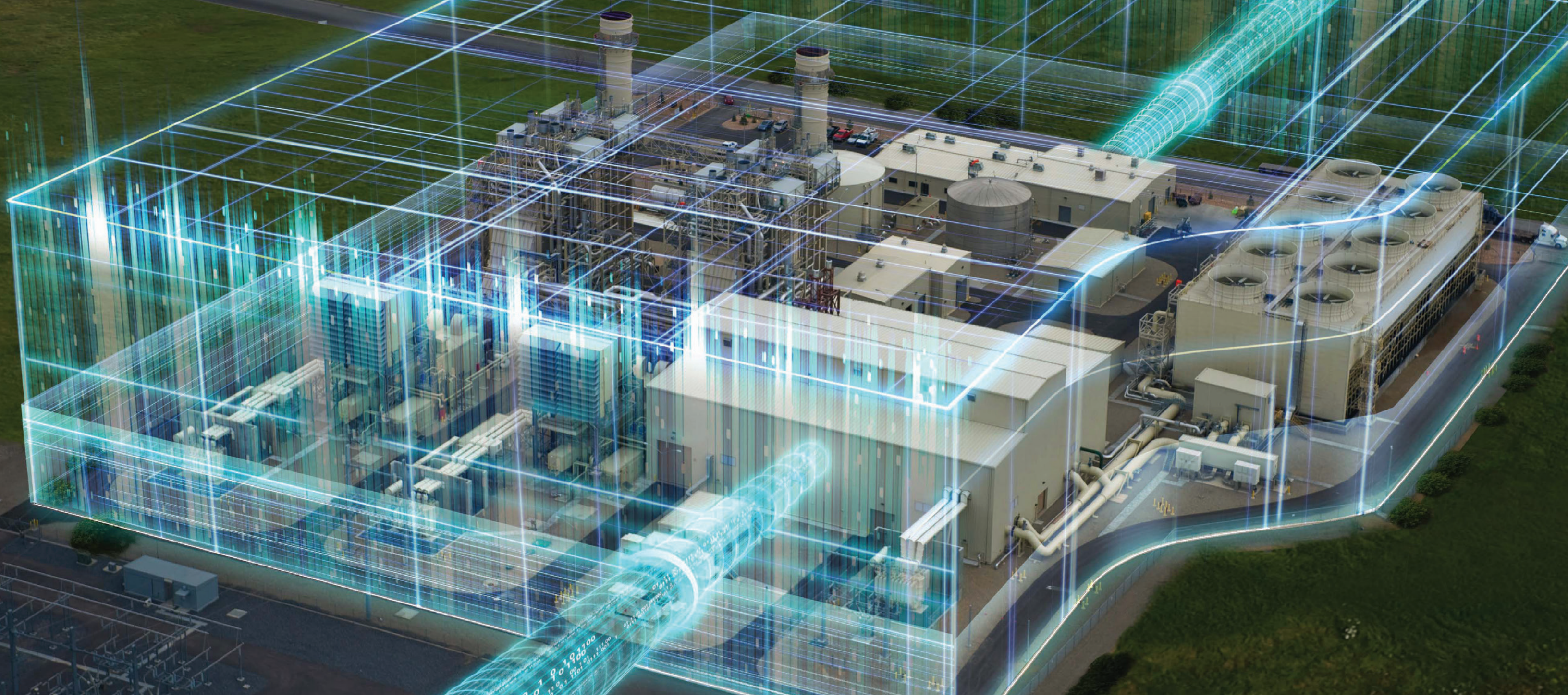


SIBERprotect™ delivers a rapid automatic cyber response solution for Operational Technology (OT) systems.

usa.siemens.com/industrial-cybersecurity

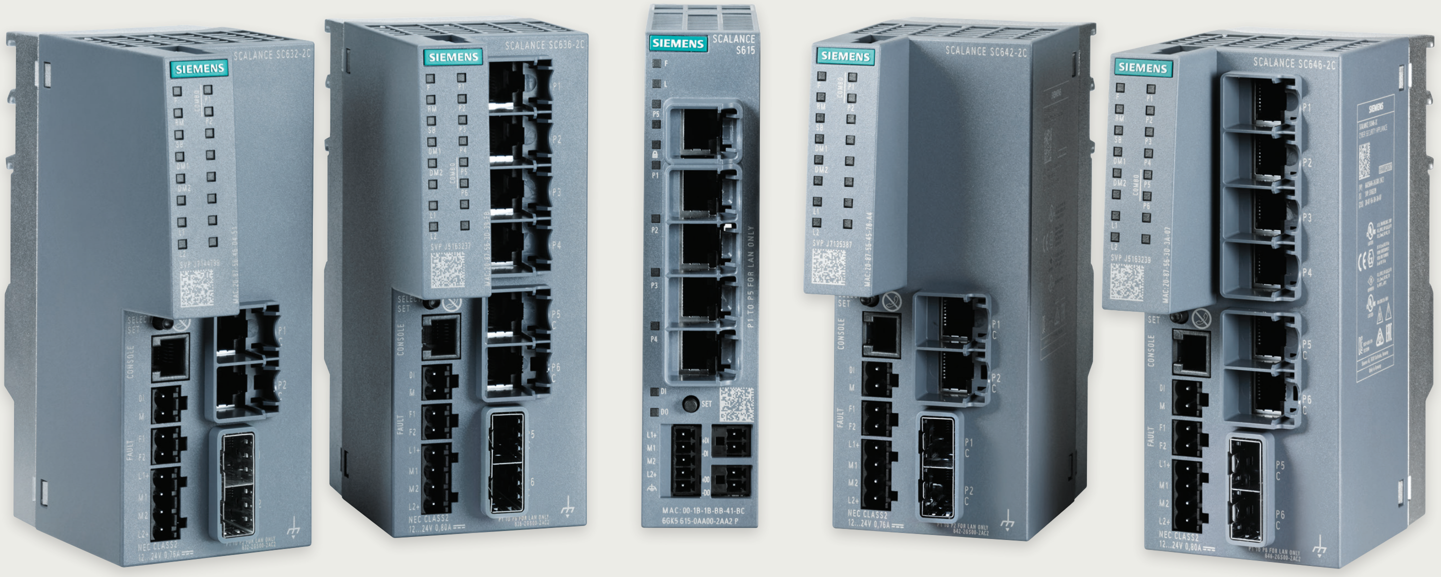
SIBERprotect is the most advanced, real-time cyber attack monitoring and response solution for OT systems. From critical infrastructure such as power plants and water treatment facilities to military depots, data centers and operations centers, SIBERprotect can respond to and dramatically limit the impact of a cyber attack within milliseconds at machine speed.If your facilities rely on OT (which virtually every one does), SIBERprotect is absolutely essential to the success of your mission.

The Next Cyber Attack is a Millisecond Away…

Cybercrime related damage is projected to reach $6 trillion annually by 2021, as concerns for cybersecurity risks are increasing. Cyber attacks are constantly on the rise, putting missions, and lives at risk. Now more than ever, it is crucial to be proactive, and protect your military installations and industrial sites with a fast and reliable technology: SIBERprotect.

The WannaCry ransomware attack infected approximately 230,000 computers globally. The ransomware spread to computer systems in 150 countries. In one specific instance, a site with 25 automation controllers required more than 2,000 working hours to eradicate and remediate all of the IT and OT computer systems in the facility. SIBERprotect allows for the ability to isolate and quarantine the infected production equipment groups and would have enabled full remediation and resumption to normal operation in less than a day.

SIEMENS



SIBERprotect works in conjunction with SCALANCE S industrial security appliances.

SIBERprotect in Operation

SIBERprotect can securely place OT into a safe state, isolated or quarantined, on credible identification of a cyber attack from advanced cyber threat detection technology provided by Next Generation Firewalls, Endpoint solutions, Threat/Risk intelligence, etc. These technologies, some enhanced with machine learning capabilities, are used to inform the SIBERprotect implementation of a credible cyber attack or operational threat. SIBERprotect then initiates a rule-based equipment management sequence to protect selected equipment and initiate other desired response actions. Rapid assessment and remediation can then be performed on prioritized equipment groups, limiting the risk of contamination. SIBERprotect provides situational awareness while simultaneously initiating emergency measures so the facility can cope better with worst case scenarios.

Advantages

SIBERprotect automation technology responds in milliseconds. SIBERprotect operates independent of the site network. Upon receiving a cyber attack notification, SIBERprotect performs a strategically predetermined automatic action sequence. SIBERprotect simultaneously provides notification of the cyber attack via lights, sirens, emails, and text messages. SIBERprotect can be activated manually by a security officer.

Key Features

- Automatically activates emergency backup equipment
- Provides a “panic button” activation capability
- Works with modern technology (e.g. AI and machine learning)
- Works with older technology (e.g. Ethernet hubs)
- Recovery can be one segment at a time or a “restore all” function
- Isolated from the site IT network to prevent being attacked
- Uses technology that OT personnel understand
- Has all the benefits of an industrial solution (speed, reliability, determinism, availability)

SIEMENS

SIBERPROTECT™

Exceptionally Fast Response Times

SIBERprotect uses SIMATIC automation technology with millisecond response times and executes independently of the site's infrastructure.

Automatic Action

SIBERprotect uses rule-based processing to determine response actions based on the requirements of each facility. Following the detection of an attack, the system uses OT to activate firewall rulesets in security devices using digital outputs, or, can manage legacy networks by controlling the power to network devices. The system can then perform emergency response actions to prepare the facility defense, continued operation, and remediation. All responses are configurable using administrator privileges on the SIBERprotect Human Machine Interface. In the event of a coordinated attack, SIBERprotect can interact with other sites using appropriate communication technology to ensure enterprise-wide security and protection.

Why SIBERprotect?

SIBERprotect provides sub-second response to a cyber attack after notification from configured real-time sources. It's ability to interact safely with existing controllers and equipment and across sites allows for warning of coordinated attacks while isolating network segments to stop the spread of malware and prevent intruder access. With SIBERprotect, work cells and equipment groups are able to continue operation while preventing recontamination during remediation. SIBERprotect helps speed remediation by simplifying the process of safely restoring systems in the desired priority order.

Reliable Attack Detection Mechanism(s)	Equipment Grouping	Network Topology
• Next Generation Firewalls • Deep packet inspection • Intrusion detection • Intrusion prevention • Security/site alarms and other status • Threat/Risk Intelligence sources • AI/Machine learning applications • Endpoint device protection with messaging • Optional Messaging server	• Individual machines • Dependent machine groupings/cells (machines that require interactivity) • Emergency/backup equipment/grouping(s)	• Separation of IT and OT networking layers • Protected interfacing network components (i.e. Next Generation Firewall(s) between IT and OT) • Protected networking interface component for each machine or machine group • Protected connectivity to emergency equipment

Legal Manufacturer

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

usa.siemens.com/industrial-cybersecurity

Order No. NTBR-SIBER-0522

This document contains a general description of available technical options only, and its effectiveness will be subject to specific variables including field conditions and project parameters. Siemens does not make representations, warranties, or assurances as to the accuracy or completeness of the content contained herein. Siemens reserves the right to modify the technology and product specifications in its sole discretion without advance notice.

SIEMENS