Enterprise mobility management at your own pace: a three-phase approach
Just about every organization today needs a mobility strategy. The business advantages are many: mobile employees can access up-to-date information, close sales, collaborate and make informed decisions while they’re away from the office. Mobility has empowered organizations across the spectrum, from healthcare providers to the military. One popular mobile strategy is a bring-your-own- device (BYOD) policy that lets employees use their own devices for work tasks. The beauty of BYOD is that organizations can empower hundreds or thousands of employees with all the business advantages of mobility without investing huge amounts of money in corporate-issued mobile hardware. BYOD also pleases users, who get to work with the devices and applications they know and love.

However, BYOD and other mobility strategies must address the perils of unmanaged mobile devices, applications and cloud services. Mobile devices can be lost or stolen, along with any sensitive business or customer data they contain. Users can download malware through infected personal applications, email attachments or malicious websites and inadvertently introduce it into the corporate network when connecting to get their email. Often today’s most nefarious advanced persistent threats start with a malware infection. Also, people may take advantage of personal cloud file-sharing and synchronization services without any management or corporate control and then leave the organization with sensitive data in hand.

Other mobile challenges faced by organizations include providing access to Windows applications from mobile devices running on operating systems such as iOS and Android, and offering enterprise-class calendar, email, browser and other applications instead of the “lite” versions native to personal devices.

**The challenge of implementing enterprise mobility management**

That’s why managing and monitoring mobile devices, applications and data are at least as vital to overall security and productivity as managing desktop PCs. Mobile device management tools have evolved to address all these challenges, from managing just the device and its lifecycle, often known as mobile device management (MDM), to securing mobile applications, connectivity and data as users increasingly select the same device for personal purposes and work. Unfortunately, deploying a complete enterprise mobility management (EMM) solution that meets all organizational and user needs and supports multiple mobile platforms can seem daunting.
It’s important to understand, however, that EMM tools and strategies are not an all or nothing proposition. Organizations can take a thoughtful, phased approach to mobile enablement, providing basic mobile connectivity, management, security and services at first, then moving on to empowering employees further and taking the appropriate steps to protect the organization in the process. This white paper presents a three-phase plan for mobile empowerment, management and security using the Citrix XenMobile EMM platform. Such a strategy breaks down the process of empowering employees with the benefits of mobility and managing and securing the environment into stages that organizations can tackle at their own pace.

**Phase One: Get Me Mobile**

Many organizations start their mobile empowerment journey with the simple goal of connecting mobile devices to corporate email via the devices’ native email client software and Exchange ActiveSync, while providing MDM features that help them monitor and manage the devices throughout their lifecycle.

MDM features are the most mature functionality in EMM solutions and often similar across platforms. They include:

- Centralized role-based discovery and management of iOS and Android mobile devices and users to prevent rogue users from connecting to the corporate network
- Centralized enrollment and provisioning of mobile devices with required business applications
- User self-enrollment and provisioning so employees can start working with their mobile devices instantly, rather than waiting for IT
- Application whitelisting and blacklisting based on preconfigured policies, allowing users to download and install applications IT has approved as secure and blocking those proven to be a risk
- Corporate online app stores that allow users to browse, download and install pre-approved mobile business applications easily
- Detection and blocking of rooted or jailbroken devices, which can be a security hazard
- Partial or total remote wipe of data if the device is lost, stolen or fails to connect after a preconfigured period of time
- Enforcement of policies regarding passwords, authentication, wireless connectivity, data encryption at rest and in transit, camera use and other functions

XenMobile MDM Edition offers all of these features across multiple mobile platforms and simplifies enrollment of user devices. IT gains important capabilities, including pushing out internal root certificate authority (CA) certificates to devices during enrollment and configuring default home pages for browsers, bookmarks and URL blacklists and whitelists.
XenMobile MDM also simplifies integration of the user’s native email client with Exchange ActiveSync. However, shortly after gaining mobile access to their work email, many users encounter the problem of downloading and sending large files with their mobile devices. More often than not, they turn to public cloud storage services beyond the reach of IT. Rather than drive up data storage costs and increase the likelihood of data leakage, Citrix ShareFile allows mobile users to easily access, share and sync files, regardless of whether they are stored behind the corporate firewall or on the desktop or laptop.

ShareFile is vital for security-conscious organizations seeking to avoid the use of consumer file-sharing services, which operate outside the control of IT and were never created with the security needs of enterprises in mind. ShareFile provides all the file sharing and synchronization functions of the most popular cloud services, giving users access to their most important, most current content. It also provides stringent, policy-based management and security for IT. For example, IT can configure and enforce policies that prevent access by unapproved users, cutting and pasting of sensitive information into emails and printing sensitive documents. IT can also set up policies that revoke access when a user leaves the organization.

Android and iOS device users get integrated mobile document editing and annotation capabilities, including advanced features such as comments and tracked changes. ShareFile integrates with Microsoft Outlook so users can send ShareFile links with tight controls as an alternative to less-secure and more bandwidth- and storage-hungry attachments.

XenMobile and ShareFile offer a great start for a deployment without undue complexity. This solution empowers users with basic mobile capabilities and business benefits and protects enterprise networks and sensitive files and information from data leakage, malicious attacks and device tampering.

Phase Two: Make Mobile Better

The Get Me Mobile phase gives organizations some experience with mobility and addresses the needs of users who simply want to connect their devices to the company network for work email. Users and IT can get comfortable with enterprise mobility policies and tools without overwhelming complexity. However, at some point, many users and enterprises will demand more capabilities to increase productivity levels, particularly if BYOD is part of the picture. Users then turn to IT to make their mobile experience better.

For example, they may want to access business applications other than email, meaning IT may have to provide access to internal business data from CRM, ERP and other systems. If BYOD has been implemented, IT must start addressing the challenge of separating and protecting corporate applications and data from employees’ personal data and apps on the device. It may also be time for email and mobile browser applications that are more secure and enterprise ready than the native, consumer-oriented versions provided by Apple and Google. For example, users may need an email app that allows them to forward meeting invitations with attachments or launch online meetings directly without having to enter a nine-digit access code. These are examples of standard email features that people are accustomed to using on their desktops and laptops.
Containerization, also known as sandboxing, is the best way to separate work applications from personal apps and data with stringent policies that restrict or forbid interactions between the two. XenMobile MDM has a robust, flexible, easy-to-implement approach to containerization. It allows IT to apply a host of policies—including FIPS 140-2-compliant AES-256 encryption, password authentication, application-specific micro VPNs and data leakage prevention—to protect enterprise resources from exposure to personal data and applications and prevent leakage of sensitive information. Developers and IT can take advantage of the XenMobile SDK to integrate policies into internally developed applications or wrap third-party applications with the same policies via a single line of code.

XenMobile MDM provides an application-specific micro VPN to enable any mobile app to access an organization’s internal network, avoiding the need for a device-wide VPN that can compromise security. In addition to encryption, micro VPNs employ data compression and optimization to ensure fast transmission, even across weak connections. This feature is especially attractive for organizations with users who frequently travel internationally.

Citrix offers the Worx App Gallery, which provides the industry’s fastest growing ecosystem of third-party Worx-enabled business applications, pre-wrapped with security policies and verified by Citrix. Citrix also provides its own enterprise-level Worx mobile apps for Android and iOS devices, including WorxMail and WorxWeb.

WorxMail has also been carefully designed for a “better than native” user experience and adds a host of user-friendly features that go beyond what native email clients deliver. Users can take advantage of internal and external out-of-office notifications and single-click “running late” messages. They can join online meetings or audio conferences from an email with a single click, add attachments to meeting invitations and get an intuitive, graphical view of other users’ calendar availability. IT can apply granular data leakage policies and other measures to protect corporate email and attachments, such as controlling or preventing users from cutting and pasting sensitive information into emails, forwarding or printing sensitive email and opening, editing or saving attachments in unapproved applications. All enterprise emails, contacts and calendar items are separated from personal applications and information on the device.

Email is the #1 app users want most

What mobile applications do you currently use for work?

Smartphone

<table>
<thead>
<tr>
<th>Application</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email</td>
<td>94%</td>
</tr>
<tr>
<td>Calendar</td>
<td>72%</td>
</tr>
<tr>
<td>Web browser</td>
<td>65%</td>
</tr>
<tr>
<td>SMS (texting)</td>
<td>59%</td>
</tr>
<tr>
<td>Instant messaging/chat</td>
<td>40%</td>
</tr>
<tr>
<td>Note-taking application</td>
<td>33%</td>
</tr>
<tr>
<td>Employee intranet or firewall</td>
<td>22%</td>
</tr>
<tr>
<td>Web meeting or audio conference</td>
<td>17%</td>
</tr>
<tr>
<td>Team document sharing</td>
<td>15%</td>
</tr>
<tr>
<td>None of these</td>
<td>4%</td>
</tr>
</tbody>
</table>

Source: Forrester Research 2013
Any web links in WorxMail messages are automatically opened in the secure WorxWeb browser, a sandboxed mobile browser with a friendly, better than native experience. It can secure all enterprise connections with a micro VPN and allows IT to apply granular policies to prevent data leakage across sandbox boundaries.

With a Make Mobile Better strategy, organizations can dive into all the competitive benefits mobility has to offer.

**Phase Three: Make Mobile Complete**

A recent Citrix customer survey indicated Windows business applications still play a vital role in mobile organizations, but porting those applications to multiple mobile operating systems can be an overwhelming, resource-devouring challenge. Citrix has been the most important player in the virtual desktop and application space for decades, providing users with easy access to virtual Windows applications via Citrix XenApp, and to entire Windows desktops via Citrix XenDesktop, with fast performance and enterprise-level security. Citrix can also solve the challenge of mobilizing Windows apps.

Citrix HDX Mobile makes it easy to deliver Windows applications to any type of device, including touch-enabled smartphones and tablets, while enhancing performance over mobile networks. The HDX Mobile SDK enables developers to make any custom Windows app mobile-device aware by leveraging device features such as multi-touch gestures, native menu controls, camera and GPS support within the virtual app. By downloading the appropriate Citrix Receiver client for their device, mobile users can securely access these Windows apps.

Delivering remote access to Windows apps from a mobile device makes it easy for IT to support a variety of platforms, as opposed to attempting to develop apps for the growing array of native device operating systems. In addition to providing a faster, simpler alternative to porting Windows apps to mobile platforms, this
approach is highly secure. Applications and data can reside within the datacenter for maximum security, or the interface can be held locally on the mobile device for offline use. A powerful policy engine enables granular control of user tasks based on the device, network and app they are accessing.

Finally, Citrix solutions have been perfecting secure, remote access technology for over 25 years, providing users with high-performance application access from a mobile device.

The XenMobile solution also includes Citrix NetScaler Gateway, which provides fast, centrally controlled, scalable mobile access to all Windows, SaaS and internal web applications on any device. NetScaler Gateway harnesses advanced techniques to scale and accelerate application delivery. It provides mobile users with advanced, secure single sign-on and authentication capabilities so they don’t have to remember multiple passwords. It provides IT with secure, fine-grained application access control with more than 60 application-specific policies and advanced security features such as Denial of Service attack protection, application-level firewalls and SSL offloading.

**Tap into the power of mobility at your own pace**

This phased strategy based on Citrix XenMobile allows enterprises to move at their own pace, balancing mobility and flexibility with management and security at every step. The execution of a comprehensive mobility strategy must have a starting point. It can be simple, inexpensive and evolve over time. With XenMobile, enterprises have access to all the features and functionality they need to fulfill their mobile strategy today and tomorrow. Why not start today?
About Citrix

Citrix (NASDAQ:CTXS) is a leader in virtualization, networking and cloud infrastructure to enable new ways for people to work better. Citrix solutions help IT and service providers to build, manage and secure, virtual and mobile workspaces that seamlessly deliver apps, desktops, data and services to anyone, on any device, over any network or cloud. This year Citrix is celebrating 25 years of innovation, making IT simpler and people more productive with mobile workstyles. With annual revenue in 2013 of $2.9 billion, Citrix solutions are in use at more than 330,000 organizations and by over 100 million people globally. Learn more at www.citrix.com.

Copyright © 2014 Citrix Systems, Inc. All rights reserved. Citrix, XenMobile, XenApp, XenDesktop, WorxMail, WorxWeb, NetScaler Gateway and ShareFile are trademarks of Citrix Systems, Inc. and/or one of its subsidiaries, and may be registered in the U.S. and other countries. Other product and company names mentioned herein may be trademarks of their respective companies.