Cisco IoT System Security: Mitigate Risk, Simplify Compliance, and Build Trust

What You Will Learn

Manufacturers, energy and transportation providers, and smart cities are gaining a competitive advantage by harnessing the Internet of Things (IoT). But connecting more things in more places creates new security challenges. Mitigating risk requires a combination of cybersecurity and physical security. This white paper, intended for business managers and operational-technology specialists, describes Cisco® IoT System Security - a comprehensive portfolio of products to mitigate risk, simplify compliance, and build trust.

Challenge of Securing the IoT

The IoT is expected to grow from more than 12 billion devices in 2015 to 50 billion by 2020. Each device is a potential entry point for a network attack by insiders, hackers, or criminals. In a Forrester survey of organizations around the world, 47 percent of the industrial organizations that use or plan to use the IoT had previously experienced security breaches in their industrial applications.[1]

Securing the IoT poses new kinds of challenges:

- **Scale:** Your security solution needs to scale cost-effectively - potentially to hundreds of thousands or millions of endpoints.
- **Remote locations:** You might install devices such as sensors in unmanned locations that are difficult to reach, such as roadsides, railways, or utility substations. Attackers can tamper with these devices without being seen. The cybersecurity and physical security devices you deploy to protect them must stand up to extreme environmental conditions, fit in small spaces, and not require a trip by field technician for routine updates and maintenance.
- **Availability:** OT teams hesitate to use standard discovery and threat-response technologies for fear they will take down critical systems. Even a simple port scan causes some IoT devices to stop working, and the cost of downtime can far exceed the cost of remediating all but the most severe incidents. In fact, some OT teams would rather have **no** cybersecurity protection rather than risk an outage due to a false positive. This leaves them blind to threats within their control networks.

Are You Ready for the Internet of Things?

- 73 percent of business decision makers expect the IoT to cause security threats to increase in severity over the next two years.[2]
- 49 percent of business decision makers cite security threats among their top application challenges.[3]
- 78 percent of IT security professionals are either unsure about their capabilities or believe they lack the visibility and management required to secure new kinds of network-connected devices.[4]
- 46 percent of IT security professionals do not believe that that current policies apply to IoT devices and provide visibility into those devices.[5]

[1] Forrester, “Security: The Vital Element of the Internet of Things,” 2015
[2] Global Market Insite (GMI), a division of Lightspeed Research, from a Cisco-sponsored study
[3] ibid
[4] SANS Institute, Securing the Internet of Things
[5] ibid

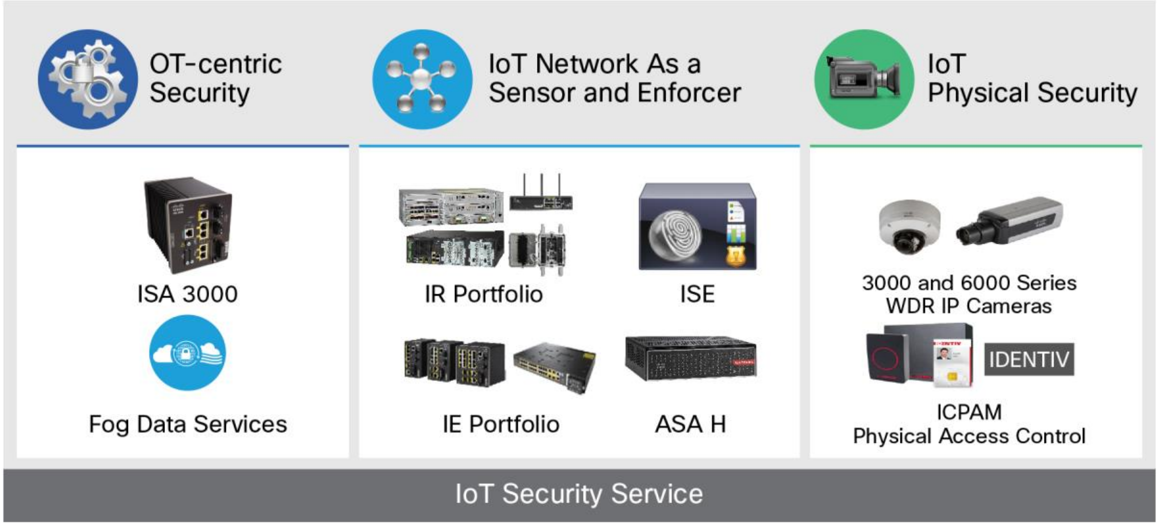
A comprehensive IoT security solution needs to do the following:

- Provide visibility into applications, users, protocols, and anomalies.
- Allow critical systems to continue operating even when under attack.
- Simplify compliance with industry or government regulations.
- Scale cost-effectively to accommodate more IoT devices or more data.
- Increase situational awareness and accelerate incident response. Situational awareness requires a combination of video surveillance, identification of people and devices, and collection and analysis of telemetry and logs.
- Integrate IT and OT processes. Connecting OT systems to the IT network increases the value of your existing IT security investments and policies.

Cisco IoT System Security

Cisco IoT System Security meets these requirements. It delivers security at scale, simplifies compliance, and builds trust. It provides all cybersecurity and physical security solutions you need, all supported by one vendor (Figure 1).

Figure 1. Cisco IoT Security Product Portfolio



IoT Network as Sensor and Enforcer

Build security right into your network by using Cisco network infrastructure to sense anomalous network activity and enforce policy. These network devices:

- Provide fast VPN performance using hardware acceleration
- Enforce policies consistently
- Detect and mitigate distributed denial-of-service (DDoS) and other attacks
- Prevent misconfigurations that attackers can exploit
- Identify the type of device and provide the appropriate access control
- Control access to IoT devices based on the user and device identity, using Cisco Identity Services Engine (ISE)

OT-centric Security

Gain application visibility, consistently enforce policy, and simplify compliance. Deploy the Cisco 3000 Industrial Security Appliances (ISA) to:

- Take advantage of proven threat management from Cisco ASA with FirePOWER™ Services
- Support OT protocols and applications
- Detect and protect against OT specific threats including DDoS, operational safety, and insider attacks
- Gain visibility into the protocols, devices, and applications you specify
- Secure Internet connectivity with high-performance VPN, Domain Name System (DNS), Dynamic Host Configuration Protocol (DHCP), and Network Address Translation (NAT)

The ISA 3000 is compact and ruggedized, and suited for outdoor and harsh environments. It is certified for major industries.

IoT Physical Security

Receive an alert the moment activity is detected near an IoT device in an unmanned area. The alerts come from video surveillance cameras, physical access controls, and IoT sensors for motion detection and more. The cameras in our solution produce useful images, even when backlight and illumination vary in the same scene, using IP cameras with wide dynamic range (WDR) technology.

The Cloud and the Fog: Partners in the Internet of Things

The fog extends the cloud to be closer to the things that produce and act on IoT data. Any device with compute, storage, and network connectivity can be a fog node. Examples include industrial controllers, switches, routers, embedded servers, and video surveillance cameras. Deploy fog nodes anywhere with a network connection, including on a factory floor, on top of a power pole, alongside a railway track, in a vehicle, or on an oilrig. To mitigate risk, activate Fog Data Services on any Cisco fog node to encrypt data at the network edge.

Services and Partner Ecosystem

In addition to technology, we provide the professional services and partner ecosystem you need to secure the IoT. Cisco services include:

- Industrial Cyber Security Capability Assessment
- Industrial Cyber Security Reference Architecture
- Industrial Cyber Security Plan, Design, and Implementation
- IoT Physical Security Services

Benefits

IoT System Security helps you:

- **Gain a competitive advantage:** Knowing that data and systems are protected, you can confidently put the IoT to work to improve efficiency, safety, or customer experiences. Find out sooner about events such as cyber attacks, equipment outages, and unsafe conditions, and automate response based on policy.
- **Mitigate risk in a cost-effective manner:** Gain visibility into IoT devices and enforce your security policies by using your network infrastructure and OT-centric security appliances.

- **Maximize uptime and comply with regulatory requirements:** Apply your existing IT security expertise to OT.
- **Simplify compliance:** IoT System Security consistently enforces policy. It also segments the network to simplify compliance and reduce audit scope.

Why Cisco?

When you work with Cisco to secure your IoT environments, you receive technology and expertise from the leader in network security. IoT System Security products are designed for the unique demands of IoT, such as protecting devices in harsh environments and enabling industrial control systems to continue operating when under attack.

Finally, working with Cisco simplifies deployment and ongoing support throughout the solution's lifecycle. You get everything you need from one vendor: cybersecurity, physical security, and professional services.

For More Information

To learn more about Cisco IoT System Security, visit http://www.cisco.com/go/iotsystemsecurity.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Printed in USA C11-735952-00 10/15