Citrix XenMobile Mobile Application Management Advantages

CITRIX®

As enterprises transition from corporate owned and managed laptops, tablets and smartphones to Bring Your Own Device (BYOD), enterprise mobility management (EMM) has shifted from managing the entire mobile device (MDM) to securing and managing just the enterprise applications (MAM) and data each device houses and connects to.

Why? When employees mix personal and work lives on a laptop, smartphone or tablet, asserting tight device-level control is a sure path to user dissatisfaction and resistance, not to mention reduced productivity. EMM solutions seek a strategy that strikes the right balance between security and user personal flexibility and freedom. They do so through a combination of:

- Containerization employing a variety of technologies and strategies that cut off or limit communications between enterprise and personal mobile applications and allows organizations to provide stronger controls around its apps and data without having an impact on the privacy of the user.

- Encryption of all sensitive enterprise data both at rest on the device and in transit over WiFi connections and the Internet, in order to prevent data exposure in the case of device loss or theft.

- Secure VPN Access utilizing per app or micro app VPNs technology to protect corporate resources accessed by mobile users.

- Secure Mobile File Sharing / Mobile Content Management to provide users with the same or better collaboration and convenience they get from consumer oriented services.

However, while most EMM solutions offer the capabilities listed above, EMM solutions differ in the implementation of these capabilities particularly as it relates to Mobile Application Management (MAM). It's important to understand these MAM differences in order to make the right decision for your organization to satisfy your users as well as protect your information.

MAM Approaches

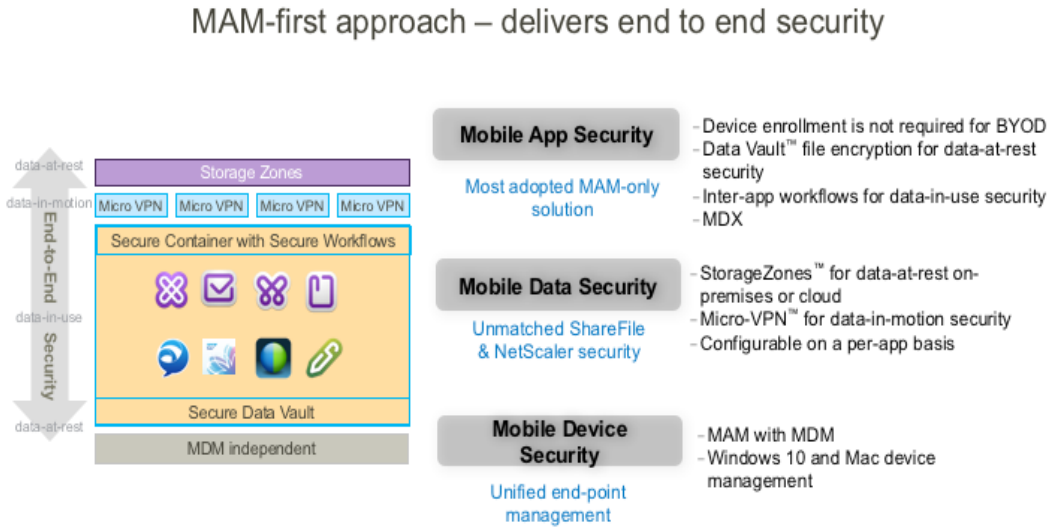
Mobile Application Management (MAM) has traditionally been deployed as a technology layered on top of Mobile Device Management (MDM). In fact, for many use cases, MDM technology is required to make MAM work. Here are some examples:

- An MDM device passcode policy is required to apply device level encryption which provides application layer security.
- MDM is used to push and maintain user certificates for application layer security.
- MDM is required for Per App VPNs.
- MDM is required for data in use controls such as open-in.
- MDM is required for application Single Sign-On.

Many of these MAM with MDM solutions take advantage of mobile device operating system management API's to leverage the containerization, encryption, VPN and other features offered by each mobile device platform. They may also leverage other device-specific technologies, such as Samsung Knox, offered by device manufacturers on top of the capabilities offered by the mobile OS.

A MAM with MDM approach can only harness platform security capabilities by enrolling end user devices in an MDM solution, and in many cases they require setting device-level restrictions that don't differentiate between personal and business use. The result is a poor user experience and less security control for managing BYO devices. As such, many organizations seek solutions that can employ robust MAM without MDM or MAM Only that is MAM completely on its own without relying on device enrollment in order to meet user satisfaction, privacy and security concerns particularly for BYOD.

While most EMM solutions only offer MAM with MDM, Citrix XenMobile allows enterprises to deploy MAM with MDM or MAM Only enabling enterprises to select the best approach to protecting application data based on their specific use case, security and user requirements. We refer to this as our MAM First Strategy.



XenMobile MAM Only Approach

Citrix XenMobile's MAM Only approach provides MAM features which sit on top of--or even instead of--those capabilities offered by each mobile operating system or function.

XenMobile's MAM Only approach essentially allows you to apply "MDM-like" polices at the app level rather than the device level. For example, with MDM you can lock, wipe and selectively wipe the device. With XenMobile's MAM Only polices you can also lock, wipe and selectively wipe but rather than apply these actions to the entire device (a personally owned device in many cases) you can apply them to each individual managed app.

In addition, MAM with MDM solutions generally depend on encryption technology built into the mobile operating system (requiring a device PIN code to be set) to protect data on the device. However, XenMobile's MAM Only solution provides its own AES 256-bit encryption using FIPS 140-2-validated OpenSSL libraries across all its mobile platforms.

There's no need to enroll a device to take advantage of XenMobile's separate encryption, and XenMobile's encryption operates even when the device passcode is not present. Another benefit of device-independent encryption: if the device's encryption becomes compromised, the security of separately encrypted data is not affected.

The advantage of XenMobile's MAM Only solution is not only MAM independence from MDM, but a more consistent application of MAM policies across different devices and device operating systems.

A sure way to determine if your MAM solution requires MDM is to check devices for the presence of an MDM profile. If one exists, if there's no VPN icon or encryption requires a passcode, then the MAM solution is not MDM independent.

MAM Containers are Not All Alike

Containers which separate personal and business data is at the core of the different MAM strategies, but EMM solutions take a different approach. One approach, employed by Samsung KNOX, BlackBerry and other EMM solutions, is to divide the user device into two completely separate "workspaces," sometimes called personas: one for personal and one for enterprise use. The enterprise workspace holds all the protected enterprise email and other applications, which are usually available through a specialized enterprise app store, while the personal space contains all the user's personal apps and data.

Organizations can leverage MAM with MDM to apply numerous policies to the enterprise workspace, but constantly switching between personas to mix work and pleasure is frequently inconvenient for the user. Such a scenario may not only have an adverse impact on productivity, it can lead to user resistance, which in turn, can lead to the use of workarounds that expose the organization to security issues, data breaches and malware. Even though these solutions do offer separation between personal and business, they still rely heavily on device-level settings or restrictions, such as device PIN codes, to provide data protection.

As noted earlier, XenMobile offers MAM with MDM and as such, supports these workspaces. In addition, Citrix offers its own containerization with its Citrix MDX technology that balances enterprise application and data security with a satisfying user experience.

XenMobile MAM Only Container - Citrix MDX

Citrix's containerization strategy is based on its MDX technology which does not require MDM. Additionally, instead of dividing the device and the user experience into completely separate personas, Citrix MDX technology allows users to view and access enterprise and personal applications without having to switch constantly back and forth between two separate environments. Instead, using XenMobile's MDX Toolkit, enterprise IT can build MDX into individual enterprise applications with the policies and containerization strategies necessary to protect associated sensitive information. This is important as it provides a more seamless, productive experience for the user while providing the necessary protections for the enterprise.

MDX technology includes three core elements:

1. Data protection with active policy enforcement – MDX offers more than sixty

different policies controlling how MDX-enabled apps can send and receive data and interact with other apps. It can also restrict device/OS features when certain risky apps, such as the camera or microphone, are employed. MDX provides the engines needed to enforce these policies within the app at all times without requiring communication to the XenMobile server. These policies are enforced even in airplane mode.

2. Data protection with separate encryption – MDX includes its own FIPS-140 validated AES-256-bit encryption library, which encrypts sensitive data within the app completely separately from the device's provided encryption. Separate encryption is offered on all platforms and provides necessary data security without requiring device PIN codes.

3. Data protection over the air – MDX technology includes MicroVPNs communicating through the Citrix NetScaler Gateway. NetScaler is also FIPS validated. When combined with XenMobile, it offers an organization a complete end-to-end FIPS- validated solution. NetScaler provides the most scalable, (with more than 100,000 simultaneous encrypted sessions) secure connectivity to resources located behind the enterprise firewall.

Citrix provides the MDX toolkit to third party mobile app vendors as well as enterprise organizations to use to transform internally developed apps into MDX-enabled enterprise applications, often through just a few steps or a single line of code. Once an app is MDX-enabled, enterprises can apply scores of policies and capabilities that ensure the application and its data are always protected. This is a huge benefit for organizations building their own apps. Citrix MDX technology allows the developers to focus on building the best user experience for his or her app without requiring expertise in building enterprise grade security and access controls – without requiring device enrollment.

Some of these policies include:

Application interaction, document exchange and data flow policies that block, permit or restrict the opening of documents in non-MDX enabled applications, as well as attaching sensitive documents to emails and copying, cutting and pasting information into emails and other application documents. Printing of documents can also be restricted if necessary.

User Authentication policies that can require users to input a passcode to unlock the

MDX-enabled app when it starts or resumes after a configured period of inactivity. A new alternative adds convenience by allowing the substitution of Touch ID for a passcode, where the user is able to access an application through a fingerprint scan on supported iOS devices. Other types of multifactor authentication can also be required on an application-by-application basis.

Online session policies that require users to have an enterprise network connection to use an app at all times or after a configured offline grace period.

Geofencing policies that set a maximum geographic radius for application access. So for example, IT can restrict the use of certain enterprise applications when the user leaves the country, travels to untrusted parts of the globe or even when the user simply leaves the enterprise campus. In such instances policies can be configured to simply alert the user or log the action, rather than always locking the application.

Kill Pill is a new feature that allows IT to direct MDX-enabled apps to be either locked or wiped if the device isn't able to contact the XenMobile server beyond a configurable interval. This can be particularly useful if a device is switched to airplane mode after falling into unauthorized hands.

Other MDX capabilities offered include:

- User certs for application authentication can now be distributed and managed without the requirement of MDM enrollment.
- Shared devices for MAM allows users who share a device to access personalized apps and data without having to re-enroll the device.
- MAM-only 2 factor authentication with single sign-on for all managed apps.
- Over 50+ MAM-only policies supported today with no requirement for an MDM profile.

Data in transit encryption and secure VPN options

EMM solutions differ in the approach to encrypted data in transit. Encryption in transit can be applied via app-specific micro VPN's that activate every time enterprise applications need to

connect to the enterprise network or encryption in transit can be applied through a per app VPN approach.

Micro VPN's are superior to device-level so called per-app VPN's, as each app establishes its own micro VPN tunnel, protecting the enterprise network from any other applications on the device. When the app closes the VPN is removed. IT can even configure apps to use different gateways for different levels of authentication and authorization. Micro VPNs are not dependent on device enrollment.

XenMobile Micro VPN to secure data in transit and secure network access

XenMobile Micro VPN's utilizes data optimization and compression techniques to ensure only minimal data is transmitted in the quickest time possible, which is advantageous for both data security and the user experience.

Citrix XenMobile can apply VPN tunnels to ActiveSync email, including its own secure mobile productivity apps. In most EMM solutions these are not available for the device's native email client software. XenMobile also offers micro VPNs across iOS, Android and Windows, while per app VPN solutions only offer VPN's for mobile operating systems, such as iOS that provide such support natively. In addition, with XenMobile's micro VPN capabilities, split tunneling is offered in a flexible ON setting that can configure encryption only for traffic destined for the corporate intranet; in an OFF setting, where all traffic is sent through the VPN tunnel regardless of destination; or REVERSE, where all traffic goes through a VPN tunnel except traffic to and from an intranet application or domain.

Citrix XenMobile Micro-VPN	Per App VPN (The Other Guys)
MDM not required	Requires MDM/MDM profile
Optimized for BYOD – MDM Independent	BYOD users must agree to a managed device
IT can set Micro-VPN on per app basis	Per App VPN is applied to all managed apps
Available for iOS, Android and Windows	Only available for iOS because it's part of the OS
Better SSO with support for Windows credentials, certificates, SAML, Kerberos or user name/password	Limited SSO (Certificates and Kerberos only)
PAC File/proxy support (WorxWeb) and automation	No PAC File support

Secure File Sharing / Mobile Content Management (MCM) Options

EMM solutions vary in their secure file sharing and MCM capabilities to further protect mobile application data. Some EMM file sharing solutions require administrators to upload user files first before mobile users can access their files. Other solutions are not tightly integrated into secure MDM independent productivity apps including email and calendar.

Citrix ShareFile – a leader in secure file share and sync

ShareFile is XenMobile's enterprise-class mobile file sharing application, which provides the same or better features and convenience as consumer friendly Box and DropBox, but with enterprise-level security and management. Some of the security features of ShareFile include:

Flexible Storage Rather than forcing users to store all information in the cloud, organizations have the flexibility to choose one or more options for file storage. Customers can choose to leverage ShareFile Storage Zones to store shared files either on-premises behind the firewall to meet stringent security, compliance and data sovereignty requirements; in the Citrix ShareFile cloud service; or in another public cloud storage service of their choice. ShareFile can store files on internal 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.

Metadata security A special Restricted Zone feature encrypts ShareFile metadata with a customer key so Citrix cannot see or access the names of files and folders. IT can also require users to authenticate to an enterprise server in addition to the ShareFile cloud in order to access their files.

DLP and MDX integration allows organizations to apply their existing data leakage prevention tools and policies to ShareFile file sharing. Organizations can also choose to leverage ShareFile's own DLP data classification and restrictions, such as restricting opening of files to certain applications and cutting, copying and pasting text into other files and applications and emails and attaching and printing files. View-only access can be applied to files as necessary. Users can also be required to use ShareFile links in emails instead of file attachments for ShareFile content security, and incoming email attachments can be sent automatically to ShareFile folders. .

Citrix Secure Productivity Apps

Mobile productivity applications are another area of differentiation between EMM solutions. Some EMM solutions take the approach of support native productivity apps and security application data through a MAM with MDM approach.

XenMobile takes a MAM ONLY approach and delivers its own set of enterprise MDX-enabled productivity apps including a secure but full-featured email client, personal information manager, secure Web browser, as well as an enterprise-grade note taking and task application.

Summary

As more and more mobile users mix their personal and business lives on their smartphones, tablets and laptops, enterprises will have to adjust to the flexibility and freedom users demand, while still managing and securing the use of enterprise mobile applications and data. MAM provides the key to this crucial mobile balance. In addition, enterprises need to be aware of the different type of MAM approaches – either MAM with MDM or MAM Only and determine which approach to apply depending upon their specific use case. Citrix XenMobile provides customers with the flexibility to choose between either approach. In addition, XenMobile's MAM Only approach provides the most robust set of security policies in a manner that doesn't impinge on the user's mobile freedom and productivity.

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