Industrial Cybersecurity

Utilities

Enable visibility

Secure touchpoints

Provide rapid incident response

Prepare for the shift to cloud

Utility industry: A prime and consistent target

Critical infrastructure for energy and utilities is vital to personal safety, economic growth, and national defense. There is growing interest in the topic from senior utility executives, regulators, and customers around the world. There are also legitimate concerns about ensuring that adequate resources and focus are directed to the task of securing critical infrastructure. The growing issue of cybersecurity and its impact on energy resources highlights fundamental risks to a nation's critical infrastructure. Efficiently addressing these cybersecurity issues requires a clear understanding of the current security challenges and specific defensive countermeasures. A holistic approach – one that uses specific countermeasures implemented in layers to create an aggregated, risk-based security posture – helps to defend against cybersecurity threats and vulnerabilities that could affect these systems. This approach, often referred to as defense in depth, provides a flexible and usable framework for improving cybersecurity protection when applied to control systems.

The risk to utilities globally from cyber attacks is broad and business-impacting, including:

- Employee health and safety
- Lost revenue
- Intellectual property theft and ransomware
- Hard costs for remediation, compliance fines, and reputation damage

Protect your critical industrial systems with Cisco's leading cybersecurity portfolio.

Benefits

- Enable visibility into industrial control systems (ICS) to inventory and develop baselines for devices, applications, and traffic profiles
- Secure touchpoints where people and their devices interact with ICSs
- Add tools that enable and inform rapid incident response
- Prepare for the inevitable shift of operational technology (OT) components moving to the cloud
- Align with industry security standards such as NERC|CIP and NIST

"One of the biggest vulnerabilities of the IoT is a lack of visibility. Defenders are simply not aware of what IoT devices are connected to their network. (Manufacturers) need to move quickly to address this ... because threat actors are already exploiting security weaknesses in IoT devices."

2017 Cisco Midyear Cybersecurity Report

ICS and SCADA visibility

The foundational objective for applying cybersecurity to utility assets is to enable visibility into critical ICS and SCADA environments. This visibility provides security operators the data needed to understand the system's baseline for devices, applications, and traffic. These baselines are critical and form the basis for identifying anomalies that result from cyber intrusions by malware, worms, viruses, and other system exploits. Cisco's portfolio enables this real-time visibility and anomaly detection with:

- Cisco Firepower® Threat Defense (NGFW)
- Cisco 3000 Series Industrial Security Appliances (ISA)
- Cisco Stealthwatch® analytics
- Industrial Ethernet (IE) switches with NetFlow
- Deep packet inspection for Modbus, Ethernet/IP, and DNP3

Malware protection

Protecting the vulnerable touchpoints where people and their devices interact with the ICS/SCADA systems is critical to reduce threats from malware delivered over the web, email, and USB storage. Cisco offers the industry's most advanced malware detection and prevention with:

- Cisco Advanced Malware Protection (AMP) for Endpoints and AMP for Networks
- Cisco Talos™ global threat intelligence

Time to detect (TTD) and time to respond (TTR) will determine how long an attacker controls a compromised system, and ultimately determines the impact of the attack.

The capabilities offered for ICS/SCADA visibility and malware protection help dramatically decrease TTD and TTR, which limits the impact on production.

Industry standards

The cybersecurity capabilities offered in Cisco's portfolio map directly to industrial cybersecurity standards such as:

- NERC|CIP
- ISA-95,ISA-99
- NIST

Cloud readiness

Core ICS and SCADA functions will likely remain on-premises for many years to come, but software for OEM and third-party data analytics and machine maintenance are moving to the cloud. Prepare the organization to adapt to these cloud models with confidence, using cloud security tools from Cisco:

- Cisco Umbrella™
- Cisco Cloudlock™
- Cisco Stealthwatch Cloud

Take the next step

Cisco has the infrastructure expertise, services, and strategic partnerships needed to:

- Secure business IT and operations
- Spur faster decision making
- Enable new business models without compromising reliability, security, or network response time

For more information

Contact your Cisco representative or learn more online at www.cisco.com/go/smartgrid.