MDM and beyond: Rethinking mobile security in a BYOD world
## Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>3</td>
</tr>
<tr>
<td>Introduction</td>
<td>3</td>
</tr>
<tr>
<td>Current business challenges with BYOD</td>
<td>4</td>
</tr>
<tr>
<td>Securing mobile devices through MDM</td>
<td>6</td>
</tr>
<tr>
<td>Securing mobile content through enterprise mobility management</td>
<td>6</td>
</tr>
<tr>
<td>The solution: Citrix enterprise mobility management</td>
<td>7</td>
</tr>
<tr>
<td>Moving forward</td>
<td>12</td>
</tr>
<tr>
<td>About Citrix</td>
<td>14</td>
</tr>
</tbody>
</table>
Summary

This white paper discusses the security challenges posed by bring-your-own device (BYOD) and how they can be addressed through the management of mobile devices, apps and data. Read on to learn how you can embrace BYOD with full security and control, as well as provide a simple and streamlined user experience.

Introduction

Everyone is on the go—especially in business. With today’s mobile-centric computing, user demands have increased and new mobile systems have emerged with deeper functionality and much more diverse usage than ever thought possible. The ways we’re doing business are changing rapidly, yet we’re still narrowly focused on the traditional approach for managing and securing mobile systems: at the device level. One thing is clear—IT is out of the loop when it comes to BYOD. And when IT is out of the loop and mobile devices are not properly managed and secured, significant business risks emerge.

Regardless of who purchased the mobile device, if it’s being used for business purposes, it needs to fall under IT’s umbrella of protection.

Mobile device management is one answer, enabling IT to lock down and control every mobile device in the enterprise. While MDM provides essential capabilities for securing corporate content, whitelisting and blacklisting mobile apps, wiping lost or stolen devices and other needs, it’s only one element of a complete strategy for secure BYOD. To unlock the full benefits of BYOD and user mobility, IT needs the flexibility to be able to deliver any type of app—mobile, web, Windows or SaaS—on any type of device, with full security and compliance for the enterprise and a convenient, productive experience for users.
Current business challenges with BYOD

Information security lessons have taught us that it’s all in the implementation. Many organizations already have BYOD programs for smartphones, yet there’s still chaos. This is due, in large part, to the fact that many businesses are not capable of moving quickly. Prompt and agile response to mobile computing is needed through risk assessment, policies and the appropriate technologies. Given the bureaucracy, politics and complex cultures in organizations today, these things often take time—a long time—to adequately address.

With countless devices, apps and islands of information scattered about, managing mobile computing is nothing short of overwhelming. It’s this literal disarray that has created formidable challenges for even the most well-run IT shops. IT managers and administrators see these changes happening before their eyes. The pressure to support any and all devices and all applications from any location is real. Unfortunately, the IT and security resources needed to effectively support such mobile environments are not growing proportionately.

Forrester Research predicts that there will be 760 million tablets in use by 2016.1 Without question, the tablet is becoming the business device of choice. When the multitude of mobile operating system platforms—including Apple iOS®, Google Android®, BlackBerry® and Microsoft Windows®—are combined with the immeasurable number of mobile apps for business and personal use, it’s easy to understand IT’s desire to lock down tablets along with other devices. But in today’s world of mobility, IT should be focusing on ways to allow users to do more with their mobile devices, not less. This calls for a strategy with greater flexibility than what is permitted by the point solutions for device or application management available in the market today.

Users expect to be able to take full advantage of mobility benefits. They want to do their jobs better. They know how mobile devices can improve productivity and enhance collaboration with colleagues and clients, and they want to be able to do all of this on a device that’s full of personal pictures, files and other private information. Therein lie some of the greatest challenges with BYOD.

How does IT realistically manage and control such an environment? How do you balance securing business content with honoring user privacy? The obvious solution is for IT to control—to the greatest extent possible—personally owned devices. But employees often reject such mandates, and today’s extended workforce of trusted partners, contractors and others cannot agree to a “lockdown” solution. This makes it impossible for all parties to agree on a solution, and BYOD risks go unaddressed because of delayed decisions.

An important factor in BYOD is that many businesses refuse to acknowledge the extent of the data security problem they face. Given what’s at stake, at this very moment IT departments can show their organizations what they’re made of by taking back control, supporting business needs and giving users what they want.

Further exacerbating the problem is the increasing diversity of work locations—employees work at the office, at home, at client sites and while traveling. Any place is fair game for work—and for business content exposures. As the lines between “working mobile” and “working in the office” continue to blur, users expect the mobile experience to keep up. In order to properly manage the complexity associated with mobile devices and the infinite possibilities for work locations, IT professionals and other decision-makers must come up with a systematic means for managing business content rather than incorporating piecemeal solutions focused solely on managing the physical devices themselves.
Consumerization of IT and BYOD are no longer exceptions to the rule. Instead, they’re top IT considerations that must be built into your system architecture up front. To be effective, your strategy for secure BYOD needs to address every aspect of mobile computing—not just the devices themselves, but also the apps and data they contain.

**Securing mobile devices through MDM**

For organizations seeking to get control over the consumer devices in their environment and the way they are used, MDM can be a valuable first step. Traditional MDM solutions enable IT to implement essential security measures such as password enforcement, device encryption, data backup, audit logging and remote wipe. Still, while these are important capabilities, they remain only a partial solution to the secure-BYOD challenge. To unlock the full benefits of user mobility, IT needs a more flexible and granular way to deliver any type of app—mobile, web, Windows or SaaS—to any user, on any type of device, with full security and compliance for the enterprise.

**Securing mobile content through enterprise mobility management**

An enterprise mobility management (EMM) solution goes beyond managing mobile devices themselves and also provides capabilities to manage their content, including apps and their associated data, documents and other files, as well as email. IT gains more granular, flexible ways to secure and control user mobility while providing greater freedom and a more convenient, productive experience for users. Embracing this new approach to BYOD will allow you to minimize costs and maximize network scalability while maintaining efficient system management and security.
To fully empower mobile productivity, IT needs flexible security and control over mobile devices, apps and content. A key concept here is “flexibility.” As the lines between “working mobile” and “working in the office” continue to blur, users expect the mobile experience to keep up. IT needs tools that allow them to quickly respond to these demands.

At the core of the BYOD challenge is the complexity of today’s mobile apps. Mobile devices used to have standard web browsers with limited functionality. Now, any given enterprise has numerous mobile apps running on a myriad of mobile platforms. To strike a balance between security and usability in the mobile context, you now have to consider:

- Balancing the protection of sensitive business content while maintaining privacy for personal content
- Providing users with a seamless, high-performance experience
- Maintaining flexible access control based on job roles, devices, locations and connectivity

Mobile technology is moving extremely fast, and demands are increasing quickly. This means IT leaders must speed up their processes, including the deployment of the proper technologies and the implementation of reasonable mobile security controls. Ultimately, IT has to reach new levels of agility to support new mobile devices, apps and services moving forward. A complete EMM solution can help.

**The solution: Citrix enterprise mobility management**

When managing BYOD, you need one point of control. The ability to capture, administer and secure all devices, platforms, users and applications from one location can eliminate a tremendous amount of pain from your BYOD experience.
At the same time, it’s essential to provide the best possible user experience to empower people with complete mobile productivity. An enterprise mobility management solution from a proven vendor is the only reasonable choice.

**Solution Options**

Since the proliferation of BYOD and mobile computing in the enterprise, numerous built-in and mobile device management technologies have attempted to solve the problem by just securing the device. This has included capabilities such as:

- Password enforcement
- Device encryption
- Data backup
- Audit logging
- Remote wipe

While these security controls are an important first step, true mobile security needs to go further. IT needs a way to empower users with any app their work requires—including Windows, web and SaaS as well as mobile—on any device they choose, without sacrificing security and control.

That means being able to manage not only devices, but also the apps and data they contain. After all, true business risk involves content—and that’s what you need to protect. According to the Citrix Enterprise Mobility Report (http://www.citrix.com/content/dam/citrix/en_us/documents/products/citrix_mobility_report_may2012.pdf), IT managers and administrators share this increasing focus on securing content—not just devices.
Citrix goes beyond traditional MDM point solutions and other enterprise mobility management solutions in three ways:

1. A smarter approach to managing and controlling business content in addition to the devices on which it is accessed and used

2. An enhanced mobile user experience that allows users to easily get work done with seamless, consistent access with single sign-on and high performance from any device, anywhere

3. Solution breadth that provides end-to-end, integrated endpoint services, networking, security and an enterprise app store, as well as the ability to control and deliver data services and any type of app—mobile, web and Windows

Citrix XenMobile is a complete enterprise mobility management solution that provides all the essential capabilities for the new mobile enterprise, including:

- **Enterprise-grade MDM with all devices managed** – Citrix XenMobile™ MDM Edition, a key component of XenMobile, provides role-based management, configuration and security of corporate and employee-owned devices. IT can enroll and manage any device, blacklist or whitelist apps, detect jailbroken devices and perform a full or selective wipe of a device that is out of compliance. Users can use any device they choose, while IT can ensure compliance of corporate assets and the security of corporate content on the device.

- **Sandboxed mail, browser and documents** – Citrix XenMobile includes the key productivity apps that users need to get their job done. With Citrix @WorkMail, Citrix @WorkWeb and Citrix ShareFile integration, users get beautiful apps including email, calendar, contact and a full browser for access to intranet and extranet sites, as well as access to documents from anywhere—all secured with MDX technologies. These apps live in a sandboxed container, which ensures that corporate data is encrypted and always under IT control.
Security for mobile and BYO apps via Citrix MDX Technologies – Citrix MDX Technologies enable complete management, security and control over native mobile apps and their associated data. With MDX, corporate apps and data reside in a container, separated from personal apps and data on the user’s mobile device. This allows IT to secure any custom developed, third-party or bring-your-own (BYO) mobile app with comprehensive policy-based controls, including mobile DLP and the ability to remote lock, wipe and encrypt apps and data.

A unified app store to access any app on any device – A unified app store provides a single place for users to get their mobile apps—both internally developed and third-party—as well as web, datacenter and Windows apps on any device. People can easily choose the apps they need for their job and have them instantly available on their device. As they move among their favorite devices, their chosen apps follow to ensure full productivity in any scenario.

Federated identity and single sign-on – Citrix XenMobile leverages Microsoft Active Directory to instantly provision and de-provision all of a user’s mobile, web, datacenter and Windows apps based on user identity and role. Through the unified app store, employees get single sign-on to all of their approved apps and can easily request access to apps for which they are not currently authorized. Once approval is obtained, they get immediate access.

Scenario-based access controls for dynamic network protection – With Citrix XenMobile, IT can define comprehensive access and control policies that use endpoint analysis and each user’s defined role to determine which apps and data to deliver and what level of access to content should be provided. By ensuring that the appropriate level of access to apps and data is granted for each scenario, these granular security controls support enforcement of corporate security policies and standards.
Citrix XenMobile provides one control point for device management, secure access to mobile, web and Windows applications, and secure access to and management of corporate data. As an integrated solution for heterogeneous environments, XenMobile goes beyond MDM point solutions by:

- Isolating and controlling business apps and data without affecting personal data
- Implementing context-aware security policies based on the user’s identity, device and location
- Unifying access to everything users need to be productive, including their intranet resources, external SaaS apps, mobile apps, Windows apps and business documents with single sign-on
- Providing a high-performance user experience with seamless, secure access to all apps and data

At the heart of the solution are the following Citrix MDX Technologies:

- **MDX Vault** – MDX Vault separates corporate mobile apps and data from personal apps on mobile devices in a secure business container. Using MDX Vault, IT is able to manage and control native mobile business apps and data instead of managing an employee’s device. The business apps in MDX Vault can be secured with encryption and mobile DLP technologies and can be remotely locked and wiped by IT.

- **MDX Interapp** – MDX Interapp ensures that all MDX-enabled apps can interact with each other for a seamless experience. MDX-enabled apps are integrated so that these apps only open other MDX-enabled apps; for example, a link clicked in the @WorkMail email app automatically opens the @WorkWeb mobile browser, not Safari. In addition, MDX Interapp controls the communications between apps so that IT can enforce policies around
activities such as cut-and-paste between apps—for example, allowing cut-and-paste between MDX-enabled apps but not to apps not protected by MDX, or by preventing use of a camera when using a specific MDX-enabled app.

- **MDX Access** – MDX Access provides granular policy-based management and access controls over all native and HTML5 mobile apps. IT can centrally control and configure policies specific to mobile apps such as the type of device or network that is being used, the device passcode, or upon detection of a jailbroken device. MDX Access also provides the industry’s first application-specific VPN access into a company’s internal network. Using a micro VPN allows businesses to eliminate the requirement for a device-wide VPN, which can compromise security. Instead, an app-specific VPN tunnel is created for the mobile and web apps accessing a company’s internal network remotely.

Citrix XenMobile also delivers follow-me data access to documents from anywhere. The solution’s ShareFile component provides highly secure file edit, sync and share capabilities from any mobile device. ShareFile, Citrix XenMobile and Citrix Receiver work together to provide role-based access controls and remote wipe and lock capabilities, creating a seamless, secure mobile experience for all apps and docs.

Citrix enterprise mobility management allows IT to manage business content and lets users take full advantage of all their devices’ functions. Everyone wins.

**Moving forward**

The new mobile enterprise is here. Business network and application use is shifting from traditional computers to mobile devices. Securing and controlling these devices is an important step, but it’s only the beginning. Beyond core MDM capabilities, IT needs more granular, flexible ways to empower users with all the
apps their work requires—mobile, Windows, web and SaaS—on the devices of their choice. IT managers must be able and prepared to shift their infrastructure to accommodate new ways of working that will continuously evolve.

Mobile security used to be out of sight and out of mind. It’s now impossible to ignore, yet businesses still haven’t reached the level of mobile control that’s needed. Whether or not IT departments have the proper mobile security controls, they’re still responsible for keeping business information and assets in check.

The complexities of mobile computing are creating exponential business risks. Regardless of business size or industry, no organization is immune. With mobile computing, a single misstep is all it takes to create serious business problems. You have to look at the big picture. Once you realize that mobile computing as we now know it is not going away, you can start developing a strategy to ensure you do it right and in ways that can be leveraged into the future.

With today’s diversity of devices and apps, mobile has become virtually unmanageable. Set your business and your users up for success. Don’t let your users be the ones who tell you about mobile security mishaps. The proper technologies, well managed, can be the key to gaining control over your mobile environment today and moving into the future.

An enterprise mobility management solution will provide you with the visibility, control and automation needed to ensure your smartphones and tablets are kept in check, while allowing users to be as productive on the go as they are in the office. You cannot afford to ignore the risks inherent to mobile computing; it’s arguably the most exposed area of your business right now.

The important thing to remember is that you’re in control here. By implementing technologies and processes that address every element of mobile computing—not just devices, but also their business content—you can allow users to securely access corporate applications, email and documents from all their devices, while still meeting all your requirements for security and compliance. Once you have the
proper systems in place, you can easily deploy the right policies and controls based on your specific business needs. In the end, business risks will be minimized, users will be productive and happy, and IT will have done its job.

About Citrix

Citrix (NASDAQ:CTXS) is the cloud computing company that enables mobile workstyles—empowering people to work and collaborate from anywhere, accessing apps and data on any of the latest devices, as easily as they would in their own office—simply and securely. Citrix cloud computing solutions help IT and service providers build both private and public clouds—leveraging virtualization and networking technologies to deliver high-performance, elastic and cost-effective services for mobile workstyles. With market leading solutions for mobility, desktop virtualization, cloud networking, cloud platforms, collaboration, and data sharing, Citrix helps organizations of all sizes achieve the kind of speed and agility necessary to succeed in an increasingly mobile and dynamic world. Citrix products are in use at more than 260,000 organizations and by over 100 million users globally. Annual revenue in 2012 was $2.59 billion. Learn more at www.citrix.com.

©2013 Citrix Systems, Inc. All rights reserved. Citrix, XenApp, XenDesktop, XenMobile, ShareFile, Receiver and MDX Technologies are trademarks or registered trademarks of Citrix Systems, Inc. and/or one or more of its subsidiaries, and may be registered in the United States Patent and Trademark Office and in other countries. All other trademarks and registered trademarks are property of their respective owners.