Excitement in the industry is extraordinary as the announcement of the planned integration of Citrix XenMobile and Microsoft EMS/Intune has now become a reality. This whitepaper will detail these many valuable features that are now available to Citrix and Microsoft customers.

Citrix Endpoint Management (formerly XenMobile) Integration with Microsoft EMS/Intune

Table of Contents

"What's the best way to partner with Microsoft? Learn from what Citrix has done for 20 plus years"

Brad Anderson| Corporate Vice President | Microsoft Enterprise Mobility + Security

Citrix and Microsoft partnership

"To further help companies deliver great productivity experiences for their employees, while enabling IT professionals to help protect company data across both cloud and on-premises applications, Citrix and Microsoft are integrating Citrix XenMobile and NetScaler with the Microsoft Enterprise Mobility Suite (EMS.)" -Citrix & Microsoft press release at Citrix Synergy 2016

The history of the Citrix and Microsoft partnership dates to the 1980s with the first of many licensing agreements.[1] The origin of Citrix XenApp was based on Windows technology and it was eventually licensed to Microsoft to form the basis of Microsoft Terminal Services.[2]

Fast forward several decades, through a variety of successful joint ventures, and Citrix and Microsoft have once again announced several innovations together. This announcement included and has delivered on innovations with a variety of Microsoft products, but we'll focus on those pertaining to Microsoft EMS.

Microsoft EMS overview

Microsoft EMS stands for Microsoft Enterprise Mobility + Security. From product perspective it includes the following:

- Azure Active Directory Premium – the Microsoft identity hub that enables single-sign-on for all resources from anywhere and it includes security aspects such as conditional access and multi-factor authentication.
- Microsoft Intune – is the Microsoft mobile device management and mobile app management solution which provides security controls for users, data, and apps on mobile devices.
- Azure Rights Management – provides document level security which manages and enforces rights to access protected data.
- Microsoft Advanced Threat Analytics – provides real-time security monitoring utilizing big data to identify threats and notify of risks

EMS is licensed through several Microsoft offerings with different sets of features that vary by enterprise needs. EMS includes Intune licenses; therefore, every EMS customer may utilize Intune MDM and or Intune App Protection capabilities.[3]

Differentiation

"XenMobile integration with Intune EMS (which will be delivered as a feature of our XenMobile and Citrix Workspace solution) provides additional security and productivity benefits for EMS customers."
-Calvin Hsu, Vice President of Product Marketing, Citrix Workspace

As part of the Citrix Secure Digital Workspace, XenMobile allows IT to configure and apply micro-VPN connectivity to mobile applications. This means that each managed mobile application on the device has its very own private micro-VPN from which application data can flow securely from the endpoint to corporate resource locations behind the firewall. The XenMobile SDK that enables it has been added to the Intune App SDK and therefore it may be enabled for any "enlightened" apps, or apps which are integrated with the SDK, such as the Intune browser.

At the same time, ShareFile, the Citrix market leading EFSS and collaboration solution and XenMobile's flagship application, Secure Mail, are now compatible and manageable by Intune. This means that Intune App Protection policies can be applied to ShareFile and Secure Mail placing it in the same container as other Office 365 mobile applications. Now, for example, a document received as an attachment in Secure Mail can be opened in Office 365 without ever leaving Intune App Protection. Citrix Secure Mail does not use a cloud proxy which is a big advantage for enterprises who do not want corporate email being cached in the cloud.

Getting Started

Citrix XenMobile and Microsoft EMS both provide mobile device management, and mobile application management. The joint mobile technology will be delivered and evolve as cloud services.

Microsoft Graph API Overview

Microsoft Graph eliminates complexity for developers by unifying authentication and combining all API entry points into one. It validates identity once then gives broad access to Microsoft cloud hosted services including full access to Azure Active Directory and the gamut of Office 365 applications.

To call Microsoft Graph, an app must acquire an access token from Azure Active Directory (Azure AD), Microsoft's cloud identity service. The access token contains information (or claims) about the app and the permissions it has for the resources and APIs available through Microsoft Graph. To get an access token, an app must be able to authenticate with Azure AD and be authorized by either a user or an administrator for access to the Microsoft Graph resources it needs.[4]

Citrix Cloud overview

Citrix Cloud provides the world's best integrated technology services for secure delivery of apps and data. It is a cloud-based management facility that unites all our leading technologies into a single management and

[1] https://www.citrix.com/content/dam/citrix/en_us/documents/go/citrix_timeline.pdf

[2] https://en.wikipedia.org/wiki/XenApp

[3] https://www.microsoft.com/en-us/cloud-platform/enterprise-mobility-security-pricing

[4] https://developer.microsoft.com/en-us/graph/docs/concepts/auth_overview

delivery platform. It provides a **single plane** across all our technologies to manage central functions such as administration, identity management, authentication, service provisioning, licensing and license management, service availability, monitoring and reporting.

Citrix Cloud has in-baked the Microsoft Graph APIs within the Citrix Cloud Admin console to allow configuration and deployment of Office 365 apps alongside Citrix mobile apps, Public app store apps, Web apps, SaaS apps, Virtual apps and desktop.

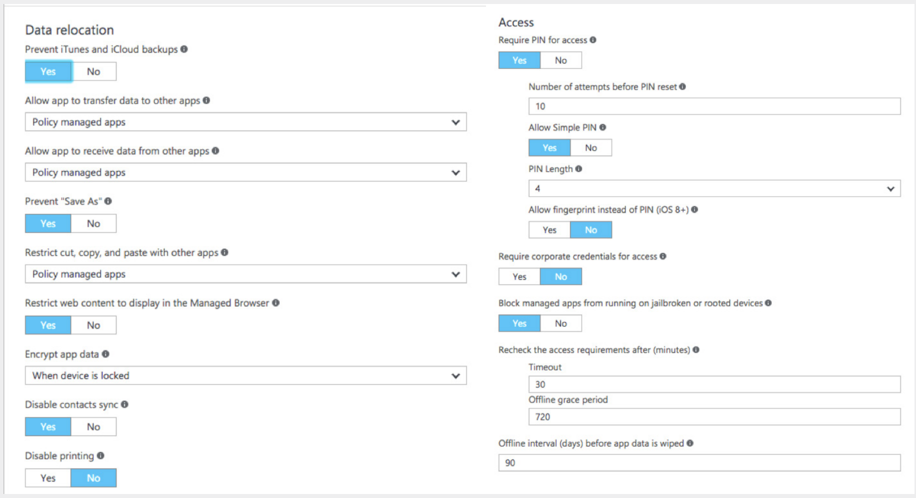
Intune Overview

Intune app protection policies help protect sensitive enterprise data. As app-level policies they may be used independent of the MDM solution that may be used which allows company data to be protected with or without enrollment. The policies it provides allow IT to restrict access to company resources and keep data within their purview.

There are currently 10 **Data relocation settings** for iOS which focus on controlling data movement for managed apps including use of iCloud, transfer to and from managed apps and non-managed apps, web display within Intune browser, encryption, and printing.

There are another 11 **Access settings** for iOS which focus on device access setting including pin characteristics, jailbreak detection, corporate credentials, offline timers, minimum OS version, app version, and SDK version.

Data Relocation and Access Settings



Data relocation

Prevent iTunes and iCloud backups
[✓ Yes] No

Allow app to transfer data to other apps
Policy managed apps

Allow app to receive data from other apps
Policy managed apps

Prevent "Save As"
[✓ Yes] No

Restrict cut, copy, and paste with other apps
Policy managed apps

Restrict web content to display in the Managed Browser
[✓ Yes] No

Encrypt app data
When device is locked

Disable contacts sync
[✓ Yes] No

Disable printing
Yes [✓ No]

Access

Require PIN for access
[✓ Yes] No

Number of attempts before PIN reset
10

Allow Simple PIN
[✓ Yes] No

PIN Length
4

Allow fingerprint instead of PIN (iOS 8+)
Yes [✓ No]

Require corporate credentials for access
Yes [✓ No]

Block managed apps from running on jailbroken or rooted devices
[✓ Yes] No

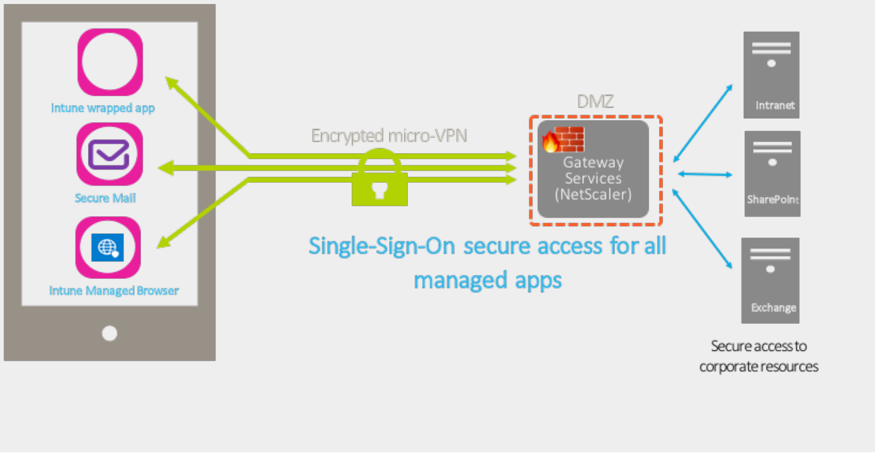
Recheck the access requirements after (minutes)

Timeout
30

Offline grace period
720

Offline interval (days) before app data is wiped
90

Micro-VPN to on-premise data for Intune Browser and Intune wrapped apps


Intune wrapped app
Secure Mail
Intune Managed Browser
Encrypted micro-VPN
DMZ
Gateway Services (NetScaler)
Single-Sign-On secure access for all managed apps
Intranet
SharePoint
Exchange
Secure access to corporate resources

XenMobile integration with Intune EMS overview

The first release of XenMobile integration with Microsoft EMS/Intune adds value to Intune customers as well as existing XenMobile customers in the following four areas:

1. **Unique* Micro-VPN to on-premises data for Intune Managed Browser and Apps
2. **Unique* Secure Mail and Citrix Apps for Intune for advanced security and DLP
3. **1st to market* Native Integration with EMS and Intune via Microsoft Graph APIs
4. **Enhanced* Citrix Workspace Value-Add with advanced security and compliance

1. Micro-VPN to on-premise data for Intune Browser and Intune wrapped apps

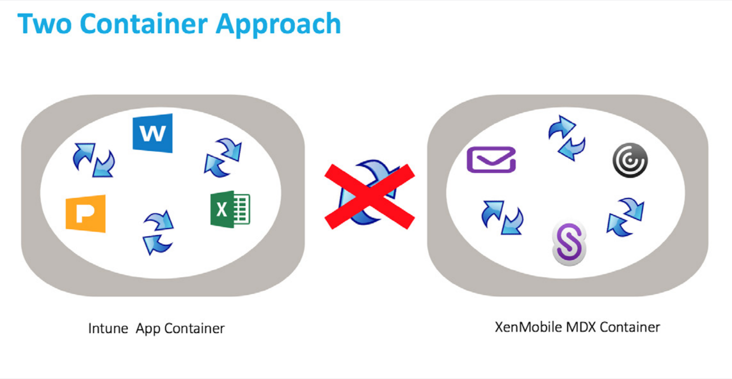
Today we bring the value of Citrix XenMobile micro-VPN to Microsoft Intune aware apps, such as Microsoft Managed Browser. It also allows enterprises to wrap their own line-of-business apps with Intune and Citrix to provide micro-VPN capabilities inside an Intune mobile app management (MAM) container. Citrix XenMobile micro-VPN enables your apps to access on-premises resources. You can manage and deliver Office 365 apps, line-of-business apps, and Citrix Secure Mail in one container for ultimate security and user productivity.

Micro-VPN brings the remote access capabilities of the market leading NetScaler Gateway to mobile devices via apps integrated with the XenMobile SDK. It is an on-demand application VPN connection that is initiated by Secure Hub on mobile devices to access corporate network sites or resources.

Sample use cases:

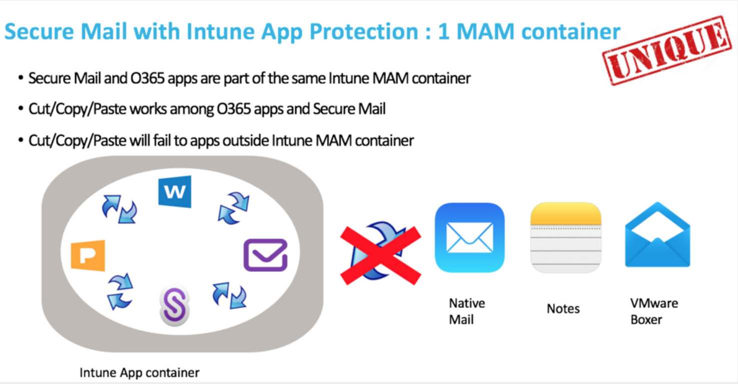
- With XenMobile micro-VPN capability, a user can access Internal resources using the Intune Browser, which now has XenMobile micro-VPN SDK embedded, without requiring a device level VPN or full MDM enrollment.
- With XenMobile micro-VPN capability, an IT admin can enable access to Line of Business App Servers hosted On-premise, behind the intranet DMZ/(s), without having to setup a device level VPN or having to go through full MDM enrollment.

Two Container Approach



Two Container Approach

Secure Mail with Intune App Protection: 1 MAM container



Secure Mail with Intune App Protection : 1 MAM container

- Secure Mail and O365 apps are part of the same Intune MAM container
- Cut/Copy/Paste works among O365 apps and Secure Mail
- Cut/Copy/Paste will fail to apps outside Intune MAM container

2. Secure Mail, Secure Web & ShareFile for Intune for advanced security and DLP

Citrix Secure Mail is an Enterprise Grade mail client that supports Exchange Active Sync, Lotus Notes Traveler as well as Microsoft Modern Auth. It lets users manage their email, calendars and contacts on their mobile phones and tablets. To maintain continuity from Microsoft Outlook or IBM Notes accounts, Secure Mail syncs with Microsoft Exchange Server and IBM Notes Traveler Server. As part of the Citrix suite of apps, Secure Mail benefits from single sign-on (SSO) compatibility with Citrix Secure Hub. After users sign on to Secure Hub, they can move seamlessly into Secure Mail without having to reenter their user names and passwords. (NOTE: Secure Mail supports single sign-on (SSO) with XenMobile MDM only)

Secure Mail now supports Multi MAM containers. Secure Mail can be deployed with XenMobile proprietary MAM (MDX) as well as Intune App Protection. This is essential for exemplary user experience stronger DLP controls between Citrix apps and Office 365 apps.

Before, the Office 365 apps used to be governed by MAM policies of Intune App Protection. Similarly, Citrix Secure Mobile apps such as Secure Mail and Secure Web would be governed by XenMobile MAM. Two MAM containers do not interfere with each other. However, this means that the policies governing both containers such as time out, passcode etc. are different for both, causing poor user experience. On the other hand, the DLP policies defined for Intune App Protection (that protects Office 365 apps) were not applied to Citrix apps and hence cut/copy/paste between Office 365 apps and Citrix Secure apps would not work.

Thus, Citrix decided to adopt Multi MAM container approach for its flagship apps: Secure Mail and ShareFile soon to be followed by Secure Web and Citrix Receiver. Now the mentioned Citrix apps will have one version of app on the app store which can be configured with either MAMs. Intune aware Secure apps will be referred to as “Enlightened apps”.

Now a customer can configure all the above-mentioned apps as part of the Intune App Protection container with the choice of MDM (XenMobile or Intune). This allows for a single set of app protection policies governing Office 365 apps as well as Citrix apps leading to heightened user experience. Moreover, the DLP controls of Cut/Copy/Paste also do not hamper transfer of data between Office 365 apps and Citrix XenMobile Apps as data is allowed to move within the same Intune App Protection container. Citrix XenMobile is the only mobility vendor which supports multiple containers allowing its apps to offer unparalleled security and seamless user experience.

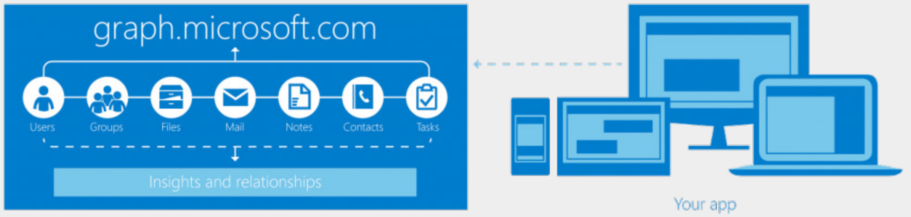
Sample use case: Copy content from a protected Microsoft word document and paste it successfully in Intune enlightened SecureMail. Try to paste the same content in Safari, Notes or any other app and it would fail due to app protection policies.

3. Native Integration of Citrix Cloud with EMS and Intune via Microsoft Graph APIs

Graph APIs are also leveraged by Intune as app protection policies for Intune App Protection container. Thus, any app using Graph APIs can be governed by the Intune App protections policies. The biggest benefit of using Graph APIs is that now Office 365 apps can also be configured with Data Loss Prevention (DLP) controls without having to login separately into Azure portal.

Graph.microsoft.com is a Microsoft API several years in the making that allows developers to integrate with broad cloud functionality across Azure, and Office 365. It enables IT to rapidly build solutions for employees, customize and harness Microsoft functionality in the cloud.

Graph API Overview: https://developer.microsoft.com/en-us/graph



4. Citrix Workspace Value-Add with advanced security and compliance

Citrix XenMobile Enterprise is a comprehensive Unified Endpoint Management (UEM) solution that that supports a variety of Mobile platforms including Windows 10, MacOS, and Chrome OS among others. Its capabilities are extended through integration with Citrix Workspace products including NetScaler, ShareFile, XenApp and XenDesktop.

MDM

XenMobile Mobile device management (MDM) protects data by leveraging device-level policies provided by the device manufacturer or platform provider. With the help of these policies, IT can configure, secure, and support mobile users. For example, IT can enable device-wide encryption and automatically lock or wipe a device. The XenMobile MDM solution supports a wide variety of mobile device policies and a variety of platforms.

XenMobile MDM supports XenMobile MAM and Intune App Protection. While both XenMobile MDM and Intune MDM are sound device management options XenMobile MDM can augment the value, Intune provides by adding:

- Automated Actions – react to events, user or device properties, or the existence of apps on user devices and establish the effect on the user's device based on triggers in the action. When an event is triggered a variety of actions may be triggered ranging from notifying administrations, to locking apps, to selectively wiping "corporate" apps and data to name a few.
- Security Features – XenMobile is FIPS compliant, provides several multi-factor authentication options Azure Active Directory, Client Certificates and Derived Credentials through integration with the Citrix market leading NetScaler appliance which includes built in DDOS protection, and is a focal point for Citrix Analytics to provide global contextual security.

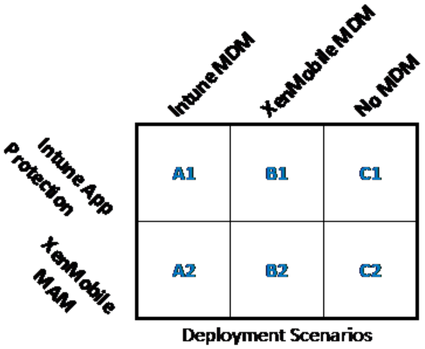
MAM

XenMobile provides mobile application management (MAM) options so organization can select the mobile app management strategy that's best suited to meet your security and privacy requirements. Protect application data either by leveraging device and platform security or by taking the XenMobile MAM-only approach, which requires no device enrollment. The XenMobile MAM-only approach is ideal for BYOD situations where user privacy prohibits the use of an MDM client or device enrollment and management.

Deployment models

Citrix XenMobile and Microsoft EMS can work together in a variety of ways, yet we're focusing on integration with Intune deployment models or scenarios. The diagram below lists possible mobility management scenarios with XenMobile and Intune. Choosing the right scenario will depending on several factors such as mobility requirements or current licensing investment. While each has merits the goal is to highlight the solution that provides "best of" what Citrix and Microsoft have to offer together.

We'll refer to the four key integration areas described in the XenMobile integration with Intune EMS overview as "XenMobile Value-Add."



	Intune MDM	XenMobile MDM	No MDM
Intune App Protection	A1	B1	C1
XenMobile MAM	A2	B2	C2

Deployment Scenarios

Citrix delivers powerful and differentiated MDM

For enterprises with high-security posture

Automated Action Framework

Triggers

- AD user disabled
- Location service disabled
- Device jail-broken
- Device unmanaged
- Available RAM
- Domain name
- Installed app name

Automated Actions

- Selective wipe
- Revoke device
- Send notification
- Etc.

Rich Compliance & Governance configurations

Config Restrictions

- Policy Scheduling
- Geo-fencing
- Location tracking
- Deployment Order and Rules

App Access

- Required, Forbidden, Suggested

MDM Enrollment and Auth

- **8 modes** – high security, url, url+pin, url+passwd, 2F, name+pin, name+pwd

Integration with Cisco ISE for MAC filtering for intranet vs guest access

App Install/Uninstall – app name

Additional Platforms

Today

- Samsung SAFE
- Windows Mobile CE

Roadmap

- Chrome
- Pi

(A1) Intune MDM + Intune App Protection + XenMobile value-add
This may be a popular scenario for existing Microsoft EMS customers that are utilizing Intune as MDM (Devices enrolled). XenMobile will provide value-add in several areas including enlightened ShareFile, SecureMail, Intune Browser with XenMobile SDK, NetScaler NAC, and the XenMobile integration with Intune EMS wizard to facilitate Intune configuration. Moreover, no reenrollment required. Adds value instantly.

(A2) Intune MDM + XenMobile MAM + XenMobile value-add
Not applicable.

(B1) XenMobile MDM + Intune App Protection + XenMobile value-add
This is the recommended deployment model which brings together all the benefits. It provides an excellent admin experience due to access to Microsoft Graph APIs within the same console. All Citrix apps are Intune Enlightened and hence may share data securely within a single container with DLP. It also includes all of the XenMobile value-adds and it provides an excellent user experience.

This model leverages comprehensive XenMobile UEM with Intune MAM for Office 365 apps as well as Secure Mail.
Note: No other UEM vendor can offer the above-mentioned capabilities of the B1 deployment model.

(B2) XenMobile MDM + XenMobile MAM
This is the full XenMobile Unified Endpoint Management solution and for existing XenMobile customers this would-be business as usual. XenMobile customer would be able to continue to use Office 365 alongside XenMobile MDM + MAM provisioned apps, but would not be a part of the same container and therefore not share in Intune App Protection.

This is a classic GRAPH API integration which other EMM vendors can also do.

Feature	XM MDM + XM MAM + Intune MAM (O365 only) Model B2	XM MDM + Intune MAM (throughout) Model B1	Intune MDM + Intune MAM + XM Value Add Model A1
MDM			
MDM capabilities for iOS, Android, Windows 10 and macOS	Yes	Yes	Yes
Support for Apple Device Enrollment program (DEP) and App volume purchase (VPP)	Yes	Yes	Yes
MAM Capabilities			
Seamless data transfer between Office 365 apps and Intune Enlightened Secure Mail	No	Yes	Yes
50 + MAM only policies for Citrix Secure apps and Citrix MDX wrapped apps	Yes	No	No
DLP controls for Word, Excel, PowerPoint and other Intune managed O365 apps	Yes	Yes	Yes
Micro-VPN per-app VPN (clientless SDK) to on premises resources	Yes	Yes	Yes
Managed Citrix apps: Secure Mail, Receiver, ShareFile, Secure Web	Yes	Yes	Yes
Citrix Workspace Benefits			
Single pane of glass for admins to manage complete Workspace apps and Data (Mobile, Web, Virtual)	Yes	Yes	No
Single pane of glass for end users (Mobile, Web and Virtual)	Yes	Yes	No
Integrated Workspace performance analytics	Yes	Yes	No
SSO onto Citrix Virtual apps and Desktops via Smart Access	Yes	Yes	No
Citrix UEM Platform Capabilities			
Flexibility to set Deployment Scheduling, deployment order and deployment rules	Yes	Yes	No
Support for Shared Devices	Yes	Yes	No
Support Location Tracking (without device Supervision)	Yes	Yes	No
Support for Derived Credentials for Device Enrollment	Yes	Yes	No
Invitation based MDM enrollment	Yes	Yes	No
App wrapping as a service in the cloud	Yes	Yes	No
Support for Chrome OS, Raspberry Pi and Things	Yes	Yes	No
Choice of automated actions for compliance violation	Yes	Yes	No

(C1) No MDM + Intune App Protection + XenMobile value-add
This model provides great value for Intune customers who find MM enrollment intrusive and use third party VPN solutions to access corporate resources behind the firewall. However, the downside of third party VPN solutions is that they increase the increase maintenance, can be inconsistent, require expensive infrastructure, licensing, and operational costs. Moreover, the device VPN solutions as well as per-app VPN solutions generally are not efficient for mobile devices and cause battery drain. On the other hand, Citrix propriety micro-VPN is clientless and is driven by NetScaler. Now Intune customers using Intune browsers (with or without Intune MDM) can leverage the Citrix micro-VPN to access Intranet resources.

No device enrollment or device level VPN required.
Note: No UEM, other than XenMobile, can claim to provide micro-VPN for Intune apps or Intune wrapped apps without MDM enrollment or use of legacy device VPN clients.

(C2) No MDM + XenMobile MAM
This is the traditional XenMobile solution for BYOD scenarios and for existing XenMobile customers this would-be business as usual. XenMobile MAM offers 70+ policies and is one of the most mature MAM container in the industry, yet Citrix recommends that our customers investigate platform MAM as well as Intune App Protection for standardization.

Comparison

Our endeavor is to provide flexibility to our customers and allow them to make the right decision. There is no one deployment model that's necessarily better than the others, rather a solution that best meets the needs of joint Citrix and Microsoft customers. The chart below provides a reference to compare key features offered by the different deployment models.

Conclusion

Citrix and Microsoft have once again announced several innovations together that provide flexible scenarios to security and delivery of apps and data. Choosing the right scenario will depend on customer needs, yet our common goal is to deliver a solution that will meet their requirements by providing the "best of" what Citrix and Microsoft can offer together.

About the Authors and Contributors

Amandeep Nagra is a Senior Product Marketing Manager specializing in Citrix Secure Digital Workspace.

Matthew Brooks is a Senior Technical Marketing Manager specializing in Citrix Secure Digital Workspace.

A special thanks to the reviewers of this Security Whitepaper:

- Alex Rubio
- Gene Schmidt
- Kevin Binder

Enterprise Sales
North America | 800-424-8749
Worldwide | +1 408-790-8000

Locations
Corporate Headquarters | 851 Cypress Creek Road Fort Lauderdale, FL 33309, United States
Silicon Valley | 4988 Great America Parkway Santa Clara, CA 95054, United States