At-a-Glance

Cisco Connected Factory Security

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[1] 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

Manufacturers view data security as a top barrier to realizing the value of IoE. And this threat is increasing as manufacturers adopt new technology standards and converge the traditional boundaries between IT and operational technology systems and organizational silos.

Statistics show manufacturing faces a particularly dangerous security situation:

- Manufacturing was the most targeted sector in 2013, accounting for 24 percent of all targeted attacks (Symantec[2])
- Industrial networks top the list of systems most vulnerable to cybersecurity issues (McAfee)
- More than 1000 industrial automation and control systems (IACS) were targeted by the Dragonfly espionage malware program in 2014[3]
- The number of attacks on industrial supervisory control and data acquisition (SCADA) systems **doubled** from 2013 to 2014[4]
- "Aging industrial machinery infrastructure presents huge security challenges that will continue to grow in the coming months and years."[5]

IACS in operational technology networks are inherently vulnerable due to their use of proprietary hardware and software, with little to no security built in to legacy factory networks. This vulnerability is actually increasing as manufacturers implement IoE capabilities across their factories and connect their plant assets to higher-level applications.

Benefits

- **Gain 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 your 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, such as Rockwell Automation.

[1] Source: Cisco Consulting Services, "IoE Value Index Survey", 2013, *2013-2022

[2] Quoted in April 2013 article in the Business of Federal Technology

[3] BBC, Energy firms hacked by 'cyber-espionage group Dragonfly', July 1, 2014, http://www.bbc.com/news/technology-28106478

[4] Dell Security Annual Threat Report, https://software.dell.com/whitepaper/dell-network-security-threat-report-2014874708

[5] Dell Security Annual Threat Report, https://software.dell.com/whitepaper/dell-network-security-threat-report-2014874708

"Gaining visibility into this world of previously undetected cyberthreats helped reassure our team that we were doing the right thing by adding intrusion prevention technology across our industrial network."

Charles Harper
Director of National Supply and Pipeline Operations,
Air Liquide

Security and Business Agility in the Age of IoE

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.

Your business is evolving to integrate and deploy converged IT and operational technology networks, predictive maintenance tools, machine systems, plant-floor mobile applications, and cloud-based services. At the same time, you need to harness the benefits of the analytics those deployments create. Therefore, it is important to take a **holistic** approach with these efforts, one that facilitates a business-driven security blueprint and strategy that serves as an effective defense for the entire manufacturing value chain.

Industry Leading Holistic Security

We designed Cisco Connected Factory – Security to address the specific security risks of IoE deployments from a holistic perspective (see sidebar). 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 data-analytic algorithms 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 ensures policy compliance, operating system updates, and software patch deployments
- Securely and remotely troubleshoot machines and issues with new product introductions

How It Works

To protect your factory and build on the previously released Cisco Connected Factory Automation and Connected Factory Wireless solutions, the latest release of Connected Factory Security includes the following converged access security products, technologies, and services.

Security Identity Services

- Supports multiple external identity repositories, including Microsoft Active Directory for both authentication and authorization
- Allows plant administrators to configure and manage wired and wireless user access based on authentication and authorization services available from a web-based GUI console
- Simplifies administration with integrated management services from a single administrative interface

Industrial DMZ

- Enables a holistic, industrial DMZ approach through an architecture that supports security and business needs
- Provides standard network services for control and information disciplines, devices, and equipment found in modern IACS applications
- Includes firewalls, remote access VPN services, IACS application hosts, and network infrastructure devices, such as switches, routers, and virtualized services in the proven, validated architecture

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 Cisco Connected Factory – Security, or to schedule a demo, visit www.cisco.com/go/factorysecurity and contact your Cisco representative.

Network Address Translation (NAT)

- Allows for the reuse of IP addressing (for cookie-cutter plant-floor machine and device addressing) to increase ease of integration without introducing duplication errors in IACS application architectures
- Increases security in that it can be configured to translate only specific IP addresses from within a cell or area zone to the higher levels of the plant, while maintaining IP addressing commonly repeated by machine builders
- Aids users in deploying NAT-capable networks with planning and design guidance to optimize architectures for IACS application needs

Connected Factory Starter Kit

- Allows you to try the solution's new technologies and capabilities on a small scale with minimal financial investment
- Delivered as a prepackaged and validated set of equipment and services that creates a living lab on the factory premises

C45-734463-00 05/15