Factory Security: Safeguard Your Industrial Network

Opportunities and Challenges of the IoE

The growth of the Internet of Everything (IoE) is creating efficiencies and cost savings across the entire value chain, presenting a $3.9 trillion value opportunity for manufacturers. Yet this exponential growth of connections and integration between people, processes, data, and things also presents added security risks.

Manufacturing: A Target-rich Environment

Manufacturing is the number one targeted Industry for Cyber Espionage. Combined with an aging industrial machinery infrastructure, there are significant security risks and challenges. In fact, manufacturers view data security as a top barrier to realizing the value of IoE. As they adopt new technology standards and converge the traditional boundaries between IT and operational technology systems and organizational silos, security threats intensify.

What's the impact of security breaches?

- Loss of proprietary or confidential information and intellectual property
- Violation of regulatory requirements
- Loss of public confidence ("headline" risks to brand)
- Economic loss
- Impact on national security

Industry-leading Holistic Security

Factory Security is designed to address the specific security risks of IoE deployments from a holistic perspective. A holistic approach to IT and operational-technology data security effectively prevents, detects, and mitigates security threats to company intellectual property, capital assets, reputation, and privacy.

A holistic approach facilitates a business-driven security blueprint and strategy that serves as an effective defense for the entire manufacturing value chain. The result is a solution that transforms diverse manufacturing processes into a unified, tightly integrated, and secure communication system, linking infrastructure, machines, processes and people.

Learn more about the holistic security benefits and how to:

- **Gain a competitive advantage** by protecting intellectual property and physical assets from cybertheft.
- **Speed security threat resolution and reduce downtime,** driving efficiency gains across facilities.
- **Build positive brand reputation** internally and externally by safeguarding employee and customer information.
- **Improve overall equipment effectiveness** (OEE) with ubiquitous, secure, and reliable access to plant assets, including secure remote access where it is important for your factory.
- **Ensure effective, robust plant-floor security** with validated designs and proven methodologies from Cisco Services and industry-leading partners including Rockwell Automation.

Take the Next Step

Cisco has the infrastructure expertise and strategic partnerships needed to secure business IT and OT, spur faster decision-making, and enable new business models without compromising reliability, security, or network response time.

To find out more about Factory Security, or to schedule a demo, visit www.cisco.com/connected-factory-security and contact your Cisco representative. And to find out more about our unique partnership with Rockwell Automation, visit www.cisco.com/go/rockwellautomation.

 DEC15CS943 09/15