



SECURE

Cybersecurity for your digital transformation

Services and solutions from Schneider Electric

se.com/cybersecurity

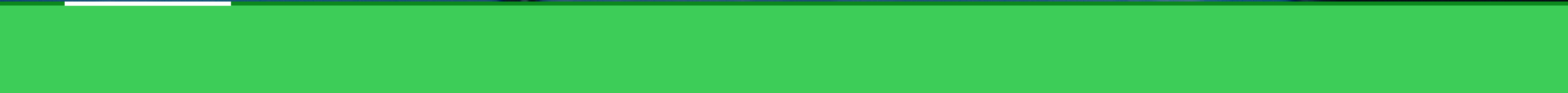
Life Is On

Schneider
Electric

Table of contents



The value of cybersecurity



Securing your digital transformation

With the increasing use of digital technologies such as cloud computing, mobile, the Internet of Things (IoT) and artificial intelligence, the world is more connected than ever. But besides new opportunities, greater connectivity also brings new challenges and increases vulnerability.

Cyber threats and incidents are a major operating and business risk for every digital enterprise. In the age of digitization, creating and executing a strategy that allows you to see, reduce, and respond to cyber threats and risks is critical. It's the only way to secure your operations and achieve your financial objectives.

Growth in IoT connected devices by 2030

6x
IoT Device Growth
between 2020-2030

32.1 billion
connected IoT
devices in 2030

Sources:
Statista, Schneider Research Institute

**Want to learn
more about the
latest trends in
cybersecurity?**

Visit our
cybersecurity blog

Growing cybersecurity threats

With businesses relying more on the internet and connected assets, cyber attacks have become a constant threat to companies in every industry. That's why most enterprises have come to understand the importance of having a cybersecurity strategy in place.

97%

of organizations have gaps in its cloud risk management plan.

Source:
PWC 2024 Security at the epicenter of innovation

\$23.84 trillion

Cybercrime losses expected by 2027

Source:
Statistica 2024 Cybercrime Expected To Skyrocket in Coming Years

43%

of CISOs reported breaches causing unplanned downtime, highlighting business continuity as the top cyber attack risk

Source:
PENTERA

58%

of organizations consider their exposure to cyber attack high or very high

Source:
Hiscox 2022 Cyber Readiness

Services and solutions for all industries



The three pillars of cybersecurity

Any cybersecurity strategy is only as strong as its weakest link. That's why it is fundamental to identify and mitigate risks by applying standards and good practices throughout the whole line of defense which must integrate people, processes, and technology.



Strong cyber protection requires an educated and aware workforce. In many cases, your people are your first and last line of defense. A crucial element of this area is creating and communicating a company-wide security culture, advanced by ongoing training.



In order to identify and eliminate cyber risks, you need to establish and adhere to good processes, practices, and policies. Companies should begin with consistent, regular risk and threat assessments and gap analyses.

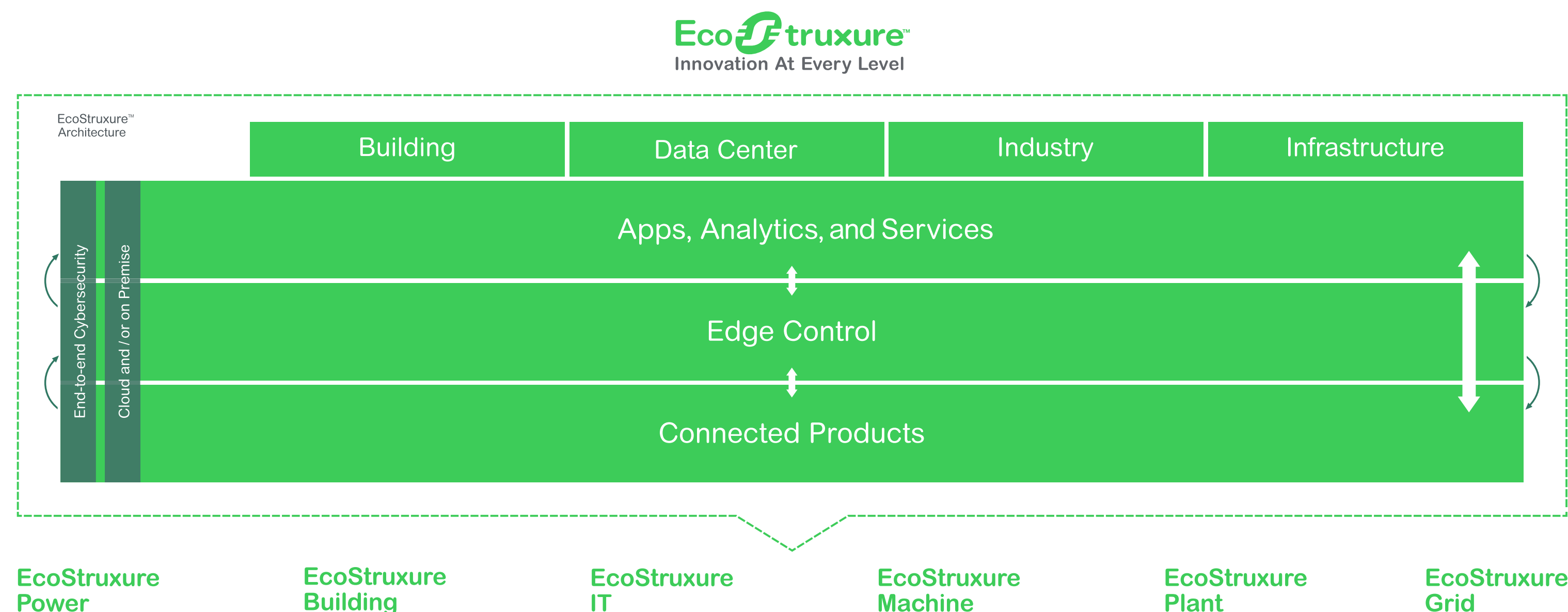


Your cyber defense is only as strong as the technology deployed to manage and control your operations. This aspect is all about protecting what your company develops and deploys, as well as ensuring that the technology coming from your supply chain vendors is secure.

Cybersecurity at every level

As a manufacturer itself, Schneider Electric embeds security throughout its vendor-neutral, open, IoT-enabled architecture and platform: EcoStruxure™. It includes an open but tailored stack of connected products; edge control level solutions and software; and cloud-based apps, analytics, and services.

End-to-end cybersecurity supports applications and data analytics, embedded across these layers, which converge IT and OT equipment and solutions, software, and services within six domains of expertise.



A defense in depth approach

Companies expect that the products they buy include everything necessary to mitigate cybersecurity risks. But the products alone are only a starting point. The way the systems are implemented and integrated into your environment is also critical. The processes for implementation and integration of systems must protect the integrity of your environment.

Once the systems are operational, many other aspects must be considered as part of the overall operation, depending on your risk assessment. These range from simple firewalls to network segregation and testing.

Besides that, there are dedicated services that provide an objective perspective and broader experience in reviewing or developing your solution design, training your team, or even providing an ongoing managed security service.

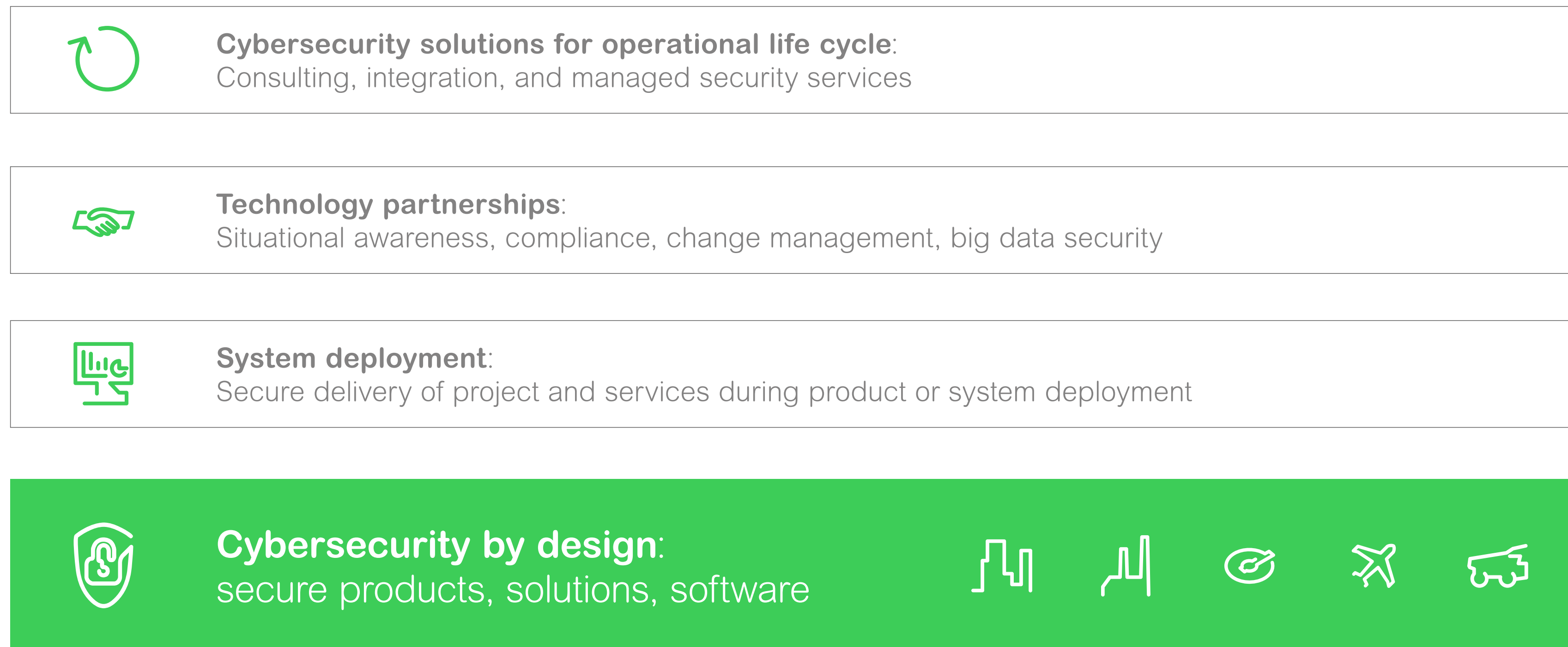
Serious about cybersecurity?

[Sign up for the Schneider Electric Cybersecurity Virtual Academy](#)



Addressing cybersecurity challenges on multiple levels

Effective cybersecurity encompasses your entire OT environment – from products and systems through to ongoing services



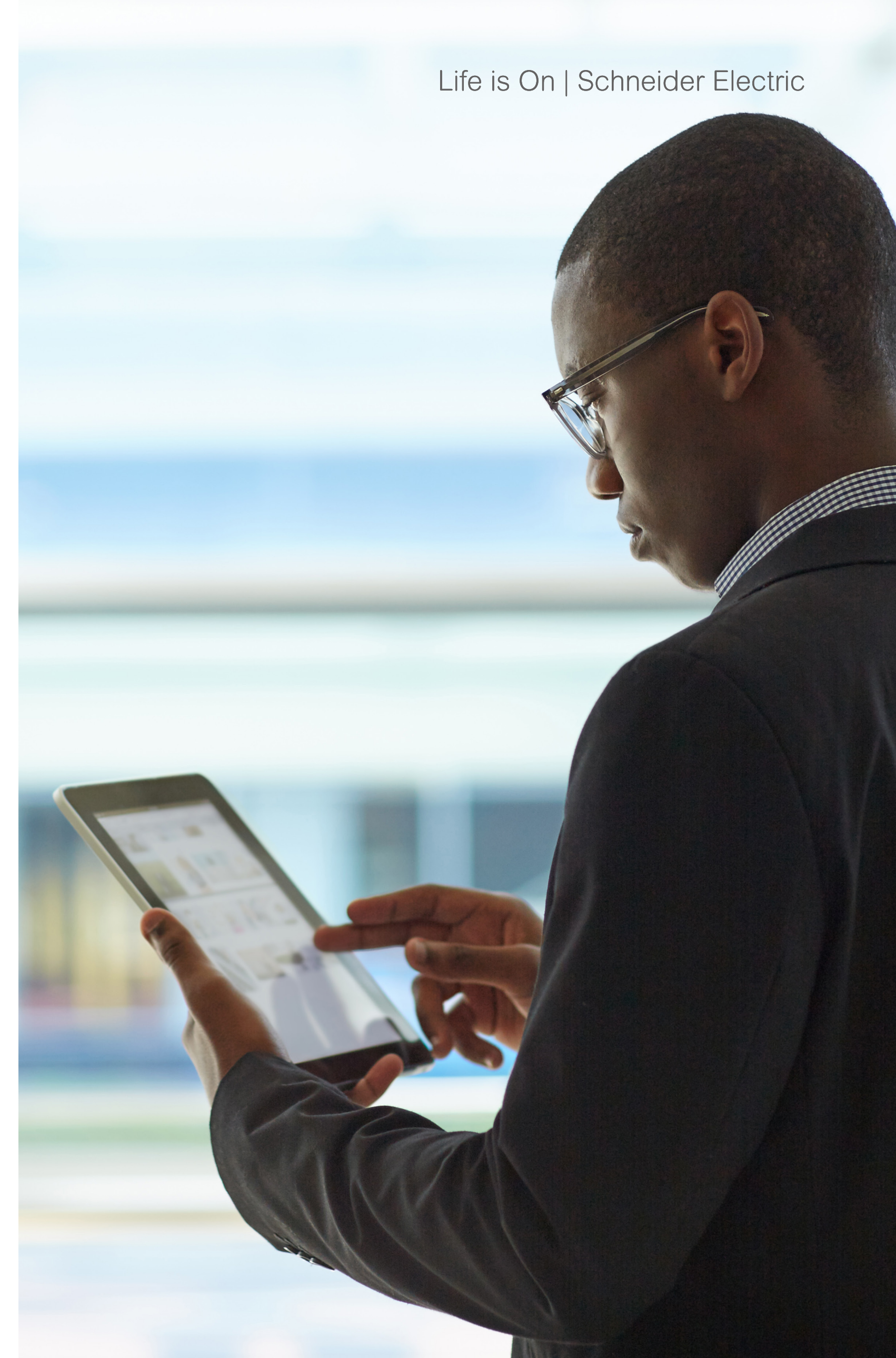
Defense in depth approach

Our 360° cybersecurity solutions include:

- A certified team of cybersecurity experts who understand your process requirements, enterprise needs, and business environment.
- A dynamic ecosystem of partnerships and platforms including governments, universities, and suppliers that help drive research, policy, and collaborative projects to produce a holistic, security-conscious offering.
- An ISO conformant vulnerability management process that is activated upon external notification, vulnerability disclosure, or customer report.
- An advanced global threat intelligence center that actively monitors cyberspace for threats to our products and customers.
- 150+ products that are cybersecurity standards certified for electrical and process installations.

**Want to learn more about
our cybersecurity solutions?**

[Visit our YouTube channel](#)



A photograph of two men in an office setting. One man with a beard and a bun is sitting at a desk with a laptop, looking intently at the screen. Another man with curly hair is leaning over his shoulder, also looking at the laptop. The scene is dimly lit, with a window in the background. The text 'End-to-end cybersecurity' is overlaid in white on the image.

End-to-end cybersecurity

Global cybersecurity standards

Products guided by the ISA / IEC 62443-4-1 standard address security from the very beginning of product development through the life cycle. This standard is employed within Schneider Electric services and solutions.

Schneider Electric is a founding member of ISA Global Cybersecurity Alliance.

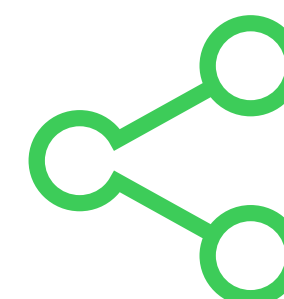


ISA / IEC 62443-4-1 Standard

World's only consensus-based standard for automation and control system applications



Flexible framework to address and mitigate current and future security vulnerabilities



Defines requirements and procedures for implementing secure systems



Leverages a holistic approach, bridging the gap between operation and information technology, as well as between safety and cybersecurity

Our solutions for your operational life cycle

Schneider Electric is committed to providing solutions that support your needs for cybersecurity protection across all business types and industries. We apply a rigorous mindset, policies, and methodologies in the development of our products and the implementation of our solutions.

Skilled and certified professionals provide vendor-agnostic services to help you assess your risk, implement cyber-specific solutions, and maintain your defenses over time at your location.

Security Consulting

- Policy and procedure
- Asset inventory
- Gap analysis
- Risk and threat
- Compliance

Design & Implementation

- Defense in depth
- Secure architecture
- Asset management
- Security assurance level
- System hardening
- Solution integration

Training

- Security awareness
- Security engineer
- Security administrator
- Advanced expert

Monitoring

- Firewall Security
- Device Management
- Threat Management
- Device Security
- OT SIEM Support

Maintenance

- System upgrades
- Security patches
- Incident response



Our solutions for your operational life cycle

Security Consulting

Our cybersecurity consultants will help you assess and review your systems to detect gaps, risks, uncover any security malpractices, assess your staff's security competencies, provide emergency response services, and more.

Design & Implementation

With an understanding of your unique needs, requirements, and knowledge of best practices and industry standards, our engineers can design, develop, and implement an effective security architecture. We help protect your critical infrastructure through a 'defense in depth' based security

approach that can be customized to meet your needs, from elements of basic SL-1 compliance to a comprehensive solution.

Monitoring

The cybersecurity solutions will be monitored to detect threats, apply patches as well as to ensure the smooth functioning of devices and the system as a whole.

Maintenance

It is critical to continually review and update your cybersecurity protection. We work with your team to ensure that your systems and skills are up-to-date and tested regularly to maximize your security and peace of mind.

Training

People are the most important element in ongoing, effective cybersecurity protection. Designing and delivering effective training for different roles in your organization is critical. From basic awareness to expert-level skills, our team can help you develop your company's cybersecurity culture by designing and delivering a range of training and education.

Cybersecurity solutions portfolio





The solutions we design and implement are flexible and customized to meet your specific needs and requirements. The most critical cybersecurity solution elements are defined in four categories.

Permit – manage access to operations systems and information through network and physical controls.

Protect – implement specific controls as part of the operations systems for ongoing protection.

Detect – monitor the operating environment to detect and communicate threats.

Respond – develop procedures and systems to support rapid response to cyber incidents to contain and mitigate attacks.

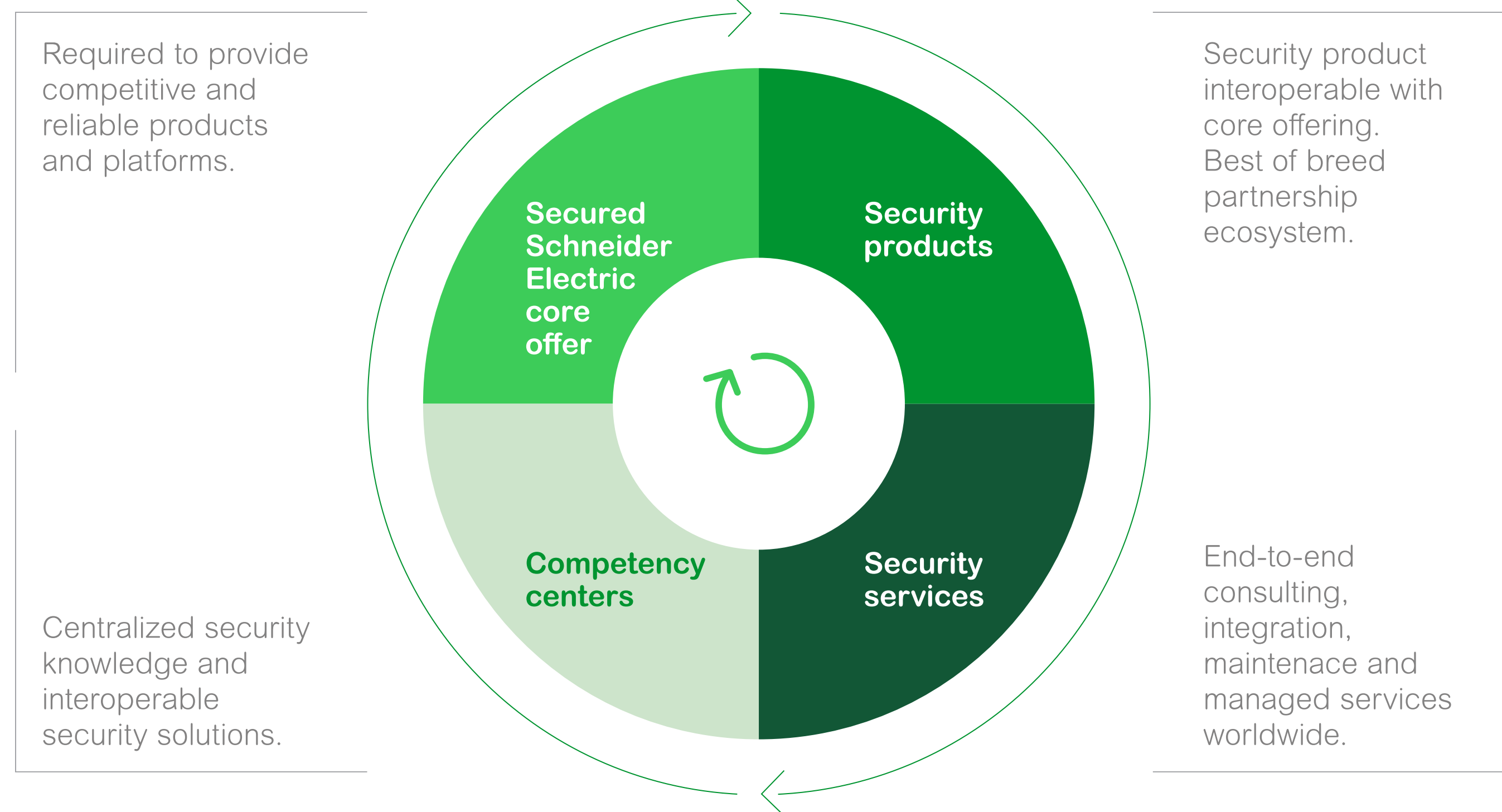
 Permit	 Protect	 Detect	 Respond
<ul style="list-style-type: none"> • Authentication, Authorization, Accounting • Multi-Factor Authentication • Network Segmentation • Secure Remote Access • Physical Security 	<ul style="list-style-type: none"> • Endpoint Protection, Anti-malware, • DLP, HIPS, Whitelisting • Removeable Media Control • Patch Management • Managed Security Services 	<ul style="list-style-type: none"> • Security Information & Event Management (SIEM) • Network Performance Monitoring • Asset Identification • Anomaly Detection • Intrusion Detection 	<ul style="list-style-type: none"> • Backup / Disaster Recovery • Forensics • Incident Response

Cybersecurity for the digital age

Whether you're not sure where to start, or need help to implement a cybersecurity strategy, our experienced and qualified experts will work with your unique situation and requirements to help address your cybersecurity challenges with solutions that fit your needs.

We understand and apply cybersecurity solutions from your operations perspective while integrating appropriate IT policies and requirements – this is our difference and your advantage.

Our 360° Cybersecurity Solutions



Managed Security Services

Schneider Electric's 24x7 Managed Security Service offers contextualized vulnerability management, threat monitoring, incident response support, and customer-relevant threat intelligence.

Core Service Outcomes

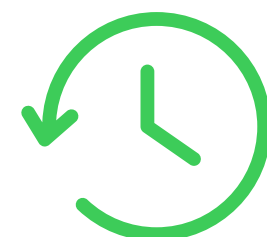
- 24x7 Security Coverage
- IT-OT Security Synergy
- Consistently meet compliance
- Have a trusted advisor in your back pocket



Core	
Assets Management	Asset Inventory and Visibility
Vulnerability & Risk Management	Vulnerability Analysis
Threat and Incident Management	Threat Detection and Response
Cybersecurity control Management	Cyber Devices Health Monitoring
Compliance Management	Regulation Compliance Reporting
CS Performance Management	KPI and Reporting
Security Platform Maintenance and technical support	



Immediately Improve Security Posture

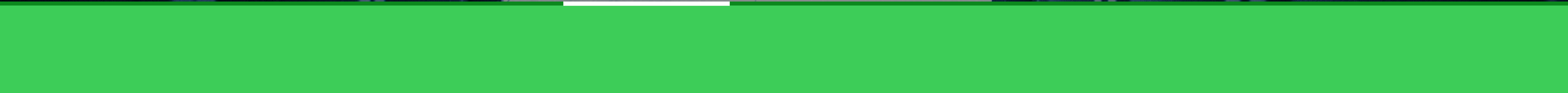


Accelerate Time to value



Reduce Mean Time to Detect and Respond

Global partners and presence



A rich ecosystem of partners

Every company today must leverage an extended enterprise approach to address and eliminate vulnerabilities. The advantage of an open ecosystem is that it can be enhanced by solutions from other industry-leading vendors. That's why Schneider Electric works with our global partners to deliver the best possible products, services, and solutions.



Global reach

Schneider Electric has a rapidly growing global team focused on cybersecurity. We leverage a strong IT experience and deep knowledge of the OT world to help customers understand what they have today and where the biggest gaps are in managing cybersecurity.

Our quick reaction team is ready to help our customers act quickly in case of a cyber attack – to assess potential damages and recover.

Schneider Electric is a proud member of:

- ISA Global Cybersecurity Alliance
- Cybersecurity Coalition
- Cybersecurity Tech Accord



Team certifications



Increasing cybersecurity across industries

No matter which industry you operate in, Schneider Electric can help you implement an overarching cybersecurity solution. Our vast expertise covers all industries from Food & Beverage to Oil & Gas and Petrochemicals.



SITE #1

(France – Leading food production company)

Cyber offering:

- IT / OT integration
- DMZ implementation
- Design and deploy secured architecture
- Global user management system, network monitoring

Success factor:

- Customized solution meeting customer's global operation demands
- Centralized host and network solutions meeting industry and national standards



SITE #2

(Qatar – LNG leader in the Middle East)

Cyber offering:

- Cybersecurity Demilitarized Zone (DMZ) implementation
- Modernization of CS controls in OT Network
- 3rd party IT / OT integration for ICS

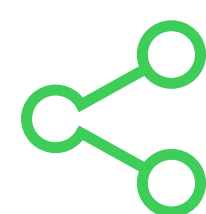
Success factor:

- Customized systems offered for ICS, OT Network, + IT interface
- Managed multi-vendor, OEM systems

Strengthening your cybersecurity



Strong cybersecurity
is a business
requirement.

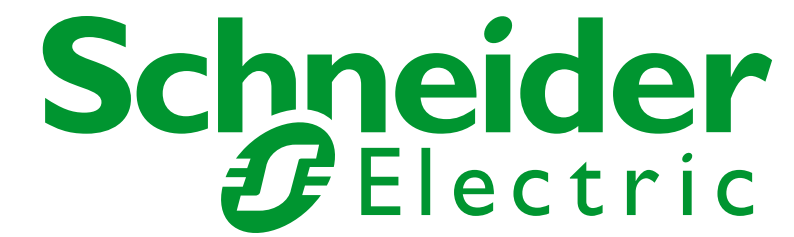


**Secure data
collection and
transmission** is critical
when harnessing
the benefits of IoT.



Schneider Electric
is committed to
supporting your digital
transformation.

Life Is On



Visit our website to learn more about how to protect your business from cybersecurity threats.

se.com/cybersecurity



Contact our cybersecurity team: cybersecurity-services@se.com

Schneider Electric

35 rue Joseph Monier
92500 Rueil-Malmaison, France
Tel : +33 (0)1 41 29 70 00