Unified Endpoint Management

Security and Productivity for the Mobile Enterprise

The workplace has evolved from stationary employees working on IT distributed Windows work desktops and laptops to mobile users playing and working on personal roaming laptops, tablets and smart phones. Ten years ago client management tools (CMT) such as Microsoft SCCM and LANDESK were the enterprise choice for managing scores, hundreds or thousands of IT distributed Windows systems. In an era of mobility, BYOD and the Internet of Things (IoT), however, client management tools (CMT) must evolve.

Instead, for a growing number of IT organizations, the future lies in Unified Endpoint Management (UEM), which combines CMT with EMM (Enterprise Mobility Management) providing a single pane of glass to manage and secure, devices and operating systems, whether laptops, smart phones, tablets or any other device. Increasingly, UEM means EMM, with the user, rather than the individual device as the management focus. For users, UEM helps enable a single unified workspace with easy, consistent collaboration and information access from any device.

In the next few years, many analysts believe that organizations will employ EMM systems to manage PC's and Macs. This means that EMM has the potential to manage and secure more than one billion Windows 10 devices over the next several years as more and more organizations make the transition to the new OS. Organizations moving into a more mobile, global era should consider seriously whether a partial or total transition from separate CMT and EMM platforms to a single UEM tool such as Citrix XenMobile makes sense for them.

In the next few years, organizations will also need to extend unified management solutions to cover the emerging enterprise Internet of Things (IoT), including sensors, beacons and other similar devices. Luckily, EMM solutions such as Citrix XenMobile have been moving forward to encompass IoT devices as well.

Why EMM

There are many reasons why UEM via EMM makes sense for a lot of organizations.

Symplicity CMT and EMM tools have significantly different ways of working, and, for many organizations, require a separate set of staff and training for each. It's a no brainer that managing all devices from a single pane of glass makes more logical business sense. Not only is it less expensive to invest in a single management tool than two or three but

This means that EMM has the potential to manage and secure more than one billion Windows 10 devices over the next several years as more and more organizations make the transition to the new OS.

significant operational savings can come in reduced staff resources and training, allowing organizations to leverage existing staff for more strategic purposes.

Consistency in management, security and usability is important for enterprise user productivity and information protection. Even small unintended differences in security and management policies among devices, applications and information can expose holes in the security infrastructure that allow hackers and malware to penetrate the organization. Consistency in mobile access to applications and information is also important for user productivity. UEM offers consistency in several ways:

•It's inherently easier to implement a single set of enterprise management and security policies across all devices and users with a single UEM solution than with two separate sets of tools.

•User helpdesk services and system troubleshooting are more consistent with a single management platform, and with operating systems, such as Windows 10, that are themselves have more consistent interfaces across different types of devices.

•Reporting is obviously easier and more comprehensive with a single platform, which can be useful when planning and calculating the costs of hardware and software upgrades or refreshes.

•Windows 10 introduces its own consistency with a common operating system, application development tools and set of API's across desktop and mobile devices. Users can get all their devices' applications from a single secure, corporate approved app store and work with enterprise applications and information both on their devices and the corporate network in a much more consistent way.

•Microsoft recently announced the Centennial App Converter, which will convert even legacy Win32 apps into the Universal Windows Platform apps, so organizations can add them to the Windows app store, where they can be administered by an EMM solution such as XenMobile.

Mobile Friendly Management Conceived at a time when devices were stationary, corporate distributed, and mostly connected to the enterprise LAN, CMT tools required desktops and laptops to be LAN connected and joined to an enterprise domain with a set of group policy objects for initial configuration and subsequent management to take place. A user could not typically connect, configure and upgrade his or her own device. This was the job of IT, which acted as the ultimate super user.

With legacy CMT solutions, IT spends a lot of time creating one or a few sets of custom system images and pushing them over the LAN to a few, scores, or hundreds of network connected desktops and laptops, or uses an image deployment service for up to $25 per system. With such a methodology, bringing a new device on board or replacing a lost or stolen laptop with all the requisite applications are resource and time consuming processes that hamper user productivity. CMT application distribution is also IT centric, requiring complex distribution packages.

By contrast, EMM API's and tools such as Citrix XenMobile were designed from day one to support roaming, wirelessly connected mobile users on their chosen devices. Users can acquire a device with the vendor configured operating system and applications and use an enterprise EMM portal and configuration app to enroll and configure their device themselves over the air according to corporate settings and policies --all with little to no IT touch or help.

Users can also use a corporate app store portal to download and install IT preapproved applications. Cloud SaaS and virtual applications have become much more prevalent in the enterprise, so in many cases applications don't have to be downloaded at all. If necessary, IT can still push out applications and updates to hundreds of globally roaming devices.

OS and applications updates were much less frequent a few years ago and very time and resource intensive and LAN dependent. Mobile operating systems today tend to run on a cloud service model with much smaller, more frequent updates, which makes a lot more sense for the roaming mobile user.

Containerization One of the ways EMM and mobile OS API's enable BYOD and corporate owned, personally enabled (COPE) workstyles is through containerization. Using application wrapping, encryption and other similar methods, IT can separate corporate and personal applications and data on the device such that interactions among them are disabled or restricted according to enterprise security policies.

Containerization accomplishes both malware protection and Data Leakage Prevention (DLP). Since enterprise and personal applications and data on the device are walled off from each other, any malware downloaded with personal applications or browsing has no impact on containerized enterprise applications and cannot be transmitted to the enterprise network when the device connects. Most EMM solutions such as XenMobile enforce this separation as well with per app virtual private network (VPN) connections activated automatically when certain enterprise applications connect to the corporate LAN. Per app VPN's connect a single application, rather than the entire device, shutting out any malware from personal application use.

Similarly, most operating system API's and EMM systems allow IT to configure and enforce a number of policies that regulate users' ability to cut and paste data from enterprise to personal applications, paste or attach enterprise data or files to personal email messages, and print files containing sensitive data.

With Windows 10 laptops, desktops and EMM, containerization can be accomplished via digital rights management through the enforcement of Bitlocker encryption of all enterprise applications and data. IT can then leverage policies that prevent users from cutting and pasting encrypted content into unmanaged applications not using BitLocker encryption, including personal email client software. Any data downloaded from services such as SharePoint or a shared network are also encrypted. Thanks to Centennial, containerization can be accomplished with legacy Win32 applications as well.

Windows 10 delivers many other critical enterprise management features IT needs across devices. IT can push down and enforce a raft of policies and settings, enforce password and encryption, enable self-enrollment of new devices through Azure Active Directory or a third party EMM solution, manage corporate provisioned apps separately from user installed apps, distribute Windows 32 apps via .msi packages, enforce and deploy updates, and prevent access to dangerous Web sites, all without having to touch the device connecting it to the enterprise LAN. Any Win32 application that can't be leveraged this way can be deployed to mobile devices via desktop virtualization using solutions such as Citrix XenApp and Xen Desktop. While the full breadth of management features may not equal those offered by CMT, the most critical and widely used management capabilities are there and will continue to evolve.

Windows 10 Redstone 1 update added new management features and more will be added with Redstone 2, due for Spring 2017.

With OS X Lion, Apple also started giving the desktop operating system most of the same policy based, self-enrollment management API's as iOS and more will come with macOS Sierra.

The Citrix UEM Solution

Citrix is the only EMM provider with a full, integrated UEM suite that includes Citrix XenMobile for UEM across all iOS, Google Android and Windows 10 devices, including desktops and notebooks. Citrix also offers XenApp and Xen Desktop for Windows desktop and application virtualization; a full IoT integration, automation and messaging platform via its Octoblu acquisition; and Podio, a powerful and highly flexible Web based platform for organizing mobile collaboration and business processes across globally dispersed teams.

Citrix XenMobile is providing increasing support for all operating system enterprise management API's as they are introduced and adds its own unique capabilities that deliver management consistency across device operating systems. These include full FIPS 140-2 compliant AES 256-bit encryption, its own MDX containerization features on top of those offered by operating system API's and its own toolkit and SDK for wrapping individual applications with the policies and containerization strategies necessary to protect their associated sensitive information. This is important as XenMobile provides a seamless, productive experience for the user at the same time as it provides consistent, necessary protections for the enterprise.

XenMobile also offers its own mobile enterprise level Secure applications, such as Secure Mail and Secure Web, across iOS, Android and Windows 10 mobile and desktop systems and devices.

Secure Mail is an enterprise email client and personal information manager with a user friendly interface much like those of device native email client solutions, but with scores of additional features that enhance security and usability in an enterprise setting.

With Secure Mail, all corporate email, contacts, and calendar items are stored completely separate from the personal applications on the device. Secure Mail can be accessed via single sign-on after the user logs into Secure Hub, and offers multifactor authentication, remote wipe, and encryption in transit and at rest. IT can also enforce restrictions on email attachments, and printing and cutting and pasting of information from other applications into emails.

Secure Mail integrates with organizations' existing data leakage prevention (DLP) tools, which monitor and restrict content sent out in enterprise emails. Secure Mail also offers outstanding convenience features, such as viewing availability of meeting invitees, including online meetings and phone conference links in new meeting invitations and joining online meetings via a single touch.

Secure Mail integrates tightly with XenMobile's Secure Web mobile app, so that all email Web links are opened in a secure, sandboxed web browser environment. Secure Mail also integrates tightly with Citrix's own ShareFile file sharing application, which is discussed below, so that ShareFile links rather than file attachments can be embedded in emails for tighter control over content sharing.

Secure Web is a secure browser alternative that IT can use to place policies and restrictions on Web browsing, particularly when connecting to the corporate network and intranet. Organizations can apply policies that govern which websites users can and cannot access, what enterprise firewall proxies are used to access them, and can analyze and filter URL's to ensure they're safe.

ShareFile is XenMobile's enterprise-class secure mobile file sync and share application, which provides the same or better features and convenience than consumer friendly Box and DropBox, but with enterprise-level security and management. Rather than forcing users to store all information in the cloud, organizations can leverage ShareFile Storage Zones to store shared files either on-premises behind the firewall, 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.

Secure Forms is Citrix's easy-to-use full-featured drag and drop solution that novices can use to create, populate and store mobile forms-based applications running on a variety of devices. Secure Forms helps organizations digitize and automate manual workflows and processes rapidly and eliminate double data entry and paperwork in the field. And perhaps most important, Secure Forms leverages

With Windows 10 and macOS Sierra, Enterprise Mobility Management Solutions can deliver a single Unified Endpoint Management capability for all mobile users, devices and applications.

all the powerful security and management features of Citrix XenMobile to protect and secure enterprise data and integrates seamlessly with other XenMobile functions and productivity applications.

Finally, organizations can use Secure Hub (the XenMobile enterprise app) to provide access to Secure apps, other mobile apps (either commercial third-party or enterprise developed), Web and SaaS services, and even Windows desktops and applications based on Active Directory group policies.

Octoblu Citrix is unique in offering an integrated IoT automation, monitoring and analysis tool named Octoblu. With Octoblu, Citrix extends mobility management to the emerging IoT enabled workplace where context-aware environments synthesize data from many different sources to respond to the needs of the user, increasing workplace efficiency and productivity. Octoblu software can be used to create workplace automation services such as launching a personalized desktop when a user approaches a workstation; adjusting heating, cooling and lighting and starting GoToMeeting or Skype for Business meeting when staff enters a conference room; and using beacons to connect user automatically to nearby printers. The IoT possibilities are limitless.

Podio adds a powerful, free enterprise cloud based mobile collaboration platform combining team conversations, processes and content sharing and integrates tightly with Citrix XenMobile security and management. Podio provides equivalent or better collaboration capabilities than enterprise solutions costing tens of thousands of dollars.

With Windows 10 and macOS Sierra, Enterprise Mobility Management Solutions can deliver a single Unified Endpoint Management capability for all mobile users, devices and applications. Enterprises should examine these solutions closely to see if UEM can not only simplify and slash the cost of managing, securing and simplifying the mobile workplace, but take the mobile enterprise into the era of IoT. Only Citrix offers a complete UEM solution that includes integrated management, security, application and desktop virtualization, mobile collaboration and enterprise IoT enablement. With Citrix solutions, the enterprise can realize the dream of the single integrated mobile workspace.

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