Cisco Connected Factory – Security

Manufacturing: A target-rich environment

Many manufacturers view data security as a top barrier to realizing the value of IoT. And this threat is increasing as manufacturers adopt new technology standards and converge the traditional boundaries between IT and Operational Technology (OT) systems and organizational silos.

Statistics show manufacturing faces a particularly dangerous security situation:

- Nearly 40% of manufacturing organizations reported targeted attacks and advanced persistent threats as high security risks to their organizations (Cisco 2017 SCBS Study).
- 28% of manufacturing organizations reported a loss of revenue due to one or more attacks in the past year (Cisco 2017 SCBS Study).
- Industrial networks top the list of systems most vulnerable to cybersecurity issues (McAfee).
- “Aging industrial machinery infrastructure presents huge security challenges that will continue to grow in the coming months and years” (Dell Security Annual Threat Report).

Automation and control systems in OT networks are inherently vulnerable due to their use of proprietary hardware and software, with little to no security built into aging legacy factory networks. This vulnerability is actually increasing as manufacturers implement IoT capabilities across their factories and connect their plant assets to higher-level applications.

Benefits

- Safeguard production integrity.
- Gain competitive advantage by protecting sensitive information, intellectual property, and physical assets from attack.
- Speed resolution of security threats and reduce downtime, driving efficiency gains across facilities.
- Improve Overall Equipment Effectiveness (OEE) with secure, and reliable access to plant assets, including secure remote access.
- Help ensure effective, robust plant-floor security with validated designs and proven methodologies from Cisco® Services and industry-leading partners, such as Rockwell Automation.

> **“...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

We designed Cisco Connected Factory – Security and IoT Threat Defense to address the specific security risks of IoT deployments from a holistic perspective. Cisco IoT Threat Defense for manufacturing is an architectural approach to security. Protect your Industrial Ethernet infrastructure with a prescribed, regimented approach to security while still adhering to a standard defense-in-depth approach commonly followed in manufacturing facilities. Employ a suite of integrated, interoperability-tested security products, starting with the Cisco Identity Services Engine (ISE) and Cisco TrustSec®, which facilitate extensible, scalable segmentation using group- and device-based access policy throughout the network. These are layered with Cisco Stealthwatch®, Cisco Umbrella™, and Next-Generation Firewalls, as well as Cognitive Analytics, Cisco AnyConnect® VPN, and Advanced Malware Protection (AMP).

Cisco Security Services puts real people into the solution to help organizations make decisions about protecting their intellectual property and, just as important, their production integrity.

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. With the solution, you can:

- Securely access machine data on the plant floor, aggregate it, and apply analytics to determine optimal operation and supply chain workflows, improving efficiencies and reducing costs.
- Share intellectual property securely with global employees, partners, and vendor ecosystems, helping scale expert resources.
- Mitigate risk with a posture assessment capability that helps ensure policy compliance, operating system updates, and software patch deployments.
- Securely and remotely troubleshoot machines.

Industrial DMZ

- Connected Factory - Security supports a standard industrial DMZ approach with an architecture that supports security and business needs.
- Provides standard network services for control and information disciplines, devices, and equipment found in modern Industrial Automation and Control System (IACS) applications.
- Includes firewalls, remote-access VPN services, IACS application hosts, and network infrastructure devices, such as switches, routers, and virtualized services in proven, validated architectures.

Security and business agility in the age of IoT

The piecemeal Product or Technology-driven security strategy is no longer effective. A holistic approach to IT and operational-technology data security is required to effectively prevent, detect, and mitigate security threats to company intellectual property, capital assets, reputation, and privacy.

Take the next step

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

To find out more about Cisco Connected Factory – Security, or to schedule a demo, visit https://www.cisco.com/go/factorysecurity and contact your Cisco representative.