Securing the Internet of Everything: Our Plan to Use Identity Services Engine

Cisco IT Insights

What

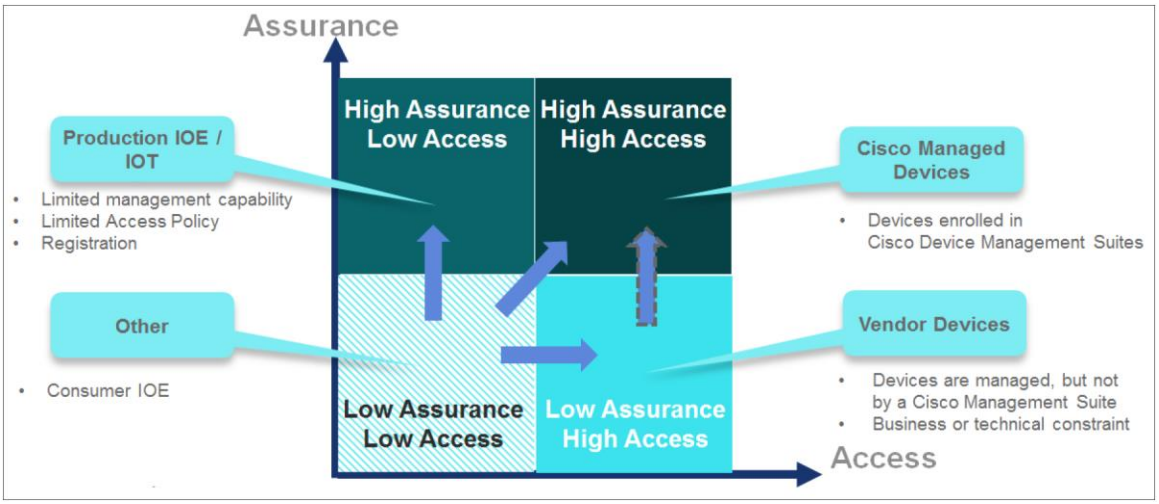
Cisco IT constantly receives requests from internal teams to connect new people, processes, data, and things to the enterprise network. The Internet of Everything (IoE) is here, and it's creating new kinds of challenges for our IT and Information Security (InfoSec) organizations.

For example, our Workplace Resources organization has asked to connect thermostats and lighting systems to the network. "From a security perspective, it's concerning," says Rich West, information security architect for Cisco. "Some Internet of Things [IoT] devices aren't manufactured by IT companies. They don't meet current security standards, such as WPA-2 [Wi-Fi Protected Access 2]. And we can't necessarily rely on consumer product manufacturers to promptly issue patches for newly discovered vulnerabilities."

The latest thinking from our Global Infrastructure Services and InfoSec teams is to mitigate IoE security risks by using Cisco® Identity Services Engine (ISE). When a device connects to the network, Cisco ISE senses the device type and then grants access according to the policy for that kind of device. We already use Cisco ISE to control access by collaboration endpoints and mobile devices. Our plan is to also write policies for new types of Internet-connected devices, such as lighting systems or thermostats.

To decide on the access policy for an Internet-connected device, we'll consider two factors. One is our trust in the device. Trust is highest if the device is registered with Cisco IT. The other factor is how much access the device really needs to do its job (Figure 1). "Printers, for example, only need to talk to print servers and PCs—not the data center network or the extranet environment," West says. "And, they definitely don't need to access source code or HR servers."

Figure 1. Access Depends on How Much We Trust the Device and How Much Access It Really Needs



We're less confident about the devices that appear in the lower part of Figure 1. That's where IoT devices belong. We'll likely develop the security policy for these devices on a case-by-case basis. If the device uses the Android operating system, we can treat it like any other Android device. Securing access by single-function devices, like those for building management or power optimization, for example, is more complicated. "Single-function devices tend to be severely lacking from a security perspective, and many were designed for the consumer market rather than enterprises," West says.

The first consumer IoT devices we expect to allow on the network will be the building management systems that the Workplace Resources organization has requested. Thermostats need very limited access: just to the Workplace Resources management console and the manufacturer's cloud, for software updates. We could define this access policy with Cisco ISE®

When Cisco ISE detected a newly installed thermostat, it would register the device automatically and apply the policy. We wouldn't have to go into the wiring closet to make sure that each of hundreds of thermostats connected to the right port.

Why

The ability to control access by device type will allow us to confidently allow more kinds of devices on the Cisco network to meet our users' needs. The risk of connecting thermostats to the network, for example, will be very low if access is limited to one management system and one cloud service.

"The ability to sense the device type and then dynamically apply policy is very powerful," West says. "It's a win for our security team. It's a win for our IT team. And it's a win for our internal clients because they'll have more freedom to innovate and can deploy faster."

For More Information

To read additional Cisco IT case studies about a variety of business solutions, visit Cisco on Cisco: Inside Cisco IT.

To view Cisco IT webinars and events about related topics, visit Cisco on Cisco Webinars & Events.

Note

This publication describes how Cisco has benefited from the deployment of its own products. Many factors may have contributed to the results and benefits described. Cisco does not guarantee comparable results elsewhere.

CISCO PROVIDES THIS PUBLICATION AS IS WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Some jurisdictions do not allow disclaimer of express or implied warranties; therefore, this disclaimer may not apply to you.

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.**