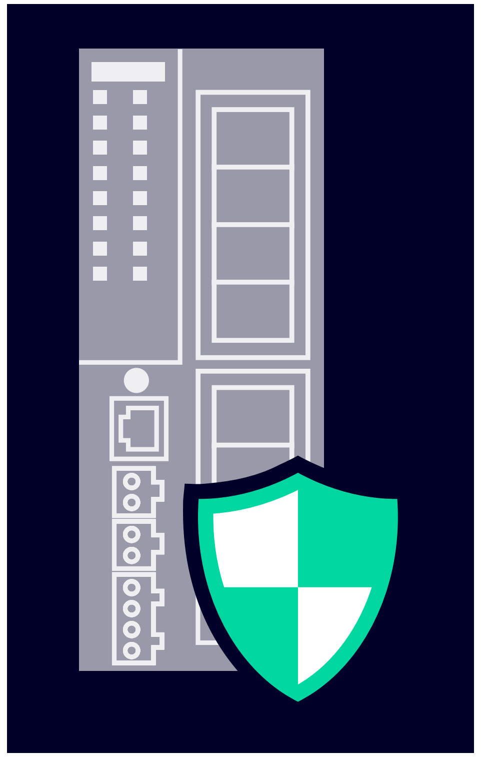
Industrial Security components from Siemens are optimized specifically for being used with automation technology and are designed to meet the special requirements of industrial communication networks.

Certifications such as from TÜV Süd (IEC 62443) prove the effectiveness of the security functions that are implemented in our network components.

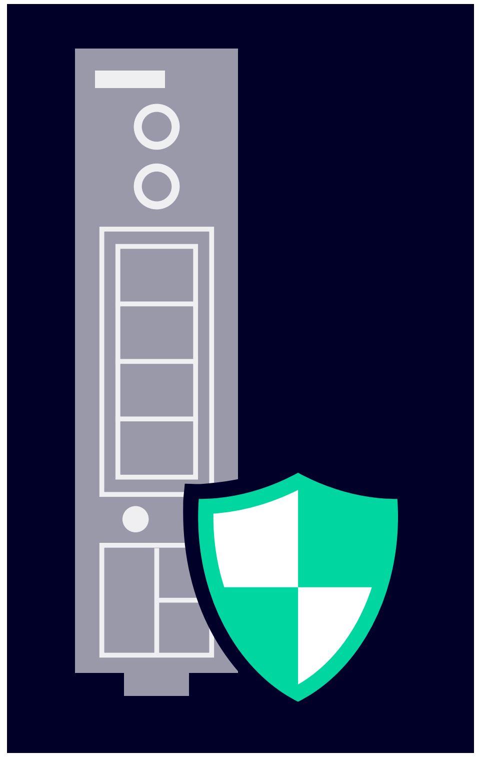
## Secure network architecture, remote access, and protected communication

To protect industrial networks and to enable using secured remote access Siemens offers a comprehensive product range with integrated security functions (Security Integrated) like SCALANCE S Industrial Security Appliances, SCALANCE M Industrial Routers for wired and mobile wireless networks (4G/5G), and security communications processors for SIMATIC S7 controllers. These products support a stateful inspection firewall and also secured VPN (virtual private network) communication for protection against unauthorized access, data espionage, and tampering.

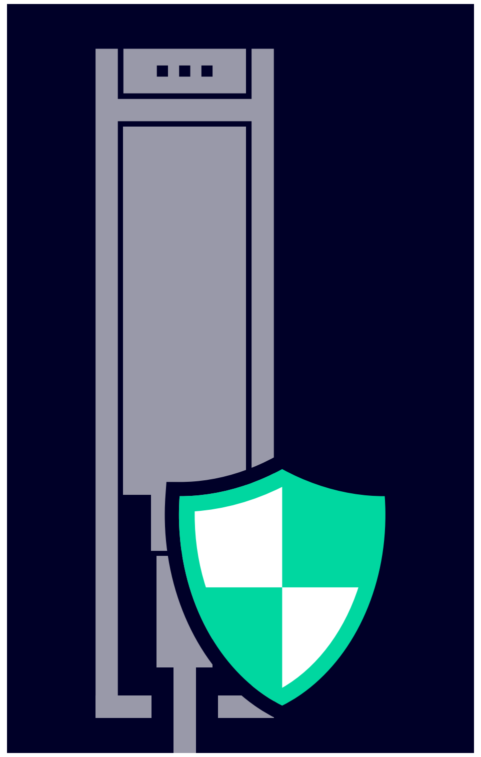
All devices can be configured in the TIA Portal and enable consistent, end-to-end security engineering. With the SINEC software solutions, it’s also possible to monitor, manage, and configure complex industrial networks, including firewall rules (SCALANCE S), centrally and around the clock, including in security-related areas.



Industrial Security Appliances SCALANCE S



Industrial Routers SCALANCE M

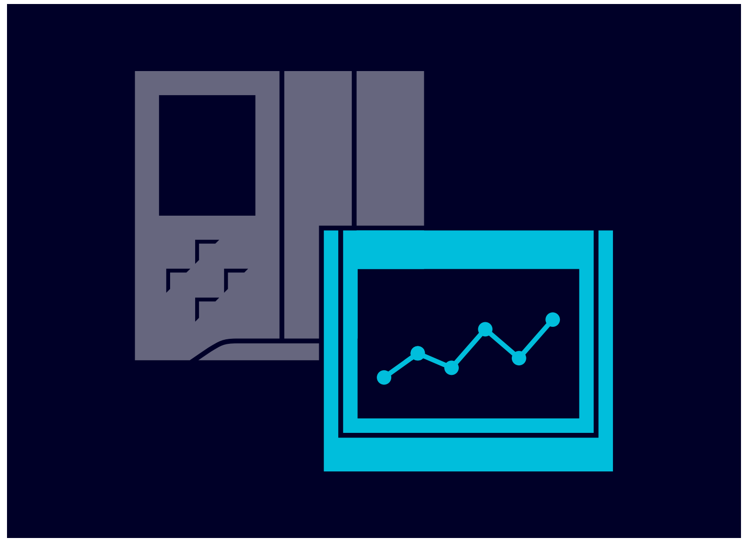


Security communications processors

siemens.com/networksecurity

# System integrity

**Protection of automation systems and control components.**
**Our integrated security features provide comprehensive protection against unauthorized configuration changes at the control level as well as against unauthorized network access, preventing the copying of configuration data and prevents any attempts to manipulate such sensitive data.**

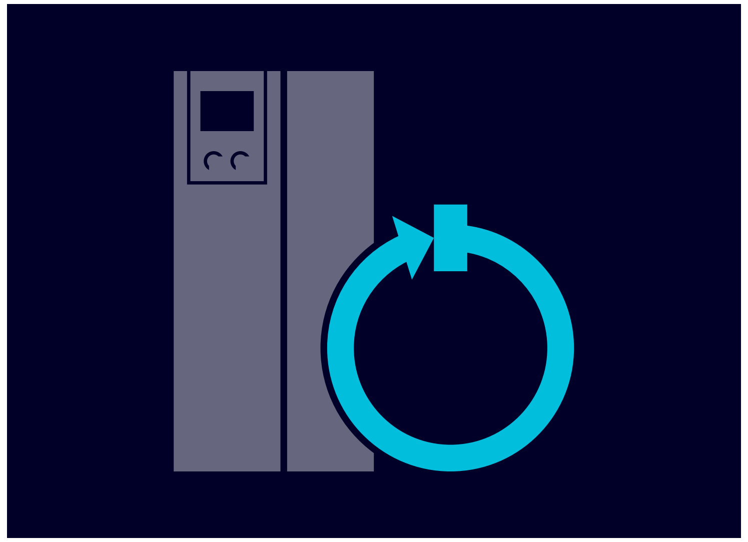


### Controllers and HMI systems

Robust controllers and HMI systems with integrated security functions for multi-level access protection, know-how and copy protection and for secure communication:  TLS based PG/HMI communication or via OPC UA.

### PC-based systems

Security functions for PC-based automation systems with whitelisting, antivirus software and system hardening for greater OS security.



### Motion control and drives

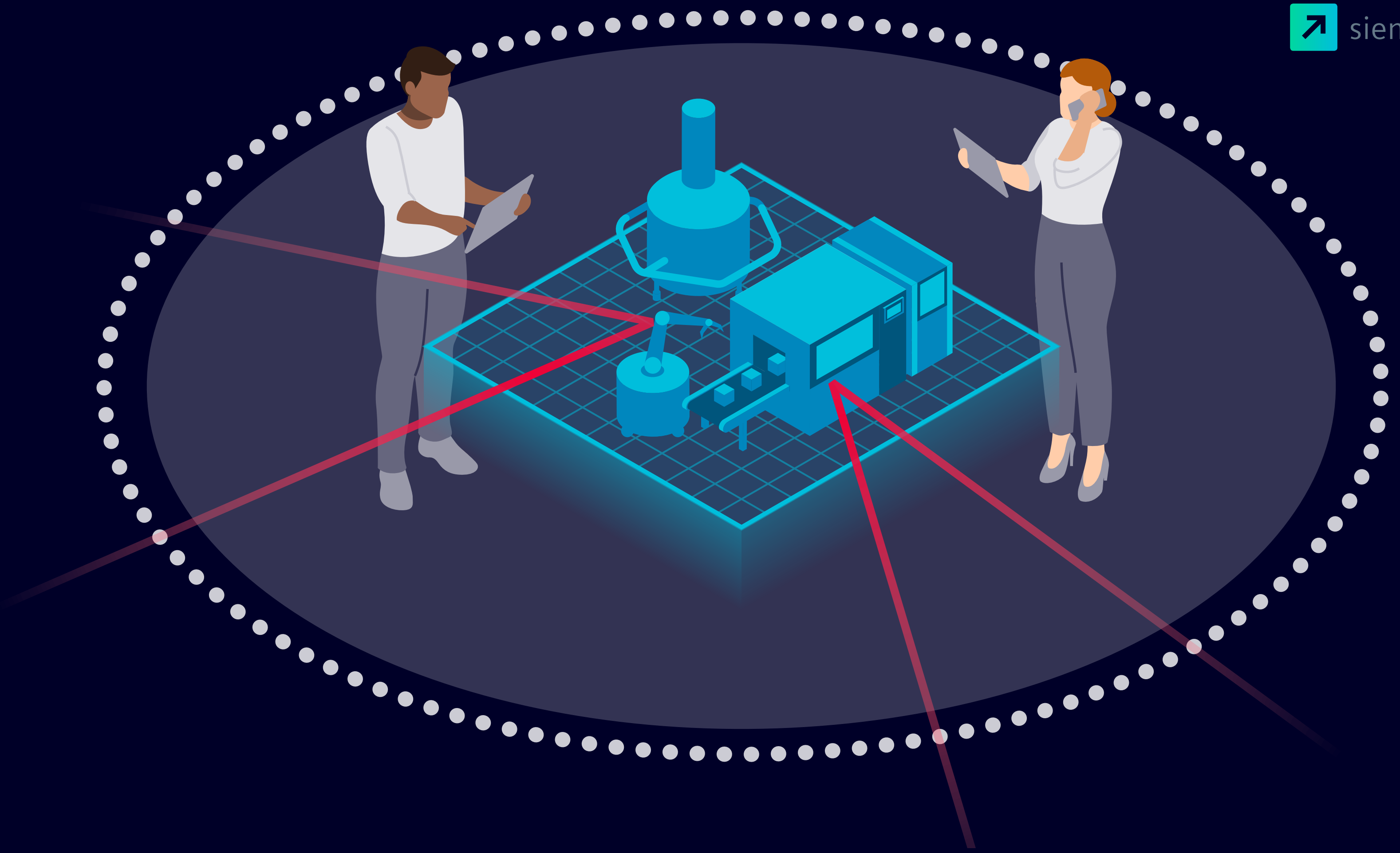
Integrated security functions in SINUMERIK, SIMOTION and SINAMICS for protecting your investment and maintaining productivity levels.

### Process automation

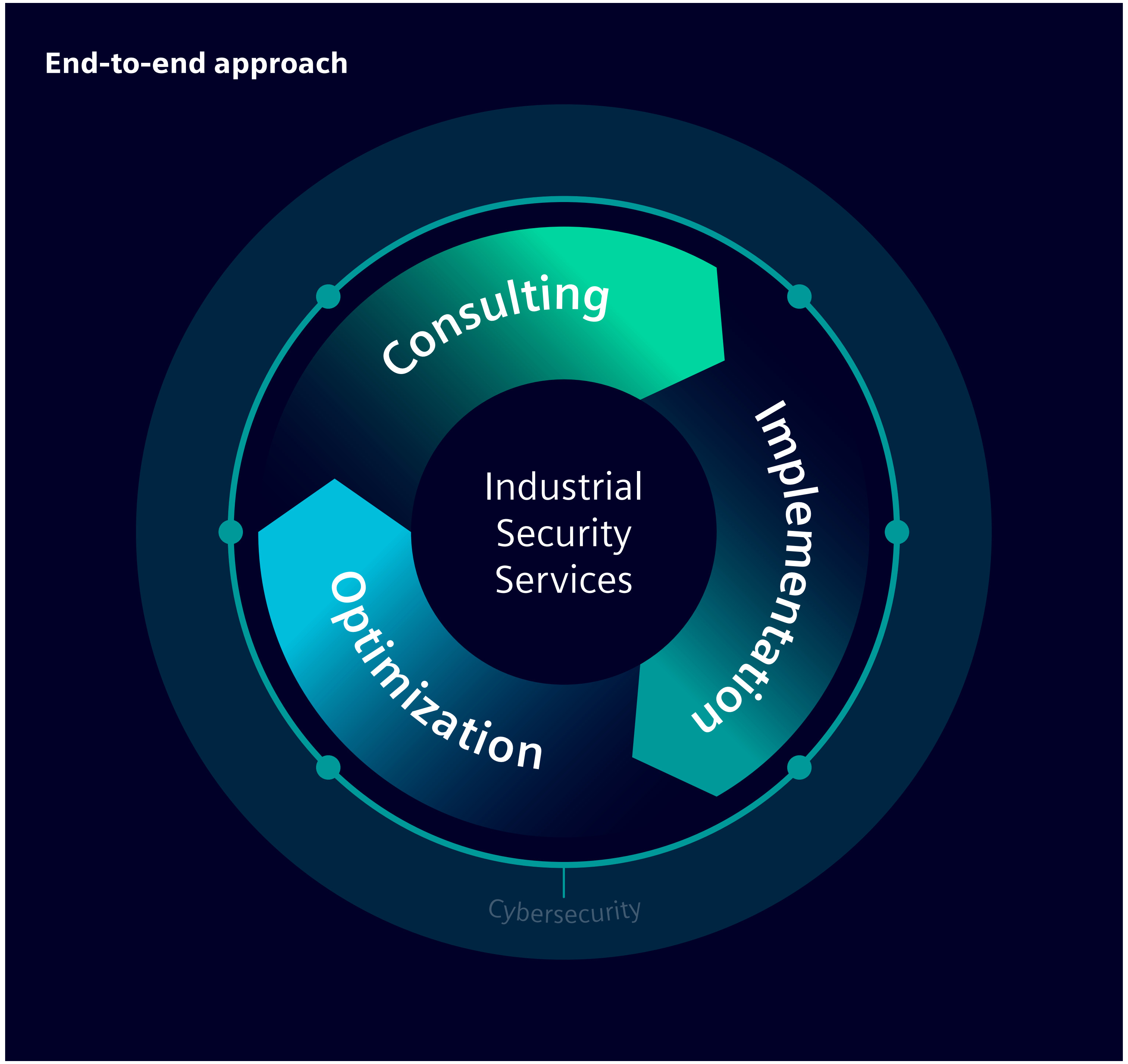
Safeguard productivity in the process industry with the Industrial Security concept for SIMATIC PCS 7 and SIMATIC PCS neo, based on the recommendations of the IEC 62443.

siemens.com/iss

# Industrial Security Services



With Industrial Security Services, industrial plants benefit from the comprehensive expertise and technical experience of a global network of experts in automation, digitalization and cybersecurity. The end-to-end approach of the industry-specific concept is based on state-of-the-art technologies as well as the applicable security rules and standards. Threats and malware are detected at an early stage, vulnerabilities analyzed in detail, and suitable comprehensive security measures are initiated. Continuous monitoring gives plant operators the greatest possible transparency regarding the security of their industrial facility and optimal investment protection at all times.



## Security Consulting

Evaluation of the current security status of an industrial environment

- Security Assessments
- Scanning Services
- Industrial Security Consulting

## Security Implementation

Risk mitigation through implementation of security measures

- Security Awareness Training
- Automation Firewall
- Endpoint Protection

## Security Optimization

Comprehensive security through managed services

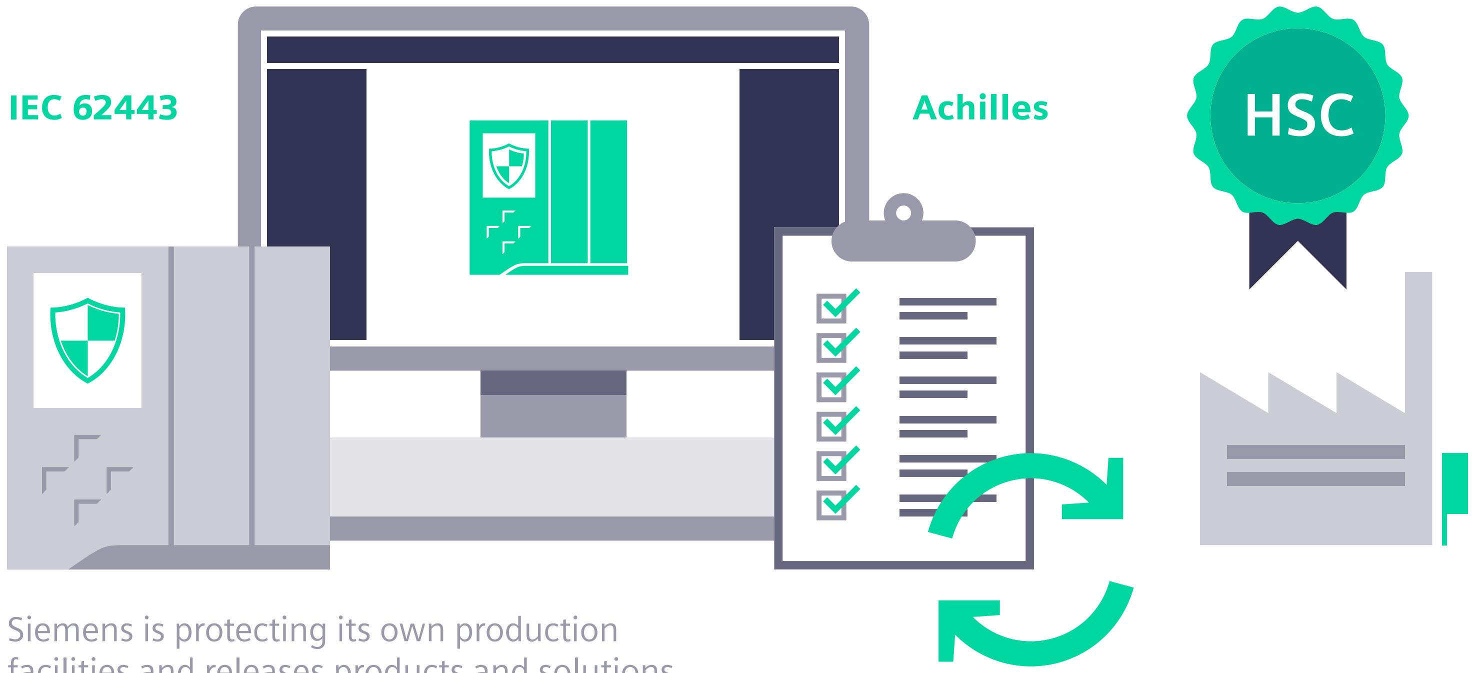
- Industrial Anomaly Detection
- Industrial Security Monitoring
- Remote Incident Handling
- Industrial Vulnerability Manager
- Patch Management
- SIMATIC Security Service Packages

# Always Active

Industrial Security is a continually changing challenge. At Siemens, we know how important Industrial Security is, and throughout the development of our automation products and solutions, we have established a series of measures and procedures for just this aspect, including within our Product Lifecycle Management (PLM), Supply Chain Management (SCM) and Customer Relationship Management (CRM) processes.

We work closely with our suppliers to ensure a high standard of security across the entire supply chain, and also check software components from third-party suppliers for possible weaknesses.

## Always active



Siemens is protecting its own production facilities and releases products and solutions that already have numerous security features.

Siemens is considering a competent team of security experts and open communication with customers and the public to be very important.

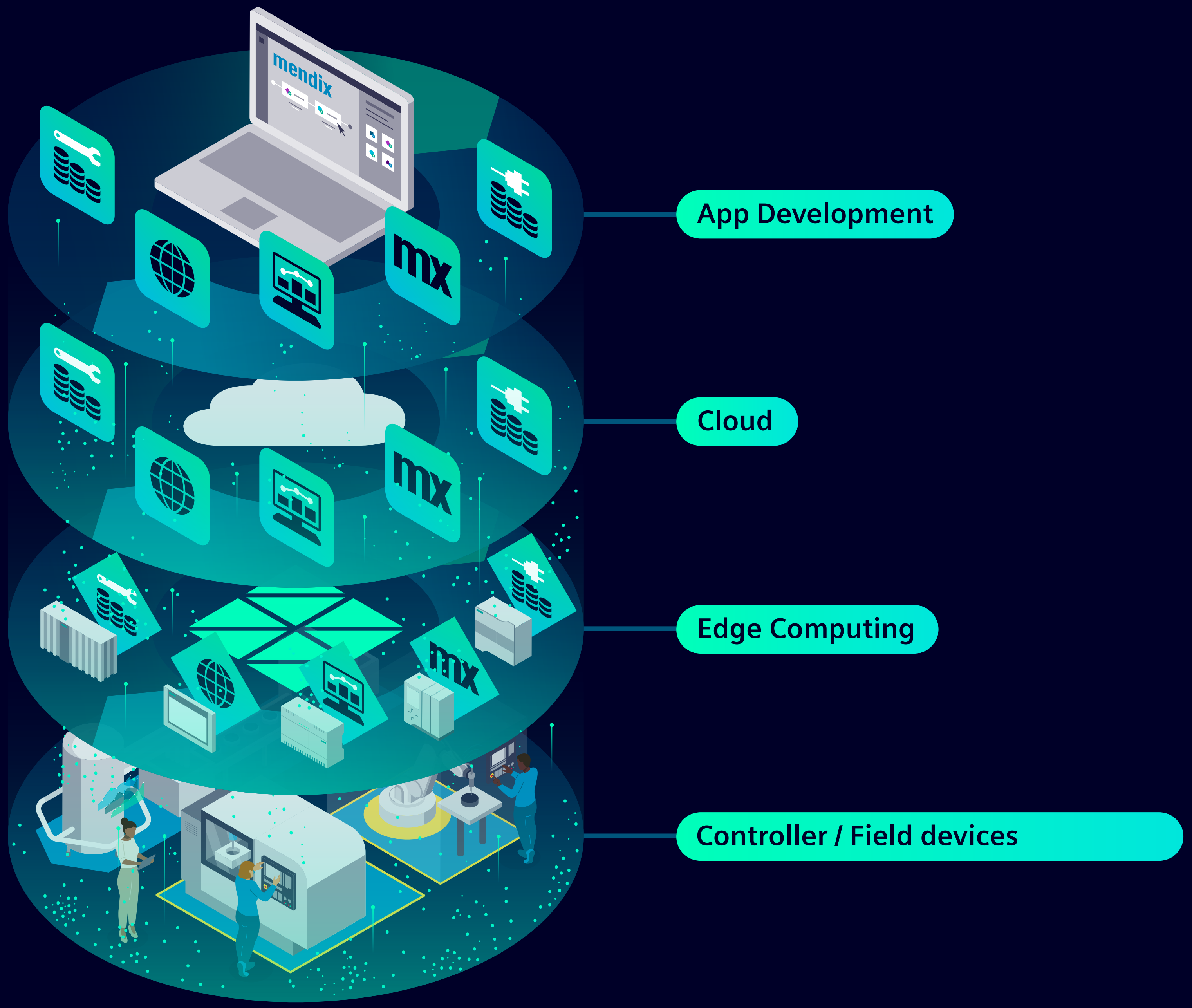
When security issues arise, we react promptly, informing our customers and providing them with recommendations, updates and security patches as quickly as possible. This means that we are now already able to comply with future legal requirements, such as those laid out in the German IT Security Act.

In addition, we are linked to over 200 security organizations around the world through the Forum of Incident Response and Security Teams (FIRST).

As a partner for industry, Siemens will work to incorporate any future IT security requirements as and when they emerge. For more information on alerts, updates and patches, visit:

↗ siemens.com/industrial-security

# Edge & Cloud Security



Industrial IoT Security reduces the surface area facing the internet. Industrial IoT Security protects a company's intellectual property (IP) through multiple rings of defense. It aligns with industry standards, best practices and customers' security objectives.

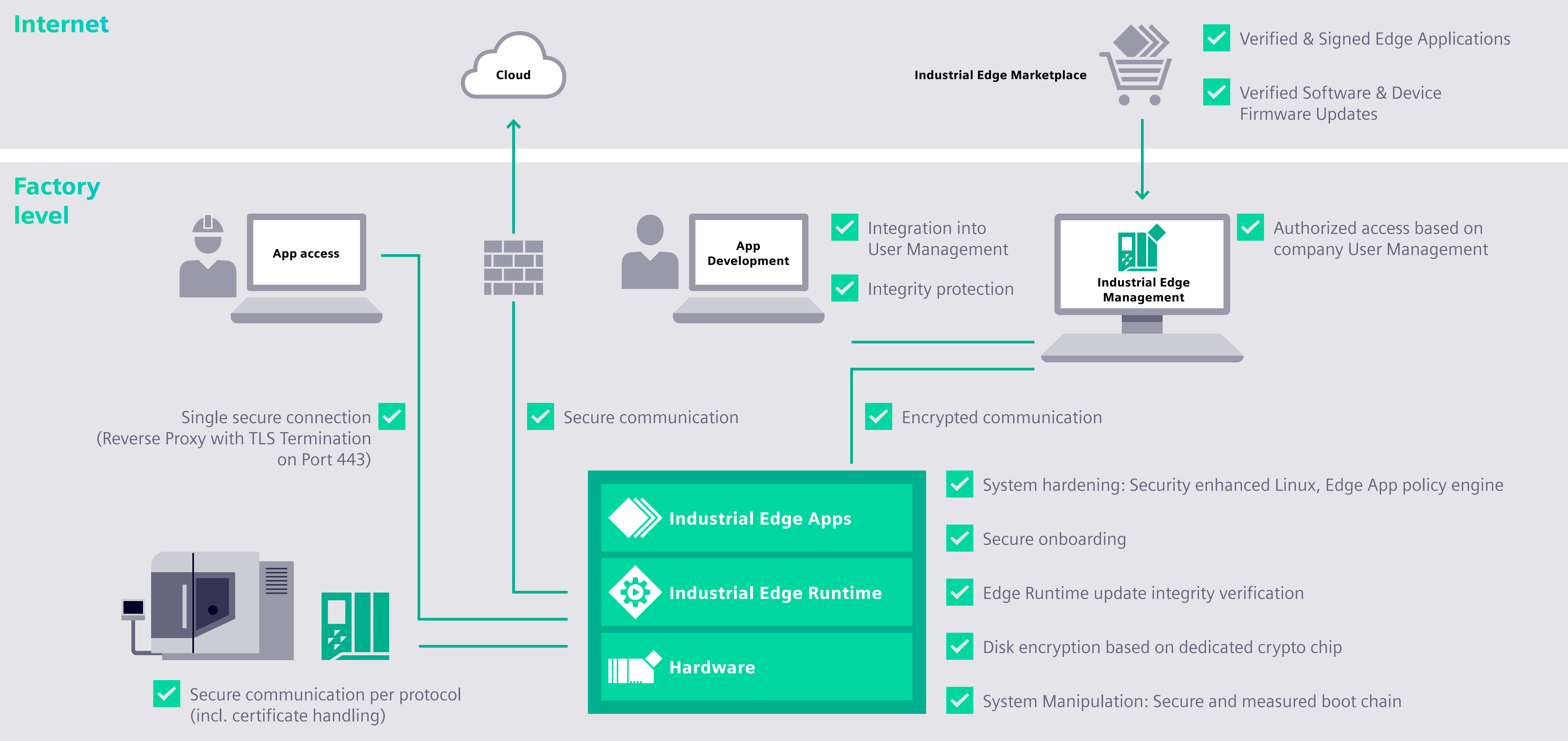
# Security is our primary requirement for Industrial Edge

Industrial Edge represents an open, ready-to-use Edge computing platform consisting of Edge devices, Edge apps, Edge connectivity, and an application and device management infrastructure. It makes it easier to collect and analyze data from industrial resources, enables a faster and more reliable rollout of apps on the shop floor, and provides central management for devices and apps with maximum scalability – and there's no need to intervene in the existing automation system (for example, to adapt controller software). Depending on your requirements, you determine what data stays local and what can be used with a cloud solution on an optional basis.

| | | | | |
|---|---|---|---|---|
| **Software level** | Container based isolation | Digital signatures for software artifacts | Certificate based authentication | Secure onboarding |
| **Operating System level** | Security enhanced Linux | No root user login | Secure and metered boot | Secure remote system update |
| **Hardware level** | Full disk encryption | Trusted Platform Module | Trusted deployment | Manufacturing device certificates |

Security overview: Industrial EdgeDevice

# Edge & Cloud Security



## Internet

Cloud

Industrial Edge Marketplace

- ✓ Verified & Signed Edge Applications
- ✓ Verified Software & Device Firmware Updates

## Factory level

App access

App Development

- ✓ Integration into User Management
- ✓ Integrity protection

Industrial Edge Management

- ✓ Authorized access based on company User Management

- ✓ Single secure connection (Reverse Proxy with TLS Termination on Port 443)
- ✓ Secure communication
- ✓ Encrypted communication

Industrial Edge Apps

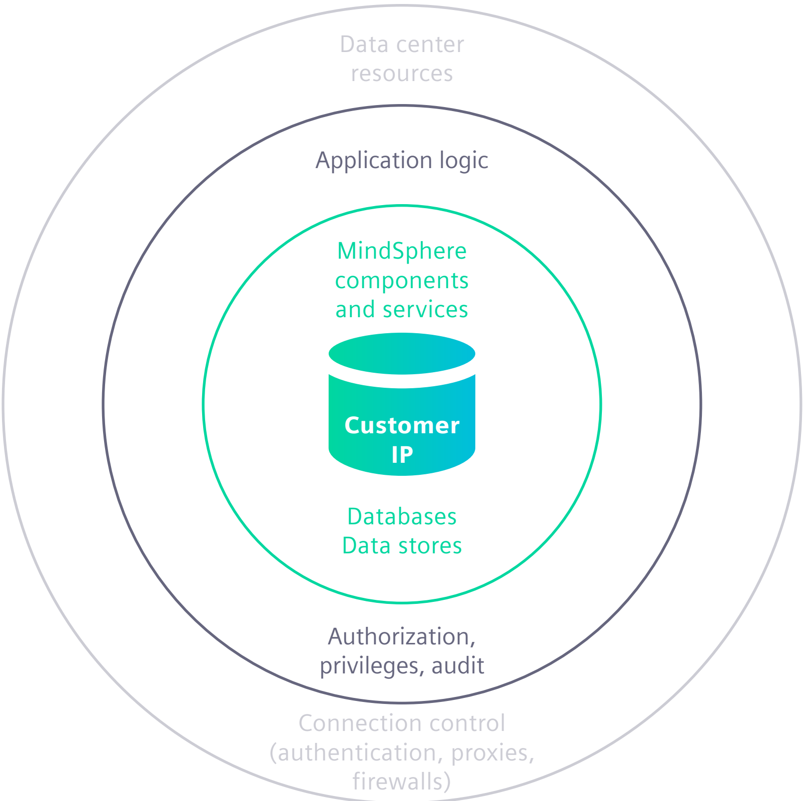
Industrial Edge Runtime

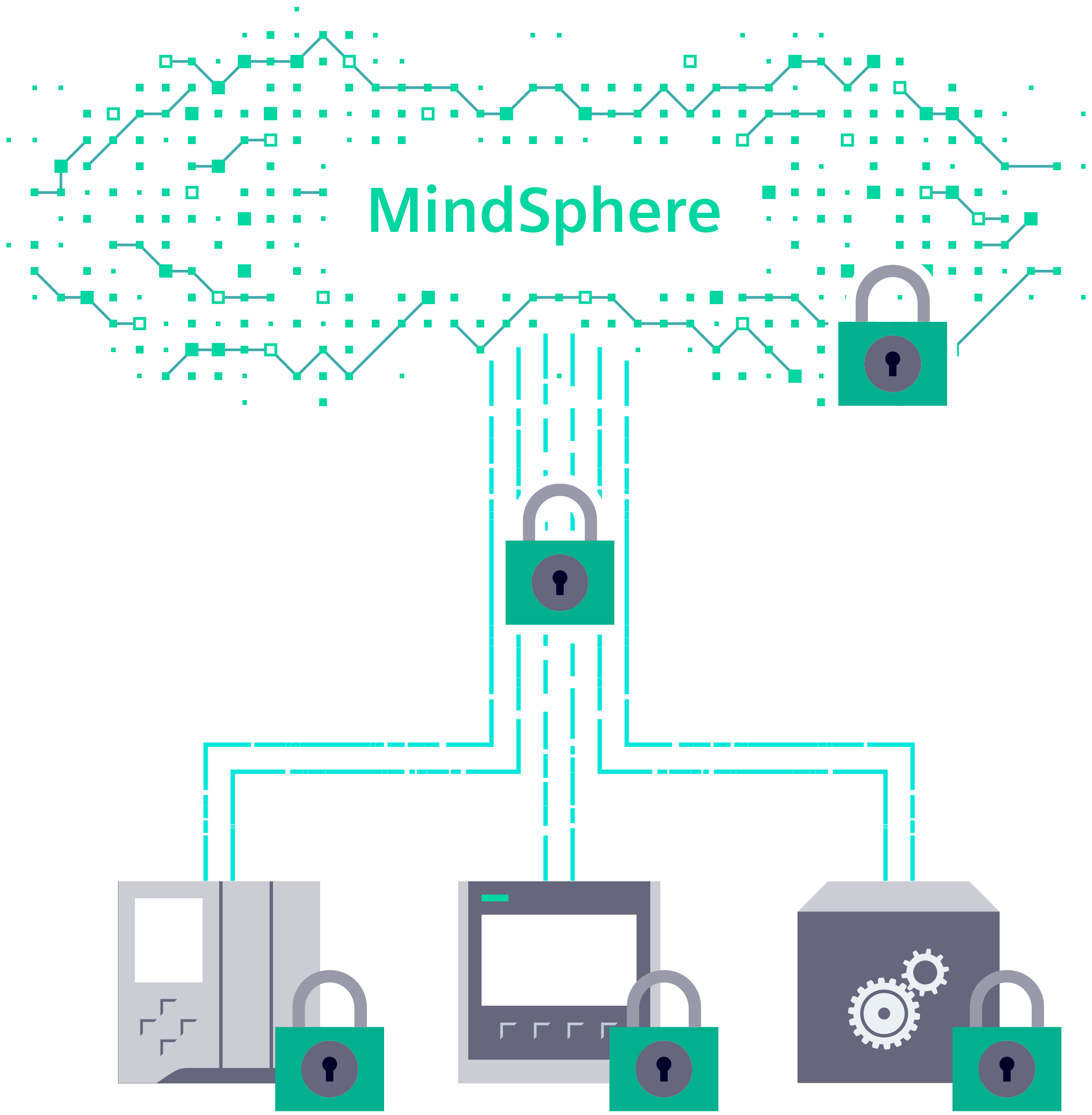
Hardware

- ✓ System hardening: Security enhanced Linux, Edge App policy engine
- ✓ Secure onboarding
- ✓ Edge Runtime update integrity verification
- ✓ Disk encryption based on dedicated crypto chip
- ✓ System Manipulation: Secure and measured boot chain

- ✓ Secure communication per protocol (incl. certificate handling)

Security overview: Industrial Edge platform


Data center resources
Application logic
MindSphere components and services
Customer IP
Databases Data stores
Authorization, privileges, audit
Connection control (authentication, proxies, firewalls)



## Data protection from the plant to the cloud

MindSphere supports single-factor and multiple-factor authentication protects log-ins as good as possible. The applications – MindApps – often contain sensitive data and hence are protected accordingly comprehensively. The data are separated physically and logically. Clearly managed access rights and access controls determine who can see and use which data.

Transmitting to and from the cloud is cryptographically protected, and connections are only accepted from authorized assets.

**Published by**
**Siemens AG**

Digital Industries
P.O. Box 48 48
90026 Nuremberg, Germany

**For the U.S.published by**

Siemens Industry Inc.
100 Technology Drive
Alpharetta, GA 30005
United States

For more information, please contact our
Customer Support Center
Phone: +49 180 524 70 00
Fax: +49 180 524 24 71
(Charges depending on provider)

Article No. DIFA-I10157-00-7600
Dispo 21507
WS 0821 iPDF

Subject to changes and errors.

The information given in this document only contains general descriptions and/or performance features which may not always specifically reflect those described, or which may undergo modification in the course of further development of the products. The requested performance features are binding only when they are expressly agreed upon in the concluded contract.