Cybersecurity Application Platform

Implementing cybersecurity controls

All companies want to leverage digital solutions and realize the benefits from the efforts of their digital transformation journey. For these benefits, companies need to consider and address cybersecurity. Increased digitalization increases the cybersecurity attack surface. An effective approach to cybersecurity is to leverage best practices and standards for your industry.

A proven approach to addressing cybersecurity is to align to standards such as IEC 62443, NIST, etc. These standards provide a phased approach to addressing cybersecurity in a structured manner. The Cybersecurity Application Platform (CAP) is designed to support customers in implementing cybersecurity controls and best practices, which ultimately leads to aligning to regulatory and governance requirements.

Key benefits

- **Reduces complexity** with one platform to monitor and maintain cybersecurity controls.
- CAP packages structured to **align to the IEC 62443** requirements.
- **Reduces time** and effort required **to perform maintenance tasks.**
- Data collected within the dashboard **allows customers to make data driven decisions** from actionable intelligence.
- Ongoing services to **improve cybersecurity posture.**
- **Flexible platform** that will allow customers to add on capabilities as new modules are created.

se.com/cybersecurity

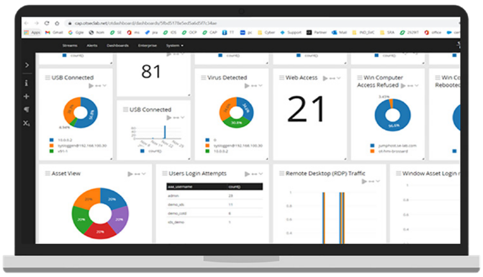
Life Is On | Schneider Electric

The CAP is an integrated cybersecurity solution that allows operations teams to have visibility to key cybersecurity data and take action to manage/maintain their cybersecurity control points. By having one platform, customers can save time and money aligning to cybersecurity standards and best practices and strengthen their OT security posture.

CAP is great solution for customers that are dealing with the following challenges:

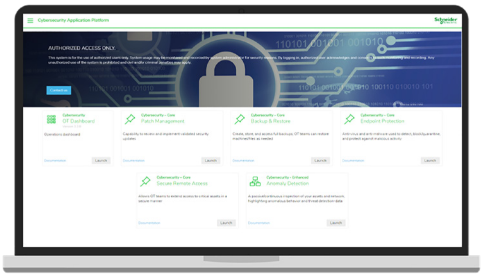
- Operations team responsible for performing cybersecurity maintenance activities – looking to optimize time and looking for simplicity in implementing controls.
- Limited resources with both IT and OT cybersecurity expertise.
- Looking to optimize cybersecurity budgets by optimizing routine cybersecurity maintenance.
- Are required or aim to meet cybersecurity regulatory requirements.

The CAP offering has three elements:



1. The Cybersecurity OT Dashboard

consolidates cybersecurity KPIs and data into an easy to read format. It also provides the visualization and data analysis to drive decision making.



AUTHORIZED ACCESS ONLY.

This system is for the use of authorized users only. System usage may be monitored and recorded by system administrator for security reasons. By logging in, authorized user acknowledges and consents to such monitoring and recording. Any unauthorized use of the system is prohibited and civil and/or criminal penalties may apply.

Cybersecurity
OT Dashboard
Operations dashboard

Cybersecurity – Core
Patch Management
Capability to review and implement validated security updates

Cybersecurity – Core
Backup & Restore
Create, store, and access full backups; OT teams can restore machines/files as needed

Cybersecurity – Core
Endpoint Protection
Anti-virus and anti-malware used to detect, block/quarantine, and protect against malicious activity

Cybersecurity – Core
Secure Remote Access
Allows OT teams to extend access to critical assets in a secure manner

Cybersecurity – Enhanced
Anomaly Detection
A passive/continuous inspection of your assets and network, highlighting anomalous behavior and threat detection data

2. The CAP Tiers – (Core, Enhanced, Optimized)

Each CAP tier allows you to take a required action such as completing a backup or performing patch management.

Our tiers provide flexibility in the level of security controls allowing you to match the CAP to your SAL requirements.

3. CAP services

Our CAP delivery includes configuration, technical support and maintenance of the CAP solution. Additionally, the monitoring aspect of the package provides insights to improve your security posture over time.

The CAP Packages

The CAP packages are aligned to IEC 62443 Security Assurance Levels (SAL). Each package has a hardware, software, and service components. The details on the packages are below:

	Core (SAL 1)	Enhanced (SAL 2)	Optimized (SAL3+)
Hardware	• Optional	• Optional	• Optional
Software	• Endpoint protection • Patch Management • Backup & Recovery • Authentication/Authorization • Secure Remote Access (enabler)	• Anomaly Detection + Asset Inventory • Multi-factor Authentication • Event/log collection and correlation (SIEM plug-in) • Network Performance Monitoring	• Threat Intelligence • Vulnerability management • Incident Response • Managed Service Platform
Service	• Delivery, maintenance, reporting • System Hardening (Optional)* • Network Segmentation (Optional)*	• Delivery, maintenance, monitoring • Custom Consulting Services	• Continuous managed services • Delivery, maintenance, monitoring • Pen testing (Optional) • Incident response tabletop exercises

* optional if already completed

The capabilities within the CAP packages provide controls aligned to the security levels of IEC 62443 when implemented as part of a cybersecurity program.

Experienced, capable, and globally available

Schneider Electric's global team of cybersecurity experts understand the unique needs and challenges for OT systems and technologies. Our focus is on finding solutions that fit your unique requirements, regardless of the systems you use.

Our experts will work with you to understand your requirements and help implement and customize the right level of security to meet your specific needs. We work with leading cybersecurity product experts to bring the right solution to your operation to ensure that your people, processes, and technologies are protected.

Contact us today to learn more about our Cybersecurity Assessment Services and our full range of solutions that can support your needs for cybersecurity protection across all business types and industries.

se.com/cybersecurity

Life Is On | Schneider Electric

Schneider Electric Industries SAS
35, rue Joseph Monier - CS 30323
F92506 Rueil-Malmaison Cedex