SIEMENS
Ingenuity for life

Protecting productivity with Plant Security Services

Identify vulnerabilities and threats at an early stage. Take proactive measures. Achieve optimal long-term plant protection.

siemens.com/plant-security-services

Comprehensive protection from cyber attacks

Industry-specific and scalable: The optimum protection level for your plants

Quickly growing and continuously new security risks and cyber threats necessitate fast reactions. Production processes in particular are always offering new areas for attacks and therefore require an especially high level of protection. With Siemens Plant Security Services, industrial companies benefit from comprehensive expertise as well as the specialist skills and knowledge of a global network of experts for automation and cyber security.

The comprehensive approach of a customer-specific concept is based on modern technology and thus fulfills the currently applicable security codes and standards. Threats or malware are detected at an early stage, the weaknesses are analyzed in detail and suitable security measures are immediately implemented.

The scalable offer includes comprehensive consulting, technical implementation and continuous service (Manage Security). The portfolio is available for existing Siemens plants as well as for technical plants from third-party providers.

Long-term protection for industrial plants: transparency through monitoring and analysis

In the event of a security incident, responses can be quickly initiated, customers informed and suitable security patches and updates prepared. The service can also be optimally adjusted to meet individual customer requirements. No matter what industry is involved, a plant-specific security roadmap ensures the best possible security level with a significantly reduced risk.

Continuous monitoring provides plant operators with the greatest possible transparency for the security of their industrial plants, ensuring especially good investment protection at all times. The powerful integral Global Threat Intelligence databases analyze and detect newly developing threats. The corresponding adjustments are made immediately and continuously. Changing threat situations are met with adjustments before threats can develop. The industry-specific, comprehensive and modular portfolio provides engineering that is not only perfectly customized but also tailored to your budget.

Industrial corporations trust Siemens Plant Security Services, whose transparent overview of security status enables plant operators to concentrate on their core business at all times. The sensitive topic of cyber security belongs in the hands of practiced experts: Siemens Plant Security Services.

Assess Security

- IEC 62443 Assessment
- ISO 27001 Assessment
- SIMATIC PCS 7 & WinCC Assessment
- Risk & Vulnerability Assessment

Manage Security

- Industrial Security Monitoring
- Remote Incident Handling
- Perimeter Firewall Management
- Perimeter Firewall Review
- Anti Virus Management
- Whitelisting Management
- Patch & Vulnerability Management

Implement Security

- Security Awareness Training
- Security Policy Consulting
- Network Security Consulting
- Perimeter Firewall Installation
- Clean Slate Validation
- Anti Virus Installation
- Whitelisting Installation
- System Back-up
- Windows Patch Installation

Assess Security for a risk-based security roadmap

Assess Security includes comprehensive threat analysis, identification of risks and specific recommendations for security measures.

Your benefit:

A plant-specific and risk-based security roadmap ensures a comprehensive and optimized security level.

IEC 62443 assessment

- **Complies with IEC 62443 standards**
- **Available for plants from Siemens and third-party providers**
- **Inquiry-based**
- **Recommendations for risk mitigation (report of up to 30 pages)**

ISO 27001 assessment

- **Complies with ISO 27001 standards**
- **Available for plants from Siemens and third-party providers**
- **Inquiry-based**
- **Recommendations for risk mitigation (report of up to 30 pages)**

SIMATIC PCS 7 & WinCC assessment

- **Complies with SIMATIC PCS 7 and WinCC security concept**
- **Special for SIMATIC PCS 7 and WinCC systems**
- **Inquiry-based**
- **Recommendations for risk mitigation (report of up to 30 pages)**

Risk & vulnerability assessment

- **Data-based analysis of threats, weaknesses and gaps**
- **Risk classification and evaluation accounting for system criticality**
- **Recommendation of risk mitigation measures (report of over 100 pages)**
- **Basis for a risk-based, plant-specific security roadmap**

Implement Security for risk mitigation measures

Implement Security provides the implementation of protection measures to improve the security level of plants and production facilities.

Your benefit:

Prevention of security gaps and better protection against cyber threats thanks to technical and organizational measures.

Security awareness training

- **Web-based SITRAIN training**
- **Establishment of security awareness among plant personnel: including the current situation and handling of threats, risks and the detection of security incidents**

Security policy consulting

- **Introduction of new and testing of existing security-related standards, guidelines and processes for plant security**
- **Integration in existing office IT security guideline**
- **Implementation of recommendations, e.g. patch and backup strategy, handling of removable media**

Network security consulting

- **Support in planning and segmentation of the automation network in security cells in accordance with IEC 62443 and the SIMATIC PCS 7 & WinCC security concept**
- **Planning of a DMZ network (perimeter)**
- **Specification and checking of plant perimeter firewall rules**

Perimeter firewall installation

- **Installation, configuration and testing of the firewall and firewall rules**
- **Backup of configuration in accordance with automation firewall appliance**
- **Evaluation of customer-specific applications, e.g. adjustment of the Intrusion Detection/Prevention Systems (IDS/IPS)**

Clean slate validation

- **Identification of security risks with two different virus scanners: McAfee Command Line Scanner and Kaspersky Rescue Disk**
- **No installation necessary: use of USB flash drives and command line instructions**

Anti virus installation

- **Installation and configuration of virus protection software: McAfee Virusscan Enterprise**
- **Installation of a new central management console: McAfee ePO1 (recommended by more than 10 antivirus agents)**
- **Compatibility evaluation for SIMATIC PCS 7 systems**

Whitelisting installation

- **Installation and configuration of a whitelisting application: McAfee Application Control**
- **Installation of a central management console: McAfee ePO5 (recommended by more than 10 whitelisting agents)**
- **Compatibility evaluation for SIMATIC PCS 7 systems**

System back-up

- **Performance of a one-time backup of critical plant systems using Symantec System Recovery Software (to be provided by the customer)**

Windows® patch installation

- **Installation of Microsoft® operating system patches using the customer's own WSUS server[2]**
- **Compatibility evaluation: Installation of patches recommended by manufacturers and approved by the customer**

[1] ePO – McAfee ePolicy Orchestrator
[2] WSUS – Microsoft Windows Software Update Server

Manage Security for comprehensive protection and transparency

Manage Security comprises regular monitoring and updating of the implemented measures via our Cyber Security Operation Center (CSOC).

Your benefit:

You can achieve the greatest possible transparency regarding the security status of your plants and proactively prevent potential threat events thanks to our global security experts.

Industrial security monitoring

- **Continuous analysis and correlation of log data as well as comparison with "Global Threat Intelligence" databases**
- **Detection, classification and immediate notification on the detection of security threats or incidents**
- **Continuous overview of current plant security status with monthly status reports**

Remote incident handling

- **Rapid response by Siemens Industrial Security experts**
- **Collection of information, cause analysis and criticality analysis with tools including intelligence mechanisms, malware sandboxing and monitoring of weaknesses.**
- **Recommendations for the correction of any consequential damage**

Perimeter firewall management

- **Monitoring, alarm annunciation and monthly reporting**
- **IDS/IPS management of the intrusion detection/prevention system**
- **Adaptation of existing firewall configuration and rules**
- **Backup/upgrading of firmware and software**

Perimeter firewall review

- **Firmware weakness analysis**
- **Redundancy checking as well as semantic analysis of firewall rules**
- **Validation of firewall configuration against network structure (consistency checking)**
- **Support for a wide range of firewall technologies**

Anti virus management

- **Updating of virus signatures and periodic virus scans in accordance with software manufacturer recommendations**
- **Detection of potential false alarms[1] through close cooperation with virus protection software manufacturers**
- **Monthly reports on plant condition regarding malware detection and prevention**
- **Central management possible through ePO console[2]**

Whitelisting management

- **Updating and management of activated whitelisting guidelines (definition of approved and executable software packages)**
- **Monthly reports on plant condition regarding malware detection and prevention**
- **Implementation of rules for application control with customer approval**
- **Central management possible through ePO console[2]**

Patch & vulnerability management

- **Available for SIMATIC PCS 7 software, Microsoft® operating systems, Adobe® Reader and Flash**
- **System-specific information on known weaknesses and patch availabilities**
- **Recommendations for plant-specific patch strategy**

[1] ePO – McAfee ePolicy Orchestrator
[2] »False positive«, ausschließlich für Siemens-Produkte

The effective security strategy

Defense in Depth

With increasing digitization, comprehensive security in automation is becoming increasingly important. Industrial security is therefore a key element of Digital Enterprise, the Siemens solution on the route to "Industrie 4.0" (the fourth industrial revolution). With Defense in Depth, Siemens offers a multi-layer concept providing both complete and in-depth protection for your plant. The concept is based on plant security, network security and system integrity in accordance with the recommendations of ISA 99/IEC 62443.

Plant security

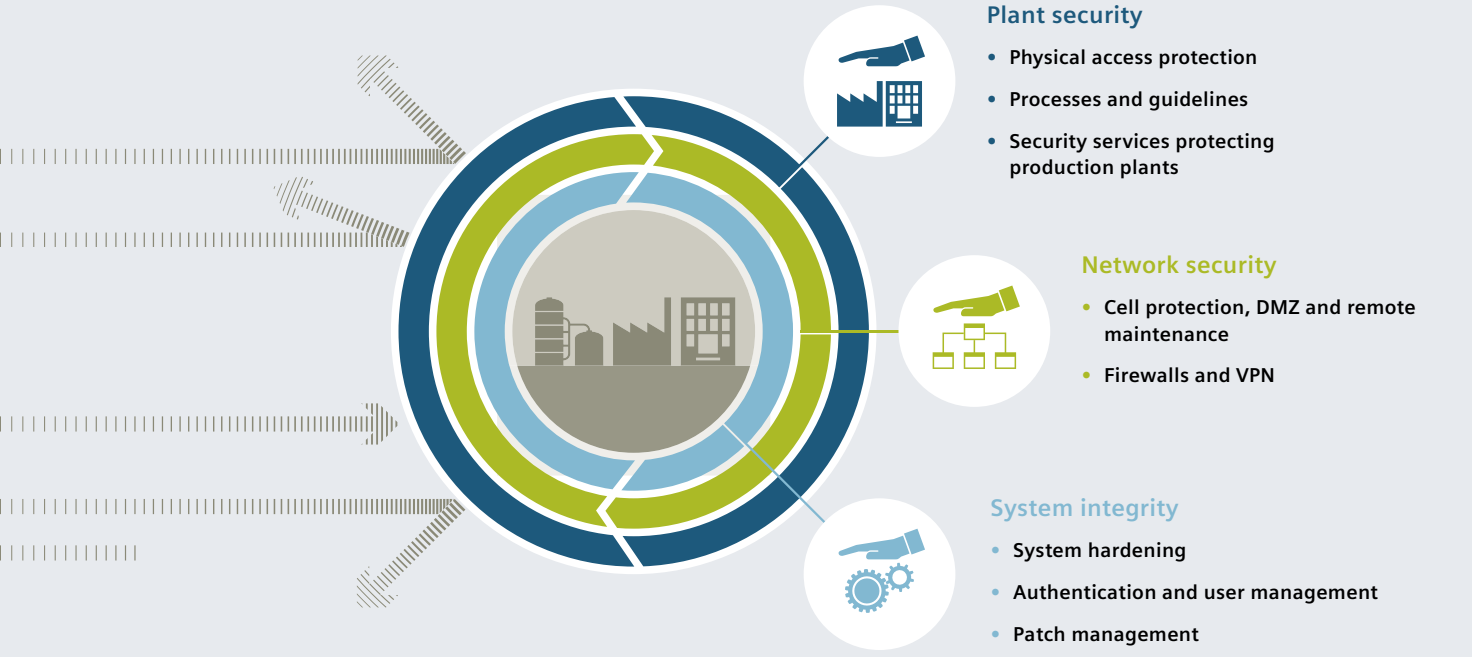
Plant security uses various methods to secure physical access by persons to critical components. This starts with classic building access and extends to the protection of sensitive areas with code cards. The customized Industrial Security Services include processes and guidelines for comprehensive plant security. This includes aspects such as a risk analysis of the implementation of suitable measures and their monitoring up to regular updates.

Network security

Protecting production networks from unauthorized access is now particularly indispensable at the connections to other networks (e.g. office or Internet). The segmentation of individual subnets such as the cell protection concept with SCALANCE S or the security communications processors for SIMATIC provides additional security here. Data transfer can also be protected using VPN, such as for global remote access to distant plants via the Internet or mobile phone network using SCALANCE M.

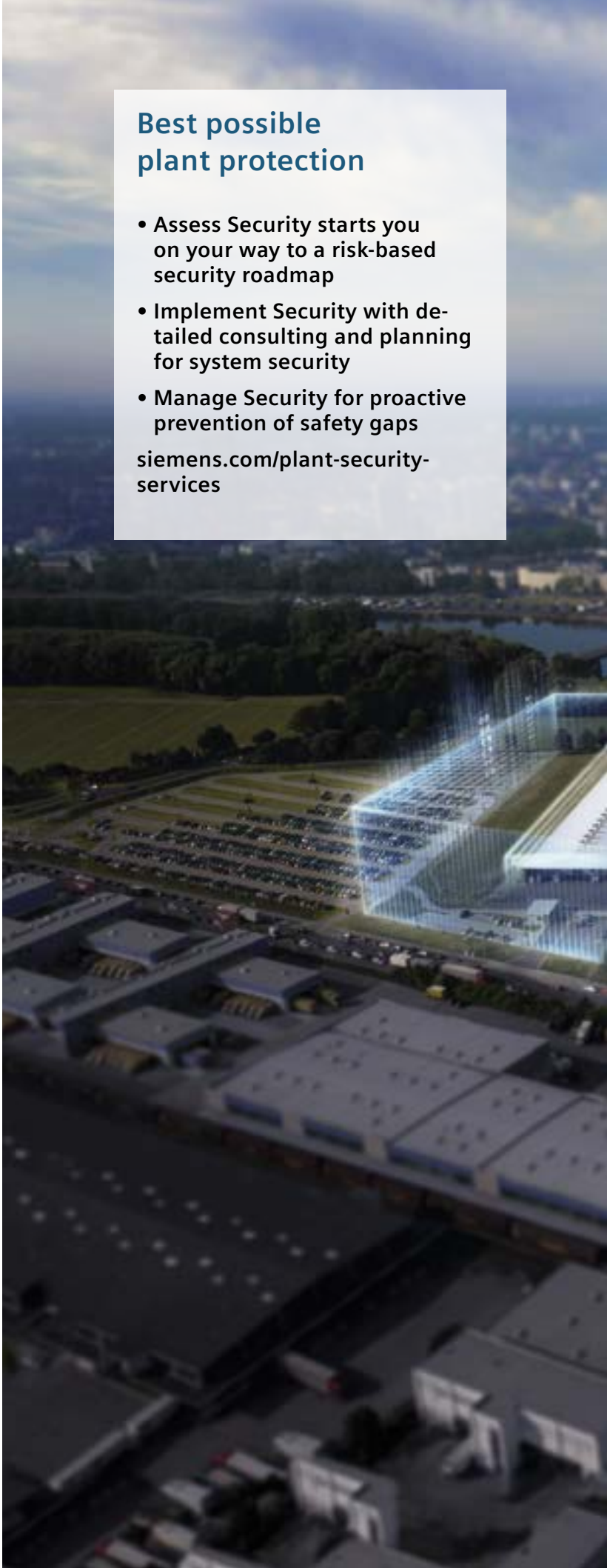
System integrity

The third foundation block of Defense in Depth entails ensuring system integrity. This includes the protection of automation systems and controls such as SIMATIC S7 controls as well as SCADA and HMI systems against unauthorized access or the protection of the information they contain. It also includes the authentication of users and their access privileges as well as hardening of the system against attackers.



Siemens AG
Digital Factory
Postfach 48 48
90026 Nürnberg
Deutschland

Subject to change without prior notice
Article-No.: DFPL-B10009-00-7600
Dispo 21639 WS 04161.0
Printed in Germany



Best possible plant protection

- **Assess Security starts you on your way to a risk-based security roadmap**
- **Implement Security with detailed consulting and planning for system security**
- **Manage Security for proactive prevention of safety gaps**

siemens.com/plant-security-services