Cisco and Citrix for Productive and Secure Enterprise Mobility

CITRIX®

CISCO

Contents

Introduction

Implementing enterprise mobility initiatives has become a priority for virtually every IT organization. Modern workers increasingly see work not as a physical location but as an activity facilitated and made more productive by a dynamic choice of evolving mobile technologies. An ever-increasing array of laptops, tablets, and smartphones has fundamentally changed the ways people collaborate and communicate for work, raising new business expectations for productivity and streamlined operations. At the same time that adopting enterprise mobility helps attract and enable talented workers, it can present new concerns for IT departments.

Organizations everywhere must come to terms with this new reality, whether supporting bring-your-own (BYO) devices or corporate-owned, personally enabled (COPE) devices. Many have attempted to accommodate this new class of mobile user on existing infrastructure, with less-than-desirable security, performance, and user experience. Failing to address these requirements can present risks to the enterprise, hamper expansion of a mobile and productive workforce, and inhibit the organization's agility and competitiveness in the process.

Building an effective mobility infrastructure that is extensible and scalable to meet the full set of business needs and variety of user workstyles can be complex, extending beyond the abilities of any one vendor (Figure 1). Moreover, the complex technology and the significant number of necessary integration points can mean significant time and expenditures for organizations attempting to put the pieces together on their own.

With a wealth of experience and expertise, Cisco and Citrix are bringing their industry-leading technologies together in a tested and validated Cisco Mobile Workspace Solution with Citrix, including important integration for simplified deployment and operation. By taking an architectural approach and building on this joint framework as new mobility requirements emerge, organizations can be confident that their current and future mobility and BYOD investments will result in positive business outcomes.

Figure 1. Integrating all of the technologies required for secure enterprise mobility can be complex, expensive, and difficult to scale.

Mobile Infrastructure Opportunities and Challenges

Effective enterprise mobility solutions must honor seemingly contrasting goals. Infrastructure solutions must streamline delivery of applications, information, and communications services to mobile devices to enhance user productivity and flexibility. At the same time, they must protect the fundamental interests of the organizations that deploy them.

A Compelling Productivity Imperative

Traditionally, employers provided access to necessary enterprise systems and productivity applications from desktop and laptop computers that were often the most advanced tools available to employees. A combination of trends, including personal mobile devices, cloud delivery, and new application models, is opening new opportunities for organizations to enhance productivity and competitive advantage. With the explosion in consumer devices, employees now typically own highly advanced productivity tools for their own personal use. While many IT departments resisted supporting these devices for work-related activities at first, the need to do so has become imperative, not just for employee productivity and satisfaction but also for business growth and agility. Further, while mobile devices were initially the property of users, many organizations now provide tablets and smartphones to their workforce, specifically to enhance productivity.

Mobile devices provide anywhere, anytime access to resources needed for productive work, along with a seemingly endless choice of hardware and software tools. Employees can enjoy the freedom to select the right tool for the job, and the portability of applications, desktops, data, and communications tools, independent of platform and operating system. New productivity solutions are constantly improving the quality of the mobile experience and providing access to new kinds of data, including rich media, video, and collaboration.

New Challenges for Mobile Users

From an end-user perspective, mobility infrastructure must enhance, rather than detract from the benefits of mobile devices, despite several challenges.

- **Simplifying access.** Though mobility solutions are rapidly evolving, one of the largest challenges remains: connecting to the mobile infrastructure and accessing corporate resources with ease and speed. The number of device possibilities, the range of connection types and locations, and the lack of standardized approaches can translate to difficulties for users. Ultimately, effective mobility solutions need to be as simple as possible, providing a consistent experience no matter where and when users are connecting and considerable similarity across device types.
- **Securely using personal devices for work**. The coexistence of work and personal applications and data on mobile devices is a given, but it also poses challenges. Corporations are worried about the introduction of malware and viruses from personal data and downloaded apps and files, and have concerns about compliance issues and protection of intellectual property. Meanwhile, users want to keep their personal information private.

- **Retaining productivity advantages**. Organizations want to embrace the productivity benefits of mobile devices, but they also recognize the need to apply appropriate security and policies to protect corporate data. If corporate security measures are too intrusive or cumbersome, they can quickly erase productivity gains from mobile working. A corporate application that degrades the mobile user experience is clearly counterproductive

Challenges for IT Infrastructure and IT Departments

The benefits of enterprise mobility—such as the choice of using any device anywhere—are sometimes seen as antithetical to traditional IT requirements for security and support. The same power and fundamental portability that make mobile devices so compelling for personal productivity can also present security liabilities and management complexity for IT departments. More than merely accommodating multiple mobile devices, supporting true enterprise mobility requires careful consideration of multiple IT issues.

- **Supporting myriad devices and operating environments**. In many organizations, it is no longer feasible for IT departments to mandate devices and common operating environments. Complicating matters, the modern mobile worker is likely to employ multiple devices such as a smartphone, tablet, and laptop, and may upgrade or change them out frequently. These devices, in turn, may run diverse operating systems, including Microsoft Windows, Mac OS, Apple iOS, or Google Android. This crush of new devices creates a potentially large variety and volume of new devices with “instant-on” expectations, and adds the risk of exponentially increasing support needs.
- **Maintaining secure access to the corporate network**. Supporting a choice of endpoint devices must not mean sacrificing security. IT departments need to be able to establish the minimum security baseline, including Wi-Fi security, VPN access, and perhaps add-on software to protect against malware, that all devices must meet before being granted access to the corporate network. Due to the wide range of devices, it is also critical to identify and authenticate each device and user connecting to the network. Because the infrastructure used for employees is often extended to contractors, vendors, and guests, IT departments need to be able to apply different security policies for each.
- **Facilitating rapid expansion and control of mobile applications**. Allowing corporate access for mobile consumer devices means mitigating risk from less-regulated consumer applications (and malware) connecting through the network. In addition, organizations must maintain tight control over corporate applications, from installation to operation to removal. Once enterprise mobility is established, organizations need to move rapidly to enable and deploy touch-friendly versions of corporate applications validated to run on the multitude of mobile platforms.
- **Protecting data and preventing data loss**. One of the largest challenges of any enterprise mobility implementation is protecting corporate data. IT departments must protect business data, and create data access policies for both corporate-managed and employee self-supported and managed devices Additionally, some industries must comply with confidentiality regulations such the Health Insurance Portability and Accountability Act (HIPAA), security regulations such as Payment Card Industry (PCI) standards, or more general security practice regulations such as Sarbanes-Oxley.

- **Enforcing company usage policies**. It may be relatively straightforward to generate policies regarding what kinds of devices may be used on the corporate network or what minimum corporate applications must be present on mobile devices. What is often lacking, however, are tools to effectively manage and enforce these policies so compliance is automatic.
- **Ensuring device visibility**. In a mobile enterprise, each employee is likely to have three, four, or more devices simultaneously connected to the network. Many will have multiple modes, enabling them to transition from wired Ethernet to Wi-Fi to 3G/4G mobile networks, and move in and out of these different connectivity modes during a session. To confidently provide access, IT staff must have tools that provide visibility into all of the devices on the corporate network and beyond.
- **Maintaining wireless LAN performance and reliability**. As wireless access becomes pervasive, performance expectations for wireless networks have risen to match those for wired networks, including reliable connectivity, high throughput, and fast application response times. Not only does the sheer number of connected devices challenge these expectations, but the prevalence of data-rich voice, video, and other real-time collaboration applications places additional demands on the wireless network.
- **Managing the mobile device life-cycle**. In accordance with established corporate policy, supporting enterprise mobility means onboarding, managing, and offboarding users and their mobile devices on demand. To optimize productivity, onboarding must be simple and fast, ideally with automation enabling user self-service without IT intervention. To protect the company, offboarding when an employee leaves or is terminated and selective wiping of applications and data in the case of device loss must likewise be rapid and automated.
- **Developing and delivering applications to mobile devices with maximum speed and lowest cost**. IT departments must create infrastructure and delivery mechanisms that allow the broad set of applications to be delivered to mobile devices in the manner that best meets user and business needs. Depending on user experience, time to delivery, development and maintenance time/cost, and security, it may make sense to deliver applications as native apps, HTML5, software-as-a-service (SaaS)/web, or virtual applications. The infrastructure should enable IT staff to choose the most appropriate model for hosting, managing, and delivering each application.

Deploying Secure Mobile Infrastructure with Cisco and Citrix

Organizations are fast realizing that adopting a strategic approach to mobility is a top priority for their ongoing success. However, the dynamic nature of mobile technology and the myriad technologies and vendor offerings can make it difficult to navigate that address near-term requirements while providing a platform for future needs. A good strategy is to partner with leading vendors working closely together to develop a comprehensive mobility architecture and solution. To provide this option, Cisco and Citrix have collaborated to deliver Cisco Mobile Workspace Solution with Citrix, a solution that offers user experience and productivity along with simplified and secure IT infrastructure that is cost-effective to manage. Because enterprises have a broad range of users with different workstyles and application requirements, Cisco Mobile Workspace Solution with Citrix is flexible and extensible to support different business and user needs.

A Comprehensive Mobility Infrastructure Solution

Effective mobility infrastructure requires highly diverse technologies that work together in a seamless fashion (Figure 2). Cisco and Citrix have long recognized the complementary nature of their technologies and the benefits of working together on enterprise mobility solutions. As a part of Cisco Mobile Workspace Solution with Citrix, Cisco provides strengths as a leading computing, networking, and security provider with expertise in unified communications and collaboration. Citrix offers expertise and leadership in application and desktop virtualization as well as emerging mobile device management (MDM), mobile application management (MAM), and enterprise file sharing.

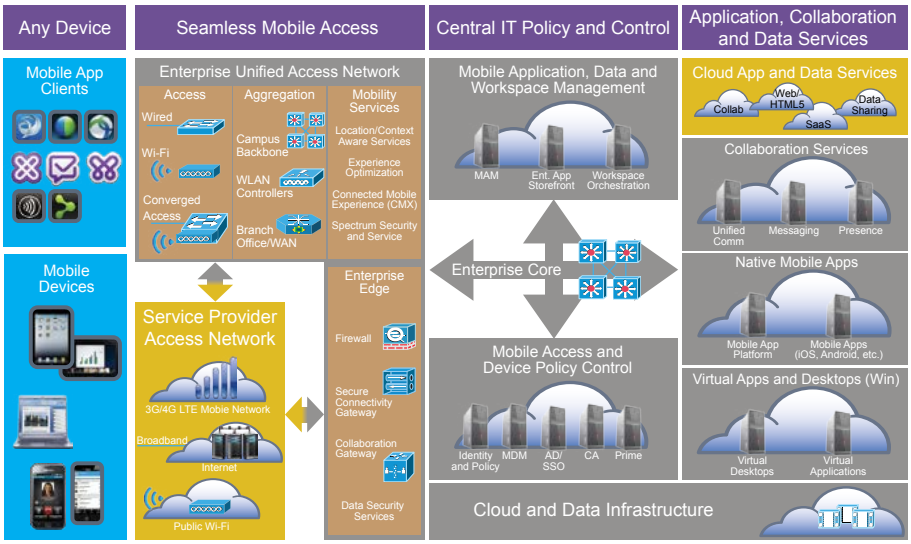

Figure 2. Cisco Mobile Workspace Solution with Citrix provides a comprehensive architectural approach to enterprise mobility.

Together the two companies provide an ideal and unique technology combination and are working together on technology integrations, such as Citrix XenMobile with Cisco® Identity Services Engine (ISE), combining mobile device intelligence with identity management.

Optimizing the User Experience

The smooth and seamless operation of most modern mobile devices implies that users will have little patience for enterprise mobility solutions that are cumbersome or difficult to configure. Cisco Mobile Workspace Solution with Citrix creates a simplified and elegant user experience that features extensive self-service and automation. Users can easily onboard and provision multiple devices with application access, and can easily deprovision or offboard applications as they switch or upgrade devices.

Accessing secure corporate data is likewise straightforward. User access to native HTML5, web, and virtualized applications is transparent and seamless. IT teams can use the solution to securely and seamlessly deliver third-party applications for different platforms. IT departments can also choose mobile collaboration apps from Cisco, such as Jabber® and WebEx®, or Citrix Worx applications to provide sandboxed email, browser, and document sharing, while XenMobile offers a unified

corporate app store that automates key provisioning tasks. Multifactor single sign-on takes the complexity out of authentication for multiple corporate applications. XenMobile also provides automation for key tasks, for example, creating micro-VPNs on the fly for access to internal web applications. The Application Visibility and Control (AVC) functionality of Cisco wireless LAN controllers optimizes the user experience by prioritizing specific mobile apps.

Simplified IT Infrastructure and Secure Operations

A combined approach allows Cisco Mobile Workspace Solution with Cirrix to simplify enterprise mobility infrastructure as well as its secure operation. Cisco networking and the Cisco Unified Computing System™ (Cisco UCS®) provide stable and scalable virtualized infrastructure that allows organizations to start small, yet offers dynamic growth potential for enterprise mobility. Citrix likewise takes an end-to-end lifecycle approach when it comes to mobile applications, providing the largest ecosystem of apps built specifically for business. In addition, Citrix XenApp with the Mobility Pack and software development kit (SDK) rapidly mobilizes existing Windows applications without the need to develop a full mobile application interface.

The integration of Cisco and Citrix technologies pays other dividends as well. Cisco ISE and XenMobile MDM integration lets organizations configure, secure, provision, and support mobile devices. Citrix Receiver and Cisco wireless LAN integration means mobile users get high performance from virtual desktop infrastructure (VDI) applications.

Solution Architecture Overview

Mobile technology continues to be one of the fastest areas of development. This dynamism means that building a comprehensive and extensible enterprise mobility solution can be complex and fraught with risks. Organizations can easily expend considerable resources integrating diverse technologies from multiple vendors, yet end up with a complex and costly operational model.

Cisco and Citrix understand that creating effective mobile infrastructure involves more than merely connecting devices, running some applications on a mobile platform, or expanding wireless coverage. Instead, it requires a comprehensive, integrated solution that solves challenges up and down the technology stack. Cisco Mobile Workspace Solution with Citrix provides an end-to-end solution that combines best-in-class technologies from both companies. This approach provides all of the pieces needed for a complete infrastructure solution for enterprise mobility, taking complexity and cost out of the decision-making process, the design and deployment process, and ongoing operations.

Cisco Mobile Workspace Solution with Citrix (Figure 3) promotes business efficiency and agility through consistent, seamless, and highly secure access to any combination of virtualized, cloud-based, web, and native applications, as well as access to content and communications on any mobile device from any location. While comprehensive, the solution is modular and easily adaptable to existing infrastructure and specific mobility requirements.

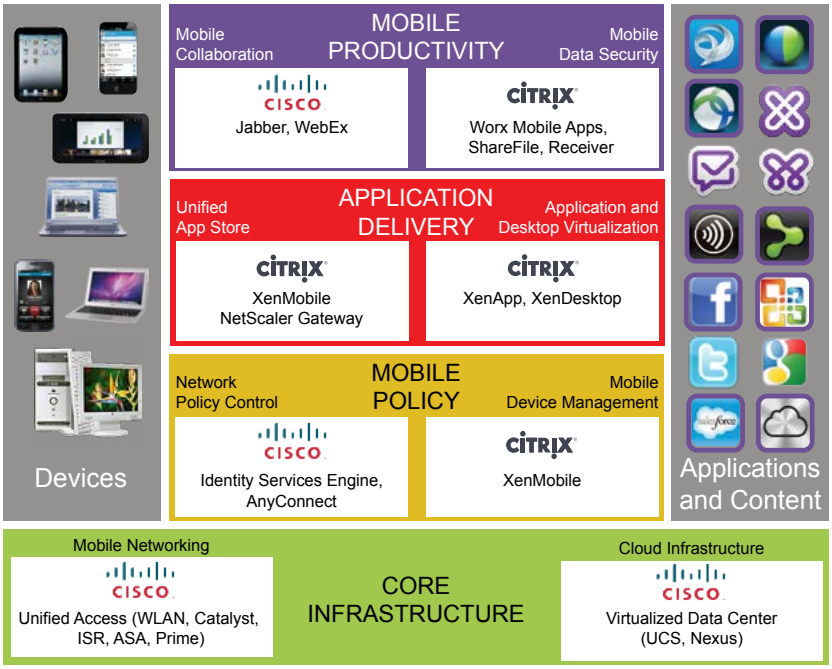

Figure 3. Cisco Mobile Workspace Solution with Citrix provides a comprehensive architectural approach to enterprise mobility infrastructure, securely connecting users with the applications and content they need.

Both Cisco and Citrix understand that successful adoption of mobility technology must be done at an organization's preferred pace and in the context of existing infrastructure. Therefore, the joint mobility architecture allows implementation in distinct phases (Figure 4). Because the phases affect different areas of mobility infrastructure, organizations can take a measured and progressive approach to deployment.

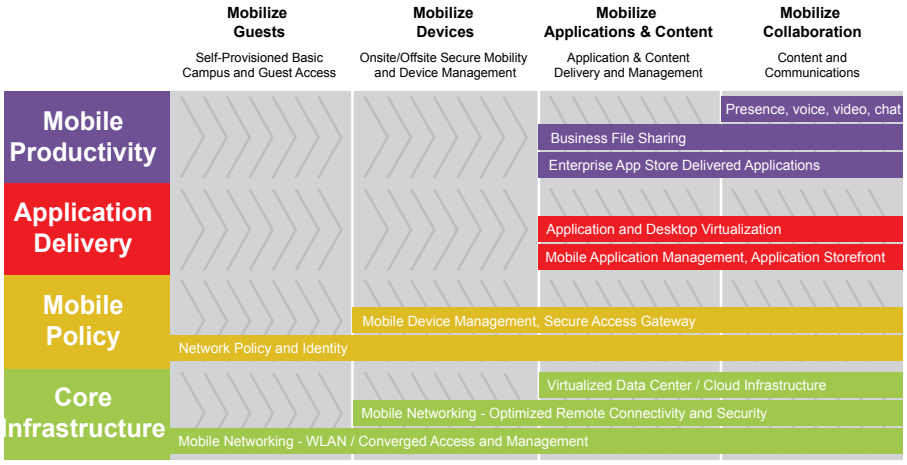

Figure 4. Cisco Mobile Workspace Solution with Citrix offers a phased approach to mobility infrastructure adoption.

Core Infrastructure

The rapid influx of new mobile devices can quickly challenge wireless bandwidth, network bandwidth, and virtualized server resources. In fact, many organizations initially enable mobile capabilities, only to discover that their networking and computing platforms do not scale well enough to support the new load. It is important to have a sound strategy for providing necessary capacity and scalability for virtualized cloud infrastructure and mobile networking.

The core infrastructure layer of the joint mobility architecture is designed to host and deliver the full range of applications and content required by mobile devices. It includes proven mobile networking technologies for securely connecting the full array of end-user devices. It also includes virtual data center and cloud technologies for hosting the full range of native, web, SaaS, virtual, and HTML5 applications and their associated data. The design of the core infrastructure layer (Table 1) allows organizations to scale easily from small pilots through large, enterprise deployments.

- **Infrastructure for mobile networking**. Cisco solutions for mobile networking provide convergence of wired and wireless networks into one physical infrastructure with network-wide intelligence, performance, and integration with the Cisco Open Network Environment. The solution also delivers comprehensive lifecycle management, performance assurance, and compliance, simplifying network management across wired and wireless networks. The solution includes Cisco wireless LAN controllers, Catalyst® switches, Integrated Services Routers, Adaptive Security Appliances, Aironet® access points, and Cisco Prime™ for converged lifecycle and performance assurance management. The latest generation of Cisco Catalyst switches combines wired and wireless into a single platform, providing further operational benefits to network operators.
- **Virtualized data center infrastructure**. Increased efficiency and scalability of virtualized data center infrastructures are key to facilitating mobility. The exponential growth in mobile device usage depends directly on the cloud for consistent access to the expanding array of hosted and managed applications and data. To help organizations move toward a virtualized data center, Cisco UCS unifies computing, networking, virtualization, and storage access into a single integrated architecture. Featuring Cisco Nexus® switches and fabric extenders combined with powerful Cisco UCS servers, this unique architecture provides end-to-end server visibility, management, and control in both bare-metal and virtual environments. This architecture is well aligned to the high performance and efficiency needed for hosting virtual applications and desktops and mobile, web, and HTML-5 apps and data, as well as the device and application management services needed to deliver a complete enterprise mobility solution.

Table 1. Core infrastructure from Cisco.

Cisco Mobile Networking for Unified Access	
Cisco WLAN controllers and access points	Provide the visibility, scalability, and reliability needed for highly secure, enterprise-scale wireless networks
Cisco Catalyst switches	Help scale network infrastructure for growing business needs, increase network intelligence with visibility and control, simplify operations, and improve security for users and applications
Cisco Integrated Services Routers	Deliver applications and highly secure collaboration through the widest array of WAN connectivity at high levels of performance (up to 75 Mbps)
Cisco Adaptive Security Appliances	Provide a robust suite of highly integrated market-leading security services, unprecedented flexibility, modular scalability, and feature extensibility
Cisco Prime	Allows the rollout of unified access services, providing highly secure access and tracking of mobile devices, while assuring application performance and end-user network experience
Cisco Cloud Infrastructure for a Virtualized Data Center	
Cisco UCS	Consolidates resources, accelerates server deployment, and simplifies management through unified infrastructure and powerful Cisco UCS servers
Cisco Nexus switches and fabric interconnects	Provides the network foundation for next-generation unified fabric data center

Mobile Policy

Enterprise mobility means allowing people to access content from whatever device and location they prefer, but convenient access must not lead to compromised corporate security. IT staff must be able to apply appropriate levels of security and access control even as they improve the experience for mobile users. In the Cisco Mobile Workspace Solution with Citrix architecture, this critical functionality is handled by a combination of network policy control and mobile device management (Table 2).

- **Cisco network policy control**. Beyond the individual strengths of solution components, integration of Cisco ISE and XenMobile MDM brings considerable power to the joint solution. This integration allows device intelligence to be evaluated and acted upon in the context of policy and network intelligence. For example, jailbroken or unregistered mobile devices can be easily detected, with policies automatically applied to keep them from accessing corporate networks, applications, and data.
- **Citrix mobile management**. XenMobile delivers enterprise-grade MDM with role-based management, configuration, security, and support for both corporate-owned and employee-owned devices. Users enroll their own devices, and policies and apps can then be provisioned to those devices automatically. IT staff can also blacklist or whitelist apps, detect and protect against jailbroken devices, troubleshoot device and app issues, and wipe or selectively wipe a device that is lost, stolen, or otherwise out of compliance. Users can choose virtually any device, while IT departments can help ensure compliance with

policies regarding corporate assets and secure corporate content on the device.

Table 2. Mobile policy components in Cisco Mobile Workspace Solution with Citrix.

Cisco Network Policy Control	
Cisco Identity Services Engine (ISE)	Offers an all-in-one enterprise policy control platform that can reliably enforce compliance, enhance infrastructure security, and simplify service operations
Cisco AnyConnect® Secure Mobility	Combines industry-leading Cisco Web Security with next-generation remote access technology
Citrix Mobile Device and Application Management	
Citrix XenMobile MDM	Provides a comprehensive platform to configure, secure, support, and manage mobile devices
Citrix XenMobile MAM	Offers a library of security controls that can be integrated into any app, either with a single line of code or a postdevelopment wrapper that requires no additional code

Application Delivery

Mobile users need access to a wide range of applications, from specific mobile apps to corporate websites to legacy Windows applications. For efficiency, IT departments seek to foster user self-service and automation wherever possible. Citrix is in a unique position to deliver the entire mobile device ecosystem with a choice of native or virtual presentations to the device. Citrix can also deliver the complete mobile application lifecycle, from development, deployment, and management to access control and data protection, and ultimate removal of the application (Table 3).

- **Unified App Store**. XenMobile includes a unified corporate app store that provides a single place for users to access all of their apps—native mobile, web, HTML5, SaaS, and Windows—on any device. Users can easily choose the apps they need for their job and have them instantly available on their devices. As they move among their favorite devices, their chosen apps follow them to help ensure full productivity in any scenario. Through the unified corporate app store, users are given secure, multifactor single sign-on (SSO) access across all apps.
- **Application and desktop virtualization**. As organizations embrace enterprise mobility, the demand for mobile-enabled applications and desktops can be overwhelming. While some applications merit redevelopment, in other cases it is beneficial to provide rapid mobile access to existing desktops and legacy applications without recoding. XenDesktop transforms Windows desktops and applications into an on-demand service. XenApp enables any Windows application to be virtualized, centralized, and managed in the data center and instantly delivered as a service to users anywhere, on any device. XenApp with the Mobility Pack and Mobile SDK allows Microsoft Windows apps to be mobilized with little investment while the organization develops specific mobile apps.

Table 3. Application delivery components from Citrix.

Citrix Unified App Store	
Citrix XenMobile	Provides a comprehensive solution for managing mobile devices, apps, and data, so users have the freedom to experience work and life their way
Citrix NetScaler	Optimizes, secures, and controls the delivery of all enterprise and cloud services while maximizing the end user experience for mobile devices
Citrix Application and Desktop Virtualization	
Citrix XenApp	Offers on-demand self-service application delivery for enterprise applications, allowing any Windows application to be virtualized
Citrix XenDesktop	Transforms Windows desktops and applications into an on-demand service that can be consumed by a choice of mobile devices

Mobile Productivity

Once people are connected and have appropriate access, they need tools that can make them productive. Knowledge workers need to be able to find each other, collaborate, and share applications and data, exchanging information in a manner that meets IT requirements without compromising productivity. While Cisco Mobile Workspace Solution with Citrix provides mobile access to the broadest range of applications, collaboration tools, and data, the solution also delivers specific technologies that augment other applications on the market (Table 4):

- **Mobile collaboration**. Mobility has done wonders for individual productivity, but the true promise of mobile enterprise technology lies in enhancing the productivity of work groups. Cisco provides tools that help teams be productive from anywhere, on any device. Mobile employees need to be able to find the right people where ever they are, see if and how they are available, and initiate collaboration using their preferred methods and tools. Cisco Jabber lets employees access presence, instant messaging (IM), voice, video, voice messaging, desktop sharing, and conferencing. Cisco WebEx web conferencing combines file and presentation sharing with voice, HD video, and new Meeting Spaces, allowing employees to meet anywhere with anyone.
- **Secure mobile data**. For enterprise mobility to pay dividends in terms of productivity, people need to use their devices to collaborate and access secure corporate content without compromising either corporate security or their own private data and applications. Unfortunately, developing new applications can be slow and costly, and blocked apps can quickly cause frustration and paralyze the productivity gains everyone expects from mobile technology. Citrix Worx Mobile Apps such as WorxMail, WorxWeb, and ShareFile allow separate and highly secure corporate information access and data sharing without affecting device privacy. Users can also access data from corporate stores such as Microsoft SharePoint. Citrix Receiver lets organizations quickly mobilize and deliver existing applications (such as Windows apps), while IT staff consider which corporate applications will ultimately be redeveloped and deployed in mobile versions.

Table 4. Mobile productivity components from Citrix and Cisco.

Cisco Mobile Collaboration	
Cisco Jabber	Lets users access presence, instant messaging (IM), voice, video, voice messaging, desktop sharing, and conferencing
Cisco WebEx	Allows users to meet online, sharing files, information, and expertise
Citrix Mobile Data Security	
Citrix Worx Mobile Apps	Allows IT to enforce mobile settings and security for e-mail, calendar, contacts, and web access
Citrix ShareFile	Provides full-featured and secure data sharing and sync built for the enterprise
Citrix Receiver	Offers an easy-to-install software client that lets employees access applications, desktops, and data easily and securely from any device, including smartphones, tablets, PCs, and Macs

Managing the Enterprise Mobility Lifecycle

The Cisco Mobile Workspace Solution with Citrix technology stack is comprehensive, and it is also extremely flexible. The technology stack can be implemented in its entirety or incrementally, based on the specific use cases that need to be supported. In understanding how these technologies work together, it is useful to explore how the solution can be used to accomplish different phases of the enterprise mobility lifecycle (Figure 5).

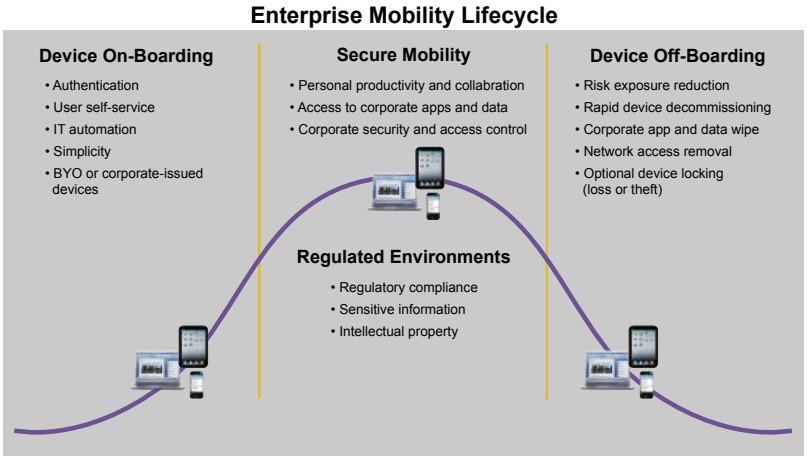

Figure 5. The enterprise mobility lifecycle requires diverse functionality.

Use Case 1: Device Onboarding and Basic Productivity

With the ability to choose one or more devices in a market characterized by increasingly brief device lifecycles, employees need a way to enroll new devices and provision their workspace very quickly and easily. Cisco Mobile Workspace Solution with Citrix provides rapid onboarding of new devices without intervention from IT staff.

Scenario

The following steps might be typical in a device onboarding scenario:

- **Initialization and registration**. The user brings a new device to the network, perhaps shrink-wrapped right from the store. The user connects to the provisioning wireless LAN (WLAN) service set identifier (SSID). The network recognizes that this is a new device and presents a registration dialog after verifying that the user is authorized to participate in the mobile service.
- **MDM enrollment**. The network also automatically recognizes that MDM enrollment is required according to the business policy, and directs the user to enroll the device. The user device is enrolled in the MDM service, and provisioning is completed. As part of provisioning, the corporate WLAN SSID security profile is installed on the device, as well as a unique certificate and a business container that separates business and personal data on the device.
- **Device provisioning**. The user is then presented with a corporate app store showing the apps that are relevant to the user's role in the company. Mandatory apps are downloaded automatically, and the user can easily install them without IT intervention. The app store also shows recommended apps and any pre-purchased apps. The user installs collaboration tools from the app store, along with native apps optimized for the device. The user then connects to the corporate WLAN SSID, authenticates to the network and is automatically given the level of access based on his or her role.
- **Getting to work**. After onboarding, the user IMs a work colleague and asks if they are available for a call. A call is launched enabling the two coworkers to share voice and video on their mobile devices. They decide they need to add a third person and launch a web conference to work on a spreadsheet in real time. After the meeting, the resulting file is checked into the collaboration platform, and the link to the file is shared securely with the other participant.

Cisco and Citrix Products

The following Cisco and Citrix technologies work together throughout Use Case 1 to facilitate onboarding.

- Cisco WLAN works in conjunction with ISE to provide access control and the ability to sense new devices, which are then redirected to the registration and enrollment portal. Cisco ISE communicates with XenMobile MDM to provide a comprehensive access policy, including user, network, and device context. This integration also helps ensure that noncompliant devices (jailbroken or rooted devices or devices with blacklisted apps) are blocked from accessing corporate assets. ISE coordinates the device enrollment process, helping ensure that all

new devices are detected and controlled. Additionally, ISE forces these devices to be registered with XenMobile MDM, providing a single point for network access control and policy enforcement.

- XenMobile StoreFront provides a comprehensive corporate mobile app store that can be tailored to the role of the user.
- After onboarding, Cisco collaboration apps, including Jabber and WebEx, provide a seamless way for users on mobile devices to stay connected with other people in their business through IM, voice, video, presence, and web conferencing.
- ShareFile provides a secure method for mobile users to share data files they are collaborating on together. This approach avoids the overhead of storing those files in unsecured areas on mobile devices, and likewise avoids concern if the device is lost or stolen.
- Cisco WLAN uses AVC to recognize business applications including Jabber, WebEx, XenApp virtual apps, and Worx Mobile Apps, providing the ability to give priority to that traffic and improving the user experience.

Use Case 2: Secure Mobility

While many organizations are openly adopting enterprise mobility programs, the challenges of information security can be a stumbling block for some industry segments. In industries such as healthcare, financial services, and government, the need to protect customer data for privacy or compliance with industry-specific regulations can quickly outweigh the need for mobility. Similarly, companies working with sensitive information or intellectual property have significant concerns about losing valuable information via a lost or stolen mobile device. The challenge for IT is to provide mobility and a choice of devices to users working in industries that require more stringent security policies.

Scenario

This scenario extends the story from the previous use case and assumes that the user is a clinician who works in a hospital and needs to access patient records as a part of her job. Hospital policy mandates that access to applications and data on mobile devices must not leave data on the device, where it could be compromised or shared inappropriately.

- **Accessing sensitive data.** Due to her position, the clinician has been authorized to access a patient records app. This app, which is virtualized and centrally hosted, appears automatically in the app store on the clinician's personal or corporate-owned device. With access to the virtual app, she can view and update patient data, which is not stored on the device but instead is securely hosted in the data center.

- **Launching a legacy application**. The clinician also needs to use a legacy application that does not run natively on the mobile device. That app, refactored for a mobile device with touch capability, is also available from the app store and is hosted in the virtual environment.
- **Sharing sensitive information**. As part of a consultation, the clinician needs to securely share a patient record with a colleague. The clinician updates a patient record from her mobile device, and colleagues are then automatically notified of the changes so that they can view the record.

Cisco and Citrix Products

Cisco and Citrix technologies provide highly secure access to sensitive data along with essential collaboration, all without putting the data at risk.

- The Cisco WLAN works in conjunction with ISE to provide access control, limiting access to corporate resources that the user is entitled to. ISE communicates with XenMobile MDM to continually check the ongoing compliance of the mobile device to detect malware or a compromised OS. ISE and XenMobile MDM can also coordinate to enforce access policies, such as requiring the user to set a PIN lock/password on the mobile device. Once on the network, the user can access XenDesktop virtual applications and desktops hosted on Cisco UCS in the data center via the Citrix Receiver client on the mobile device. After the virtual applications or desktop have launched, the user can roam from patient to patient without having to reboot the apps or desktop each time, allowing her to spend more time with patients.
- The XenMobile Mobility Pack automatically refactors and skins Windows desktops and apps for mobile devices. The XenMobile SDK allows development teams to mobilize existing Windows apps so users can take advantage of native device features such as camera, touch, GPS, etc. Citrix AppController provides federated SSO, improving the user experience and security.
- For collaboration, Citrix Receiver and XenDesktop provide a comprehensive virtualized workspace, allowing both legacy and secure apps to be accessed by mobile devices while ensuring that sensitive data never leaves the datacenter. ShareFile lets mobile users securely share data files in a way that is not going to cause concern if the device is lost or stolen. For additional security, the Worx Email and Worx Web clients can be deployed to provide secure email and web access, further protecting against sensitive data loss.

Use Case 3: Device Offboarding

People lose their mobile devices. Sometimes they are misplaced, other times stolen. Corporate data and applications remaining on a lost or stolen device can be a concern for IT. Can that device still be used to gain access to the corporate network? Can the thief recover and use the corporate data stored on the device? A similar challenge occurs when an employee leaves the company. IT is often asked to immediately terminate their access to corporate assets, including the network and corporate apps and data. The challenge for IT is how to allow freedom of device choice and mobility while retaining the ability to quickly revoke a device's access and comprehensively eliminate the threat of sensitive data loss.

Scenario

This scenario describes a device loss, which is similar to decommissioning a device in the event of employee termination.

- A user reports a theft or loss of a mobile device to the IT department. IT staff debriefs the user and, based on the person's role, decides it is too risky to allow the missing device to have access to corporate data.
- IT staff immediately lock the device. The device can also be wiped, with the assurance that only corporate apps and data will be removed and that personal apps and data will still be intact if the device is recovered.
- IT staff then revokes the device's network access and remotely removes the corporate apps and data. This act renders the device incapable of accessing the network and removes the possibility that an unknown party could access corporate data stored on the device.

Cisco and Citrix Products

As with previous scenarios, Cisco and Citrix technologies work together to protect corporate data on a lost or stolen device, or in the case of employee termination.

- All along, Cisco ISE and XenMobile MDM have been coordinating to enforce access policies—such as requiring the user to set a PIN lock/password on the mobile device. As a result, if the device falls into the wrong hands, the data is still protected by a password and unlikely to be accessed. The ability to initiate a remote lock on the device further minimizes the chances of unauthorized access. Additional protection can be set by the IT administrator via XenMobile by specifying that multiple failed attempts at a PIN/password entry would result in the device being locked and the data being removed automatically.
- ISE, communicating with XenMobile MDM, can execute the organization's business policy automatically, remotely wiping the corporate apps and data from the device to help ensure that it can no longer be accessed. ISE can also immediately revoke network access, blocking any further attempts by the device to gain access to the network and company resources.
- As a precaution, providing a secure file sharing service with Citrix ShareFile can be an effective way to monitor and control what data gets stored. This approach prevents export of data to unsecure areas and thus the potential removal of corporate data, lowering risk in the event of a lost or stolen device.
- For additional security, the Worx Email and Worx Web clients, along with Citrix Receiver, let IT organizations enforce email and Internet access policies, such as those for handling email attachments, using VPNs, and accessing URLs. IT staff can also prevent the use of certain apps that might jeopardize corporate data..

Conclusion

Enterprise mobility has become an irresistible technology shift that most organizations must embrace to encourage worker productivity and capture the best talent. At the same time, deploying mobility infrastructure requires careful consideration to provide necessary scalability, capacity, and availability of applications for mobile users. Security for corporate data and applications is of paramount importance to any enterprise mobility deployment.

As a part of their strategic alliance, Cisco and Citrix provide a compelling and complete enterprise mobility infrastructure solution and roadmap in the form of Cisco Mobile Workspace Solution with Citrix. Technologies from both firms are carefully combined into a comprehensive solution stack to minimize the time, cost, and risk of deploying enterprise mobility infrastructure. Cisco and Citrix continue to work together to integrate solution components, providing greater simplicity and performance for mobile users and reducing the burden on IT staff. Cisco and Citrix continue to validate and document these joint solutions for mobility in the form of Cisco Validated Designs.

For more information on Cisco Mobile Workspace Solution with Citrix, please visit cisco.com/go/byod and citrix.com/cisco.

About Cisco
Cisco (NASDAQ: CSCO) is the worldwide leader in IT that helps companies seize the opportunities of tomorrow by proving that amazing things can happen when you connect the previously unconnected. Learn more at www.cisco.com.

About Citrix
Citrix Systems, Inc. (NASDAQ:CTXS) transforms how businesses and IT work and people collaborate in the cloud era. With market-leading cloud, collaboration, networking and virtualization technologies, Citrix powers mobile workstyles and cloud services, making complex enterprise IT simpler and more accessible for 260,000 organizations. Citrix products touch 75 percent of Internet users each day and it partners with more than 10,000 companies in 100 countries. Annual revenue in 2011 was $2.21 billion. Learn more at www.citrix.com.