Transforming the Enterprise with Secure Mobility

Employees who can work securely anywhere help Cisco gain revenues, improve productivity, and deliver better customer service.

The Journey to Employee Mobility at Cisco

Cisco is a very different company from what it might have been because of secure mobility. Ten years ago, Cisco employees worked in cubicles, usually in the same building and same floor as their manager and the rest of their team. Today, Cisco employees are highly mobile, and they work in global, distributed teams.

For example:

- Cisco has more than 70,000 teleworkers or “day extenders.”
- More than 70 percent of employees work from home at least one day a week, and more than 25,000 work from home three days a week.
- 63 percent of managers manage one or more people remotely.
- 40 percent of Cisco employees do not work in the same city as their manager.
- 28 percent of Cisco employees work in a distributed team; 23 percent are on the road.

Employees are mobile because we support everyone with technology and policies that allow them to work flexibly in terms of time, place, and device. We deliver this capability through Cisco products for secure wireless LAN (WLAN) and home and remote access (Cisco Virtual Office and VPN), as well as softphones, Cisco® WebEx®, Cisco Spark™, and extension mobility features. Our bring your own device (BYOD) policies and program allow employees to use their personal mobile devices to access the Cisco network, after the device is registered and confirmed as compliant with our security requirements for making it a secure or trusted device.

The following statistics indicate the scope of Cisco IT’s secure mobility deployment (all data as of late 2015):

- The corporate wireless network has about 10,400 access points in buildings worldwide, which we are transitioning to the Cisco Aironet® 3700 Series.
- This WLAN is accessed by more than 135,000 corporate laptop computers, most of which run Microsoft Windows, although we also support Apple Macintosh computers and a small number of Linux PCs. This ubiquitous wireless enables Cisco employees to move anywhere within any office and still maintain a high-bandwidth, high-quality connection to the Cisco network.
- Extension mobility capabilities on almost all of the 129,000 hardware phones in Cisco offices let employees log into any Cisco office phone anywhere in the world and make it their own.
- Cisco Jabber® for softphone, instant messaging, and presence for all 135,000 laptops (PC and Mac), and for most of the 70,000 mobile phones and pads owned and used by Cisco employees, enable people to use voice and video connections when they are not near a video phone or office TelePresence™ unit.

- Cisco AnyConnect® VPN client on those same 135,000 laptops, and some 30,000 trusted BYOD mobile devices, enable employees to connect securely to the Cisco network from any Internet connection via wired, wireless, or G3/4 connection.
- Cisco Virtual Office hardware VPN routers in more than 29,000 home offices enable selected employees to work from home as they choose, helping them time-shift work for a more flexible work/life balance and conduct meetings with people in different time zones easier. This solution also fosters traffic avoidance and carbon footprint reduction.
- Employees have registered approximately 70,000 mobile devices in our BYOD program, and about half of those employees have registered multiple devices. Nearly 60 percent of the BYOD devices are Apple iPhones, with a moderate number of Android phones and Apple iPads, as well as a very small number of Windows-based and Blackberry smartphones.

BENEFITS SUMMARY
ENTERPRISE • Cost savings • New revenues and faster sales cycles • Better customer service • Productivity gains • Business continuity • Reduced carbon footprint
EMPLOYEES • Work flexibility • Global teamwork • Higher satisfaction

Cisco has gained multiple business benefits from secure mobility, starting with our first implementation of a WLAN in 2000, through VPN connectivity, and the redesigned office spaces and BYOD policies of recent years. These benefits and details about what we have implemented in our mobility journey are the focus of this article.

The hidden story behind all those benefits is security. In the past, corporate employees worked in one place, secured behind locked doors. Their work was done on a wired private enterprise network, protected by various barriers from the Internet and from the outside world. Security meant guarding the border walls between “inside” and “outside.”

In today’s mobile environment, those borders have evaporated. Work is no longer a place you go to. It’s an activity that can happen in an office, at home, or a customer location, coffee shop, hotel room, or airport. The benefits of this new mobile environment are many. But without new ways to secure it, no enterprise could tolerate the security risks of flexible workplaces. Security is the hidden enabler of the new mobile culture.

How Cisco Benefits from Secure Mobility

Like many enterprises in the information economy, connectivity to our corporate network is a vital resource for helping Cisco employees do their work. By providing secure wireless network connections both inside and outside the office, Cisco has realized benefits for our enterprise business and our employees.

Cost savings. Giving our employees more mobility options has reduced our costs for office facilities, devices, and service plans.

For example, an open-space, flexible office design based on employee mobility, called the Cisco Connected Workplace, gives employees more choice for where and how they work while they are in Cisco offices. It recognizes that many of our employees spend most of their time working from home, at a customer site, or while traveling so they don’t need an assigned, full-time workspace in a Cisco building. Instead, at select Cisco offices globally, employees can work at any open workspace, whether an individual workstation, a group collaboration area, or a traditional meeting room.

As of early 2014, approximately one-quarter of Cisco employees worked in Cisco Connected Workplace environments, producing savings of US$51 million per year from reduced expenses for real estate rent, building construction, facility maintenance and utilities, furniture, cabling, and equipment room space.

We developed a BYOD program in response to employee demand for using their personal smartphones and digital tablets for work communications and tasks. They no longer wanted to carry a separate, company-issued phone for business use. The BYOD program has made our employees happy, and it produces annual savings of $1.35 million because Cisco no longer pays for as many corporate devices and service plans. Online support resources for the BYOD program also produce cost savings through a 33 percent reduction in help-desk requests related to mobility.

BYOD comes with its own security risks. For example, how do you make sure that if an employee's phone is lost or stolen, the wrong people can't download the corporate data inside? Or, worse yet, they can't use the device to access the enterprise network to obtain even more sensitive data? Cisco IT addresses this risk by requiring specific security features on the device, including password locks and remote wipe. We call this the Trusted Device Model.

New revenues and faster sales cycles. Cisco salespeople spend a lot of time out of the office, so it's easy to see how secure mobility can help them work more effectively. What's notable is how much of an impact that mobility can make on revenues. Our internally developed SalesMobile app helps to rapidly process an average of $1.5 billion to $2 billion in Cisco revenues each quarter. Another significant result: Approval of non-standard sales deals is accelerated by up to 40 percent, helping us receive those revenues sooner. In addition to tablets and smartphones, the SalesMobile app is available for selected wearable devices such as the Apple watch.

Cisco Sales Connect is another popular mobile app among salespeople, who use it to easily locate relevant, up-to-date solution brochures and related content, saving nearly 15 minutes for a typical search. This app is also used by many Cisco channel partners globalwide.

Secure mobility has had a significant impact on Cisco's ability to generate more sales and improve the productivity and effectiveness of sales teams. "It's a tremendous benefit if you can spend 30 minutes and get a sale approved during this week or month or quarter, if all it takes is making a phone call outside of office hours," says Steve Bingham, industry director for global enterprise sales. "Without the ability to make calls conveniently, a lot of business activity would keep being pushed out because of time-zone differences."

By using Cisco-developed mobile apps, Bingham is able to view dashboards of current sales activity and handle approvals for deals and routine requests. He also uses the Cisco Jabber and Cisco Collaboration Meeting Rooms (CMR) Cloud apps to start calls from his mobile device for collaboration with his team of sales representatives, no matter where they are located at that moment.

"I'm looking forward to having mobile apps that will enable us to handle even more sales tasks when we are away from the office," says Bingham.

Improved customer service and responsiveness. Mobility allows Cisco salespeople to respond promptly to a text message or phone call from a customer. Cisco IT has developed tailored mobile apps that allow a sales representative to check on the status of a customer order or support case with only a few clicks.

Mobile apps also play a vital role in monitoring and managing our outsourced manufacturing operations. For example, the apps alert Cisco supply chain managers and company executives when a problem in a manufacturing line could impact product shipments.

"We found that smartphones are being used more than laptops, so we are designing our apps to take advantage of that interface," says Mukunda Joshi, engineering manager for Cisco supply chain IT. "Critical alerts appear immediately on the device's home screen, and when the employee clicks on the alert, it automatically opens the app and displays the relevant case so they can take action right away."

Productivity gains from mobility. Employees get more done when they have the ability to work conveniently.

For example:

- Cisco employees who telecommute get back their normal commute time – on average, more than an hour and a half each day – and give back about half of that reclaimed time to the company; that is, when they don't have to spend 95 minutes in traffic, they spend about 45 additional minutes working.
- Employees who remember being tethered to their desks without wireless say that they are able to add more than 45 minutes of productive time to each workday, for an estimated productivity gain of about $280 million per year.
- Cisco employees report that using their mobile devices gives them an extra 15 minutes of productive time each day, for a value of $300 million annually to the company.
- Additionally, many of the 80 mobile apps in our internal Cisco eStore are focused on helping employees work more productively. A one-stop-shop service catalog for all IT services, eStore is built using Cisco Prime Service Catalog and Cisco Process Orchestrator. It's accessible from all device types, via a web browser or mobile app, and integrated with Enterprise Service Management to automate service provisioning across disparate systems. Cisco eStore results in a simplified user experience and faster service.

Table 1 categorizes the Cisco-developed or approved third-party mobile applications that are available for employees to download from our internal eStore.

Table 1. Examples of Mobile Apps Used by Cisco Employees

Cisco Mobility Use Cases	Mobile App Examples
Work Productivity	Maps for Cisco facilities, employee directory, Cisco event information, travel planning and expense reporting, approval handling, and access to cloud-based file storage
Collaboration	Cisco Jabber, Cisco Spark, Cisco WebEx® meetings, internal social media sites
Sales	Sales reports, price quotes, and orders; demonstration apps for Cisco products
Human Resources	Employment information; tracking and request submission for time off
Remote Access	Cisco AnyConnect Secure Mobility Client
Rich Media Communications	Cisco TV
Management Dashboards	Key financial and business intelligence data; supply chain quality monitoring; customer support escalations
Technical Support	Management tools for customer support cases

Employee satisfaction. We form teams with the right employees for the work, no matter where those employees happen to live. As a result, many of our teams are global, with multiple time zones to span for project communications and collaborative work. Our mobility technologies and policies allow these teams to get things done faster and to get the right people involved in decision-making, without requiring someone to be in the office at very early or very late hours to participate in a conference call.

Workplace flexibility also leads to higher employee satisfaction. In a 2014 survey, our mobile employees rated their satisfaction higher by 10 basis points compared to employees who work in traditional offices. Additionally, Cisco Connected Workplace buildings were rated higher by employees than buildings that do not have flexible work areas. "The ability to do my job from anywhere is one of the things that makes Cisco a great place for me to work," says Arun Joshi, director, Cisco on Cisco.

One of the biggest drivers for employee satisfaction and for recruiting new hires, according to human resources surveys, has been the ability to telework. About 70 percent of Cisco employees work from home at least one day a week, and more than 35 percent work at least three days a week from home. These telecommuters tend to work more hours, yet get more satisfaction from having the flexibility to manage their life and work as they please.

More options for business continuity. All Cisco employees have the VPN tools that enable them to work securely from any location, including home, using the best available Internet access. This work flexibility has given us more options for continuing business activity through employee work.

Business continuity typically means backing up data centers or network access to prepare for a major disruption such as a large natural disaster or pandemic. However, most business interruptions occur for smaller reasons, such as road closures due to flooding or snow or building closures due to water leaks.

When a Cisco employee can't work in their normal Cisco office, they can simply work from the next-best option, whether it's home or another company building or any place with Internet access. Cisco has made it through several building outages without missing productive work. And when they are sick, Cisco employees are more likely to work from home, because they know they don't have to be in the building to be productive.

Global teamwork. Teleworking enables more global teamwork. While networking has eliminated most of the distance between global workers, it hasn't done away with time zones. Working from home enables people to meet with each other across a wider span of time, such as early in the morning or later in the evening, without having to go into work and significantly disrupt their lives. The range of people each Cisco employee can work with has expanded by a few extra time zones because of teleworking.

"With the ability to use my smartphone to do my work, I carry my office in my pocket," says Arun Joshi, who manages a team of IT advisors with members located in the United States, the United Kingdom, Australia, and India. "Because everyone on my team travels frequently, secure mobility is especially important because it allows us to be reached easily, especially when we need to discuss urgent customer issues."

Reduced carbon footprint. People who don't drive into work save time and reduce Cisco's carbon footprint. Our typical Cisco teleworker avoids about 95 minutes on the road each day. Some of that time they use to enrich their private lives and some of it to do work, with an estimated additional productive value of $277 million, according to a 2008 Cisco study. That same study showed that by telecommuting, Cisco employees prevented about 47 metric tons of greenhouse gasses from being released and saved themselves more than $10 million per year in fuel costs.

How Cisco Implemented Secure Mobility

Since 1999, we have been creating a secure network infrastructure to support mobility through WLANs, remote access, and the BYOD program.

WLAN coverage in most facilities. A campus or in-building WLAN in most Cisco facilities provides ubiquitous data and voice connectivity for employees, wireless Internet access for guests, and connectivity for mobile devices (Table 2). Regardless of their location, on large campuses or at remote facilities, wireless users have the same experience when connecting to voice, video, and data services on the Cisco network.

Table 2. Cisco Solutions Implemented for Wireless Networking

Wireless Network Solution	Description
Cisco Aironet 3700 Series Access Points	Supports Wi-Fi devices that meet the 802.11ac specification with high-density deployments
Cisco 8500 Series Wireless Controllers	Provides centralized control, management, and troubleshooting for WLANs
Cisco Mobility Services Engine with Cisco Connected Mobile Experiences	The Cisco Mobility Services Engine (Cisco MSE) is a physical or virtual appliance that uses Wi-Fi to increase visibility into the network, deploy location-based mobile services, and strengthen security. The Cisco Connected Mobile Experiences application suite runs on Cisco MSE to locate mobile devices and deliver relevant, personalized services to their users.

Improved security for wireless. Cisco employees recognized the value of wireless mobility long before Cisco IT. Many individuals set up “shadow IT” access points when WLAN technology first became available, because wireless gave them the freedom to move about the room and still be productive. Internal Cisco studies showed that once WLAN became common, employees connected for close to 90 minutes more every workday.

Employees from the “before wireless” era remember meetings where no one could access data they needed to continue a discussion or project. Access to wireless connectivity enabled significant productivity improvements once employees could remain connected anywhere in a Cisco building. With the advances in wireless protocols and bandwidth, employees essentially have no need to ever connect their laptops through a wired Ethernet port, even when working in a Cisco office.

However, extending the traditional wired network to a shared wireless network exposes a lot of traffic to potential snooping. Good security was a critical prerequisite that allowed Cisco IT to make a broad implementation of WLAN in company buildings. Cisco IT participated extensively in standards bodies that developed wireless security protocols, including Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), and WPA2 Enterprise.

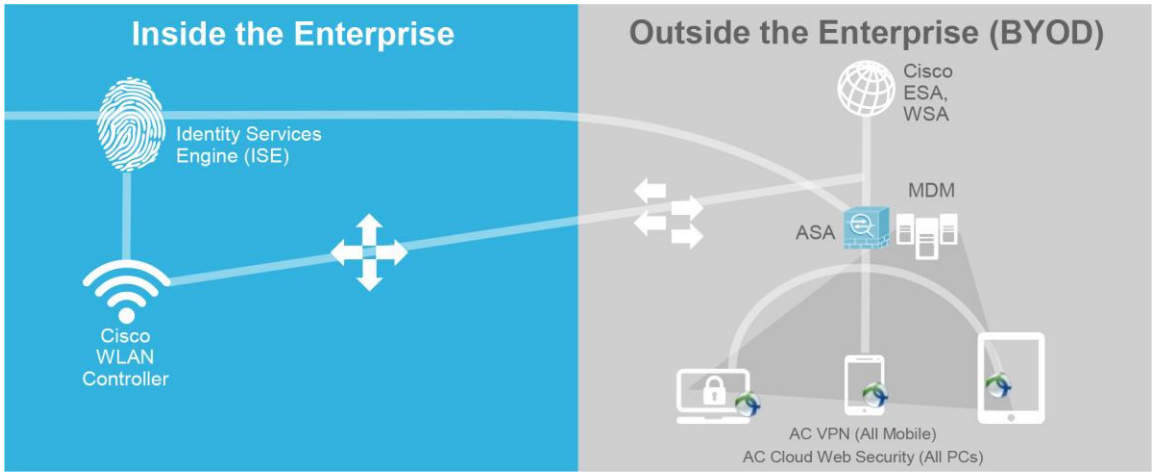
By providing extensive WLAN coverage, we avoid the security risk that arises when employees install unauthorized access points. Additionally, WPA2 authentication and encryption are part of all Cisco IT wireless deployments.

Remote access security. Employees who telecommute use the Cisco Virtual Office solution to connect their corporate laptop, a Cisco IP phone, and perhaps a Cisco TelePresence® endpoint. In addition, many employees often work from home or other locations by using their mobile devices. No matter their location or device, these employees need secure remote access to the Cisco network.

For remote access, Cisco continues to use features such as two-factor user authentication, Secure Sockets Layer (SSL) Layer 2 tunnels, and IP Security (IPsec) Internet Key Exchange (IKE) v2 encryption, as well as Cisco Adaptive Security Appliance (Cisco ASA) firewall protection for VPN connections.

Figure 1 shows how the Cisco IT security infrastructure extends this remote access support for the BYOD mobility program.

Figure 1. Security Infrastructure for Remote and Mobile Access



One of our key protective measures is the context-aware security provided by the Cisco Identity Services Engine (Cisco ISE). Context awareness evaluates the factors of how, where, and when an access attempt is being made as well as the traditional factors of who the users claim to be and what they are trying to do. By evaluating all of these context factors, Cisco ISE can detect a potentially fraudulent login attempt or restrict the level and type of user access, such as when an employee uses a public Wi-Fi network instead of a secure VPN.

Table 3 lists additional Cisco solutions we use to manage remote access security.

Table 3. Cisco Solutions Implemented for Remote Access Security

Remote Access Security Solution	Description
Cisco Cisco ISE	Enforces our security requirements based on user, device, and access context as well as mobile device compliance with corporate policy.
Cisco TrustSec® technology	Uses software-defined segmentation to simplify provisioning of network access, accelerate security operations, and consistently enforce policy anywhere in the network.
Cisco ASA	Authenticates the user and encrypts the mobile data stream so it cannot be read if intercepted
Cisco Email Security Appliance (Cisco ESA)	Screens all email that originates outside Cisco, blocks known spam, and looks for suspicious content or irregularities.
Cisco Web Security Appliance (Cisco WSA)	Screens all requests to access external websites from a device that has the Cisco AnyConnect Secure Mobility Client and is connected through Cisco IT's web security gateways. Based on Cisco's internal security policy, Cisco WSA can block or monitor access to entire websites or to specific features such as chat, messaging, video, and audio.
Cisco Virtual Office	Delivers secure, comprehensive, and manageable IP phone, wireless, data, and video services to teleworkers over an encrypted VPN, giving users a transparent, office-caliber experience.
Cisco AnyConnect Clients	Provides reliable, encrypted, and persistent connectivity to the corporate network from laptops, smartphones, and tablets. Operates in conjunction with the mobile device management (MDM) system.

BYOD security. Our BYOD program takes advantage of the existing security architecture for remote access, but it adds device-focused protective measures.

A big concern of any BYOD program is what information and applications a mobile device can access when it connects to the corporate network. We handle this concern by categorizing specific devices as either secured or trusted.

Secured devices must support a 10-minute PIN lock timeout, a 6-digit PIN, and the ability for Cisco IT to remotely wipe the device. Any devices that do not respect these settings simply cannot connect to our network.

Trusted devices meet all of these requirements plus they support native content encryption in the operating system and remote management by Cisco IT. Encryption is important because it allows the user to access and store sensitive information from within Cisco's core network. Additionally, Cisco IT uses third-party MDM applications to make sure the device is registered and complies with the corporate security posture.

Figure 2 shows how the distinction of trusted and secured devices determines which applications and network areas a user may access.

Figure 2. Application Access for Secured versus Trusted Devices

Secured devices can access email, calendars, contacts, Cisco WebEx conferences, Cisco Spark, and Cisco Jabber. Going beyond these basic services, trusted devices can also access applications and information within the Cisco core network, including sensitive corporate data.

To connect to the intranet, employees need to download onto their device the Cisco AnyConnect Secure Mobility Client, which is available in the Cisco eStore. Cisco AnyConnect provides employees secure access to corporate resources and business-critical applications so they can work from anywhere, whether they're on their corporate laptop or personal mobile device. The Cisco AnyConnect client launches in 1 to 2 seconds, without the employee having to log in. This capability makes the user experience as simple and consistent as it would be without a VPN connection.

Bringing Secure Mobility into Your Enterprise

IT and information security departments have always struggled to enable the business to do more while also limiting the risks associated with new capabilities. Now, security technology has reached a level that can give an enterprise confidence about extending mobility to more employees and business functions. To help customers plan their deployment, we offer design guides and Cisco Validated Designs for many aspects of a secure mobility program.

Cisco's journey to employee mobility has been a gradual one, with each step building on the other, and all built upon the foundation of end-to-end network security. Our customers can apply a similar journey to supporting mobility for their employees and reap the benefits of business transformation along the way.

For More Information

Cisco IT Methods: How Cisco IT Designed a Secure BYOD Architecture

Cisco IT Methods: How Cisco IT Deployed and Manages BYOD

Cisco security solutions

Cisco mobility solutions

Cisco remote access solutions

Cisco Validated Design: Campus LAN and Wireless LAN Design Summary

Remote Access VPN Technology Design Guide

BYOD Design Guide

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.**