Citrix XenMobile and Windows 10

With version 10, Windows has moved the once desktop operating system firmly into the era of the mobility and the cloud. Windows 10 is a wholly new unified operating system that brings desktop, mobile and cloud worlds together, not only in the user experience, but in enterprise endpoint management as well. With its XenMobile end user mobile management platform, Citrix does the same, allowing enterprises to manage all their employees' corporate, Bring Your Own Device (BYOD), Choose Your Own Device (CYOD) and Corporate Owned, Personally Enabled (COPE) Windows 10 devices—desktops, laptops, smart phones and tablets—from a single pane of glass.

A Single Unified Operating System

With Windows 10, Microsoft has leveraged its desktop and laptop heritage as an advantage by introducing a single operating system, development and management platform across all devices and applications.

For the first time, Windows 10 can run on any Windows 10 compatible device, whether it is a desktop system, laptop, tablet, smart phone or even Xbox. Microsoft is releasing Windows 10 Mobile for tablets and smart phones, but considers it an edition of Windows 10, rather than a separate OS, and has built all editions on a common architecture and a consistent user interface, with adaptations for smaller screens and touch screen interfaces when appropriate.

Windows 10 also includes the platform and concept of "universal apps," which allow the development of Windows Runtime apps that can be ported and rolled out to any type of Windows device in the enterprise, with minor changes in the codebase. The result will be applications, including Microsoft Office, that have almost identical functionality and very similar interfaces across devices. Windows 10 mobile devices won't be able to run Win32 desktop applications directly, however. Microsoft also provides software development kits for porting Apple iOS and Google Android apps to Windows 10.

Aside from the OS and unified application platform, Windows 10 also has a unified management layer across desktop, laptop and mobile devices, allowing all Windows 10 devices to be managed from a single enterprise mobility management (EMM) platform such as Citrix XenMobile. Windows 10 provides a unified set of mobile device management (MDM) API's, unified application storefronts for application distribution and user self service and will offer its upcoming Enterprise Data Protection feature set across all devices.

Mobile, Cloud Centric Management

Managing Windows desktops and laptops has always been an IT-datacenter-centric experience, requiring endpoint systems to be network connected and domain joined or touched by IT to receive updates, images and new operating system versions. Such a scenario is not well suited to an era of global roaming mobile workers and poses security risks when users are disconnected for several hours or days.

Running two separate management platforms for desktops/laptops and mobile device s is

inherently inefficient, resource intensive and prone to management and security policy conflicts. Organizations that are still running previous versions of Windows may want to keep their two separate management platforms to accommodate devices and users running those operating systems. However, with Windows 10 there is now the option of combining the management of all devices in a single management platform with common policies.

Aside from a single platform, however, Windows 10 management of mobile, desktop and laptop devices is now much more EMM centric and suited to a global, mobile, cloud oriented work environment than it was before. As with other EMM-oriented mobile platforms it includes the following capabilities:

Self Enrollment With Windows 10 EMM, users can now self enroll any new device, including desktops and laptops and any COPE, BYOD, and CYOD devices quickly and easily without any IT involvement. The new version allows the use of Azure Active Directory, which means enrollment can be cloud based, rather than requiring a network connection to an enterprise datacenter, and can be done over any public or private wired or wireless network.

Windows 10 also offers an alternative IT mass rollout option with settings preconfigured.

Unified Application Stores Similar to iOS and Android, Windows 10 now offers Web based app stores. These include Microsoft's Windows Store, a public repository for Microsoft and third-party vendor applications for all Windows 10 devices, and Windows Store for Business, the enterprise managed application repository for in-house and custom applications. IT can use the Windows Store for Business to provision users with applications and users can download and install their approved enterprise apps without help from IT. The Windows Store for Business includes bulk purchase and application metering and reclamation capabilities as well.

Even Win 32 applications can now be managed via the app store. A unified application catalog allows IT to distribute applications from any location, including the cloud and VDI. Users can access the catalog in a self service scenario and browse, search and install available applications based on their Active Directory user and group rights.

Continuous Updates Microsoft calls Windows 10 the last version of Windows. From now on Windows 10 will have a service orientation, with regular updates and feature improvements, rather than major releases. Microsoft will distribute continuous updates to ensure users have all the latest features and security fixes. IT can use Microsoft Update or a local Windows Services Update Server to distribute updates and choose among three different update scenarios:

- **Current Branch** is consumer focused and packages new features together with updates, rather than as service packs and new releases.
- **Current Branch for Business**, BYOD -focused option that delivers critical updates and new features separately at different times, allowing IT to test new features before deployment.
- **Long Term Servicing Branch**, for more mission critical applications, allowing new features to be packaged together and deployed at specific times chosen by the organization.

Single Sign-on Azure Active Directory will let organizations connect on premises with cloud based resources and allow users not only to self provision their devices but to have single signon across in-house and SaaS applications, including Microsoft Office 365.

Security

Organizations continue to wrestle with security threats and breaches and the security and compliance issues that come with a BYOD, CYOD, or COPE environment. Windows 10 comes with a hefty supply of new EMM style security features to protect enterprise information and applications in these environments. They include:

Multifactor Authentication Windows Hello is a feature that allows multiple methods of user authentication to the device, including pictures, gestures and biometrics (such as fingerprint, facial and retinal scans when

3D infrared cameras or fingerprint readers are available on the device), sometimes in addition to a PIN. All Windows Hello data is stored and encrypted locally on the device. Once a user is authenticated to the device, Microsoft Passport uses a public/private key pair to let users authenticate securely to and access compatible applications, Web sites and networks without a password. Multiple users can use one device via Windows Hello.

Device Guard is a threat protection feature that can supplement or even replace traditional endpoint protection solutions. It uses a combination of hardware and software to lock down a device so it can only run trusted applications and/or code signed by trusted signers—such as specific software vendors, the Windows Store, or your own organization—as defined by your Code Integrity policy. It's an effective way to protect against zero day attacks and other threats that traditional malware protection solutions often miss. Device Guard can use both hardware technology and virtualization to isolate the Device Guard mechanism from the rest of the operating system.

Secure Boot protects devices from malware that loads during the boot process. With Secure Boot the UEFI firmware checks the cryptographic signature of any program attempting to load before the OS, including the OS bootloader. In Windows 10, Secure Boot can be turned off on a desktop but not a mobile device.

Health Attestation then uses a Health Attestation module to communicate measured boot data to a trusted remote cloud service. The Health Attestation remote service performs checks on the measurements and conveys the device boot integrity and health securely back to the device. An MDM solution can use this information to determine if a device is compromised in some way, and pass the information to an identity provider to allow or refuse access to sensitive content.

100 plus new policies for application white and black listing, open in settings, copy and paste and other restrictions.

Per app VPN's that allow individual apps to connect to enterprise and other data securely over the air or the wire.

Enterprise Data Protection, (EDP) is currently in testing and will be released for broader testing at a later date. Its features will be built into the operating system and administered through an EMM solution such as XenMobile.

EDP will be the mechanism that protects enterprise applications and data in a BYOD, CYOD or COPE environment, where they share or can be accessed by devices that hold personal and potentially harmful user applications and associated data.

EDP allows IT to identify enterprise apps and data and implement policies that regulate exactly how the data can be shared. It then follows and protects enterprise data via containerization, data encryption, and sophisticated data loss prevention. It also enables enterprise data wiping on remote mobile devices without any impact on personal data and ca n produce tracking and audit reports of app and data usage.

Unlike other mobile platforms, Windows 10 EDP achieves containerization without forcing the user to switch manually between enterprise and personal environments and credentials on the device. Instead, both personal and business apps are displayed on the same screen and can be accessed at any time.

IT simply creates a list of enterprise resources, including IP addresses, domains and email accounts. Any data originating from these resources is recognized as business data and encrypted in transit and at rest in a secure virtual container. IT can also create a list of authorized enterprise applications that have permission to access certain business files and data and apply a host of policies around copying, cutting and pasting sensitive data or files into other applications, posting images on social media and other related actions. Unauthorized actions can be blocked or simply tracked and audited with a warning sent to the user.

EDP also introduces the concept of Enlightened apps, which can access and recognize both enterprise and personal data and containerize and protect enterprise data automatically. For example, Outlook can be configured with both a personal and business email address and separate emails in two separate inboxes, applying enterprise policies to enterprise email only.

When it is complete, Windows 10 management and security will be formidable competitors with similar features on other mobile platforms.

Citrix XenMobile

Citrix XenMobile is a full featured enterprise mobility management (EMM) solution that allows IT to discover, secure, apply policies to and manage all its users' devices running Apple iOS, Windows Mobile, Windows 10 or Google Android. Not only does XenMobile provide comprehensive classic mobile device management (MDM) capabilities, such as device discovery, lifecycle management, policy enforcement, user self enrollment, and remote device lock and wipe. It also includes full encryption, application wrapping, containerization and data security features for Apple iOS, Google Android and Windows Mobile that allow users to mix enterprise applications and data with their personal applications and data safely, without risk of enterprise malware infections or data breaches.

Citrix XenMobile's Worx Home is the launching pad that empowers Apple iOS, Google Android and Windows Mobile users with secure enterprise class email, Web browsing and file sharing mobile apps. Worx Home also includes ShareFile, a secure, enterprise-class, fully managed file sharing and collaboration alternative to consumer file sharing solutions such as DropBox and Box, providing users with secure access to all their files from any device.

Through XenMobile and Citrix XenApp or XenDesktop integration, users can access their XenApp and XenDesktop apps and thus their Windows desktops within the Worx Home interface, without having to log in separately.

With Citrix XenMobile users can combine corporate and personal lifestyles easily, without burdensome restrictions, while corporate IT can track and secure all the mobile devices, business applications and business application data.

XenMobile Windows 10 Support Today

Today, XenMobile Windows 10 support includes the following:

Enrollment of Windows 10 smart phones, tablets, notebooks and desktops, including user self enrollment via Azure Active Directory, with autodiscovery of the appropriate XenMobile MDM server after the user types in an enterprise email address. Azure AD enables a cloud based MDM server enrollment. Upon enrollment, the XenMobile MDM server can apply policies, push out applications and settings to the device and check device compliance with enterprise security rules.

Worx Home with Worx Mail, Worx Web and other Worx Apps are currently available for Windows 10 phones only. Today, only Citrix Worx applications are wrapped and containerized on a Windows 10 phone. Other Worx-enabled apps from third party vendors or developed internally are not yet supported for Windows 10.

Microsoft Office 365 can be deployed today across Windows 10 devices via the XenMobile Enterprise Store, along with a complete set of Worx-related security policies, such as Office 365 per app VPNs and XenMobile FIPS 140-2 compliant AES 256-bit encryption of Office 365 data at rest. Organizations can also apply XenMobile application wrapping and containerization features, cloud backup, "open in" file restrictions, geo-location and numerous other security policies across Office 365 apps and files. Users can open Worx mail file attachments and ShareFile documents in Office 365.

Exchange Activesync and S/MIME support provides users with access to enterprise email and to push certificates, including SCEP certificate distribution, and WiFi, VPN, configuration settings, to the device. Third-party VPN plug-ins can be applied to support

per-app VPN's. XenMobile can act as the SCEP server and gateway.

Health Attestation to retrieve security information about each device, including boot process, Bitlocker and Secure Boot enablement and other relevant security information that helps IT determine if the operating system has been compromised, jailbroken or otherwise tampered with. Policies can then be applied if the device is not compliant, including wiping the device, sending notifications to the user, labeling the device as noncompliant, or sending emails to administrators.

XML scripts to deploy additional policies, such as disabling phone cameras, launching and locking applications on startup, and support for features such as Windows Hello.

Remote Lock and Wipe of enterprise applications and data in the event of device loss and theft.

Future XenMobile Windows 10 Support

Application Distribution will be supported when XenMobile provides support for Microsoft Business Store portal.

Worx apps, Windows Business Store, and Enterprise Data Protection when it becomes available from Microsoft) will be supported on all Windows 10 devices in the near future, as will Long Term Servicing Branch updates.

Containerization will be offered across all third-party Worx Apps on all devices when Windows 10 EDP is available and supported by XenMobile.

Summary

Windows 10 will certainly accelerate the shift towards Unified Endpoint Management by Enterprise Management Solutions including XenMobile to manage any device (desktop, laptop, smartphone, tablet) and any platform (including iOS and Android). The ability to reference any device from a single location saves significant IT resources that can be used for more strategic purposes. Be sure to watch for additional Windows 10 management and security features supported by XenMobile.

CITRIX®

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