How Cisco IT Deployed and Manages BYOD

Cisco IT Methods

Introduction

Before Cisco IT had a bring-your-own-device (BYOD) program, employees were finding their own ways to access email and work files from their own smartphones and tablets. Our BYOD program lowered costs, improved user productivity and satisfaction, and reduced security risks.

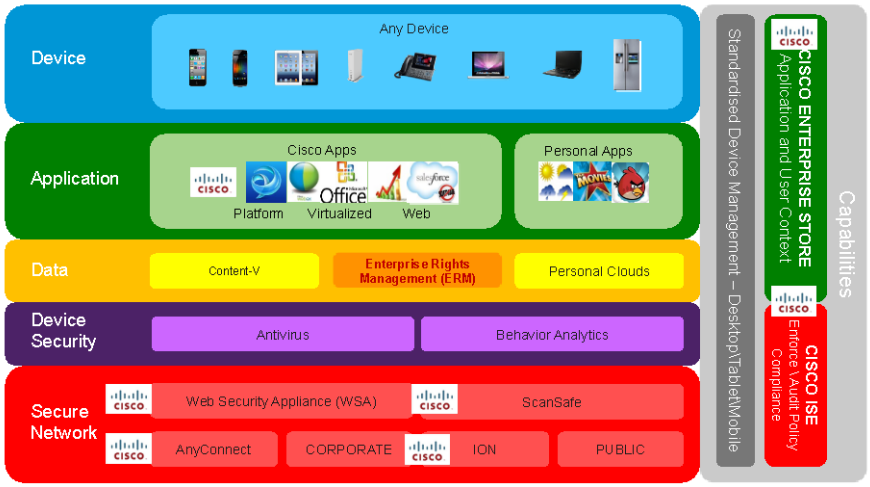
Our BYOD Solution

Today, all Cisco employees can connect to the network using any mobile device that meets Cisco security standards. These include iPhones, iPads, Android devices, Windows devices, and BlackBerry devices. Most employees choose and pay for their own device. Either the employee or Cisco pays for the service plan, depending on the employee's role. Employees use these devices throughout the workday. They can receive calls to their office number on their mobile device. They can synchronize their device's native calendar, email, and contacts with the corporate Microsoft Exchange environment. They can use collaboration applications such as Cisco WebEx® Meetings and Cisco Jabber™. And they can establish a secure VPN connection to the intranet to view internal webpages, approve sales, submit expense reports, find the nearest available meeting room, and more.

Our BYOD solution takes advantage of Cisco technologies we had already deployed for other solutions:

- Wired, wireless, and VPN access networks.
- Cisco Identity Services Engine (ISE), which enforces security policies based on who is asking, when, how, and from what device.
- Unified communications and collaboration applications: These include Cisco Unified Communications Manager, Cisco WebEx, and Cisco Jabber. These applications, too, reside on Cisco Unified Computing System (UCS).

Figure 1. High-Level Architecture



Design

We designed the solution to provide secure access to collaboration tools and the intranet with as little development and test as possible. Therefore, we decided early on to not internally develop software agents for encrypting content on mobile devices and synching with Microsoft Exchange. The reason is that internal development would require constant regression testing as mobile device vendors updated their operating systems. Instead, we decided to use the native encryption, email, calendaring, and contacts capabilities in each device's operating system.

We use Microsoft ActiveSync to synch devices' native email, calendar, and contacts with Microsoft Exchange. ActiveSync also provides basic security functions, such as enforcing use of a PIN to unlock the device and enabling remote content wiping. BlackBerry Enterprise Server (BES) syncs email, calendar, and contacts for BlackBerry users.

Application Design

The Cisco IT Mobility team worked with applications teams throughout the entire project lifecycle: planning, deployment, implementation, and operations. They worked with the applications teams for Windows Messaging, Windows Exchange, Cisco WebEx, Cisco Jabber, and Cisco AnyConnect Secure Mobility Client.

Our guiding principle for application design was to make the user experience at least as easy with a smartphone or tablet as it is with a laptop. To accomplish this, we used the native capabilities of the device's operating system (email, calendaring, encryption, and so on) whenever possible. When another step is necessary, such as establishing a VPN connection, we tried to minimize the actions employees need to take. For example, Cisco AnyConnect automatically sets up a secure VPN connection whenever an employee opens any other application, such as the browser or Cisco Jabber. AnyConnect launches in just one to two seconds, and stays connected until the smartphone or tablet is turned off.

We use APIs to automate management tasks such as making sure that new users are in the right Active Directory group. APIs integrate our internally developed Enterprise Management (EMAN) platform with Active Directory, the third-party mobile device management (MDM) solution, and Cisco AnyConnect Secure Mobility Client.

We also use APIs in the eStore, to automate service provisioning. The eStore is based on Cisco Prime Service Catalog and Cisco Process Orchestrator, and integrates with the MDM, Active Directory, and Cisco ISE. The integration enabled us to automate processes such as screening employees for eligibility, sending an email notification about the service to the employee's manager, provisioning the service, and managing the service lifecycle.

Disaster Recovery

We use the same disaster recovery architecture for email and VPN access that we use for all other employee services. The email servers and Cisco AnyConnect servers are deployed in the Texas metro virtual data center (MVDC), in an active-active, load-balanced configuration. If one site goes down, the server in the other site takes over its workload. When we make changes to BYOD solution architecture, we make the change in all data centers at the same time, and test thoroughly.

Deployment

We deployed the BYOD service in the following phases:

- Automated provisioning of an email client and cellular service.
- Deployed Microsoft ActiveSync so that employees could sync contacts and email with iPhones and Android devices (2009).
- Began using Cisco AnyConnect Secure Mobility Client to connect to the VPN from selected, secured personal devices (2011).
- Built eStore, a one-stop shop for provisioning BYOD services (2012).
- Moved eStore into full production (2013).

We conducted the pilot in one building in San Jose. We used the building's existing wireless infrastructure, a pair of existing public

key infrastructure (PKI) servers in a Cisco data center, and an existing Cisco ISE cluster in another Cisco data center.

After the pilot, we rolled out the BYOD program one country at a time. In each country, we added new business functions one by one. Managers were asked to inform their employees about the program.

Security

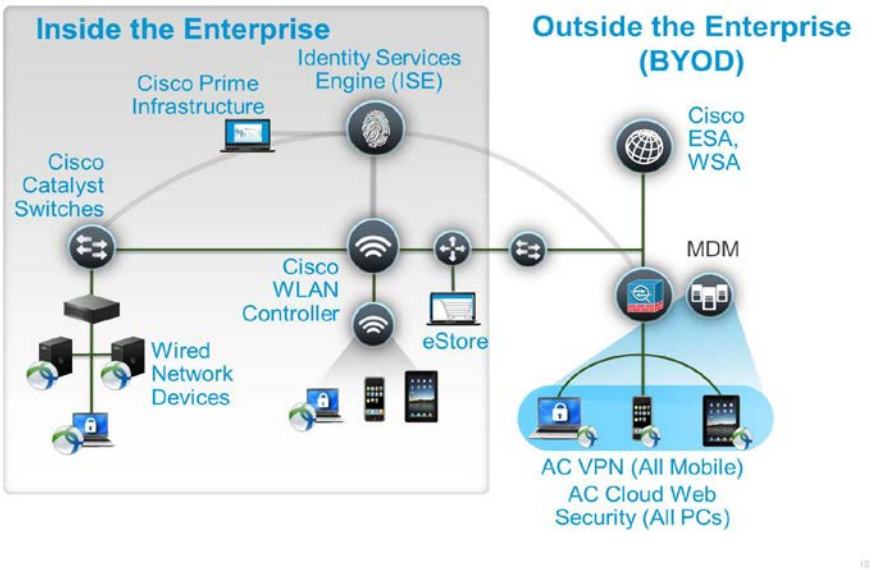
We use the native encryption capabilities in each device's operating system to secure data at rest, such as contacts and email.

Currently, only iPhones and iPads with the latest iOS version and BlackBerry devices meet our security requirements to access to data and applications on the corporate intranet. Devices based on other operating systems can access a subset of capabilities. Some can only access the employee's corporate email, calendar, and contacts.

The architecture for user access includes the following elements, shown in Figure 2:

- MDM solution: We use a third-party MDM application to check device posture and deliver applications: 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 time out, remote wipe enabled, contents encrypted, and anti-malware enabled.
- Cisco Identity Services Engine (ISE): After the MDM solution checks whether mobile devices comply with security policy, Cisco ISE enforces the policy by denying access to devices that are out of compliance. If an employee attempts to access internal resources from a personal device, Cisco ISE controls that access based on Active Directory settings. We put these settings in place before the BYOD program started.
- Cisco AnyConnect Secure Mobile Client: Employees who want to access the intranet from mobile devices need to download the Cisco AnyConnect Secure Mobility Client. AnyConnect supports a secure connection to the intranet using IPsec Internet Key Exchange (IKEv2) and Secure Sockets Layer (SSL) protocols. Clients connect through the Cisco ASA Adaptive Security Appliance 5500, which authenticates the user and encrypts the mobile data stream so that it cannot be read if intercepted.
- Cisco Web Security Appliance (WSA): The WSA screens all requests to access external websites from a mobile device that has the Cisco AnyConnect Secure Mobility Client. WSA evaluates websites based on reputation as well as content. Based on Cisco internal security policy, it can block or monitor access to entire websites or to specific features such as chat, messaging, video, and audio. Cisco IT blocks only about 2 percent of website requests, but this 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 like Trojans or Trojan downloaders.
- Cisco Email Security Appliance (ESA): Cisco ESA screens all mail that originates outside of Cisco, regardless of the device used to access the email. It blocks email from known spam providers, and also looks for suspicious content or other email irregularities. Of the 5.6 million emails Cisco receives daily, almost two-thirds are blocked. About 15 percent of email with some marketing content is allowed through, but the ESA server marks it "Marketing" or "Possible Spam."
- Cisco Prime Infrastructure: Cisco IT uses this application for end-to-end network visibility. Visibility extends from the device (including personal devices) to the data center, across wired and wireless networks. End-to-end visibility helps Cisco IT understand, troubleshoot, and fix issues related to applications and services.
- Cisco Prime Service Catalog and Cisco Process Orchestrator: Cisco employees can download mobile applications such as Cisco Jabber and Cisco WebEx through the Cisco eStore, our internal deployment of Cisco Prime Service Catalog and Cisco Process Orchestrator. The eStore automates the provisioning process. It screens for eligibility, generates an approval request, provisions the service, and manages the service lifecycle.

Figure 2. Cisco IT Uses the Same Security Architecture for BYOD, Wired Access, and Wireless Access



Employees need to register their phone number and/or unique device identifier (UDID) before they can access the Cisco network with a personal device. Device registration allows us to apply encryption to content stored on the device and to perform device management tasks such as conducting an inventory of software versions and device status.

Management

Cisco IT delivers all services, including BYOD, following the IT as a Service (ITaaS) model. We have created a dashboard of BYOD service metrics that we review monthly. These metrics include adoption rates, TCO, the number of support cases, and user satisfaction. If any metric is below our goals, we investigate to find out why, and then take corrective action.

Service Request Management

Initially, we set up an intranet website where employees could add personal devices to the network. Now employees request mobility services by visiting the social platform that Cisco uses internally. EMAN works behind the scenes to do the actual provisioning. We plan to phase out EMAN.

If an employee requests that Cisco pay for the cellular service, the request is routed to the employee's vice president for approval. If the employee pays for the service plan, the eStore sends an email to the employee's manager stating the service has been provisioned.

Configuration Management

Configuration management applies to devices as well as applications.

Whenever mobile device vendors update their hardware or software, we test the upgrade in our environment. We make sure that the changes don't affect security and that the device is still compatible with WebEx, Jabber, and our other mobile applications.

We also periodically update EMAN, the MDM tool, and eStore. We make these updates to take advantage of new devices, operating systems, or applications. For example, when Apple introduced iOS 7 in September 2013, we had to update the Cisco AnyConnect server and client software. We add new applications to the eStore monthly. We follow a process to make sure that we only add applications that are secure, high quality, and provide a good user experience.

Capacity Management

We've been collecting metrics on the BYOD program since 2009. Cisco ASA reports the number of AnyConnect users. Cisco ISE

reports mobile device usage, such as who connects and with what type of device. This information helps us accurately predict demand so that we can scale the infrastructure and decide which devices to support. For example, we saw early on that Symbian devices were losing popularity, so we didn't spend time creating Symbian versions of mobile clients.

Vendor Management

Cisco IT and Cisco Global Procurement negotiate monthly plan fees from service providers. We monitor prices to make sure that discounted voice and data plans continue to decrease at the same rate as consumer mobile services plans. We also regularly renegotiate contracts with the vendors that supply Cisco-owned smartphones. However, employees increasingly prefer to buy their own phones.

Hardware Management

The BYOD program relieved Cisco IT from having to manage mobile devices. Here is what we do manage:

- Approximately 30,000 company-paid cellular service plans from 100 global carriers. We work with Cisco Global Procurement to manage these accounts.
- IP addresses.
- Bandwidth for mobile video: We've already had to increase bandwidth inside Cisco TV studios, where employees tend to connect with multiple devices. We expect video bandwidth to become a bigger challenge when we introduce mobile video applications for employees to attend companywide meetings with an in-person experience.
- Wireless coverage: Our networking team tracks the number of wireless devices each employee uses. This helps us scale the network to provide a great user experience.

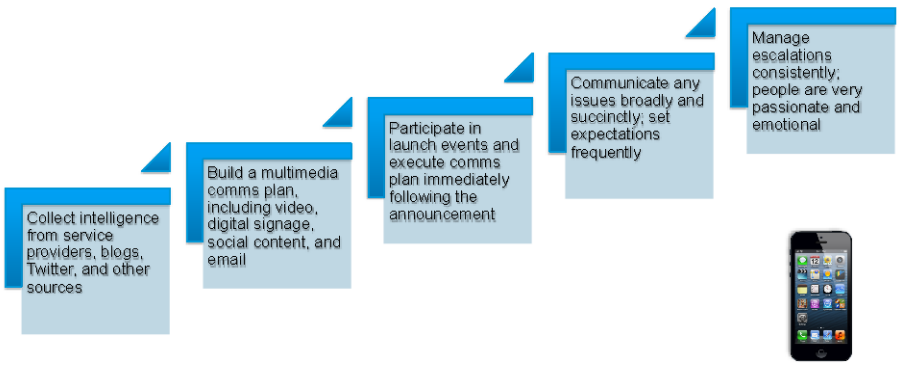
Software Licenses Management

Most of the mobile applications in the eStore are free, so we don't have to manage software licenses. We do manage cloud accounts for each employee. When new employees join Cisco, all of their cloud services are automatically set up. These include email, VPN access, WebEx, Jabber, and others. When employees leave Cisco, all of these accounts are automatically terminated.

Lifecycle Management

Following social media and other news sources helps us find out about upgrades to mobile device hardware and software as soon as we can by (Figure 3). For example, we knew about iOS 7 several months before the actual launch. This prepared us to begin using the beta software the first day it was available. On the day of the official launch, we set up a live blog.

Figure 3. Lifecycle Management



Service Management

Each month we produce a metrics package that includes adoption, helpdesk cases, user satisfaction scores, cost per user, service provider spend, and number of devices that are fully secured. This information helps us decide when to scale the network and which new applications to offer in the eStore.

We constantly monitor the Mobility community on our internal social platform for issues and suggestions. We collaborate closely with the WebEx application team to make the user experience at least as easy with a smartphone or tablet as it is with a laptop.

Service and Support

Incident Support

Despite a 100 percent increase in users, support cases dropped by 25 percent from 2011 to 2012. The reason is that employees can obtain self-help support on our internal social platform, including:

- Choosing the right device and the right service plan
- Getting management authorization
- Signing up for and installing new services
- Supporting services on multiple devices
- Troubleshooting failures problems
- Dealing with unexpected costs (especially while traveling)
- Dealing with lost or stolen phones
- Upgrading to a new phone

Employees who don't find answers to their questions in the online community can post a question or send an email through one of the lively mailer lists. Approximately six Cisco IT staff members manage responses and post new contents in all of these channels. We encourage user participation in the community.

Employees can also call our Global Technical Response Center for issues that are time-sensitive or require a high level of device expertise. We encourage self-support, and most employees prefer it because of the speed of response. The proof is that per-device case numbers have decreased by more than 50 percent since we created the Mobility community in our internal social platform.

Support Team

A small BYOD team makes sure that devices can connect to the network, are secure, and receive email. In addition, we assign at least two people to support every mobile application in the eStore. The BYOD service manager works closely with Global Technical Response Center, Cisco Employee Connection, Global Business Services, and Global Information Services.

Funding

We set up the BYOD program to operate as a self-funding business, paid for through a combination of corporate funding and cross-charges to the business units.

Initial Funding

The BYOD solution did not require the purchase of new infrastructure because it takes advantage of existing network, data center, collaboration, and security architectures. We did add approximately 10 percent more wireless access points. The only application we added was third-party MDM software.

Carrier fees represent 90 percent of the program cost. Infrastructure and management costs for Secure Mobility Services account for the remaining 10 percent.

IT workload decreased despite the addition of tens of thousands of new devices to the network. In 2013, we managed the production service with approximately 33 percent fewer staff than in 2009.

Ongoing Funding

We charge the employee's department a small monthly service fee. These charges offset our costs for developing, maintaining, and delivering mobility services. The charge to business units enabled us to scale the infrastructure as the number of mobile devices increased from 20,000 to 66,000 in four years. We adjust the charges annually to reflect actual infrastructure costs and projected costs to support more users.

Cisco has negotiated contracts with approximately 100 mobile carriers worldwide. Employees who are eligible for Cisco-paid smartphone service are added to the Cisco corporate plan if one is available. The service provider bills Cisco directly. Managers receive reports showing exceptionally large service bills for individual employees. Because their departments pay a portion of the bill, managers are motivated to meet with the employee to suggest changes to behavior or the calling plan.

Most employees pay for their own service plan, family plan, termination fees, overage charges for call minutes or data usage, and additional mobile services. These options are not allowed on a Cisco corporate-paid mobile account. We inform employees about calling plans available for people who expect to be entirely in one country, or roaming for lesser or greater amounts of time.

Lessons Learned

- **Provide ongoing user education to help keep mobile devices secure:** Our internal Mobility online community provides discussion forums, user guides, best practices, schedules of upcoming and recorded webinars, and short training demo videos. Employees who have registered their devices also receive email announcements about vulnerabilities that apply to their current service. They can sign up for mailer aliases for more information.
- **Control costs through regular eligibility reviews for employer-paid service plans:** We provide monthly feedback to employees with very high bills and to these employees' managers. High costs often result when employees switch from a BlackBerry to an iPhone or Android phone, which use more data than BlackBerry phones. Costs can also rise when employees use a mobile phone in a new country and incur roaming charges. Other ways we control costs include reviewing an employee's continued eligibility when a corporate-paid account reaches its service renewal date, and requiring employees who change jobs to reapply for mobile services approval from their new manager.
- **Provide tips to reduce mobile phone minutes:** For example, we recommend that employees:
  - Use the Cisco WebEx dial-back feature when participating in voice conferences from mobile phones.
  - Use Wi-Fi when possible when traveling, to avoid roaming charges for data access.
  - Be aware that using a smartphone as a portable Wi-Fi hotspot can result in very high bills.
- **Provide secure cloud services in response to employee demand:** Cisco information security policies prohibit employees from forwarding or synchronizing confidential information in business emails with an external cloud service that allows viewing messages on a webpage. We inform our employees about the security risks of consumer-grade services. We also try to find tools for the eStore that are as easy to use as less secure consumer cloud tools.
- **Provide resources for user self-support:** Employees who have a question about network access or phone setup might not know whether to call the Cisco helpdesk, the mobile carrier, or the phone retailer. To encourage users to find support information themselves, we continue to add content to the Mobility online community by posting, answering questions in discussion forums, and providing click-to-call access to resources. We also track frequently asked questions and work to make the answers easier to find.
- **Develop policies and procedures for deleting sensitive information when employees leave the company:** As part of the Rules of Use, Cisco requires employees to agree that their mobile device content will be wiped completely when their employment ends. Depending on the circumstances, we either wipe the device remotely or provide instructions for employees to do it themselves.

- **Educate users about Subscriber Identity Module (SIM) cards:** Many support calls are from employees who have purchased a new phone and expect to use it for work after they insert the SIM card for their old phone. Actually, they can't use the new phone until they register the UDID with Cisco IT. We advise employees to not swap SIM cards between different manufacturer's phone models, to avoid unexpected charges. For example, a 50MB plan might last a month on a BlackBerry, but only a day or two on an iPhone.
- **Make sure the wireless address space is large enough:** Some Cisco locations ran out of IP addresses. In response, the network IT operations teams increased the wireless IP address resource space in those locations.
- **Test new mobile applications and self-service portals with employees from multiple business functions:** Include employees who are not in IT, and from different countries.

For More Information

To read additional Cisco IT case studies on a variety of business solutions, visit Cisco on Cisco: Inside Cisco IT www.cisco.com/go/ciscoit.

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.**