Cisco IT Brief

Strengthening and Scaling Security with IoT Device Onboarding

The Cisco network has long connected many Internet of Things (IoT) devices such as printers, badge readers, security cameras, building management systems, and sensors. Today, Cisco uses solutions to automate and simplify security for IoT devices that connect to our network and to achieve scalability for more of these devices in the future.

The Security Risk of Unmanaged IoT

When IoT devices aren't managed, they can present a significant security risk to the corporate infrastructure (network, applications, data, etc). A primary reason is that IoT devices are often designed with limited or inadequate security controls. For example, they may not have extensive security features or support for authentication, they may operate on a principle of implicit trust, or they may use unencrypted communication protocols. As a result, these devices may provide an entry point to the corporate network for malware, distributed denial of service (DDoS) attacks, application disruption, data theft, and snooping.

Another risk arises when users bring in devices without IT authorization or visibility. Even devices connected to the network for a short time—such as for a meeting, demonstration, or evaluation—can create a network entry point. Therefore, IT is bound to disable access for these devices by default, and implement a process that is both, secure and user friendly.

Unless the Organization has adequate processes and tools for managing IoT devices, the security risks and associated costs will only compound over time. Within Cisco, the Cisco Identity Services Engine (Cisco ISE) and Cisco TrustSec® [also known as Group Based Policy, or Security Group Tags (SGT)] technology provide the foundation for our IoT security measures.

Streamlining IoT Access and Control with Cisco ISE

Cisco ISE is virtual-appliance software that gives us visibility and control for device access on the Cisco network. We use several Cisco ISE capabilities for IoT security:

- Predefined device profiles allow ISE to detect connection requests from common devices and associate the correct identity and authentication policies. ISE has predefined profiles for printers, smartphones, tablets, and IP phones and cameras. We also create custom profiles as needed for new or specialized devices.
- Access control classifies devices in order to define their permissions for network access. For example, production IoT devices are registered and follow a limited-access policy.

We also make extensive use of ISE capabilities that streamline device onboarding. We have created a simple process in our eStore IT services portal for users to request permission to connect any new device to the Cisco network. The user enters information such as device details and whether it will access sensitive data, factors that determine whether the request can be approved automatically or requires review. Additionally, the user must enter an expiration date for the device connection, a parameter that helps us avoid the security risk of devices that are connected to the network, then forgotten.

When the user request is approved, the relevant data is sent to Cisco ISE and the user may connect the device. For user device requests that can be approved automatically, the process can be completed in less than one hour, which increases user satisfaction. Both users and the IT and InfoSec teams save time because users do not need to open a support case in order to connect the device and many device profiles are already defined in ISE.

Cisco ISE can also obtain needed information from automatic scanning when a device connects to the network for the first time. ISE validates the information against existing device profiles and applies the appropriate security policies. We use this feature to identify devices such as printers and building elements that are associated with a department instead of an individual user.

Streamlining IoT Management with Cisco TrustSec

Cisco TrustSec organizes endpoints into logical security groups that make it easier to manage, apply security policies, and isolate attacks on devices.

Cisco IT Brief

Strengthening and Scaling Security with IoT Device Onboarding

As we use more IoT devices, TrustSec will help us support the needed scalability for managing security. By organizing endpoints into logical security groups, TrustSec provides flexible, software-defined network segmentation for applying security policies. This approach makes defining network access for IoT devices simpler and more adaptable to security and business needs than traditional techniques for LAN segmentation.

IT and Business Benefits

Our use of the Cisco ISE and TrustSec solutions gives us enhanced visibility and control for IoT devices, which improves overall security while allowing us to support more devices for business use.

Robust security visibility, management, and control. Cisco ISE gives us a system to implement the Cisco InfoSec plan for IoT, which specifies security review and registration of devices and control with security policies. TrustSec also creates the right isolation of traffic from IoT devices and limits their access to only the needed applications and data.

Associating devices with individual users means a new device cannot connect to the network without attribution. We can also identify the devices associated with a particular user to verify those registrations are current and appropriate.

Consistent policy deployment. TrustSec applies security policies automatically to each device group, which means our security protections are deployed in a timely and consistent manner. This benefit becomes even more valuable as our IoT deployment expands.

Cost savings. We see an average of 10,000 IoT device registrations annually. By automating each of these cases, we can save more than $350,000 a year.

Time savings. Security groups, policies, and device access profiles save time and effort for IT in provisioning and managing IoT devices. Human-managed cases could take anywhere from 24 hours to 2 weeks to manage, adding additional costs and limiting time IT network operations engineers could be spending optimizing the network, deploying new features, and managing site refreshes.

Ready for IoT growth. The security design and segmentation supported by the Cisco ISE and TrustSec solutions is scalable across the enterprise network and the cloud, which helps us be ready for IoT growth.

Next Steps: New Security Capabilities

In the future, we will be able to define multiple “stacked” policies that will allow differentiated access by IoT devices. This policy design will make it easier to define a device’s access to internal and external resources while continuing to maintain strong controls based on corporate policy.

We will also take advantage of ISE support for the Manufacturer Usage Description (MUD) standard. The MUD file, provided by manufactures, will help ISE to automatically create policies that restrict the device from accessing network traffic that it does not need.

For More Information

Cisco IoT Portfolio

Cisco Identity Services Engine
Cisco TrustSec