# Secure Mobile Collaboration with Citrix XenMobile and ShareFile



CITRIX®

Mobile devices and BYOD have brought unprecedented agility to the enterprise, allowing users to collaborate, access information and get serious work done any time, from almost anywhere on the planet. Along with this mobile user freedom and agility, however, have come unprecedented security challenges.

Mobile devices and BYOD have brought unprecedented agility to the enterprise, allowing users to collaborate, access information and get serious work done any time, from almost anywhere on the planet. Along with this mobile user freedom and agility, however, have come unprecedented security challenges.

Any time users store sensitive enterprise information on their laptops, smart phones or tablets, they subject it to theft or exposure if those devices are ever lost, stolen, or connected over insecure WiFi networks or the Internet. When users mix personal and work lives on the same device, they risk insecure personal applications and mixed personal and work data leading to sensitive data loss and theft. This could happen either advertently or inadvertently, when, for example, users send corporate information in personal emails or browse infected Web sites that introduce malware into the corporate network.

When mobile users take advantage of consumer file sharing services such as DropBox and Box, they take a risk as well, as these services were not built with enterprise management and security in mind. Even those that have enterprise features are not as manageable and tightly integrated with enterprise mobile security solutions as they should be.

Conversely, if IT imposes draconian security policies and monitors personal mobile devices and data it risks impeding employee productivity and agility. Worse, users may rebel or find ways to get around enterprise security measures so they can get their work done or prevent IT from snooping on their personal lives.

### The Citrix XenMobile Solution

The good news is that the tightly integrated package of Citrix XenMobile with ShareFile offers a superior solution for protecting sensitive enterprise information while still allowing mobile users to get work done in the manner they prefer. XenMobile with ShareFile is a particularly powerful combination as it's not only more secure than using a third-party file sharing service with an Enterprise Mobility Management (EMM) solution, it's also more convenient for users.

In this whitepaper, we'll dig into the security and management aspects of the XenMobile/ShareFile solution, with an emphasis on enterprise security and why the combination of both are the best solution for this purpose.

## Mobile Security Requirements

In the enterprise, any mobile security solution must be able to:

Deter security threats by blocking malware and preventing unauthorized access to sensitive enterprise information. This is usually accomplished through containerization, encryption in transit and at rest, and stringent access control that create a hard separation between enterprise and personal applications and data on the device.

Detect actions that may open up the enterprise to attacks and data theft and address them quickly and automatically, according to company policy.

Respond quickly to threats and vulnerabilities, such as lost or stolen mobile devices, in ways that reduce or eliminate threats to corporate information.

Remediate any security issues that could cause breaches to occur.

Citrix XenMobile provides superior capabilities to address all these requirements. And, XenMobile manages to do so while allowing employees maximum freedom and agility to use their mobile devices the way that keeps them most satisfied and productive.

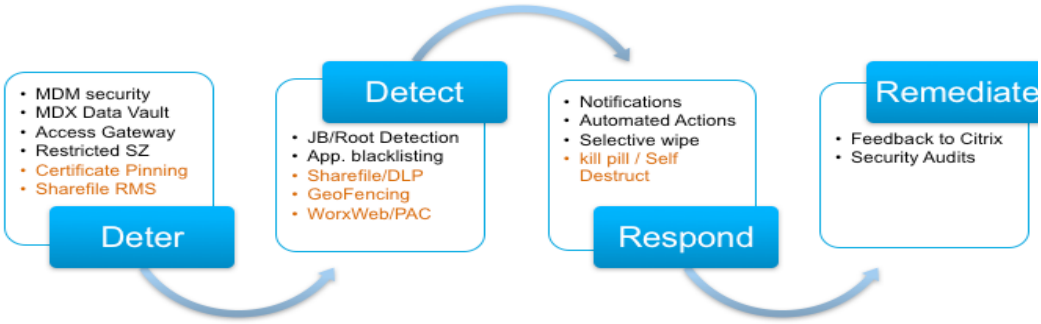



Figure 1: Citrix XenMobile and ShareFile Security Lifecycle

## Deter

Citrix XenMobile is a powerful combination of traditional mobile device management (MDM) and cutting edge Mobile Application Management (MAM) that ensures enterprise information stays isolated and protected. The beauty of XenMobile is that it's not only comprehensive and tightly integrated, it's also modular, so organizations can choose to deploy MAM only without MDM or vice versa, and still retain the most powerful security and management features of each. This is important as many BYOD users find all-encompassing MDM policies too restrictive and intrusive. Organizations deploying XenMobile with just MAM will find their information protection is airtight, even without MDM.

Deterence comes from the following XenMobile sets of features:

*Classic MDM security*, XenMobile MDM focuses on discovering, configuring, securing, supporting, monitoring, managing and decommissioning all enterprise user devices, including smart phones and tablets. With Windows 10, XenMobile can now even offer unified endpoint management (UEM) across laptops running this operating system version. XenMobile can also manage and secure Macintosh laptops.

Aside from user device enrollment--including self-enrollment-- provisioning and Exchange ActiveSync functionality, XenMobile MDM can protect enterprises from application and data threats through application blacklisting and whitelisting policies, jailbreak detection, device passcode enforcement, compliance checks, and the ability to run a full or selective remote wipe of devices suspected to be stolen, lost or out of compliance. XenMobile MDM can also configure device encryption and VPN and WiFi settings to protect data in transit and at rest and provide an enterprise catalog and portal to direct users, based on their AD role and user profile, to enterprise approved applications and cloud services.

MDM comes with full policy-based geo-fencing capabilities so IT can apply geographical boundaries to mobile device and application use. For example, IT can prevent the use of certain enterprise mobile devices and applications whenever the user leaves the enterprise campus, or simply alert the user and log the action. The same actions can be taken when the user leaves the country or travels to certain untrusted parts of the globe.

These MDM features can go a long way to securing devices from typical threats to corporate data. However, classic MDM is best applied in an environment of corporate issued mobile devices used only for work.

### *Enter MAM*

In current mobile environments, employees use their mobile devices increasingly for both work and pleasure. These users are less likely to take kindly to a locked down, carefully controlled environment where they can't download and use their own preferred applications and personal data or browse the Web freely, or one that subjects the use of their device and applications to close monitoring.

That's why mobile application management (MAM) has grown significantly in the enterprise. Rather than managing and securing the entire device, XenMobile MAM separates personal and enterprise mobile applications and data through containerization and encryption and limits monitoring and management to the device's enterprise components. The personal and enterprise worlds can then coexist on the same device without personal browsing, applications and other use posing a threat.

In fact, as they face mounting user resistance to classic MDM, some organizations have chosen to

eliminate MDM as a management and security strategy entirely and focus solely on MAM. That's why it's very important to understand that XenMobile provides full MAM capabilities without having to deploy MDM at all.

With competing solutions, many essential MAM features depend on policies configured in MDM. So, for example, deploying MAM without MDM may mean the loss of device side data storage encryption. Why? Most competing EMM solutions rely on the encryption technology built into the device operating system and can only activate it when the device is enrolled in MDM. XenMobile provides its own powerful wrapping and FIPS 140-2-compliant AES 256-bit encryption--with encryption keys stored in a protected Citrix Secret Data Vault--and can apply scores of XenMobile policies in both an MAM-only and MDM-plus-MAM deployment.

*XenMobile Containerization.* Containerization comes mostly through Citrix mobile Worx apps—XenMobile-wrapped enterprise apps provided by Citrix and its development partners--as well as enterprise or third-party developed and compiled non-public custom apps.

Citrix provides several enterprise level Worx productivity apps through Worx Home. Citrix Work productivity apps include a secure email client (WorxMail), a secure Web browser (WorxWeb), and Task and Note Taking apps (WorxNotes and WorxTasks). Hundreds of other third-party Worx apps are available as well through a Worx Gallery, and enterprises can easily create or wrap their own internally developed apps via the Citrix MDX toolkit or the Worx App SDK.

Using these Worx tools, organizations can apply scores of policies to these apps governing application provisioning, user authentication, application-to-application data flows, FIPS 140-2-compliant AES 256-bit encryption of data at rest, geo-fencing, remote wipe and automatically enabled application specific encrypted micro VPN's. They can also place scores of user restrictions on attaching files, cutting and pasting information and data from application files to other Worx and non-Worx applications such as email, opening files in other applications, printing files and more.

*Kill Pill.* Geo-fencing is another essential security measure. Unlike competing EMM solutions, XenMobile's Kill Pill can be applied to designated enterprise mobile applications in MAM, locking apps as a compliance action when users leave the permitted geographic range and even using a feature called a Kill Pill to direct apps to self-destruct after an IT-configured number of days of inactivity.

*WorxWeb PAC.* WorxWeb includes a new feature that extends proxy access configuration (PAC) files from behind the firewall to the roaming mobile device. With PAC files, all mobile WorxWeb browser traffic gets sent over an encrypted VPN to the enterprise or cloud Citrix Netscaler Gateway, which then routes traffic according to a raft of configuration rules. Organizations can configure policies that govern which Web sites users can and cannot access and what enterprise firewall proxies are used to access them and analyze and filter URL's to ensure they're safe.

*Office 365 and Security.* XenMobile allows IT to deploy Office 365 and other Microsoft apps and services via Worx Home. IT can then enforce a raft of policies around Office 365, including file encryption at rest and micro and per app VPN encryption in transit between the 365 cloud and enterprise network, or the user device and the cloud. Organizations can also deploy native mobile email or WorxMail for Exchange and enforce OS containerization features, cloud backup, "open in" restrictions, geo-location and numerous other security policies.

Other newer deterrence capabilities include:

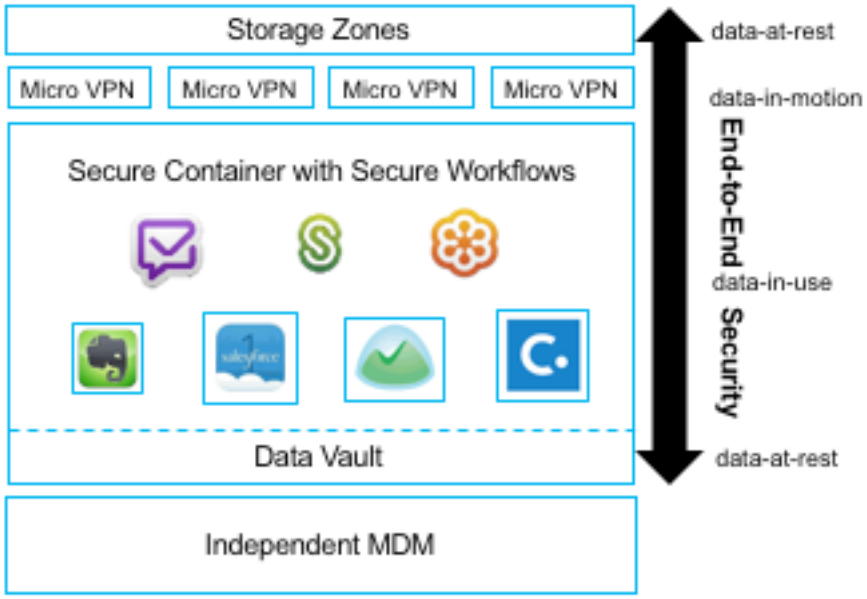
*Certificate Pinning.* Certificate Pinning reduces the likelihood of Man in the Middle attacks. When the user enrolls in the XenMobile, Worx Home asks for an email address or other information it can use to determine which XenMobile server the user should connect to. Worx Home then connects to the Citrix Auto Discovery service to find the right server and passes the info back to the device. To ensure there is no interception, XenMobile Autodiscovery also sends the device the certificate of the destination XenMobile server and does a certificate match when the device connects to it.

*Touch ID.* Touch ID provides a fingers-wipe alternative to Worx PINs (when a fingerprint scanner is available on the device), to get into enterprise MDX managed apps.

*Shared Devices and apps.* Shared Devices and Apps allows multiple employees to use a single device, with different policies for each user and complete separation of user data, applications and settings. This is a useful feature for devices employed in warehouses, hospitals and out in the field.

*Multifactor Authentication.* Multifactor Authentication is configurable on a per app basis.

Figure 2: Citrix XenMobile and ShareFile Security Solution



### *Flexible, Secure File Sharing*

ShareFile is a powerful Citrix enterprise-focused file sharing alternative that offers users the same or better capabilities than DropBox, Box and other popular file sharing services but with much more flexibility, enterprise level management and security and tight integration with XenMobile. The result is both superior data security and user convenience.

*Flexible Storage.* While most file sharing services force users to store files in the service's own cloud, XenMobile ShareFile Storage Zones feature allow enterprises to store shared files either in the Citrix ShareFile cloud service, in another public cloud storage service of their choice, or on-premises behind the firewall to meet stringent security, compliance and data sovereignty requirements. There's also the option of using any combination of the three.

For data stored on premises or in an enterprise cloud, ShareFile supports CIF based network storage systems and provides connectors for Windows network shares and Microsoft SharePoint so that files don't have to be migrated to another service in order to be shared. This is important as any data copying or migration from its original site is always a potential security issue.

ShareFile storage flexibility is not only a security advantage but a performance advantage as well, as it allows the enterprise to place files strategically in globally dispersed cloud or data centers close to dispersed and mobile users. Such a strategy can optimize network latency and data access performance. ShareFile's Storage Zone flexibility allows the enterprise to optimize storage cost as well.

*Metadata Protection.* ShareFile metadata is always stored and managed within the Citrix cloud, but a special Restricted Zone feature encrypts metadata with a customer key so Citrix cannot see or access the names of files and folders, even if they're under subpoena. IT can require users to authenticate to a customer server in addition to the ShareFile cloud.

ShareFile's overall design keeps the UI and file access completely separate to enhance performance. When a user logs into the ShareFile Web site, ShareFile delivers the shell of the user experience from the cloud, but configures a completely separate authenticated channel with the StorageZones controller to populate the listing of files and folders.

*DLP.* File and data access can be even further regulated via integration with existing enterprise Data Leakage Prevention tools or ShareFile's own data classifications and restrictions. These include a raft of polices to limit or prevent the opening of ShareFile stored files in Worx and non-Worx applications, cutting and pasting text from files to emails, attaching files, printing and more.

Extra convenience and security comes from tight integration with other Citrix Worx apps. For example, instead of using email attachments, users can be required to embed links to ShareFile files, providing more security than attachments. Policies can also be configured to store incoming email attachments in ShareFile automatically.

ShareFile integrates fully with the enterprise Active Directory but limits AD information use to firstname, lastname, email address and group data for finegrained access management, so there is no impact on AD. Users can provide View Only Access to certain files to prevent sensitive information from being altered or compromised.

## Detect, Respond, Remediate

Most of the features discussed so far fall mostly into the Deter category but XenMobile and ShareFile offer other features as well for detecting, responding to and remediating security issues as well.

*Detect, Respond.* These features include discovering jailbroken or rooted devices and the use of applications that have been blacklisted or not whitelisted by IT. When they are detected, policies can be configured to notify the user, take automated actions, unenroll or quarantine a device, issue instructions for a selective wipe of enterprise applications and data or run a Kill Pill. .

*Remediate.* Remediate features include security audits of logs to determine an organization's risk profile and reporting on repeat offenders, brute force attempts and other threats.

As the mobile enterprise lifestyle evolves, organizations need mobile management solutions that can address every aspect of mobile security and compliance without compromising employee mobile productivity and flexibility. True security can only come from flexible solutions that address every aspect of the mobile device, application and data sharing experience in a comprehensive manner, yet provide the modularity organizations require to address their particular security and user productivity issues best. XenMobile with ShareFile is just such a solution, providing capabilities that can deter, detect, respond and remediate any security challenge mobile living brings to the enterprise, while balancing security with the flexibility and empowerment mobile users need to stay productive.

**Corporate Headquarters**
Fort Lauderdale, FL, USA

**Silicon Valley Headquarters**
Santa Clara, CA, USA

**EMEA Headquarters**
Schaffhausen, Switzerland

**India Development Center**
Bangalore, India

**Online Division Headquarters**
Santa Barbara, CA, USA

**Pacific Headquarters**
Hong Kong, China

**Latin America Headquarters**
Coral Gables, FL, USA

**UK Development Center**
Chalfont, United Kingdom

CITRIX®

**About Citrix**
Citrix (NASDAQ:CTXS) is leading the transition to software-defining the workplace, uniting virtualization, mobility management, networking and SaaS solutions to enable new ways for businesses and people to work better. Citrix solutions power business mobility through secure, mobile workspaces that provide people with instant access to apps, desktops, data and communications on any device, over any network and cloud. With annual revenue in 2014 of $3.14 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