Enterprise Mobility Trends 2014

Going Beyond Enterprise Mobility Management

The enterprise today is changing rapidly. The intersection of cloud, mobility, social networking and the Internet, what analyst firm Gartner calls the, “Nexus of Forces” is making most medium and large enterprises rethink their enterprise mobile strategies. Employees are bringing their own devices, downloading their own applications and creating their own IT.
There are three main mobile trends that enterprises need to respond to—trends that will ultimately alter the way their employees perform their duties, where data and apps are stored and accessed and how productivity and collaboration are measured. These three trends include:

- **Policy**—Many companies are putting together mobile policies to help manage the influx of personal (BYOD) devices and the consumerization issues.
- **Mobile Apps**—Smartphones and tablets are driving apps in the enterprise. Today those apps are being filled by consumer-focused apps, but many enterprises are looking at extending desktop to mobile.
- **Security**—companies are looking at enforcing security requirements.

### The Five Phases of Mobility

The Apple iPhone changed so much about enterprise mobility—creating the discussions today around mobile apps, security, BYOD, consumerization—and the methods to employ these changes. The key trends of policy (BYOD/consumerization, regulations, security), mobile apps and focus on security started back in 2007 when iPhones began seriously entering the enterprise market, replacing the more secure and manageable BlackBerry devices. This kicked off what Citrix® calls the “Five Phases of Mobility,” as seen in Figure 1.

![Figure 1: The Five Phases of Mobility](image)

The five phases of mobility cover the recent history of enterprise mobility including mobile device management (MDM) and enterprise mobility management (EMM).

The next phase, really starting in earnest in the enterprise in 2015, is what we call Mobile Workspaces. Customers who are transforming their businesses with Citrix Mobile Workspace solutions, demonstrate how virtualization, networking and cloud services technologies empower new ways for people to work better. Workers need to gain access to a portable, always on, always connected working environment that follows them no matter where they go, no matter what device they
choose to use, and no matter what method of connectivity they happen to be leveraging. Next, companies will be working with their partners and customers and helping them complete the mobility journey. Finally, around 2018, enterprises will be looking to unify their mobile platforms to support employees, partners and customers, in what we are calling a Unified Enterprise Platform. Citrix will leverage this evolution today, starting from its core competencies in MDM and EMM, and look to expand to support the needs of the global enterprise going forward with cloud services, mobile applications and security solutions to support their mobility needs.

But enterprises need to start today in identifying their key initiatives based on current and future trends in mobility. As mentioned previously, the main trends this year include policy, mobile apps and security. Let’s look at each in depth.

**Enterprise Mobile Policy**

One of the first key initiatives is to develop policy on how mobility will be used in the enterprise. Enterprise mobile policy should include these main areas:

- **Identify Users** - policy should identify the different user segments. Although some policy covers all users, policy may differ depend on user requirements.
- **Hardware, software and services** - policy should dictate the types of hardware, software (OS, applications) and wireless services that will be supported.
- **Security levels** - policy should articulate the security needs of the enterprise, what security provisions will be used and details around data loss prevention, authentication and encryption guidelines, guidelines for security procedures, including lost device process.
- **Costs** - policies should detail cost responsibilities, spending guidelines etc.
- **Regulatory** - guidelines should also address local regulatory requirements. For example, holding a phone is illegal in many locations. The best advice is to require users to adhere to local laws.

Though most companies have some type of policy—most don’t go across the major areas of IT like security, networking and hardware. It’s better to have a single, combined policy than many individual ones. That doesn’t mean that the policy should be huge. Try to keep the policy to no more than five pages so that users will read it. Make getting a new device or service contingent upon agree to policy. Most MDM products can support policy endeavors and even capture agreements, location and date of policy readings by users.
Mobile Application Identification and Management

Most companies today are actively developing their strategy on mobile applications. Though most companies already support wireless email, they definitely are looking at rolling out additional support for enterprise applications—many that are being used on laptops and desktops today. However, many organizations struggle with prioritizing and mobilizing their applications. Which apps should enterprise mobilize? Often enterprises answer to that is either “I don’t know” or “Everything.” Everything is a bad answer but an easy one. Enterprises want to replace current computing platforms for mobile ones, so they think they should take everything off the desktop/laptop and put it on a smartphone/tablet. This is not a good idea. Some don’t know what should be mobilized because they aren’t close to the business. They focus on horizontal apps like email or calendaring, but potentially miss company and user-specific applications that drive business processes. Usually enterprises start out wanting to increase productivity or drive revenue. These are great goals but to be successful, enterprise need to go deeper into identifying user requirements and matching them to individual, line-of-business or corporate goals. How to do this?

First, think about the goals that the enterprise has. These could be user goals, lines of business or corporate. These will help drive the identification of the mobile process. Next, stop thinking about apps. Smarter thinking is to mobilize the needed data that will drive the business, reduce costs, increase productivity, collaboration or revenue. Apps are secondary, important for accessing and securing data, but not “killer.” Next—think about your users. Not everyone is truly mobile for his or her everyday work today. Sure many extend office hours or want an easier way to access email on the fly, but who are the real mobile workers in your company? And don’t just think about the road warriors or executives, what about those inside your buildings, or campus that may never be at their desk? Think about both increasing revenue and saving it. The business case will help a lot in identifying which users and data to mobilize. As the number of devices and applications grow in the enterprise, IT needs to look towards automating and getting tools to support that application growth. Mobile application management (MAM) adoption is growing rapidly because it helps the enterprise create, secure, distribute, manage and analyze enterprise mobile applications. Today—most EMM solutions incorporate MAM as part of their solution by supporting data containers that can secure enterprise data and implement policy (see the section, “Mobile data containers have tradeoffs”). In the past year—the idea of application containers has taken off. With app containers, apps can be forced to support enterprise policies (i.e. data movement, cut/copy/paste, encryption standards etc.). This supports a moderate to high level of security (hardware-level security is not available). Companies can quickly (in minutes) convert existing apps (via “app wrapping”), or easily add code in to new ones to enforce security and management policies. Plus this works across both iOS and Android devices, so availability is high. Already thousands of managed and secured apps are on the Apple App Store and Google Play. Many users may not even show they are secure—but they are. This is a key part of enterprises future mobile security program.

Mobile Security

Much has been written in the past on enterprise mobile security. Companies that have supported BYOD for the past few years feel that they have lost some control over where their data is accessed and stored. They’ve gone from tightly controlled systems that allow for granular policy, to loosely controlled devices
with minimal policy. Most companies have followed best practices by supporting data encryption, PIN-based authentication and some rules about data movement. But today, most applications off the public application stores don’t allow granular policy for DLP and data restrictions. Companies looking to mobilize their own applications are also looking at the use of MAM to ensure mobile policies. Mobile security is covered in-depth in our whitepaper, “Delivering enterprise information securely on Android, Apple iOS and Microsoft Windows tablets and smartphones.”

**Mobile Data Containers Have Tradeoffs**

Data security remains top of mind for CIOs as they consider how to manage consumerization and BYOD. Security is a continual investment, even more so with the emerging mobile enterprise. One of the most popular enterprise mobile management platforms, XenMobile Enterprise, includes a full suite of secure mobile apps that can help enterprises contain and manage their data. But much is still misunderstood about the different container technologies and methods for securing mobile data. Each container technology has its trade-offs, but some are rising to the top over others. To assess them it’s important to look at these four main areas: cost, availability, security level and user experience.

There are generally two ways to contain data on mobile devices: through hardware or software techniques. Hardware containerization basically runs two systems on a single device—two radios, DSPs, memory, OSes etc. One is used for personal data, one for corporate. Never the two shall meet. So even if the personal side is hit by a virus and can’t even be turned on, the corporate side still works. This is a very strong, secure solution. The problem is that it is not widely available, running two systems is costly and the user experience—switching back and forth between two systems—is poor. The need for this level of security is typically for those industries that have the highest security need, usually driven by regulations. Government, financial services and healthcare are the primary targets.

More popular are the software-based containers, of which there are three types: OS-based, application and thin-client. Some companies are promoting the use of OS-based containers. Usually a form of a hypervisor is used to run two separate OSes (on the same hardware layer)—one for business, one for personal. A single hardware platform keeps costs down; it has a high level of security, virtually separating data. Also, applications don’t need to be rewritten or designed for a specific vendor. But hardware availability is low—not every Android device is supported, the container may be proprietary to specific vendors (i.e. Samsung Knox) and iOS is not supported in this manner. The user experience of “dual-personas”, though getting better, is not one that companies have accepted yet, so is often rated lower.

Thin-client containers use web browsers to access data or apps, or are specific apps themselves, like Citrix Receiver™. They are very secure because they can be set to erase data once disconnected—so no data remains locally. However, this can be an issue for mobile users who need offline access to data and apps if not connected to the network. In the future—secure data stores can be created to allow for some offline access to apps and content. But otherwise, thin-client containers are excellent—widely available, easy to use, low cost (depending on type) and very secure. More companies—especially those with campus-oriented, or always connected employees as in healthcare, hospitality, banking, education—are using thin-client containers as part of their mobile strategy. This will only increase.
Containerization is gaining speed and adoption in the enterprise. Today the race is on to create secure and easily managed applications that offer the convenience and rich user experience of a personal app, but help enterprise control the security of movement of their data. This will be the next opportunity for vendors in this space, to increase the functionality and UE of secure data, but allow enterprises and users the freedom they need to do their job.

**Citrix Supports The Mobile Enterprise**

Citrix strategy aligns perfectly with the emerging needs of the global, mobile enterprise. In 2013, Citrix launched the XenMobile® Worx apps—which included a manageable, containerized email, calendar, contacts app called WorxMail™ and an enterprise-class web browser, called Worx Web™. The idea is to support the IT requirements for high-levels of security, with data encryption, managed open in, policies on data movement (cut/copy/paste) and other requirements IT have. It also supports the company in managing enterprise data, on user-owned devices for those that have a BYOD policy. At the same time, it gives users a better experience than they could get with the native apps. For example, file attachment is available right from the email, there is one click to dial into web conferences and conference bridges. Citrix improved upon the native experience and delighted both end users and IT. Citrix also provides tools, in an SDK and wrapping agent that allows enterprise to secure and manage their own apps through the Citrix XenMobile platform.

In 2014, Citrix announced continued progress in this area, with new apps like WorxDesktop™, WorxEdit and WorxNotes. Citrix will continue to launch more apps to fill in where enterprises and users are missing, what research firm Forrester calls the “app gap.” At the same time we will continue to work on the main areas of policy management, BYOD, mobile apps and the highest level of security.

Citrix enterprise support is centered around the Mobile Workspace. The idea is to support any user, device and any location—around apps, data, personal or business, desktop or mobile, see Figure 3.

![Image of Mobile Workspace](image-url)

**Business Class Delights Users and IT**

When enterprises first started adopting mobile devices, they went towards enterprise class devices that offered strong management and security, but not always the best user experience. The consumerization of devices reversed that by giving a great consumer experience, but little in the ways of management and security. Companies are looking to reverse this trend, and Citrix is focused on providing the alternative, a mobile device that offers a strong “business class” experience that users want, with the security and management that IT needs.

The way this is done is by giving users a better experience in their everyday business
applications that their native experience may not support. Citrix focuses on workflows by understanding how business users actually use their apps and provides shortcuts and optimizations specifically for business users. Business users answer more emails, create more content, collaborate more than the average smartphone user, yet most apps hadn’t been designed with these needs in mind. Citrix supports the scale business users need when responding to the multitude of everyday uses, made especially difficult while on the road.

But that scale is also important for IT. Most business users have more than two mobile devices, and IT needs to support hundreds and thousands of devices. Citrix mobile solutions are designed to scale for IT, to support device enrollment, application deployment, provisioning and reporting across a large number of users. Integrated with NetScaler®, the industry’s leading enterprise gateway product, Citrix XenMobile has been tested to support up to one hundred thousand transactions simultaneously. Citrix is delivering on its promise to delight both IT and their customer, the end user.

Future Mobile Needs
Citrix is assessing the future of mobility, including support for new devices, platforms and mobile apps. But Citrix also recognizes that mobility goes beyond that. The Internet of Things (IoT), wearable and virtual computing are all part of the Citrix roadmap. Citrix will continue to lead the market in terms of supporting mobile-first initiatives, integrating platforms across IT and supporting all enterprise technology needs, not just handhelds. These are key to the Citrix differentiation and makes it the leading platform for the emerging mobile workspace solutions and enterprise mobility.

Mobile Enterprise Best Practices
Citrix recommends some best practices for enterprises when implementing mobility. These include:

- Assess User, Business and IT Requirements—this is the first step in creating a strategy and policy. Companies should identify user requirements (apps., data, mobility style, devices needed).
- Segment Users—create user segments and groups for individual policy and management based on requirements. We recommend no more than ten different user segments across most enterprises.
- Design Policy Across IT—there should be one main policy document across IT to make it easier for users to read and adapt.
- Develop A Business Case—creating value, saving costs—these are the best ways to get mobile plans moving forward. Identify specific goals and steps needed to accomplish. Align to business goals too.
- Create a Mobile Center of Excellence—mobility doesn’t sit on one place. A MCOE aligns the different areas of IT, like application development, networking, security etc. around the mobility planning and lifecycle process. Also a great place to test new mobile apps, devices and services before introducing them into the work environment.

Citrix recognizes that each customer is different, so will work with each one to make sure their mobile enterprise strategy is a success today and in the future.
About Citrix
Citrix (NASDAQ:CTXS) is a leader in mobile workspaces, providing virtualization, mobility management, networking and cloud services to enable new ways to work better. Citrix solutions power business mobility through secure, personal workspaces that provide people with instant access to apps, desktops, data and communications on any device, over any network and cloud. This year Citrix is celebrating 25 years of innovation, making IT simpler and people more productive. 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 users globally. Learn more at www.citrix.com.

Copyright © 2014 Citrix Systems, Inc. All rights reserved. Citrix, XenMobile, WorxDesktop, NetScaler, WorxMail, Worx Web and Citrix Receiver 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.