Cybersecurity services

We make infrastructure security work.*

Dedicated to providing comprehensive operational technology cybersecurity protection

*Our connected world depends on security. As industries continue to introduce smart, connected technologies that link more elements of everyday life together, security becomes increasingly important.

F·T·N

Powering Business Worldwide

Virtually every system is vulnerable

Everyday, cyber-attacks against commercial, industrial, utility and government networks number in the millions. About 31% of industrial control systems have experienced a cybersecurity incident in the past 12 months.

Further, cyber-attacks are becoming more prevalent on operational technology (OT) networks, such as those that operate building security and lighting, electrical distribution, HVAC and utility systems. Whether the objective is to disrupt operations or create an entry point to higher value business assets (intellectual property, email, customer data), the tools and the techniques used for unauthorized network access are becoming increasingly sophisticated. More than ever before it is a necessity to have a robust and holistic OT cybersecurity program in place that addresses your people, processes and technology.

Eaton addresses cyber threats proactively using a broad-based defensive approach with an unwavering focus on the dangers malware, spyware and ransomware present across the globe. Many of the latest vulnerabilities are originating on assets with the least security oversight — electrical breakers, generators, industrial gateways, elevators, automatic transfer switches, fire protection systems, and motor controllers. Ensuring the security of these soft-targets is critical to maintaining the safety and uptime of your business operations and employees. A vulnerability on these pieces of infrastructure not only puts the availability of that equipment at risk, but potentially provides access to higher value targets on the primary IT network (customer and personnel info, email, financial records and more).

The Eaton-secure approach

Our cybersecurity professionals are ever-alert, working with you to examine areas that you might not think are vulnerable, or where their vulnerabilities could affect other, more sensitive systems.

We'll help you design, update and maintain your network, processes and personnel training programs so cybercriminals can't get a foothold. Eaton follows the latest cybersecurity industry standards and leverages our deep electrical expertise when servicing your facility's OT network and cybersecurity program.

New to cybersecurity? Not sure where to begin?	**Eaton Audit**
Ready to conduct a thorough assessment of your operations and implement a complete cybersecurity program?	**Comprehensive Analysis & Life-Cycle Management**

Cybersecurity primary assessment services

Assessments	What is it?	What you get out of it
Initial Audit	Provides an initial assessment of the maturity and implementation of your overall cybersecurity program with a focus on your **people, processes and technology.**	You will receive an overall Eaton fitness score and report on your cybersecurity program derived from industry standards and best practices. Your will gain visibility to your strengths and weaknesses with improvement recommendations.
Comprehensive Analysis	An **in-depth** architecture, threat and vulnerability analysis to determine your overall level of exposure. This assessment uses **passive data collection** techniques on operational systems to minimize any disruption to your operations.	An Eaton cybersecurity leader will walk you through your identified attack surface profile and associated vulnerabilities and weaknesses. A prioritized list of findings with recommendations on how to address each will be delivered.
Life-Cycle Management Never one and done.	A suite of services designed to ensure your cybersecurity program remains **comprehensive and current with industry standards and best practices.** • Commissioning service • Personnel training • Hardening service • Consulting services • Industrial network defense	Reoccurring assessment of your people, processes and technology to ensure you are keeping pace with the evolving threat space and existing practices do not erode over time.

Bad actors keep getting smarter

While we work to maintain the availability and safety of your infrastructure, bad actors are out there developing new methods to evade your security measures putting your people, operations and mission at risk.
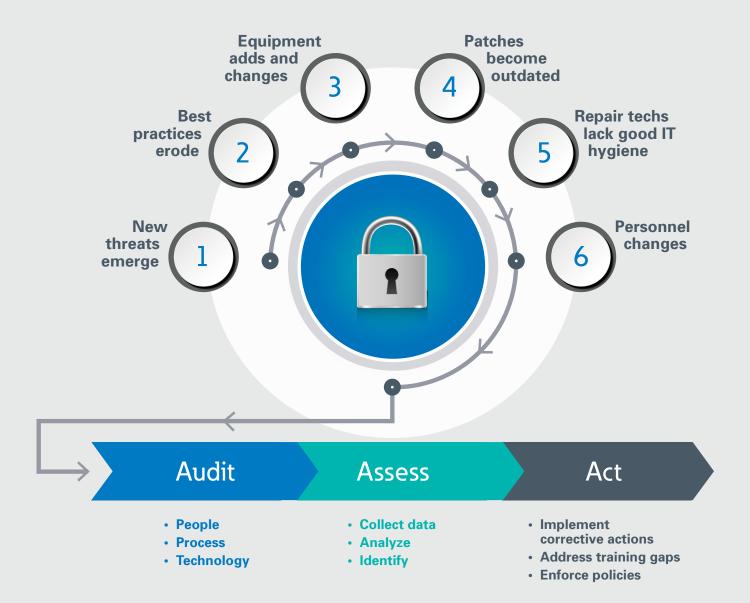
We recognize that cybersecurity techniques that are effective today may not be tomorrow. Therefore, administrators of industrial networks must be ever-alert to changes in their OT networks and constantly working to prevent operational vulnerabilities.

With Eaton, it's never "one and done". Our cybersecurity services are designed to provide complete life-cycle management to maximize the availability of your facility.

People / Process / **Eaton Cybersecurity** / Technology

Eaton's Cybersecurity Life-Cycle Management

Industry standards dictate reassessing your environment every 12–15 months

New threats emerge — 1

Best practices erode — 2

Equipment adds and changes — 3

Patches become outdated — 4

Repair techs lack good IT hygiene — 5

Personnel changes — 6

Audit
- **People**
- **Process**
- **Technology**

Assess
- **Collect data**
- **Analyze**
- **Identify**

Act
- **Implement corrective actions**
- **Address training gaps**
- **Enforce policies**

Why trust Eaton to secure your operational technology network?

Over 100 years developing products and services

Having designed hardware and software products for decades, along with providing the associated installation and maintenance services positions Eaton as the most capable cybersecurity provider in the industry for electrical infrastructure and building systems. Our experienced team of cybersecurity leaders identify and address gaps in your processes and personnel training programs to minimize your overall attack surface.

Offering deep cybersecurity experience

Customers rely on Eaton to understand, dissect and alleviate cybersecurity risk. It starts with dedicated people. Our team members meet and exceed competencies recognized by international standards organizations through rigorous, in-depth technical training programs. You can be confident that management, engineering and personnel have the knowledge and service capabilities to address advanced cyber threats.

OUR SERVICE FOUNDATIONS

NIST
SP 800-53R4, SP 800-82R2
SP 800-37 (RMF), FIPS 140-2
Critical Infrastructure Framework
NISTIR 7678 Vol 1 Rev 1

IEC
IEC 62443
IEC 62351
IEC 61850

UL
Standard for Software Cybersecurity for Network-Connectable Products (2900-1)

US Department of Defense
Unified Facilities Criteria (UFC) 4-010-06 (MIL-STD 3007)

NERC
NERC CIP

U.S. Department of Homeland Security
Catalog of Control Systems Security
SCADA Procurement Language
ICS-CERT

Best Practices
SANS
Center for Internet Security

Cybersecurity Center of Excellence

Cybersecurity is a foundational element in the lifecycle of our products and services. Cybersecurity is at the core of our "secure by design" philosophy, and it's embedded in all the Intelligent Power products and platforms we bring to market. The Cybersecurity Center of Excellence team aligns our talented people with best-practice processes and modern technologies, creating a program that trains others and helps our customers avoid the dangers of cyber-attacks.

Eaton has the first research and testing facility approved to participate in UL's Data Acceptance Program (DAP) for cybersecurity in Pittsburgh, Pennsylvania. Recently, UL approved a second Eaton lab to join the program — another industry first — in Pune, India. These accredited lab environments provide the global capability to test Eaton products with intelligence or embedded logic to key aspects of the UL 2900-1 standard.

Eaton Cybersecurity Competencies

- **Commissioning**
- **Hardening**
- **Industrial network defense**
- **Personnel training**
- **Consulting**

To more information, visit
Eaton.com/cybersecurityservices

E·A·T·N
Powering Business Worldwide

Follow us on social media to get the latest product and support information.