Securing the mobile enterprise
One of the biggest transitions taking place in IT today is the move from corporate-issued laptops and BlackBerry smartphones to bring-your-own-device (BYOD) programs that let employees use their personal devices, such as iPhones, iPads, MacBook notebooks and Android devices, for work tasks. Increasingly, users are even discarding laptops and taking only their smartphones or tablets with them.

BYOD offers many productivity and employee satisfaction benefits. Younger employees and executives increasingly expect to use the mobile hardware and software they feel works best for them, which leads to increased user satisfaction and productivity. Any organization that hopes to attract the best of the current generation should think seriously about bring your own – not just devices but also applications and cloud-based services.

A BYOD strategy also contributes to customer satisfaction, as employees with 24-hour mobile access to enterprise applications can stay up-to-date with customer and product information, handle customer issues promptly and contribute to quick decision making in the enterprise, whether they’re at work, at home or on the road.

However, BYOD also presents significant challenges, perhaps the most significant of which is security. Enterprises that open their gates to personal devices and applications must find ways to protect the organization from:

- Unknown or “rogue” mobile devices connecting to the corporate network and gaining access to sensitive enterprise information
- Malware spread by mobile applications and websites that infect the enterprise network
- Personal mobile applications that gain access to corporate content such as contacts, business applications and data.
- Hackers that take advantage of unprotected mobile devices and applications to gain entry to the network and steal sensitive information
- Unprotected public WiFi networks used to transmit sensitive enterprise information
- Leakage of sensitive enterprise information via personal or enterprise mobile email and social networking sites
- Information theft from stolen or lost mobile devices

Securing mobile devices and their connections from these threats requires a comprehensive enterprise mobile management (EMM) strategy employing a raft of powerful tools, including mobile device management (MDM), mobile application management (MAM), secure file-sharing and mobile data loss prevention (DLP) solutions.
• MDM tools allow IT teams to discover, track and manage mobile devices and applications throughout their life cycles, much as they do with corporate issued devices.

• MAM solutions create a barrier between personal and corporate applications and data so the latter are protected from the vulnerabilities and hazards of the former.

• Secure file-sharing solutions let users access and collaborate on the latest versions of their most important files, much like Dropbox and other consumer file-sharing services, but ensure that sensitive enterprise information is not compromised.

• DLP solutions prevent users from divulging sensitive enterprise information to the wrong people, either intentionally or unintentionally.

Below we list the steps for organizations to take in securing mobile devices, apps and data for creating a secure, mobile workforce.

**Step 1: MDM**

Perhaps the best-known BYOD challenges relate to mobile device management. To keep enterprise networks, applications and data secure, IT must know what devices its employees are using and be able to manage and monitor them throughout their lifecycle. The primary tools used for these purposes are enterprise MDM solutions. The most powerful, effective MDM packages provide the following essential features:

• Automated discovery, tracking and monitoring of all user mobile devices connecting to the enterprise network, including Windows and Macintosh laptops, iPad and Android tablets and smartphones. Tracking hundreds or thousands of devices is essential, as each user may have three or more.

• Fine-grained, role-based management of users and devices based on enterprise management and security policies

• Centralized management and enforcement of device passwords, locking down potential device security hazards such as cameras, GPS or printing capability and encryption of the device where available

• User self-enrollment. To optimize productivity, enrollment of devices in the MDM platform should be quick, enabling people to access email and enterprise applications as soon as possible. Once roles, rights and policies have been assigned, better MDM solutions let users self-enroll new devices and gain access in minutes while keeping the enterprise protected.

• Centralized provisioning and distribution of required enterprise mobile applications, configuration settings, policies and application updates.

• An enterprise-approved unified app store, similar to Apple’s iTunes, offering additional applications. As today’s mobile users leave Windows-based laptops at home, enterprise app stores should also provide all devices with access to Windows applications, as well as any cloud and SaaS services approved for users.
• Whitelisting of applications determined by IT to be safe and compliant and blacklisting of those deemed unsafe

• Jailbreak detection for IOS devices and rooting detection for Android devices. Jailbreaking allows users to gain administrator privileges and use unauthorized applications, services and functions such as WiFi tethering, which uses the phone as a WiFi hotspot.

• Geolocation capabilities that allow IT to find devices that have been lost or stolen and detect their use outside a permitted area, such as a school or hospital campus, against organizational policies

• Remote locking of devices and remote wipe to remove all sensitive corporate data and applications in the event the device is lost or stolen or the user leaves the company. Automated un-enrollment should also be provided so users can no longer connect to corporate networks, applications and data after they move on.

**Step 2: Secure access**

The next step after management is providing secure mobile access to enterprise applications and data, particularly email, contacts and calendars.

Any EMM strategy must include secure, remote mobile access with robust enterprise identity management, authentication and authorization, and granular application and data access controls. Some email access solutions require IT to place components in the enterprise DMZ. A more secure strategy places all backend components behind the corporate firewall.

To prevent snooping over unsecured connections, all data transmissions between mobile devices and the enterprise network should be secured via a virtual private network (VPN) connection with robust data encryption. A VPN used to be an open connection from the device to the corporate network, but a more recent and secure strategy is to assign micro VPNs to individual applications so when a user launches an application it is immediately VPN enabled without enabling the entire device. Each micro VPN is unique to a specific application, protecting it from any other device or micro VPN communication. Micro VPNs also offer data optimization via compression so performance is enhanced while actual transmission of sensitive data is minimized. Any connections to enterprise cloud services, including SaaS applications, should be VPN enabled and encrypted as well.

Finally, it’s important to be able to verify centrally that each device connecting to the network has the latest versions of required security features every time it connects, a feature called network access control (NAC).

**Step 3: MAM**

Until recently, most management and security strategies focused exclusively on MDM. However, MDM is only a first step towards mobile security. BYOD has gone beyond devices to encompass applications, data and services that users choose for both personal and enterprise use. As people increasingly mix work with pleasure, the number of applications and services to manage and the strong demands
for personal freedom make it difficult for IT to limit users to just a few approved applications. Instead, IT has sought ways to provide maximum application choice while protecting corporate applications and data on personal devices from security hazards, a concept known as mobile application management.

Most MAM solutions use a technique known as containerization to put a virtual fence around the enterprise applications and data on the device, preventing personal applications from interacting with them and vice versa. MAM solutions can also implement policies that prevent users from cutting and pasting sensitive enterprise information into personal applications such as personal email, as well as attaching documents and opening attachments in unapproved applications. Many MAM solutions also offer the ability to configure authentication for individual enterprise applications such as Microsoft Exchange or SharePoint via passwords or more-secure two-factor authentication using tokens, smart cards or device certificate validation. Application wrapping and sandboxing are other terms used for containerization.

Ideally, mobile security solutions should provide prepackaged, sandboxed applications, strategies for sandboxing existing enterprise applications and tools for wrapping third-party applications with sandboxing capabilities according to corporate policy.

The most obvious candidates for wrapping are enterprise email/calendar/contacts software. Containerization allows enterprises to provide corporate email access while preventing leakage of sensitive information. Sandboxed web browsers protect the enterprise from websites that contain malware or are vulnerable to hackers.

Another form of containerization encrypts all enterprise data stored on the device, in addition to data sent over the wireless connection.

**Step 4: Windows application access**

Even as mobile users shed their Windows laptops, they still need access to enterprise Windows applications to create enterprise content and do business. There are several strategies for providing mobile devices with access to these applications, including developing new mobile applications with equivalent capabilities, porting Windows applications to mobile operating systems and providing web-based or virtual access.

**Step 5: Secure file sharing**

Another data leakage concern comes from the increasing use of mobile file-sharing services such as Dropbox, Box and Google Drive. Users take advantage of these services to store and provide access to their most recent business files for work and collaboration on the go. Unfortunately, these services were conceived with consumers in mind and are only now starting to catch up to enterprise-level safeguards such as encryption, policy control and containerization.

That’s why the best enterprise mobile security and management solutions provide enterprise-ready alternatives to consumer file-sharing services. They offer the same mobile and collaborative capabilities but add safeguards for encrypting data.
in transit and at rest, applying corporate information access and sharing policies and decommissioning access when users change leave the organization. Rather than storing the information in a public cloud, most enterprise file-sharing solutions store it behind the corporate firewall.

The Citrix solution

Citrix is the only vendor with an EMM solution that combines all of the elements described above, providing a one-stop solution to meet every mobile management and security need.

Citrix XenMobile MDM Edition discovers, tracks, provisions and manages all mobile devices—including Windows, Macintosh, iOS and Android devices—throughout their lifecycles. IT can configure management servers and users via an intuitive, web-based administrative console and import Active Directory user groups and accounts for user- and role-based management. XenMobile MDM Edition can also make requests to a certificate authority for secure, certificate-based authentication via WiFi, VPN and Exchange ActiveSync profiles.

Users can self-enroll their devices with IT-provisioned policies and applications and download and deploy any or all IT sanctioned mobile, SaaS and Windows applications from a unified corporate app store. XenMobile MDM Edition also offers mobile application blacklisting and whitelisting; detection and blocking of jailbroken devices for compliance purposes; and full or selective remote wipe of data and applications and data, depending on the capabilities of the mobile operating system.

XenMobile MDM Edition gives IT tight control across the entire device lifecycle, including:

- **Configuring** device settings and policies, such as device and application restrictions
- **Provisioning** devices via self-service device enrollment and centralized distribution of configuration, policy and application packages
- **Securing** devices, connections, applications, the network and data with multiple authentication and access policies, application and cloud service blacklisting and whitelisting, enforcement of secure application VPN tunneling and deployment of content- and context-aware mobile data loss prevention policies. Citrix offers one of the only solutions that provides automated per-app micro VPNs to ensure that all required connections are secure without exposing the network to the entire device with each connection. Two-factor authentication is also available for individual enterprise applications via tokens or client certificate validation.
- **Monitoring** devices, infrastructure, service and telecom expenses
- **Supporting** users by remotely locating, locking, geo-fencing, and wiping devices in the event of loss or theft. XenMobile MDM Edition is also one of the few solutions to provide IT with remote user device control and troubleshooting tools.
- **Decommissioning** devices by identifying those that are inactive and wiping or selectively wiping them upon employee departure. With selective wipe, the corporate profile and all associated applications, including email, are removed without affecting the user’s personal applications and information.
In addition to traditional MDM capabilities, the Citrix solution secures mobile devices, applications and users with robust MAM capabilities.

Citrix provides its own sandboxed client applications for web browsing and accessing and synchronizing with enterprise email, calendars and contacts. Called Citrix WorxWeb and Citrix WorxMail, the applications offer a rich user experience equivalent to the device’s native applications but with extensive enterprise visibility and policy creation and enforcement. With WorxMail, all enterprise email, contacts and calendar items are stored in a container separate from personal applications and information and are inaccessible to them. IT can enforce policies that encrypt all email and attachments and prevent users from opening, editing and saving email attachments in unapproved applications; forwarding sensitive information; or cutting and pasting information into other documents or emails.

WorxMail and WorxWeb are tightly integrated so that all web links contained in emails are opened in a secure browser environment. Organizations are not required to take advantage of Worx applications as part of the XenMobile solution. If IT deems it safe, users can employ native versions of these applications, or even use Outlook Web Access. IT can require encryption of all email attachments.

Aside from WorxMail and WorxWeb, Citrix provides a Worx SDK that can add sandboxing and enterprise policies to any enterprise mobile application in as little as a single line of code, either during or after development. The Worx App Gallery also provides scores of useful user mobile applications that have already been Worx enabled by third parties.

Secure file sharing is provided by Citrix ShareFile, a secure, managed enterprise alternative to Dropbox, Box, Google Drive and other consumer-oriented file-sharing services. ShareFile encrypts all user documents in transit and at rest. IT can exert tight control with granular policies, similar to those of WorxMail, to prevent leakage of sensitive enterprise information and access to sensitive files in the event a device is stolen or a user leaves the organization or changes roles.

ShareFile integrates tightly with WorxMail, allowing IT to define policies that limit the size of email attachments. If an attachment exceeds the size limit, the email message automatically provides ShareFile links instead. Alternatively, policies can be configured that prevent attachments completely in favor of ShareFile links.

Secure access to Windows applications and other enterprise applications can be provided using Citrix XenApp and Citrix XenDesktop, the company’s seasoned, market-leading virtualization solutions. Users can access applications hosted on datacenter servers or XenApp and XenDesktop can stream the application interface to any mobile device and hold it locally in a secure, encrypted file system with strict enterprise policy enforcement. Administrators can configure streaming to provide several hours of offline application access so users can be productive without an Internet connection.

Citrix Receiver provides a set of tools for adjusting the user experience to match the device, display and operating system and can even provide mobile features such as touch and pinch and zoom.
In addition to these functions, Citrix offers NetScaler Gateway to provide mobile users with fast, secure access to web-based and virtual applications. NetScaler Gateway can create encrypted SSL connections to the network, as well as application-specific encrypted micro VPNs when necessary, and can enable two-factor authentication via tokens or certificate validation for individual enterprise applications such as Exchange and SharePoint.

Citrix NetScaler application delivery controller (ADC) is a powerful application load balancer that maintains reliable, high performance for web-based applications, even during peak use periods, ensuring a positive user experience rather than the frustratingly slow or uneven performance that sometimes characterizes these applications.

Thanks to partnerships and integration with Aruba ClearPass and Cisco Identity Services Engine, NetScaler can also incorporate capabilities for fine-grained network access control and self-enrollment of guests and partner employee devices with granular enterprise policy enforcement. Cisco and Aruba solutions can analyze guest and partner devices to ensure they have required endpoint security functions and the latest updates before they connect.

Another native advantage of NetScaler is its robust application-level firewall, which protects the enterprise from evolving and sophisticated application-level attacks and permits deployment of all web components behind the firewall, rather than in the less-secure enterprise DMZ.

**Conclusion**

The mobile enterprise faces unprecedented challenges as users’ personal and work lives continue to blend. Only a comprehensive, centrally managed EMM strategy and toolset can meet all these challenges without leaving the enterprise vulnerable to malware, hacking and information theft. Citrix is the only mobile management vendor that provides a one-stop solution to every security challenge of BYOD, balancing user freedom and satisfaction with stringent enterprise management, compliance and security requirements.

For more technical details on the full breadth of Citrix mobile security features, read the XenMobile Security Whitepaper on www.citrix.com/xenmobile.