SIEMENS

Ingenuity for life

Securing your critical infrastructure

RUGGEDCOM Cybersecurity Solutions

siemens.com/ruggedcom/cybersecurity

Cybersecurity from the inside out

Every minute of downtime costs companies in a multitude of ways:

- Outages in critical infrastructure networks as technicians work to resolve communication disruptions
- Security breaches with potentially devastating impacts to public safety – and to a company's brand
- Expensive repairs from damage to equipment or systems
- Specialized IT technicians needed to reconfigure networks
- Industrial espionage or theft of intellectual property affecting the integrity of operations

Critical to your success

More than just a safe or a vault, effective cybersecurity must be a holistic approach to protecting systems against unauthorized access or attack. With billions of Internet-of-Things (IoT) devices connected worldwide, cybersecurity is crucial to the success of the digital economy.

Cyber attacks and threats have escalated and become more sophisticated with the convergence of Information Technology (IT) and Operational Technology (OT).

Automation and data-driven operations require a strong cybersecurity system to protect assets, equipment, and intellectual property while reducing downtime.

Defense in Depth

The benefits of interconnected operations also bring potential threats from web-based hackers, which can cause downtime and disruption. Threats from malware, external attacks, or a vulnerable point in a network can grind operations to a halt.

What's more, regulatory bodies often require disclosure of security breaches to ensure stakeholders are aware when personal and confidential industry information has been compromised. Being aware of potential attacks is the first step in neutralizing them, in order to meet and exceed security standards and reporting requirements.

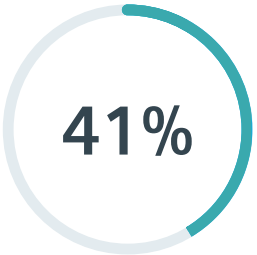
Enter Defense in Depth, an approach to digitalized operations based on the IEC 62443 standard that takes into account attacker motivations and a network's unique design to create a unified solution which protects against current and future threats.

say they are confident in their current abilities to maintain security for IIoT devices and systems

Source: The 2018 SANS Industrial IoT Security Survey: Shaping IIoT Security Concerns, July 2018

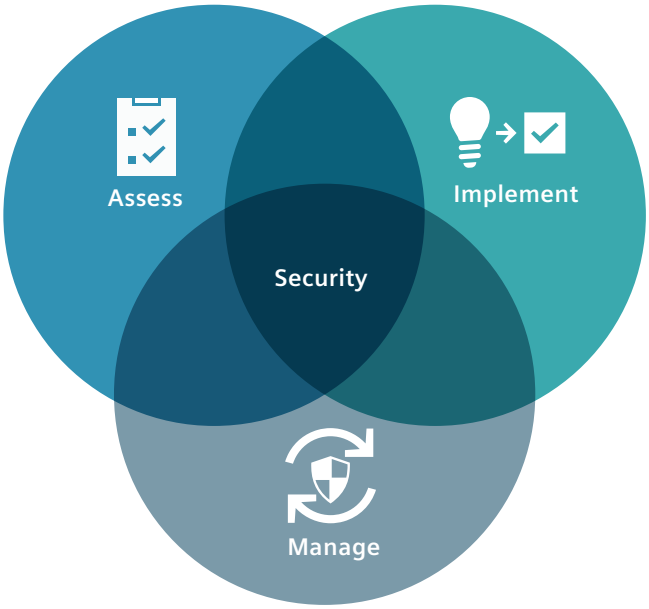
is the current estimate that cybercrime cost the world last year, or 0.8% of glo bal GDP

Source: McAfee, Economic Impact of Cybercrime – No Slowing Down, February 2018



of Industrial Control Systems (ICS) attacked at least once in first half of 2018, up from 36.6% in 2017

Source: Kaspersky Lab, Threat landscape for industrial automation systems, September 2018



A global leader in cybersecurity

As a founding member of the Charter of Trust, Siemens is a leader in advancing global cybersecurity. Signed in Munich with partners around the world, the Charter calls for binding rules and standards to build trust in cybersecurity and further advance digitalization.

With a full portfolio of state-of-the-art products, systems, and services that protect customers' data and equipment, Siemens is a reliable and preferred partner for companies which strive for the highest standards of cybersecurity.

Through a unique and multifaceted know-how as well as comprehensive technology solutions for cybersecurity, Siemens is home to industrial network experts with more than a decade of experience assessing and designing OT networks.

Assess

Assessment of the network is the first step and the key to a successful roll-out of cybersecurity solutions.

In the network assessment phase Siemens experts analyze the number of assets the customer has. This assessment also provides insights into security vulnerabilities of customer's network.

Implement

After working to understand security needs and risks, Siemens implements a new security regime. More than just an out-of-the-box security system on top of operational technologies, everything companies do should be 'secure by design'.

Before adopting a new system, Siemens assists in design and deployment of a security solution to ensure a smooth transition. This includes pre-configuration and testing services as well as training so staff can hit the ground running and play their part in secure operations.

Manage

Managing the security of a network means staying on top of key areas: monitoring threats, keeping security solutions up to date, and ensuring quick reaction times to identify threats.

Keeping network secure does not stop with the implementation of cybersecurity solutions. In the managing phase customer manages the deployed cybersecurity solution by maintaining the software and signatures up to date.

RUGGEDCOM cybersecurity solutions

Comprehensive cybersecurity solutions on the RUGGEDCOM hardware platform detect potential attacks, reduce their severity, lower costs, and ensure compliance with a growing number of regulations.

Siemens offers cybersecurity solutions installed on the RUGGEDCOM Multi-Service Platform product family of cost-efficient, utility-grade Layer 2 and Layer 3 switches and routers – designed for harsh environments and mission-critical applications. This is combined with comprehensive network consulting services, on-site support, security assessments, integration, deployment, and training.

Siemens has collaborated with leading minds in industrial cybersecurity to bring bundled solutions with certified partner applications.

Third-party applications from leading cybersecurity companies available on RUGGEDCOM devices provide more options for addressing various security challenges.

Taking into account region-specific preferences to cybersecurity, Siemens helps create an ecosystem of comprehensive and reliable solutions customized to customers' needs. With no scheduled maintenance required and 24/7 availability, RUGGEDCOM products provide critical infrastructure access and peace of mind security.

Using RUGGEDCOM cybersecurity solutions, Siemens customers can establish an electronic security perimeter around their critical infrastructure to prevent the disruption of mission-critical applications by accidental or malicious acts.

Stateful Inspection Firewall

Stateful inspection firewall to control traffic between different zones of trust within a network. Includes Network Address Translation (NAT) to prevent unauthorized or malicious activity, initiated by outside hosts, from reaching the internal Local Area Network (LAN).

Virtual Private Networking (VPN)

Provides secure communication links over networks. Ensures confidentiality, sender authentication, message integrity, and uses IPSec (IP Security) for encryption and authentication of all IP packets at the network layer.

Strong encryption

Utilizes latest encryption algorithms for authorization, authentication and privacy. Examples include TLS and SSH at upper protocol levels, RSA and ECC for public key encryption, and 3DES and AES for stream encryption.

RUGGEDCOM Multi-Service Platform

The Multi-Service Platform product family of utility-grade Layer 2 and Layer 3 switches and routers has been specifically developed to provide multiple electronic defense layers for the protection of critical cyber assets. RUGGEDCOM Multi-Service Platform is the main point of entry between the local area network (plant floor or substation) and the outside world. The platform combines a Layer 3 router, a firewall, and a VPN in one device.

RUGGEDCOM Application Processing Engine (APE)

RUGGEDCOM RX1500

RUGGEDCOM RX1500

RUGGEDCOM's RX1500 series is a family of utility-grade Layer 2 and Layer 3 switches and routers. The RX1500's modular and field replaceable platform allows customers to select amongst Wide Area Network (WAN), serial, and Ethernet options, making it ideally suited for utilities, industrial plant floors, and rail and traffic control systems.

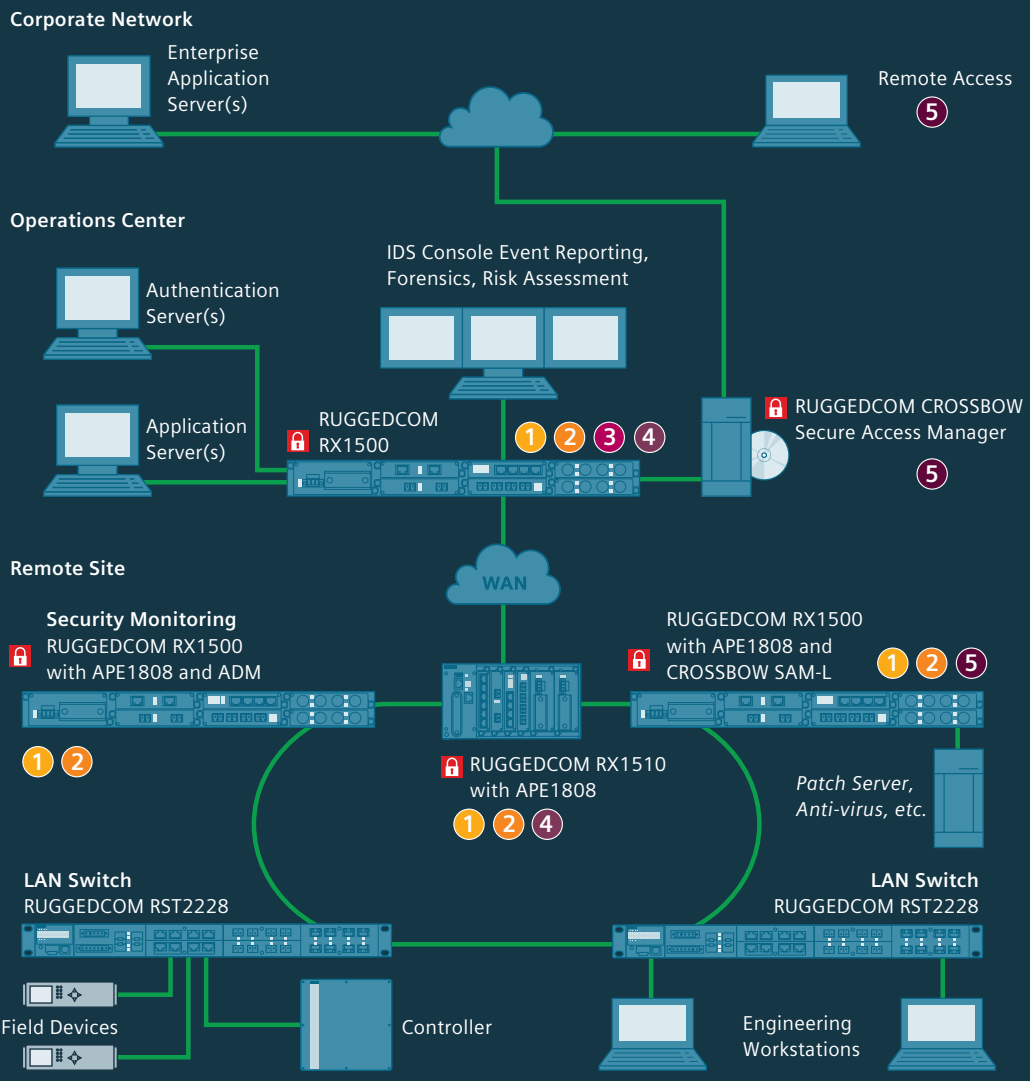
These field-proven, industry-leading devices have been coupled with cybersecurity applications to offer customized solutions of various security levels. Field-swappable modules guarantee flexibility and easy maintenance for critical applications and are certified for use in the harsh environments of electric power, transportation, and oil and gas industries.

RUGGEDCOM Application Processing Engine (APE)

The new version of the industrial application hosting platform – RUGGEDCOM APE1808 – is ideal for safely running third party software applications in harsh, mission-critical environments.

The module plugs directly into any member of the RUGGEDCOM RX1500 family, except for the RX1512, without the added complications of installing an external industrial PC. RUGGEDCOM APE1808 excels at hosting a range of applications such as next generation firewalls, network log and load processors, and intrusion sensors. Based on Intel quad core and x86_64 architecture with support for Linux and Windows 10, the RUGGEDCOM APE1808 provides a standards-based platform for commercially available software, enabling partnerships with industry leaders in cyber threat detection and prevention.

RUGGEDCOM cybersecurity solutions installed on the RUGGEDCOM Multi-Service Platform designed for harsh environments and mission-critical applications.



Industrial Ethernet

1 Anomaly-based Intrusion Detection System (IDS)

2 Deep Packet Inspection (DPI)

3 Intrusion Prevention System (IPS)

4 Next Generation Firewall (NGFW)

5 RUGGEDCOM CROSSBOW – Secure Access Control

RUGGEDCOM CROSSBOW – Secure Access Control

RUGGEDCOM CROSSBOW is a secure access management solution designed to provide assistance with cybersecurity compliance including NERC CIP (North American Electric Reliability Corporation critical infrastructure protection) and IEC 62443-1 access to Intelligent Electronic Devices (IEDs). The CROSSBOW solution focuses on delivering productivity gains for administrators and users while assisting with cybersecurity compliance in managing, securing, and reporting on remote access.

The RUGGEDCOM CROSSBOW system consists of a central server along with a number of clients connecting securely with TLS 1.2 – typically the user's desktop or laptop computers. The server contains the system database, based on Microsoft SQL Server, and manages all connections from the clients to the remote IEDs. The central server supports a high availability cluster configuration for increased reliability.

With administrator defined Role Based Access (RBA), CROSSBOW provides activity logging and data privacy as users connect to remote Intelligent Electronic Devices (IEDs). Operators are guaranteed a secure connection to field devices without going on-site or entering an application, allowing them access to devices from the comfort, convenience, and safety of the control room. Strong two-factor authentication through RSA SecurID, Active Directory, and RADIUS ensures the highest in process security.

In addition to secure access, the RUGGEDCOM CROSSBOW solution provides automated functionality for device password management, configuration and firmware version monitoring, remote connectivity verification, and data file retrieval.

Anomaly-based Intrusion Detection System

Non-Intrusive, anomaly-based signatureless Intrusion Detection System (IDS) software for mission-critical operational networks, operating on RUGGEDCOM hardware, provides early-warning notification and alerting on vulnerabilities and sophisticated cyber threats that may be undetectable by conventional IT security tools.

Deep Packet Inspection

Deep Packet Inspection (DPI) on the RUGGEDCOM RX1500 with the APE1808 examines data packets utilizing a non-intrusive methodology for mission-critical networks focusing on OT protocols (such as Modbus and DNP3) searching for potential non-compliance traffic, viruses, spam, intrusions, or user-defined criteria to determine whether the packet may pass or if it needs to be routed to a different destination for cybersecurity analysis and mitigation helping to secure communication to control centers and IT networks.

Next Generation Firewall

Utilizing a combination of RUGGEDCOM switching and routing platform, with leading Next Generation Firewalls (NGFW) functionality on a single, integrated appliance, provides for additional integrated DPI/IPS functionalities, offering security when connecting non-critical IT networks, to critical deterministic operational networks.

Intrusion Prevention System

An Intrusion Prevention System (IPS) is a capability available on the RUGGEDCOM hardware if equipped with a NGFW solution. IPS is located between the WAN and the LAN to deny the traffic that represents known threat based on a security profile.

Siemens professional services

From assessment, pre-configuration and testing services to implementation and training, Siemens has it covered.

Siemens professional services team offers:

- Discovery and analysis of the existing network assets and network architecture
- Vulnerability assessment of the network by assessing the existing security features and providing a security assessment report with recommendations on how to improve the security
- Design and deployment of security solutions and security training of the stakeholders

Published by
Siemens AG

Digital Industries
Process Automation
Östliche Rheinbrückenstr. 50
76187 Karlsruhe, Germany

For the U.S. published by
Siemens Industry Inc.

100 Technology Drive
Alpharetta, GA 30005
United States

Article No.: DIPA-B10050-00-7600
Dispo 06366
WS 08192.0
Printed in Germany

siemens.com/ruggedcom/cybersecurity

Security information

Siemens provides products and solutions with industrial security 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 security concept. Siemens' products and solutions only form one element of such a concept. Customer is responsible to prevent unauthorized access to its plants, systems, machines and networks. Systems, machines and components should only be connected to the enterprise network or the Internet if and to the extent necessary and with appropriate security measures (e.g. use of firewalls and network segmentation) in place. Additionally, Siemens' guidance on appropriate security measures should be taken into account. For more information about industrial security, please visit

siemens.com/industrialsecurity

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

To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed under

siemens.com/industrialsecurity