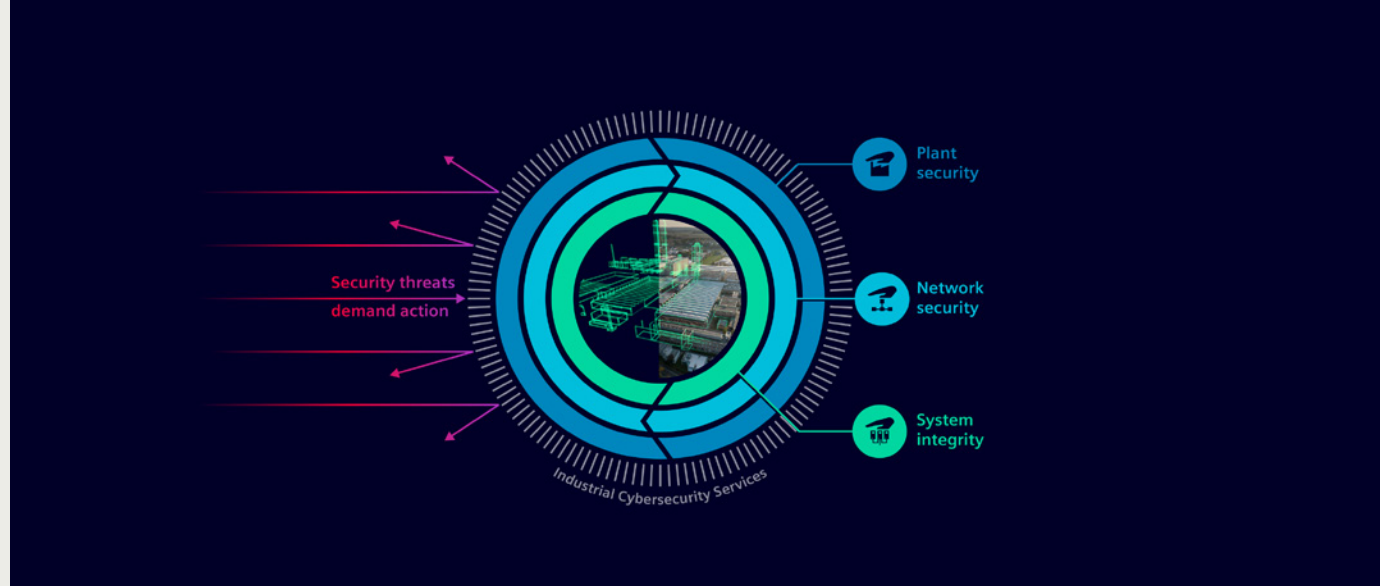




Cybersecurity for industrial networks

Ordering overview – Edition 04/2026
[siemens.com/network-security](https://www.siemens.com/network-security)



Defense in depth

To provide industrial plants with comprehensive protection from internal and external cyber attacks, all levels must be addressed simultaneously: from operations to field level, from access control to copy protection.

With this in mind, Siemens has implemented a multi-faceted “defense in depth” protection concept based on IEC 62443 recommendations, the leading international standard for security in industrial automation. An essential component of this concept is network security.



Excellent components for network security

In addition to availability, the focus is on protecting automation networks against unauthorized access. This includes checking all interfaces between IT and OT such as between office and system networks or remote maintenance access (e.g. SINEMA Remote Connect). Automation networks and systems and industrial communication can be secured by network access protection, network segmentation (e.g. “Demilitarized Zones”, DMZ), encrypted communication and the principles of Zero Trust Network Access (ZTNA). Siemens therefore offers an extensive product range of industrial cybersecurity components with integrated security functions such as the industrial cybersecurity appliances SCALANCE S, the industrial router SCALANCE M for wired and wireless networks (4G/5G) and security communications processors for SIMATIC S7.

Through the combination of the cell protection concept with zero trust principals from IT, application-specific remote access is possible for a consistent IT/OT security concept:

www.siemens.com/zero-trust

The reliability of network security components plays a major role in automation and communication networks in the energy sector and other industries where harsh ambient conditions prevail. The robust RUGGEDCOM security devices enable network security to be achieved in these environments as well.

As a complement to integrated solutions for the management and administration of secured remote accesses, other passive components are available for physical network protection, such as the IE RJ45 Port Lock.

The SCALANCE TAP104 supports the export of data traffic for advanced network analyses.



Software for efficient and secure networks

The SINEC software for network management monitors, manages and plans complex industrial networks, including firewall rules.

The SINEC Security Software Suite with SINEC Security Monitor, SINEC Security Inspector and SINEC Security Guard offers full risk transparency for OT systems.

SINEC Security Inspector determines the security status of components and networks to promptly identify any security vulnerabilities.

SINEC Security Monitor analyses the network traffic and identifies anomalies using passive, non-intrusive, and continuous security monitoring.

SINEC Security Guard is a cloud-based SaaS solution that automatically compensates for vulnerabilities and enables comprehensive security management.

Find out more: [siemens.com/sinec](https://www.siemens.com/sinec)

Specific concepts for reliable protection

With Industrial Cybersecurity Services, industrial systems benefit from the extensive 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 the latest technologies and applicable norms and security standards. Threats and malware are recognized at an early stage, vulnerabilities are analyzed in detail and appropriate comprehensive security measures are implemented. Continuous monitoring gives plant owners maximum transparency regarding the security of their industrial facility, thus providing optimal investment protection at all times.

Find out more at: [siemens.com/iss](https://www.siemens.com/iss)



Cybersecurity information

Siemens provides products and solutions with industrial cybersecurity functions that support the secure operation of plants, systems, machines and networks.

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial cybersecurity concept. Siemens' products and solutions constitute one element of such a concept.

Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place.

For additional information on industrial cybersecurity measures that may be implemented, please visit www.siemens.com/cybersecurity-industry

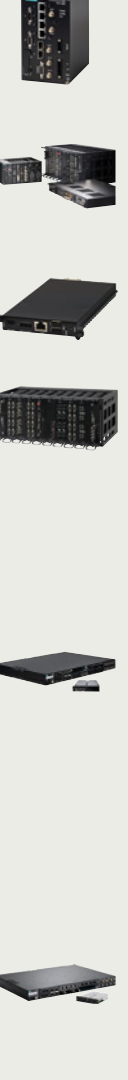
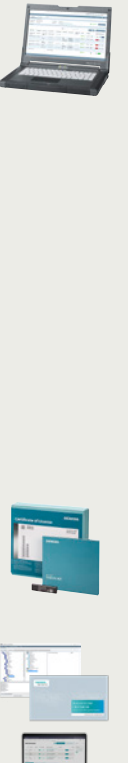
Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates may increase customer's exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Cybersecurity RSS Feed under www.siemens.com/cert

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.

All product designations may be trademarks or product names of Siemens AG or supplier companies whose use by third parties for their own purposes could violate the rights of the owners.

Order overview – Cybersecurity for industrial networks

	Application	Product	Network type 1	Network type 2	Interfaces	Comments	Article No. ¹⁾	
SCALANCE S Industrial Security Appliances for flexible network segmentation								
	Industrial Security Appliances	SCALANCE SC622-2C	Industrial Ethernet		2 × combo port with RJ45 or SFPs	Protection of devices and networks with firewall (750 Mbps data throughput); address translation with NAT/INAPT; connection to SINEMA Remote Connect	6GK5622-2GS00-2AC2	
		SCALANCE SC626-2C			4 × RJ45		6GK5626-2GS00-2AC2	
		SCALANCE SC632-2C			2 × combo port with RJ45 or SFPs		6GK5632-2GS00-2AC2	
		SCALANCE SC636-2C			4 × RJ45		6GK5636-2GS00-2AC2	
		SCALANCE SC642-2C			2 × combo port with RJ45 or SFPs	Protection of devices and networks with firewall (750 Mbps data throughput) and VPN (IPsec/OpenVPN); address translation with NAT/INAPT; connection to SINEMA Remote Connect	6GK5642-2GS00-2AC2	
		SCALANCE SC646-2C			4 × RJ45	6GK5646-2GS00-2AC2		
		SCALANCE S605			5 × RJ45	Protection of devices and networks with firewall (100 Mbps data throughput) and VPN (IPsec/OpenVPN); address translation with NAT/INAPT; SINEMA Remote Connect integrated	6GK5605-0AA00-2AA2	
		SCALANCE S615			5 × RJ45	Protection of devices and networks with firewall (100 Mbps data throughput) and VPN (IPsec/OpenVPN); address translation with NAT/INAPT; connection to SINEMA Remote Connect	6GK5615-0AA00-2AA2	
		SCALANCE S615 EEC			5 × RJ45	6GK5615-0AA01-2AA2		
SCALANCE M Industrial Routers for secured remote access via public and private networks ²⁾								
	Industrial Routers	SCALANCE M804PB	Industrial Ethernet	PROFIBUS/MPI	2 × RJ45 1 × RS-485	Router for connecting PROFIBUS/MPi automation devices to Ethernet networks; firewall and VPN (IPsec/OpenVPN); connection to SINEMA Remote Connect	6GK5804-0AP00-2AA2	
		SCALANCE M826-2		2-wire (SHDSL)	4 × RJ45 2 × terminal block (2-pin)	SHDSL; firewall and VPN (IPsec/OpenVPN); connection to SINEMA Remote Connect	6GK5826-2AB00-2AB2	
		SCALANCE M876-4		Mobile wireless GSM (2G), UMTS (3G), LTE (4G)	4 × RJ45 2 × SMA antenna connection	IP router for transparent data transmission between Industrial Ethernet and 4G mobile wireless network; firewall and VPN (IPsec/OpenVPN); connection to SINEMA Remote Connect	6GK5876-4AA10-2BA2	
		SCALANCE MUB852-1 (A1)	Mobile wireless UMTS (3G), LTE (4G), public and private 5G	1 × RJ45 4 × SMA antenna connection	IP router for transparent data transmission between Industrial Ethernet and public mobile network (5G) or the connection to private 5G networks; firewall; VPN (only in combination with a SINEMA Remote Connect device license); Connection to SINEMA Remote Connect	6GK5852-1EA10-1AA1		
		SCALANCE MUM853-1 (A1)		4 × RJ45 4 × SMA antenna connection	IP router for transparent data transmission between Industrial Ethernet and public mobile network (5G) or the connection to private 5G networks; firewall and VPN (IPsec/OpenVPN); connection to SINEMA Remote Connect	6GK5853-2EA10-2AA1		
		SCALANCE MUM856-1 (A1)		1 × M12 X-coded with PoE 4 × N-Connect antenna connection (mobile wireless, private 5G)	IP router for transparent data transmission between Industrial Ethernet and public mobile network (5G) or the connection to private 5G networks; firewall and VPN (IPsec/OpenVPN); connection to SINEMA Remote Connect	6GK5856-2EA10-3AA1		
Zero Trust for secure demand-based access to OT applications								
	Local Processing Engine	SCALANCE LPE9403	Industrial Ethernet		3 × 10/100/1000 Mbps RJ45; 1 × 100/1000 Mbps SFP; 1 × combo port; 1 × USB 3.0	Local Processing Engine with performant CPU; 64 Bit ARMv8 (4core); 4 GB RAM; Debian Linux Zero Trust Gateway by means of installation of additional software	6GK5998-3GS00-2AC2	
Industrial Security Communications Processors (CPs) for remote SIMATIC controls								
	Security Communications Processors	CP 1243-7 LTE EU	Mobile wireless GSM (2G), UMTS (3G), LTE (4G)		1 × SMA antenna connection for LTE	For connecting SIMATIC S7-1200 to the 4G mobile wireless network (LTE); for connection to control rooms via remote control protocols (DNP3, IEC 60870-5-104, TeleControl Basic); consider country approvals; firewall and VPN (IPsec/OpenVPN); connection to SINEMA Remote Connect	6GK7243-7KX30-0XE0	
		CP 1243-7 LTE US					6GK7243-7SX30-0XE0	
		CP 1243-1	Industrial Ethernet		1 × RJ45	For connecting SIMATIC S7-1200; for connection to control rooms via remote control protocols (DNP3, IEC 60870, TeleControl Basic); firewall and VPN (IPsec/OpenVPN); connection to SINEMA Remote Connect	6GK7243-1BX30-0XE0	
		CP 1243-8 IRC			1 × RJ45 1 × 18-pin socket left for connecting TS modules	For connecting SIMATIC S7-1200; for connection to control rooms via remote control protocols (SINAUT ST7, DNP3, IEC 60870-5-104); is discontinued; firewall and VPN (IPsec/OpenVPN); connection to SINEMA Remote Connect	6GK7243-8RX30-0XE0	
		CP 1543-1			1 × RJ45	For connecting SIMATIC S7-1500; firewall and VPN (IPsec); IEEE 802.1X (radius); and support of FTPS and SNMPv3 protocols for data encryption	6GK7543-1AX10-0XE0	
		CP 1545-1			1 × RJ45	For connecting SIMATIC S7-1500; firewall and VPN (IPsec); IEEE 802.1X (radius); and support of FTPS and SNMPv3 protocols for data encryption; with CloudConnect functionality	6GK7545-1GX10-0XE0	
		CP 1543SP-1			BusAdapter (BA), 2 ports (RJ45 or FO) depending on the BA type	For connecting SIMATIC ET 200SP Distributed Controller; firewall and VPN (IPsec/OpenVPN); connection to SINEMA Remote Connect	6GK7543-6WX00-0XE0	
		CP 1542SP-1 IRC			BusAdapter (BA), 2 ports (RJ45 or FO) depending on the BA type	For connecting SIMATIC ET 200SP Distributed Controller; for connection to control rooms via telecontrol protocols (SINAUT ST7, DNP3, IEC 60870-5-104, TeleControl Basic); VPN (OpenVPN); connection to SINEMA Remote Connect	6GK7542-6VX00-0XE0	
RUGGEDCOM – rugged security components for harsh environmental conditions								
	Multi-protocol Intelligent Device	RUGGEDCOM RX1400	Industrial Ethernet	Mobile wireless GSM (2G), EVDO (3G), LTE (4G)	4 × RJ45 2 × SFP 5 × SMA antenna connection (mobile wireless, Wi-Fi and GPS)	Compact Ethernet switch and TCP/IP router with LTE and fiber optic WAN options. All-in-one device for switching, Wi-Fi, routing and firewall functionality, with the option to be used as a mobile router ³⁾	6GK6014-0AM2-.....	
		RUGGEDCOM RX1510 RUGGEDCOM RX1511 RUGGEDCOM RX1512 RUGGEDCOM RX1524 RUGGEDCOM RX1536			12/24/36 ports RJ45, up to 6 line modules, up to 4 or 8 Gigabit Ethernet ports, antenna connection	Industrial hardened Layer 2 and Layer 3 switch/router; firewall and VPN (IPsec); APE module for 3rd party applications ³⁾ (except in RUGGEDCOM RX1512)	6GK6015-1AM2-..... 6GK6015-1BM2-..... 6GK6015-1CM2-..... 6GK6015-0CM2-..... 6GK6015-0DM2-.....	
		RUGGEDCOM APE1808			2 × USB 3.0 ports, 2 × Gigabit Ethernet ports, 1 × display port, 1 × micro SD card slot	Utility grade application processing engine that can run commercially available third-party software, including cybersecurity and Edge Computing applications	6GK6015-0AL2-.....	
		RUGGEDCOM RX5000			Up to six line modules for up to 98 ports	Routing and switching platform with high port density; firewall and VPN (IPsec)	6GK6050-0AM2-.....	
		RUGGEDCOM RST2228	Industrial Ethernet		28 ports, 4 × 1/10 Gbit/s and 24 × 100/1000 Mbps non-blocking Ethernet ports. Up to 4-port media modules with RJ45, SFP or LC interfaces	Multi-layer managed Layer 2 Ethernet switches with 10 Gbit/s uplinks, support for time synchronization, optional MACsec encryption and seamless redundancy functions	6GK6222-6AB.-.....	
		RUGGEDCOM RST2228P			28 ports, 4 × 1/10 Gbit/s and 24 × 100/1000 Mbps non-blocking Ethernet ports. Up to 6 × 4-port media modules with PoE, RJ45, SFP or LC interfaces		6GK6222-6PB.-.....	
		RUGGEDCOM RST2428P			Up to 6 × 4-port media modules with RJ45, SFP/SFP+, LC, FC and PoE interfaces. Up to 24 × 100/1000 Mbps or 4 × 1/10 Gbit/s SFP+ and up to 20 × 100/1000 Mbps ports	Multilayer Ethernet switch; enables higher data bandwidths with support for time synchronization	6GK6242-6PA.-.....	
		SCALANCE TAP104 for exporting entire data traffic for detection of anomalies						
	Test Access Port	SCALANCE TAP104	Industrial Ethernet		2 × RJ45 network ports 2 × RJ45 diagnostic ports	For frame export in 10/100 Mbps Industrial Ethernet networks for data analysis	6GK5104-0BA00-1SA2	
	Application	Product			Comments		Article No. ¹⁾	
Access control								
	Physical Network Access Protection	IE RJ45 Port Lock			Port lock with key for mechanical locking of RJ45 ports		6GK1901-1BB50-0AA0	
	Access Control Readers	SIMATIC RF1040R			With USB connection (1.8 m connection cable) and RS232 interface for the LF and HF range		6GT2831-6CA50	
		SIMATIC RF1060R			With USB connection (1.8 m connection cable) for the HF range		6GT2831-6AA50	
		SIMATIC RF1070R			With USB connection (1.8 m connection cable) and RS232 interface for the HF range (incl. Legic) OEM version; with neutral front film for customer-specific design; with USB connection (1.8 m connection cable) and RS232 interface for the HF range (incl. Legic)		6GT2831-6BA50 6GT2831-6BA50-0AX0	
		SIMATIC RF1140R			With RJ45 connection; Power over Ethernet, 24 V; for the LF and HF range		6GT2831-6CB00	
		SIMATIC RF1170R			With RJ45 connection; Power over Ethernet, 24 V; for the HF range		6GT2831-6BB00	
Software for control and transparent management of network access and accessories								
	Management Platform for Secured Connections and Simple Remote Access	SINEMA Remote Connect Virtual Appliance			Basic software package for 4 VPN connections; SINEMA Remote Connect Client, license key		6GK1720-1AH01-0BV0	
		SINEMA RC Upgrade OSD 64+			Upgrade with 64-1024 VPN connections		6GK1722-1VH01-0BK0	
		SINEMA Remote Connect Client V3			OpenVPN client for connecting to SINEMA Remote Connect, license key		6GK1721-1XG03-0AA0	
		SINEMA Remote Connect Client V3 (OSD)			OpenVPN client for connecting to SINEMA Remote Connect, license key, OSD (Online Software Delivery)/software download		6GK1721-1XG03-0AK0	
		SINEMA Remote Connect UMC License			License to enable the connection of the UMC server for central user management		6GK1724-2VH03-0BV0	
		SINEMA Remote Connect API License			License to enable the API interface		6GK1724-3VH03-0BV0	
		SINEMA RC IAM License (OSD)			Activation of the connection of the SINEMA RC Servers to central user management		6GK1724-7XG01-0BK0	
		SINEMA RC Layer 2 connection license			Activation of the Layer 2 option on the SINEMA RC server		6GK1724-6XG01-0BK0	
		SINEMA RC device license (OSD)			License to activate the SINEMA RC connection on a compatible SCALANCE router		6GK1724-5XG01-0BK0	
		KEY-PLUG SINEMA RC			Removable data storage medium for activating the SCALANCE M-800/ S615 connection to SINEMA Remote Connect with auto configuration		6GK5908-0PB00	
		SCALANCE CLP SINEMA RC			Removable data storage medium for activating the SCALANCE MUM85X connection to SINEMA Remote Connect with auto configuration		6GK5908-0UA00-0AA0	
	Connection to SINEMA Remote Connect with autoconfiguration							
		SCALANCE M Industrial Routers		SCALANCE M-800		Yes, with KEY-PLUG SINEMA RC	6GK8781-1.....-.....	
		SCALANCE S Industrial Security Appliances		SCALANCE S615		Yes, with KEY-PLUG SINEMA RC	6GK8751-1.....-.....	
				SCALANCE SC-600		Yes	—	
Security Communications Processors (CPs)		CP 1243-1/CP 1243-7 LTE CP 1243-8 IRC CP 1543SP-1/CP 1542SP-1 IRC CP 1543-1		Yes, firmware V3.1 or higher Yes, firmware V2.0 or higher Yes, firmware V3.0 or higher	6GK8744-0AA02-0AK0			
	Software for Network Management	SINEC NMS		Scalable Network Management System for policy-based configurations and transparent monitoring of industrial networks		6GK8781-1.....-.....		
		SINEC INS		Network infrastructure tool for central management of network services (e.g., DHCP, Syslog, NTP, RADIUS, TFTP Server)		6GK8751-1.....-.....		
		SINEC PNI Basic		Software for the rapid and simple initial setup of SCALANCE and RUGGEDCOM network components and PROFINET devices in your industrial network		—		
		SINEC PNI Professional				6GK8744-0AA02-0AK0		
	Secure Access Management Solution	RUGGEDCOM CROSSBOW		Software for managing and securing remote maintenance access for field devices according to NERC CIP standards		6GK6000-1BC43-0AA0		
		SINEC Security Inspector ⁴⁾		On-premise security test solution for IT/OT environments that determines the security status of individual components or entire production networks				