



Six Essential Steps for Unleashing the Power of Enterprise Mobility

Not too long ago, only a subset of enterprise workers was mobile. Today, nearly all workers are. This new mobile majority, influenced by the advanced capabilities of consumer devices, wants to use those devices for work. As a result:

- Workers are demanding virtual workspaces for any device with rich, collaborative experiences.
- Business leaders want to use the bring-your-own-device (BYOD) trend to reduce costs, attract and retain top talent, promote new business models, increase productivity, and improve the customer experience.
- IT must maintain adequate security measures and compliance with government and industry regulations, while delivering a next-generation workspace that is mobile, social, virtual, and visual.

By enabling new and more efficient ways of working, the next-generation workspace has the potential to build complex, talent-based competitive advantage. However, devices are merely the first step to workspace transformation.

A growing number of enterprises are taking advantage of external services to promote internal alignment across IT and business stakeholder groups and to develop a comprehensive strategy for their mobility initiatives. As you determine whether to take on this initiative alone or seek the assistance of an experienced partner to plan your mobility initiative, consider the six essential steps in Table 1.

Figure 1. The Workspace Redefined

Then: Deskbound	Now: Untethered
PC based	Handhelds rule
IT led	Employee/customer driven
Company-provided devices	Employee-owned devices
Limited connectivity	Ubiquitous connectivity
Closed network	Open network
Mobile voice	Mobile video
Separate workers	Collaborative workers
Personal productivity	Business process productivity

Device Freedom Without IT Compromise

The mobility experts at Cisco Services have helped companies all over the world untether the workforce.



Table 1. Six Essential Steps for Unleashing the Power of Enterprise Mobility in Your Organization

1	Develop a comprehensive enterprise mobility strategy
2	Optimize for virtualization
3	Prepare for the proliferation of devices
4	Determine your application strategy
5	Secure your devices, data, and network
6	Improve worker productivity and the end-user experience



Step 1: Develop a Comprehensive Enterprise Mobility Strategy

Increased mobility has enterprises reacting to requests to get mobile devices, such as smartphones or tablets, on the wireless LAN (WLAN), which in itself not difficult. All you need are a WLAN controller and a security product. However, this is purely a tactical approach that addresses only one aspect of mobility and can create system-wide issues such as poor application performance, security breaches, subpar user experiences, and more. Checklist 1 lists the steps in developing a comprehensive enterprise mobility strategy.

Checklist 1.

1. Define and prioritize what you want mobility to do for your organization
2. Clearly articulate the what, how, where, which, who, and when
3. Determine what you do not want to do
4. Identify the business use cases that support your objectives
5. Develop a corresponding mobility architecture that promotes business value
6. Assess network, security, data center, communications, and applications infrastructures

Services Snapshot

Cisco® Services worked with a metropolitan medical center to help it develop a BYOD strategy. The hospital wanted to provide medical staff and contractors secure access to applications and patient data from both personally owned and hospital-provided devices.

The hospital also wanted to provide better security and control for guest access to the network. Cisco Services began by bringing primary hospital stakeholders together. Working with network, human resources, security, IT risk and compliance, and mobility groups, consensus was built around mobility needs and use cases. We then delivered an assessment that identified gaps in the medical center's current infrastructure and provided an evolutionary roadmap to an end state architecture that supports the use cases while enabling the hospital to comply with strict security and privacy regulations.

Define and Prioritize What You Want Mobility to Do for Your Organization

When Cisco Services work with enterprises to help develop a mobility strategy, we begin by bringing both business and technical teams to the table to define and prioritize what business goals will be enhanced or enabled by mobility.

Clearly Articulate the What, How, Where, Which, Who, and When

After you've clearly articulated "why" you need enhanced mobility, move on to these questions:

- What are the challenges faced by your IT organization and employees?
- How can mobility help you solve these problems?
- Where will the mobility solutions be used?
- Which user groups need them, and which applications are required to keep them productive?
- Who will manage them?
- When do you want or need to deploy them?

Determine What You Do Not Want to Do

When you have determined what you want to do, make sure to take the time to determine what you do not want to do, because this can strongly influence the mobility architecture you ultimately deploy. Regulatory, compliance, and security groups will be strong contributors here and throughout the process.

Identify the Business Use Cases That Support Your Objectives

We've found that the most common use cases—across industries—are:

- Security for IT-provided mobile devices
- Onboarding personal mobile devices to the corporate network
- Wireless guest access
- Third-party (for example, contractor and partner) mobile device access

Develop a Corresponding Mobility Architecture That Promotes Business Value

These uses cases are instrumental in developing a corresponding mobility strategy and architecture that will promote business value around your stated goals. This approach will prevent you from taking an IT path with which you are not comfortable or that the business will not support.

Assess Network, Security, Data Center, Communications, and Applications Infrastructures

Your existing infrastructure will have a significant effect on the mobility architecture design and how it will evolve over time. Therefore it is essential to assess the following domains.

- Network infrastructure to make sure it can deliver optimal application performance and a positive user experience
- Security infrastructure and policy management to make sure of robust security across network, device, data, and application layers in support of enterprise, organizational, and regulatory compliance policies
- Data center infrastructure to make sure compute and storage resources are virtualized and can be scaled to support users and applications effectively
- Communications infrastructure to determine if it can support high-quality voice and video
- Application infrastructure to make sure it can support advanced collaborative capabilities such as unified communications and web-based video conferencing can be extended to any device, anywhere

Step 2: Optimize for Virtualization

Enterprise IT leaders surveyed in the Cisco 2012 BYOD and Virtualization Study indicated that half or more of their organization's employees could benefit from workspace virtualization. Cisco Services work with many enterprises on virtualization initiatives. Some are just embarking on desktop virtualization. Others have deployed virtual desktops and are not getting the hoped-for results.

Whatever the case, there are several ways we help our customers increase value from their virtualization investments. One thing we tell all of our customers is that virtualization should be about more than cutting costs and improving security. Today's highly competitive environments require collaboration-friendly virtual desktops. Any virtualization initiative should help employees access the people and resources they need to do their jobs effectively.

Checklist 2 is a step-by-step breakdown of how you can optimize for virtualization.

Checklist 2.

1. Collaboration-enable your virtual desktops
2. Consider user experience initially at the time of deployment
3. Create a consistent collaboration experience across devices
4. Explore different deployment and financing options to manage TCO
5. Plan for a time- and resource-intensive process

Collaboration-Enable Your Virtual Desktops

Do more than virtualize the desktop—virtualize the workspace, so you can provide advanced collaboration capabilities such as presence, IM, location, and voice and video conferencing.

Consider User Experience Initially at the Time of Deployment

User experience is the single biggest competitive differentiator for consumer technology. If voice and video quality is poor, no one will use their virtual workspace. We also recommend defining use cases for today and tomorrow to make sure that quality of experience can be maintained as new use cases are added.

Considering services for your mobility initiative?
Look for:

- An understanding of the complexities around accelerating your transition
- A track record of transforming IT into a business and revenue enabler
- Experience aligning network and business teams around use cases and objectives
- Proven ability to reduce total cost of ownership (TCO) and create return on investment (ROI)

Create a Consistent Collaboration Experience Across Devices

It's also important to create a consistent collaboration experience across devices. To enable a "work from anywhere, anytime" culture requires bringing unified communications and collaboration tools together under a single, common interface. They must be accessible from any device, in any location. Make sure your virtual desktop applications extend into your unified communications environment.

Explore Different Deployment and Financing Options to Manage TCO

Many companies today are fiscally conservative. We always advise exploring different deployment and financing options to manage your TCO. Return on infrastructure investment for desktop virtualization typically takes three or more years. There are new public cloud-based deployment models that enable the cost-efficient, self-service delivery of virtualized desktops. Strategic financing can also help bridge the gap between technology requirements and budget availability.

Plan for a Time- and Resource-Intensive Process

Planning, building, and managing a highly collaborative virtualized environment are difficult tasks. They require traditionally siloed teams within the enterprise to work together, including client computing, desktop applications, networking, security, and data center. Converging these environments requires time and expertise throughout the entire lifecycle of desktop virtualization.

A new study from Forrester¹ found that "Network teams lack the time and resources to manage and optimize their company's infrastructure given the growing business demand." Forrester recommends partnering with a strategic solution provider that has:

- A strong services arm
- Deep vertical expertise
- Experience in using the network to improve business processes
- Validated solutions
- Integrated roadmaps to promote value and protect your investment
- A modular building block approach that spans the use case spectrum—from basic guest access to desktop virtualization

Step 3: Prepare for the Proliferation of Devices

In our recent BYOD and virtualization study, Cisco surveyed 600 enterprise IT leaders from 18 industries. Among the top 10 insights:

- Mobility is pervasive: 78 percent of U.S. white collar workers use a mobile device for work purposes, and they want to control their work experience.
- The growth of mobility has affected IT profoundly: by 2014, the average number of connected devices per knowledge worker will reach 3.3.
- BYOD delivers several benefits to the enterprise; it also brings its share of challenges.

Checklist 3.

1. Use a holistic, architectural approach for everything from switches to applications
2. Use a unified network infrastructure that facilitates workspace delivery over wired, wireless, and cellular networks
3. Create a comprehensive, unified end-to-end architecture to support users, devices, and locations

¹Forrester, September 2011, Bridging the Expectations Gap: Intelligent Network Services Scale and Transform Your Business.

Services Snapshot

Cisco Services worked with a leading automobile manufacturer that initially wanted to allow employee-owned tablets onto its network.

Discrete functional IT groups were taking different approaches, creating ongoing issues. Cisco Services helped the manufacturer unify the effort and identify and prioritize use cases and develop a strategy to solve the mobility issues. The best practices and guidance we provided enabled the manufacturing company to avoid security risks and successfully meet the expectations of primary executives.

In the last 18 months, Cisco itself has witnessed some 13,000 iPads enter its BYOD program. And Cisco IT now supports more than 60,000 BYOD smartphones. If you are not feeling the pressure to “get in front” of BYOD, you soon will. How do you prevent a proliferation of employee-owned devices from burying your IT department and putting corporate data at risk? The most important step is to apply an architectural approach to BYOD.

Holistic, Architectural Approach for Everything from Switches to Applications

A growing number of managers are now acknowledging the need for a more holistic approach—one that is scalable and addresses mobility, security, virtualization, and network policy management—in order to keep management costs in line while simultaneously providing optimal experiences where savings can be realized, according to the 2012 Cisco IBSG Horizons Study.

Unified Network Infrastructure That Facilitates Workspace Delivery over All Networks

An architectural approach provides an organizing principle—or framework—for everything from switches and routers to video, servers, wireless access points, security, and business applications. It gives you a solid foundation on which to build and evolve BYOD plans and policies. An architectural approach also:

- Improves quality of experience
- Makes changes to business processes possible
- Enhances security, so intellectual property is protected

A Comprehensive, Unified End-to-End Architecture to Support Users, Devices, and Locations

Without an architectural approach, BYOD can actually hinder productivity instead of helping it due to poor performance and employees opting not to use company-provided productivity tools because they do not perform well on employees’ personal devices.

TCO will also be negatively affected without a mobility framework. Enterprises will benefit significantly by making make sure their framework is a comprehensive, end-to-end architecture that includes:

- A unified network infrastructure that facilitates secure, virtual workspace delivery across wired, wireless, and cellular networks and makes it possible to create scalable policies that can accommodate mass mobility.
- Unified policy across wired, wireless, and VPN; managed and BYOD assets; and mobile device management integration as well as context-based control, advanced segmentation, and user-specific services to make sure the right people and devices have access to the right information in the right location and to prioritize voice and video traffic.
- Unified management that provides comprehensive visibility that covers users, devices, location, and posture for both networking and mobility to enable operational efficiency and low TCO through auto provisioning, programmable networks, intuitive troubleshooting, and energy management.

Step 4: Determine Your Application Strategy

It is no longer enough to secure mobile devices. The CIO is now going to be dealing with managing public and private mobile applications. To date, security for mobility has been “all or nothing.” Virtual private networks (VPNs) gave you access to all corporate network resources, or you had very limited email and calendaring access. The untethered enterprise necessitates a shift in security practices and a new application strategy.

Checklist 4.

1. Consider a hosted enterprise app store
2. Look for a rapid, reliable, and secure vetting process for applications
3. Make sure of detection of noncompliant apps and prohibit their use
4. Seek guidance to determine which apps will be mobile, virtual, and/or hybrid

Consider a Hosted Enterprise App Store

IT security teams are usually directed toward securing the network and the devices connected to it, versus securing the applications that run on those devices. Many organizations lack the resources to evaluate an application’s ability to handle sensitive information throughout its lifecycle.

Look for a Rapid, Reliable, and Secure Vetting Process for Applications

Companies rarely have the resources to monitor sites that could breed malware, nor do they have the ability to maintain heuristic algorithms to identify such sites prior to infection. And those that decide to secure mobile apps themselves might end up having to prioritize remediations, leaving them vulnerable. For these and other reasons, a hosted enterprise app store should be strongly considered.

Make Sure of Detection of Noncompliant Apps and Prohibit Their Use

An app store needs to go beyond basic malware protection to include mobile threat management, risk intelligence, and vulnerability tracking. Look for more than a red light/green light approach to the vetting of mobile apps. The enterprise app store should vet apps using enterprise security policies and business rules that meet your specific business needs.

Seek Guidance to Determine Which Apps Will Be Mobile, Virtual, and/or Hybrid

We almost always recommend seeking guidance from professional services to help you determine which apps will be mobile, virtual, and/or hybrid.

Step 5: Secure Your Devices, Data, and Network

In a 2012 survey of IT executives and CEOs, nearly half of the companies that permit mobility and BYOD reported experiencing a data or security breach as a result of an employee-owned device accessing the corporate network. Careful planning can help your company avoid being part of that statistic.

In choosing to support BYOD, it is essential to evolve your policy and governance models to address the effects of BYOD on the enterprise.

Services Snapshot

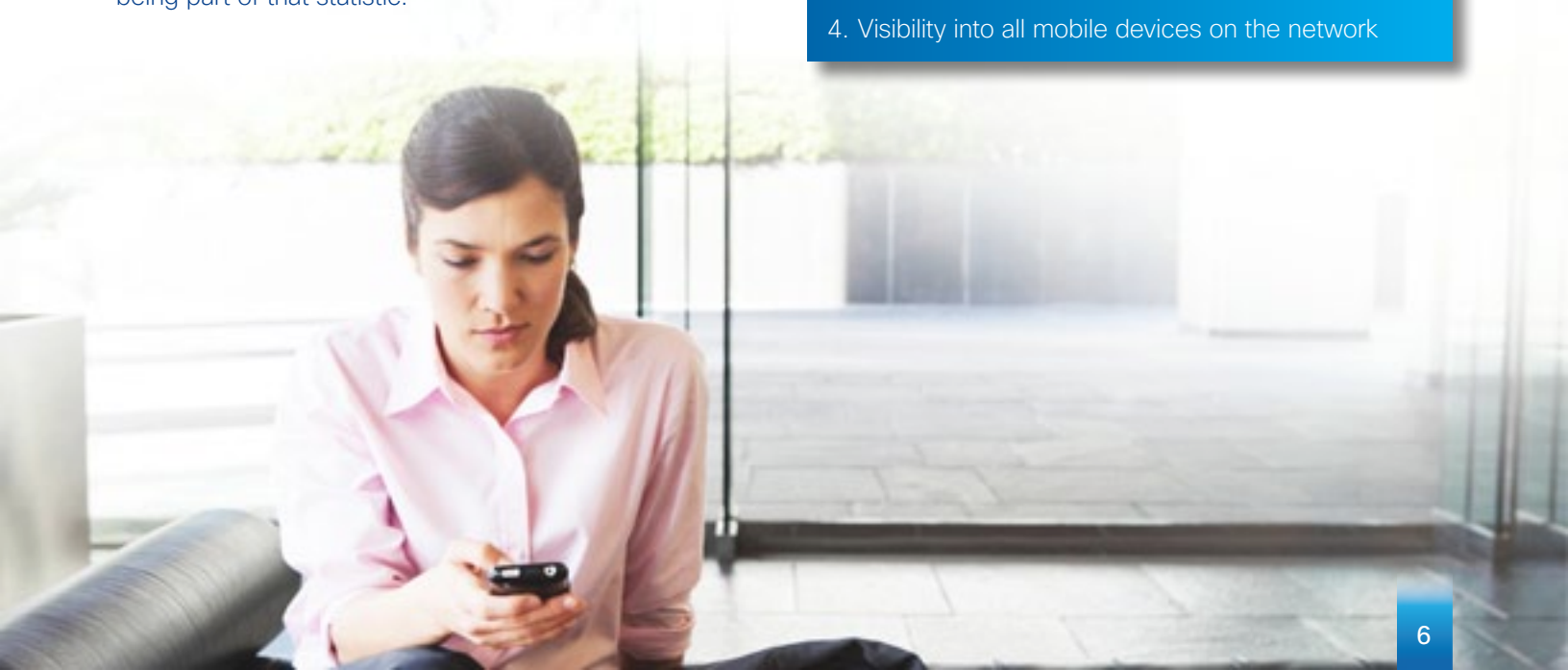
Cisco Services recently worked with a large U.S. drugstore chain. The retailer wanted to use mobility to enable faster inventory management and better collaboration with supply chain partners. Specifically, the retailer was looking for secure, high-speed wireless access from any device. And it wanted to provide that access for employees, contractors, and guests.

The Cisco Services team led IT and business stakeholders in defining use cases and the end-state network architecture. The disparate requirements from the retailer's various teams were then mapped into a phased migration roadmap that helped the IT group evolve the infrastructure supporting the retail stores, distribution centers, and the company's main corporate campus. As a result, the retailer has realized reduced risks and managed the project on budget by implementing a multiphase approach to meet its security requirements for a BYOD environment.

Checklist 5 is a step-by-step breakdown of how to secure your devices, data, and network.

Checklist 5.

1. IT pushing of capability down to end devices
2. Situational control and automated geo-specific policies
3. Partitioning of personal data from corporate data, history, and logging for business communications only
4. Visibility into all mobile devices on the network



IT Pushing of Capability Down to End Devices

IT needs to be able to push capabilities down to end devices and access control for both on-premises and off-premises apps, while providing pull capabilities for users, so they can self-provision apps.

Situational Control and Automated Geo-Specific Policies

IT must have the ability to apply situational control policies (for example, for disabling cameras on mobile devices in order to protect on-premises company assets when employees and guests are on corporate premises or in restricted areas). Another must have? The ability to remotely locate, lock, and wipe devices should there be a theft or if an employee leaves the company. It is also essential to be able to automate geo-specific policies to control roaming costs when workers are out of country.

Partitioning of Personal Data from Corporate Data, History, and Logging for Business Communications

Because BYOD devices will also be used for nonbusiness activities, IT must be able to partition personal data from corporate data and enable access to personal apps without compromising business access.

For compliance (audit) purposes, IT also needs to be able to maintain history and logging capabilities for business communications without imposing these requirements on personal communications.

Visibility into All Mobile Devices on the Network

It is important to obtain good visibility into how many mobile devices are on the network, how those devices are being used, and by whom to make sure of high quality of experience.

Our experience has shown us that these types of capabilities require unified policy management across the entire organization for both business and technical domains, including information security policies, legal requirements, human resource policies, government standards and regulations, industry standards and regulations, internal corporate regulations, workspace resources, and vendor management.

Step 6: Improve Worker Productivity and End-User Experience

The clear trend in the enterprise is to enable people to work in their own way, regardless of where they are and what device they are using. Embracing this opportunity will help you unlock the value in your people and your IT infrastructure so you can increase productivity, business agility, and customer satisfaction.

Checklist 6.

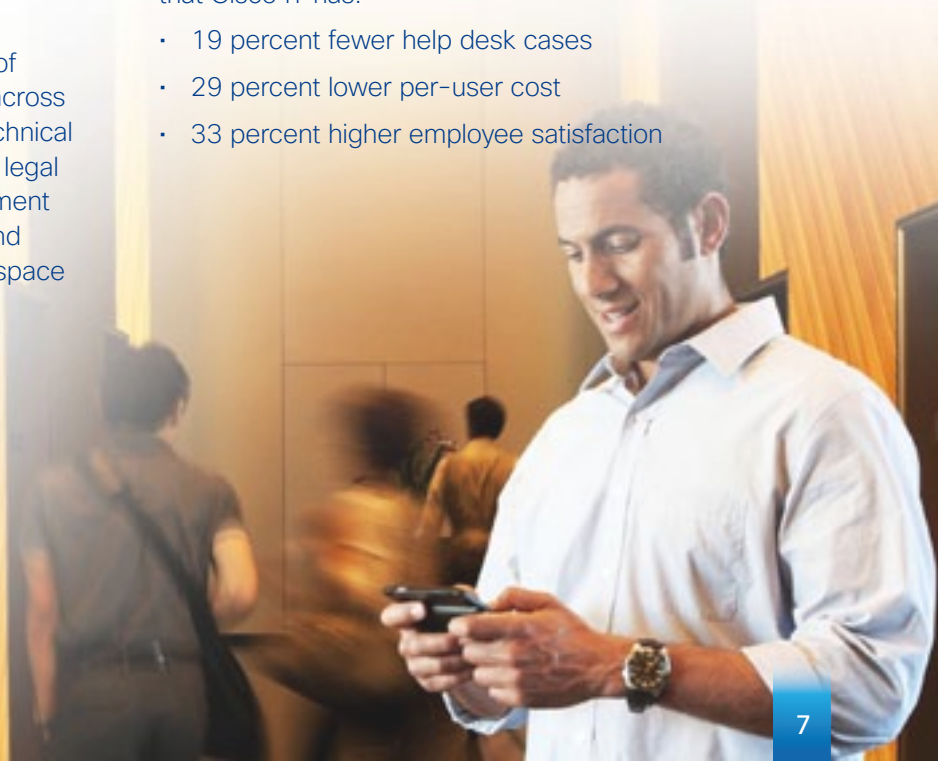
1. Do more than passively allow BYOD: actively embrace it
2. Do more than provide mobility for sales: think “all-company” mobility
3. Do more than improve business processes: redefine workflows

In our work with enterprises from all over the world, we have found that these primary strategies can help you derive maximum value from your enterprise mobility initiative.

Do More than Passively Allow BYOD: Actively Embrace It

BYOD can deliver tangible benefits as evidenced by the Cisco IT BYOD implementation results². Cisco employees pay an average of \$600 out of pocket for devices that will give them more control over their work experience. Cisco estimates that the annual benefits from BYOD range from \$300 to \$1,300 per employee, depending on the employee’s job role. Preliminary findings also indicate that Cisco IT has:

- 19 percent fewer help desk cases
- 29 percent lower per-user cost
- 33 percent higher employee satisfaction



Do More than Provide Mobility Capabilities for Sales and Execs: Think “All-Company” Mobility

The definition of mobility is expanding to include not just “road warriors” but also “corridor warriors,” as well as guest and home workers. Make sure your mobility architecture is designed to accommodate them all. Then create a phased implementation plan. Determine which users and business processes you want to affect first and move forward at a pace that makes sense for your enterprise.

Do More than Improve Business Processes: Redefine Workflows

The true value of mobility is its ability to transform workflows. Look for ways to use mobility, not just for incremental process improvements, but also to change the way work is done in your organization.

- When insurance claims agents are equipped with tablets, they can capture pictures and video of damaged property, have video calls with claims adjusters to resolve problems, and then securely file claims, all without leaving the customer’s side. These collaborative capabilities accelerate time to resolution.
- When healthcare teams have mobile devices, they can access patient files from any location. They can click to launch virtual consults with specialists—no matter where the specialists reside—and view pertinent medical data at the same time. These rich interactions improve care while reducing costs.

- When field agents have remote, on-demand access to product diagrams, video training, and expert assistance, they can quickly resolve complex problems. These advanced capabilities make it possible for agents to work more efficiently and increase customer satisfaction.

The potential business value of a transformative business process is significant. Here is one estimate: by enabling virtual access to remote experts, enterprises can expect a 4- to 6-week reduction in a typical product development lifecycle, valued at \$2-3 million for a major product. Incremental margins from this reduced time to market are valued at \$35-50 million³.

Cisco Services Can Help You

The next-generation mobile workspace will help propel enterprise productivity, company growth, and innovation, and it requires comprehensive, network-centric expertise and best-in-class, proven solutions. Cisco and its partners can deliver business value for your mobility initiative with smart services and solutions for everything from identifying objectives, business requirements, and use cases to operating, securing, maintaining, and supporting your mobility architecture.

For more information about Cisco Unified Workspace solutions and services to help you maximize the business benefits of mobility and BYOD securely for your company, [click here](#).



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.

©2013. Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R) This document is Cisco Public.

²Cisco: The Business Case for Tablets

³Cisco: The Business Case for Tablets