White Paper

The Internet of Things: Reduce Security Risks with Automated Policies

What You Will Learn

The Internet of Things (IoT) is creating extraordinary opportunities in business, education, and government. But to take advantage of these opportunities, you first need to mitigate new kinds of security risks. This white paper, intended for IT and operational technology (OT) professionals, explains a new approach to IoT security, one that:

- Extends cybersecurity solutions to the OT environment and physical security solutions to the IT environment
- Correlates and analyzes data from IoT devices the moment it arrives on the network to produce actionable security intelligence
- Acts on that intelligence automatically, according to policy, and enforces different policies depending both on the threat and on the purpose of the system that's under threat

The Internet of Things: New Benefits, New Security Challenges

Connecting previously unconnected devices to the Internet is improving the way we work and live (see sidebar). Already, people can find and reserve open parking spaces on their smartphones. Cities conserve water by monitoring soil moisture over the network and remotely controlling sprinklers. Utilities monitoring smart meters can detect outages before customers report a power loss. Manufacturing operators receive real-time alerts when equipment temperatures start rising so that they can make repairs that prevent interruptions. Mining companies improve safety by tracking the location of equipment and miners.

The Internet of Things is unleashing these and other imaginative applications in business and government. But it also complicates security, for the following reasons.

Internet of Things: A Definition

Cisco defines the Internet of Things as the convergence of IT networks, operational technology (OT), and smart objects.

Building Block	What It Does	Sample Things
Information technology	Connects IP devices	Switches, routers, firewalls, laptops, mobile devices, printers, and data center infrastructure.
Operational technology	Automates, monitors, or controls industrial devices, processes, and events	Programmable logic controllers (PLCs), supervisory control and data acquisition (SCADA) systems, and process information (PI) systems.
Smart objects	Report information or implement commands	Sensors and actuators

Each Connected Device Is a Potential Point of Attack

The IoT comprises more than 10 billion devices and will likely grow to 50 billion by 2020. Each one is a potential entry point for an attack.

New Kinds of Devices Bring New Kinds of Vulnerabilities

The billions of newly connected devices include countless types of devices. A tiny sample includes environmental sensors, wearable electronics, pipe pressure monitors, sprinkler controllers, parking space sensors, monitors that signal when trash bins are full, and industrial network devices such as programmable logic controllers (PLCs). Each type of device is vulnerable to different kinds of attacks, most not yet invented. The devices themselves have varying levels of security, and many have none at all.

Data Originates on Devices in Unsecured Locations

As the IoT grows, more of the data traveling over your network will originate from devices outside your network. Some of these devices will be in unsecured locations such as roadsides, railways, or bridges. Tampering with a device in the middle of nowhere is not difficult. Therefore, to decide whether to let traffic onto your network, you need to know what device sent it, where the device is, and whether the traffic it's supposedly sending is believable for that type of device. A trackside IP phone shouldn't be requesting access to financial database, for instance.

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.[1]
- **49 percent** of business decision makers cite security threats among top application challenges.[2]
- **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.[3]
- **46 percent** of IT security professionals do not believe that their current policies apply to IoT devices and provide visibility into those devices.[4]

IT and OT Teams Have Different Security Priorities

Many organizations have converged their IT and OT networks. When this happens, IT and OT are simply different environments on the same network. But applying the same security policy for all systems on the network will not satisfy either the IT or the OT team. Although both teams are concerned with confidentiality, data integrity, and availability, their priorities differ.

For IT teams, the top priority is data confidentiality. If a cybersecurity solution detects malware that threatens data confidentiality, the usual policy is to quarantine or shut down the affected system. For OT teams, in contrast, the top priority is availability. That's because shutting down a compromised system in a manufacturing area or power grid can cost far more than cleaning up after an attack. Stopping a system might also risk employee or customer safety.

Because of their different priorities, IT and OT teams have historically approached security in different ways (Table 1). IT concentrates on defending the network against attack and protecting data confidentiality. OT focuses on controlling physical access to systems that affect operations or safety.

[1] Global Market Insite (GMI), a division of Lightspeed Research, from a Cisco sponsored study.
[2] Ibid.
[3] SANS Institute, Securing the Internet of Things

Table 1. IT and OT Teams: Different Security Priorities, Approaches, and Methods

	IT Networks	OT Networks
Primary goal	• Protect data confidentiality	• Make sure that systems and data are always available
Approach	• Cybersecurity	• Physical security
Solutions	• Firewalls • Intrusion prevention and detection systems • Advanced malware protection • Access control	• Video surveillance cameras • Physical access controls
Methods	• Detect and mitigate cybersecurity threats • Block suspicious network activity • Protect against malware	• Segmentation • Enforce strict physical access control

When IT and OT systems share the same network, using separate systems to safeguard them no longer makes sense. Nor does it make sense for the IT team to dictate security policies in the OT environment. IoT security is not the same as IT security. It's more. In fact, using the IoT to safeguard the IoT can actually strengthen your security posture, as described in the next section.

New Model: Combined Cybersecurity and Physical Security

A comprehensive approach to IoT security requires a new approach, with three requirements.

Requirement 1: Extend Cybersecurity Security to Protect OT Systems, and Physical Security to Protect IT Systems

Extending cybersecurity and physical security solutions to both environments benefits both teams. Each team uses the same solutions but in different ways. For example, the IT team might configure the intrusion prevention system (IPS) to shut down systems when anomalous activity occurs. The OT team might configure it to alert a human operator who can use intimate knowledge of the system and business processes to decide on the best response.

Requirement 2: Program Cybersecurity and Physical Security Systems to Work Together

The real power of IoT security comes from programming cybersecurity and physical security solutions to work together. There are two benefits. First, correlating the information from multiple security systems provides a more detailed view of activities inside and outside the network. Second, security systems can communicate directly, without human intervention. Machine-to-machine (M2M) communications shave precious seconds off the response time. The security systems follow different policies for different types of events. For example, if the access control system detects the use of a badge reported as stolen, the automated actions might be to lock the door, block access to machines and computers in the area, alert security officers, and signal the video analytics software on a nearby camera to identify the individual using the stolen card.

IoT Security and Fog Computing

Swift action is critical for IoT security. For example, closing a vent or blocking a network port just a few milliseconds sooner can prevent injury or a database breach. Sending the data from IoT sensors all the way to the cloud for analysis adds latency. Much better is to analyze IoT data at the network edge, close to the devices collecting and acting on data. Analyzing IoT data at the network edge reduces latency. It offloads gigabytes of network traffic from the core network. And it keeps sensitive data inside the network. Any edge device with a processor and storage can perform the analysis. Options include Cisco® routers and switches, Cisco video surveillance cameras, and Cisco Unified Computing System™ (Cisco UCS®) servers. Cisco calls this approach fog computing because it's an extension of the cloud.

Requirement 3: Enforce Different Security Policies Depending on the Environment

The IT team writes security policies for firewalls and IPS. The policies can specify different actions depending on whether traffic is destined for the IT or OT environment. For instance, the same threat might trigger one response if the target is an IT asset such a financial-reporting database and a different response if it's an OT system such as a factory-floor robot. If the threat targets an IT system, the policy might be to shut down or quarantine the system. If the threat targets an OT system, the policy might be to simply send an alert to the system operator with intimate knowledge of the system. The operator can decide on the best response based on the risk and the nature of current processes running on that system.

Simple applications on fog nodes can enforce other types of policies. Examples include opening vents when gas levels exceed a threshold, or training a video surveillance camera in the direction of breaking glass detected by an audio sensor.

Characteristics of the IoT Security Model

- **Unprecedented visibility into security events:** Techniques include advanced video and audio analytics, the remote management of assets, and multisite event correlation.
- **Precise control over security policy:** Response to the same threat can vary depending on the system the threat is targeting.
- Comprehensive cybersecurity threat detection and mitigation.
- **Actionable intelligence:** Fog nodes analyze real-time data from switches, routers, video surveillance cameras, door controllers, and other IoT devices to detect security threats.
- **Automated decisions:** The fog nodes instruct other IoT devices to take action based on policy. Avoiding the need for human intervention when appropriate speeds up response and improves outcomes.

Picture the Possibilities in Your Industry

Industrial Plants

Control access to sensitive systems by combining two-factor identification with facial recognition. Detect when someone tries to use removable media to copy or load files. Then block the attempt and send an alert to security officers to investigate. Use video analytics and sensor data to gain early awareness of spills and other conditions that could cause accidents.

Utilities

Automatically train cameras on an area whose sensors report a problem. Operators can make a remote diagnosis to resolve problems sooner. Improve access controls by combining cybersecurity authentication and biometric identification. Automate a lockout when physical security systems detect someone tampering with a smart meter or attempting to enter a restricted area.

Mass Transportation

Increase situational awareness by automatically training cameras on potential problem areas and streaming the video feed to security officers. Monitor the location of employees by the systems they've accessed and the doors they've entered. Correlate events happening in multiple places at the same time to detect danger that a human might miss. For example, a lone individual lingering trackside might trigger a low-level alert. The threat is much greater if video analytics software picks up lone individuals positioned at intervals across a long expanse of track. A human could easily miss the pattern.

Why Cisco

Everything you need to safeguard your IoT environment is available from one vendor: Cisco.

- **Visibility:** See physical events using Cisco Video Surveillance IP Cameras, and monitor thousands of cameras from a single console using the Cisco Video Surveillance Manager. See digital events using Cisco ASA next-generation firewalls, Cisco IPS, Cisco Advanced Malware Protection (AMP), and other cybersecurity solutions. Combine these physical security and cybersecurity solutions to protect people, information, and processes from the outside as well as the inside.
- **Precise control:** Apply different security policies based on the system that's threatened. Use Cisco Identity Services Engine (ISE), Cisco next-generation firewalls, and Cisco next-generation intrusion prevention systems. Create logical groups based on the system's purpose or availability requirements using Cisco TrustSec® technology. Then program the network to enforce different policies for different logical groups. In this way, a single Cisco security solution can protect both the IT and OT environments.
- **Advanced threat detection:** After you allow traffic on the network, continue monitoring it for anomalous behavior that might emerge later by using Cisco AMP.
- **Actionable intelligence:** Find out about threats sooner using Cisco Cognitive Threat Analytics. It's a cloud service that identifies the symptoms of a malware infection or data breach using behavioral analysis and anomaly detection.
- **Automated decisions:** Automatically lock doors based on sensor or camera data using Cisco physical access solutions. When video analytics software detects that the person entering a server room is using another person's badge, automatically block network access in that room.

Conclusion

The Internet of Things complicates security by adding billions of potential attack vectors. At the same time, it can strengthen your security posture by gathering far more intelligence about threats and automating responses based on policy.

A comprehensive approach to IoT has three parts. First, extend cybersecurity and physical security solutions to both the IT and the OT environments. This step protects the network from the inside and the outside. Second, program the solutions to work together. You'll get more information about threats and speed up responses by taking advantage of M2M communications. Analyzing IoT data in the fog layer saves precious milliseconds that can make the difference between preventing a threat and trying to mitigate its damage. Finally, apply different security policies depending on the environment that the threat is targeting. Policies for IT systems can favor data confidentiality; policies for OT systems might favor system availability.

With a comprehensive approach to security, organizations are free to capitalize on the IoT to improve business, government, and safety in extraordinary ways.

For More Information

Read more about the Internet of Things at www.cisco.com/go/iot.

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 C11-734313-00 04/15