How Cisco IT Designed a Secure BYOD Architecture

Cisco IT Methods

Introduction

Many people are comfortable with their personal smartphones, tablets, and laptops, and want to use them for work. So before Cisco IT had a formal bring-your-own-device (BYOD) program, employees were finding their own ways to work on personal devices. This practice created security risks. For example, employees forwarded corporate email to their personal email accounts. Some uploaded corporate documents into public cloud storage services, most of which do not have enterprise-caliber security.

Today we have a formal BYOD program, part of our “Any Device, Anywhere, Anytime” strategy. It takes advantage of the same security architecture we already had in place for company-owned wired and wireless devices. Employees can use supported personal devices for every activity allowed on company-owned devices. That includes connecting to applications in Cisco data centers.

This article explains Cisco IT’s BYOD security policy and architecture.

Challenge: Scale Big, Control Finely

Our BYOD security architecture had to address two challenges. The first challenge was minimizing management overhead as more employees started using more mobile devices. We didn’t want to develop our own software agents. If we did, we’d have to conduct regression testing and revise code whenever device vendors updated their operating systems.

The other challenge was being able to control access based on more than just the user and device. We also wanted to factor in the user’s location, the access method (wired, wireless, or VPN), and the nature of the application feature. For example, we are comfortable allowing a manager to approve a vacation request using an iPhone in a coffee shop. But viewing salaries or approving pay raises is another matter.

Solution: Standardized Image for Popular Mobile Devices

We simplified BYOD support by distinguishing “trusted and secured” devices from just “secured” devices. This distinction determines what activities are allowed.

Employees can do everything with a trusted personal device that they could with a company-owned device. So far, our trusted devices are iPhones, iPads, Windows laptops, and MacOS laptops. We trust the native encryption capabilities on these devices. And our mobile device management (MDM) software can tell if these mobile devices have been rooted or jailbroken. If so, the connection is denied.

Most employees choose to purchase a trusted device. Around 75 percent of our 70,000 registered mobile devices are iPhones or iPads. They can use all of the services shown in Table 1. Employees who want to use an Android or Windows device can do so. However, they can only use some of the services available to trusted devices. Notably, they cannot connect to the Cisco intranet.

Before using any mobile device, employees need to register it with Cisco IT, and set up a 4-digit PIN and 10-minute password timeout. When they register the device, our MDM software enables remote wiping of content. We allow them to download their own software add-ons.

Employees who use laptops download a standardized image and antimalware agent. At the same time, they enroll in the device management system.

Table 1. Mobility Services

Mobility Service	Availability	Description
Single-Number Reach	Any mobile phone	Calls to employee's office number ring the work phone and then the mobile device. If call is unanswered, Cisco® Unity® Connection prompts caller to leave a message.
Mobile Mail Essentials	Any smartphone	Syncs device's native mail, calendar, and contacts applications with the corporate Microsoft Exchange environment. We use Microsoft ActiveSync for iOS, Android, Windows Phone, and BlackBerry.
Cisco WebEx® Meetings	Any smartphone	Enables employees to join WebEx conferences from any smartphone or tablet. They can join by video if they have a front-facing camera. Employees do not need intranet access to use WebEx because it is hosted in the cloud.
Cisco Jabber®	Any compatible smartphone	Provides presence, instant messaging, voice, video, and visual voicemail; smartphone or tablet can connect over the enterprise WLAN or a mobile data service.
Intranet Access and Applications	Trusted devices only	Enables employees to use the Cisco AnyConnect® Secure Mobility Client to access the intranet and internal tools, including WebEx Social and a growing number of Cisco eStore applications. These applications include My Expenses, My PTO, My Approvals, and more.

We Care About Three Things for BYOD Security

1 - Data That Is Stored or Entered on the Device

To secure email, contacts, and other data at rest, we use the native encryption in each device's operating system. One reason is that we know native encryption works. We enforce the use of a PIN to unlock the device and to enable remote wiping of content.

2 - Secure Access to the Cisco Network

To connect to the intranet, employees need the Cisco AnyConnect Secure Mobility Client, available in the Cisco eStore. Cisco AnyConnect automatically sets up a secure VPN connection whenever an employee opens other applications, such as the browser, Cisco Jabber, or Cisco WebEx Social. AnyConnect launches in only 1-2 seconds, without the employee having to log in. This capability makes the user experience as simple as it would be without a VPN connection.

3 – Maintaining the Device's Compliance with Policy

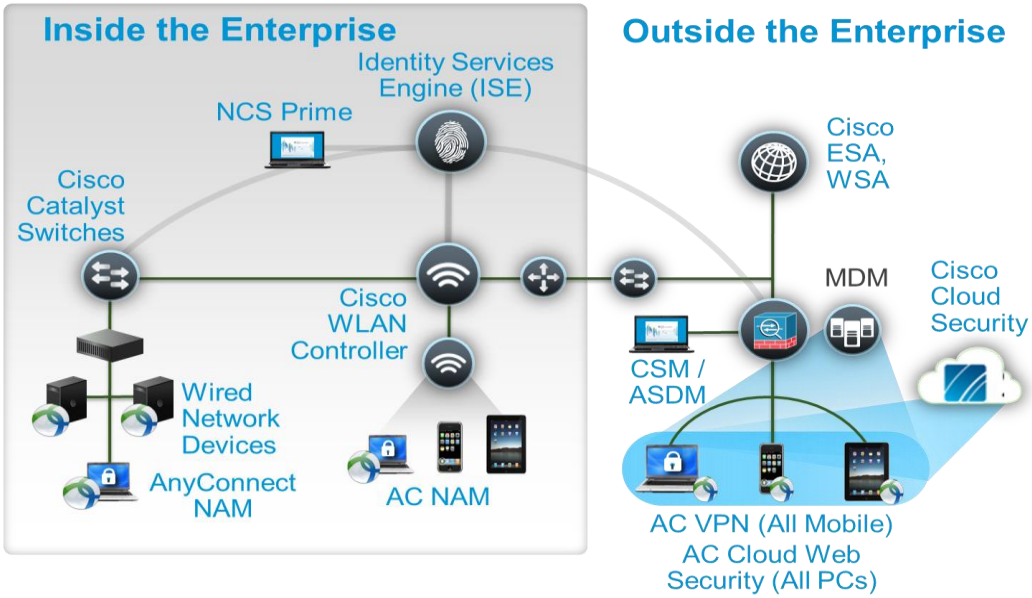
It's one thing to make sure a device is compliant when employees register them. It's another to make sure they maintain their integrity over time. For example, clicking a link to a malicious website could infect the device by depositing malware that exfiltrates data. It could result in a poor user experience by slowing performance or displaying unwanted ads. Or it could result in hackers locking data and refusing to unlock it until they receive payment. We protect personal devices from malware the same way we protect company-owned devices. That is, we use Cisco Web Security Appliance (WSA) to block access to websites. We use Cisco Email Security Appliance (ESA) to block spam that can contain malware.

Currently, we're working on a fourth BYOD security capability. We will control access based on device identity, connection type, and network access privilege. Cisco Identity Services Engine (ISE) is the technology behind this capability.

Security Architecture

Figure 1 shows our security architecture for BYOD. The same architecture is used for both wireless and wired access.

Figure 1. Cisco IT Security Architecture for BYOD



The architecture includes the following elements:

- MDM solution: Each time a device attempts to connect, the MDM tool checks to make sure the device is registered and still complies with security posture. Requirements include an approved OS version, 4-digit PIN, 10-minute timeout, remote wipe enabled, contents encrypted, and antimalware enabled.
- Cisco ISE: After the MDM solution validates that the mobile device complies with security policy; Cisco ISE applies a more nuanced policy for network access. The policy considers who, where, when, and how the mobile device is connecting, and what applications it is trying to access. Cisco ISE denies access to devices that are out of compliance.
- Cisco AnyConnect Secure Mobile Client: Employees who want to access the intranet from trusted devices need to download AnyConnect from the Cisco eStore. AnyConnect supports a secure connection to Cisco using IPSec Internet Key Exchange (IKEv2) and Secure Sockets Layer (SSL) protocols. The client connects through the Cisco Adaptive Security Appliance (ASA) 5585. The ASA authenticates the user and encrypts the mobile data stream so that it cannot be read if intercepted. After initial authentication, AnyConnect can reconnect automatically whenever the employee roams to a different network.
- Cisco WSA: We use Cisco WSA to screen all requests for external websites, whether the employee uses a fixed or mobile device. Cisco WSA evaluates websites based on reputation as well as content. It enforces Cisco internal security policy by blocking or monitoring access to certain websites or by blocking certain features such as chat, messaging, video, and audio. Within Cisco, the WSA blocks only about 2 percent of website requests, but this level amounts to approximately 6 to 7 million requests daily. Most sites are blocked because of web reputation information, while 2 percent (500,000 daily) are blocked because of malware such as Trojans or Trojan downloaders.

- Cisco ESA: Cisco ESA screens all mail to Cisco that originates outside of our company, regardless of the device used to access the email. It blocks email from known spam providers. It also looks for suspicious content or other email irregularities. Of the 5.6 million emails that Cisco receives daily, almost two-thirds are blocked. Many are spearphishing emails. About 15 percent of email with some marketing content is allowed through, but is marked “Marketing” or “Possible Spam” by the Cisco ESA server.
- Cisco Prime™ Infrastructure: We use Cisco Prime Infrastructure to view network connections all the way from the device to the data center, across wired and wireless networks. End-to-end visibility helps us understand, troubleshoot, and fix issues that affect the user experience.
- Cisco Prime Service Catalog and Cisco Process Orchestrator: We used these applications to build the Cisco eStore. Employees visit the eStore to download mobile applications such as Cisco Jabber and Cisco WebEx. The eStore also automates our provisioning process. This process includes screening for eligibility, generating an approval request, configuring the mobile device for remote wipe, provisioning the service, and managing the service lifecycle.

Management

Whenever mobile device vendors update their hardware or software, we test the upgrade in our environment. During testing, we confirm that the changes did not affect security.

Next Steps

Upcoming plans for our BYOD security architecture include:

- Creating an alert for Cisco IT when an employee behaves in an unexpected way: An example might be when a device registered to an employee who lives and works in the United States suddenly connects from another country. This capability requires identity-aware applications. The Cisco Computer Security Incident Response Team (CSIRT) has already built a solution to correlate devices involved in suspicious incidents with the user, for forensics.
- Authenticating devices that don’t use 802.1X: These devices might include building sensors or other network-connected devices that are part of today’s Internet of Things.
- Use Source Fire technology for advanced intrusion prevention: Cisco recently acquired Source Fire. We plan to include the agent in our standard software image. If a downloaded file turns out to be malicious, we’ll be able to recall it from all client devices that downloaded it.

Lessons Learned

- Decide on your security posture before you select the technology to enforce that posture. For example, do you want to require a 10-minute screen lock on your mobile devices? Examples of other requirements include encryption, an antimalware application, and device-naming conventions.
- It’s not all or nothing. Each security capability you add provides value. Even just knowing what is connected to your network, and who owns it, improves your overall security program.

For More Information

- Cisco SAFE Reference Guide
- Cisco SAFE security reference architectures

More Cisco IT information on BYOD

- Cisco IT Case Study
- Cisco IT Insights

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

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.**