Delivering enterprise information securely on Android, Apple iOS and Microsoft Windows tablets and smartphones

A technical how-to guide—updated for Android 4.4, iOS 7.1, and Windows Phone and Surface 8.1.

CITRIX®

Android, iOS and Windows-based mobile devices—including smartphones, tablets and everything in between—have transformed enterprise computing, providing new mobility and flexibility for people and IT. At the same time, they compound the challenge of maintaining effective security and privacy of business information.

Enterprise mobility calls for a new approach to security—one designed for a world where mobile devices, bring-your-own device (BYOD), corporate-owned devices with personal data, cloud apps and public networks used for storing and accessing business data have rendered traditional locked-down perimeters obsolete.

Instead of seeking to protect all the information in the enterprise, including non-sensitive public data, IT should focus on protecting what really matters, sensitive business information like intellectual property and trade secrets, as well as, regulated personally identifiable information (PII), protected health information (PHI) and payment card industry (PCI) information. This approach calls for the mapping of security measures to user roles and the selective use of a broad range of methods to secure access, control usage, prevent data exfiltration and guard against device tampering—without interfering with data availability. Enterprise mobility management plays a central role in this strategy, with capabilities centered on devices, operating systems, networks, applications, data and policy—but it's equally critical to understand the role of the mobile OS itself.

Each of the three major mobile OS platforms, iOS, Android and Windows, presents unique security issues and features. While Android offers features and benefits targeted at organizations as well as consumers, OS version fragmentation and a lack of upgrade capabilities on carrier-controlled devices pose security challenges. Apple's proprietary iOS operating system enables tight control from hardware to applications and provides a walled garden approach that reduces vulnerabilities, but also limits traditional enterprise security options. Microsoft Windows 8-based devices such as Windows Phone and Surface include advanced security features and leverage IT's familiarity with legacy Windows security technologies, but differ significantly in their security capabilities and management across OS variants.

As the leader in mobile workspace solutions, Citrix has developed technologies and best practices designed to unlock the full value of the latest mobile devices for both personal and enterprise computing. In this paper we take an in-depth look at the major mobile OS platforms, the security issues and features unique to each, and the measures IT needs to take to maintain control while encouraging productivity and mobility. We also discuss the security capabilities provided by Citrix enterprise mobility solutions including Citrix XenMobile, Citrix ShareFile, Citrix XenDesktop, Citrix XenApp and Citrix NetScaler. Together, these solutions give the enterprise control over data from the datacenter to any device and address IT's security concerns—whether policy allows enterprise data to be mobilized on the device or not.

How the security of mobile devices differs from the security of a legacy PC

Mobile security isn't as simple as mapping current and familiar PC security measures onto mobile platforms. For example, antivirus, personal firewall and full disk encryption are possible on Android and Windows Phone and Surface, but would mean denying iOS devices access to the network, because iOS does not support all of these legacy control measures at this time. Though with the application vetting Apple performs, there is little need, at least for today for on-device security applications. A security architect tasked with securely allowing iOS devices in the enterprise has to approach the issue from the standpoint of data protection instead.

The Android security architecture is very similar to a Linux PC. Based on Linux, Android has all the advantages and some of the disadvantages of a Linux distribution (distro), as well as security considerations unique to a mobile OS. However, iOS devices differ substantially from a PC from both a usability and security perspective. The iOS architecture even appears to have several security advantages that could potentially remedy some of the security challenges of PCs. Compare the PC security model and mitigations alongside Android and iOS models in a simple example as shown below, and you'll see that the control measures PCs require may not be necessary for the iOS model. In addition, Windows Phone and Surface improve on the familiar PC model in many ways.

Security measure comparison of legacy PCs, Android, iOS and Windows tablets and smartphones

Security measure	PC	Android	iOS	Windows
Device control	Add-on	Add-on	Add-on	Add-on
Local anti-malware	Add-on	Add-on	Indirect	Native
Data encryption	Add-on	Configuration	Native	Configuration
Data isolation/ segregation	Add-on	Native	Native	Native
Managed operating environment	No	No	Yes	Yes
Application patching	User-managed	User-managed	Native	Native
Access to modify system files	Requires administrator	Requires rooting	Requires jailbreaking	Requires administrator

Android architecture can be configured for a strong security posture, as is the case with an Android version adopted for U.S. Department of Defense usage. In addition, the National Security Agency supports Security Enhanced (SE) Android model, bringing SE Linux OS to the Android kernel.

Android security architecture overview

Android architecture provides a platform that allows security customization from basic to advanced. Security measures must be specifically enabled and enforced, with the Android platform offering the following:

Some of the security features that help developers build secure applications include:

- The Android Application Sandbox, which isolates data and code execution on a per-application basis, expanded with Enforcing SELinux and boot integrity
- Android application framework with robust implementations of common security functionality such as cryptography, permissions and secure IPC
- An encrypted file system that can be enabled to protect data on lost or stolen devices

Nevertheless, it is important for developers to be familiar with Android security best practices to make sure they take advantage of these capabilities and to reduce the likelihood of inadvertently introducing other security issues that can affect their applications.

How do I securely use my Android phone and tablet?

Android security architecture was designed so that you can safely use your phone and tablet without making any changes to the device or installing any special software. Android applications run in their Application Sandbox, which limits access to sensitive information or data without the user's permission. To fully benefit from the security protections in Android, it is important that users only download and install software from known trusted sources, visit trusted web sites, and avoid charging their devices in untrusted docking stations.

As an open platform, Android architecture allows people to visit any website and load software from any developer onto a device. As with a home PC, the user must be aware of who is providing the software they are downloading and must decide whether they want to grant the application the capabilities that it requests. This decision can be informed by the person's judgment of the software developer's trustworthiness, and by determining where the software came from. The Bouncer scanning feature and third-party apps help detect application-embedded malware.

Android security concerns

The Android open platform is open to rooting and unlocking. Rooting is the process of becoming root—the super-user with all rights to the OS. Unlocking gains access to modify the bootloader, allowing alternate versions of the OS and applications to be installed. Android also has a more open permission model where any file on an Android device is either readable by an application or world-readable. This implies that if any file needs to be shared between applications, the only way to allow this is through world readability.

Upgrades to the latest version of Android are not always available and are sometimes controlled by the carrier. The lack of an available upgrade could allow security issues to persist. Check Settings/More/About device/Software update to determine if the platform can be upgraded.

Support for active content, including Flash, Java, JavaScript and HTML5, allows malware and attacks through these vectors. Ensure that security solutions can detect and thwart active-content attacks.

The Android OS is a favorite target of mobile malware, including SMS Trojans that send texts to premium numbers and rogue apps that subscribe users without their knowledge to nefarious services, leak personal information and even enable un-authorized remote control of the device. This is especially true for applications from rogue app stores, which have not been security-reviewed and vetted. While KitKat adds "dozens of security enhancements to protect users," it's still best to harden Android devices run an anti-malware solution to provide a more robust security posture.

The latest Android features – and what they mean for IT

The following table summarizes the user benefits and the IT security impact of the latest features in Android 4.4 tablets and smartphones.

New and notable in Android 4.4		
Android 4.4—Kit Kat—expands the capabilities of SELinux to protect the Android OS by running in Enforcing mode by default and adds new features to control security. The implementation of these features may also vary by manufacturer and device. The following notable features and their impact are discussed in this paper.		
Android feature	**Device user benefit**	**IT impact**
Certificate handling and KeyStore enhancements	Whitelisting and Certificate Pinning ensure that only valid certificates are used, Elliptic Curve algorithms streamline strong encryption, and warnings from Certificate Authority (CA) certs added to device thwart man-in-the-middle attacks.	Welcome improvements and automation to the Android cyrpto subsystem. The introduction of a public key API and other KeyStore management features will simplify and extend IT capabilities.
Always on listening	Saying "OK Google" without touching anything activates the device. This feature is currently just on Nexus 5, but planned to expand.	Devices may wind up recording unintended conversations and may dynamically enable or disable features based on what is said.

Auto add of missing content	The automatic addition of missing contact, nearby resources, maps and location info fills in.	People who work in secured facilities, or with highly security-conscious customers should not be giving away rich location-based info and must disable this feature.
Cloud integration	Integration of local and cloud storage means that information can be automatically stored/ synced between the device, applications and the cloud.	The use of Google Drive and third-party personal filesharing services will be native to apps and enabled through API's. IT must ensure that an enterprise-grade solution is available and enabled.
SMS, Google Hangouts for SMS	People can use and configure SMS for their personal needs	While Google Hangouts is great for personal interaction, enterprise SMS must be configured and enforced for business communications.

In addition to features supplied as part of the Android operating system, device manufacturers, carriers and partners are constantly enhancing Android with new features.

Samsung SAFE and KNOX

Samsung SAFE is a security program from Samsung designed to provide enterprise-ready devices that offer security controls above and beyond what most Android devices provide. Samsung SAFE includes mobile device and application management controls such as on-device AES-256 encryption, VPN connectivity and support for Microsoft ActiveSync Exchange for native corporate email, calendar and PIM apps.

Samsung KNOX provides an extra level of protection beyond SAFE with comprehensive security for enterprise data and the integrity of the mobile platform. Features of KNOX include a dual-persona container for isolation of work and personal spaces, a per-app VPN, kernel integrity measurement and Customizable Secure Boot to ensure that only verified and authorized software can run on the device.

Citrix takes an integrated approach in supporting SAFE APIs and KNOX. Citrix XenMobile builds on KNOX with enhanced MDM and MAM controls that are managed in the administration portal; we'll explore these features later in this paper.

The iOS security architecture overview

The iOS proprietary operating system is carefully controlled. Upgrades are from a single source and Apple applications in the AppStore are vetted, including basic security testing. The iOS security architecture has incorporated a sandbox-based security architecture, as well as implementing configuration-specific security measures and tight control that spans from hardware to applications.

According to Apple, iOS security is based on:

A layered approach to security
The iOS platform provides stringent security technology and features without compromising the user experience. iOS devices are designed to make security as transparent as possible. Many security features are enabled by default, so users don't need security expertise to keep their information protected.

Secure Boot Chain
Every step in the startup process—from the bootloaders, to the kernels, to the baseband firmware—is signed by Apple to ensure integrity. Only after verifying one step does the device move to the next step.

App sandboxing
All third-party apps are sandboxed, so they are restricted from accessing files stored by other apps or from making changes to the device. This prevents apps from gathering or modifying information the way a virus or malware would try to do.

With the release of iOS 7, Apple introduced TouchID to streamline device authentication, FIPS 140-2 cryptographic protection for sensitive data, Activation Lock to further protect lost and stolen devices, and numerous behind-the-scenes security enhancements.

Security concerns about the iOS model

Apple has taken a walled-garden approach to the iOS architecture, which prevents device owners from accessing or modifying the operating system. To perform any modification, the device must be jailbroken. Jailbreaking is the process of removing protections and allowing root access to the device. Once root has been achieved, modification and customization is enabled. Apple has taken additional hardware-based measures to dissuade jailbreaking.

The latest iOS features and what they mean for IT

The following table summarizes the user benefits and the IT security impact of the latest features in Apple iOS 7.1 tablets and smartphones.

New and notable in iOS 7.1		
In addition to welcome security feature enhancements, Apple has published a document detailing iOS security from the iDevice to iCloud. The following notable features and their impact are discussed in this paper.		
iOS feature	**Device user benefit**	**IT impact**
Activation lock	When configured, a lost or stolen phone is use-less to a thief, which should discourage device theft.	Has implications on device ownership and management. Complement with enterprise mobility management.
Touch ID	Touch ID is Apple's fingerprint identity scanner, currently exclusive to the iPhone 5s. It allows seamless access to the device.	TouchID works better under 7.1 and Apple has moved the TouchID and Passcode settings into a top level, making them easier to configure.
Automatic enrollment	Users receive enterprise devices pre-configured and ready to use.	Devices purchased from Apple through the Device Enrollment Program can easily be enrolled in MDM.
FIPS 140-2	Strong, verified encryption protects all data on the device.	Enterprises that require FIPS 140-2 at the device level can now use iPhones and iPads.

iOS7.x versus Android security controls

In comparing iOS to Android, it's important to note that Android controls will vary based on the actual device, the operating system version and even the carrier. In some cases for example, older versions of Android do not offer device-level encryption.

	iOS7.x	Android
Device encryption	Yes	Varies based on device/OS/carrier
OTA encryption	Yes	Varies based on device/OS/carrier
Device password	Yes	Varies based on device/OS/carrier
Remote lock/wipe	Yes	Varies based on device/OS/carrier
App review	Yes	Varies based on device/OS/carrier
App password	Yes	Varies based on device/OS/carrier
App encryption	Yes	Varies based on device/OS/carrier
App container	Yes	Varies based on device/OS/carrier
App secure network access	Yes	Varies based on device/OS/carrier
Open in	Yes	Varies based on device/OS/carrier

Windows Phone and Surface security architecture overview

Microsoft has expanded on the familiar Windows technologies and architectures in their latest tablet and smartphone operating systems. Integrated security features such as BitLocker, Defender, SmartScreen, personal firewall and user account control build upon a strong mobile security architecture.

According to Microsoft, security for Windows Phone and Surface platforms is based on:

App platform security
Microsoft takes a multi-pronged approach to help protect Windows tablet and smartphone devices against malware. One aspect of this approach is the Trusted Boot process, which helps to prevent rootkit installation.

Chambers and capabilities
The chamber concept is based on the principle of least privilege and uses isolation to achieve it; each chamber provides a security boundary and, through configuration, an isolation boundary within which a process can run. Each chamber is defined and implemented using a policy system. The security policy of a specific chamber defines what operating system capabilities the processes in that chamber can call.

A capability is a resource for which user privacy, security, cost or business concerns exist with regard to Windows Phone usage. Examples of capabilities include geographical location information, camera, microphone, networking and sensors.

Windows security concerns

Legacy Windows-based PC operating systems are popular and highly targeted by attackers, meaning that any shared code and services between PC and mobile platforms could cause widespread vulnerability. The security-enhanced architecture of the mobile Windows platforms—especially the full Windows 8 experience—have advanced the state of Windows security.

The default user runs as Administrator, giving too much access for normal day-to-day work. It's recommended that a separate user be created for everyday usage, with Administrator privileges reserved for when administrative tasks are required. Of course, the ability for a user to become Administrator on the device is similar to becoming root—there's too much access at this privilege level that can negatively impact security.

Another big concern is that the familiar Windows security model and controls can lead to a state where the device is overly managed by IT. This will result in the familiar my-way-or-the-highway approach to security and usability; unjustified and excessive IT management will force users to adopt another device.

The latest Windows features – and what they mean for IT

The following table summarizes the user benefits and the IT security impact of the latest features in Windows Phone and Surface 8.1 tablets and smartphones.

New and notable in Windows Phone and Surface		
Microsoft has revamped the mobile Windows platforms, directly integrating enterprise security features. The following notable features and their impact are discussed in this paper.		
Windows feature	**Device user benefit**	**IT impact**
BitLocker	Device encryption in Windows Phone 8 utilizes BitLocker technology to encrypt all internal data storage on the phone with AES 128.	User-managed encryption is not appropriate for sensitive enterprise data. IT needs to enforce enterprise management of encryption.
Windows Defender	This feature helps guard your PC against viruses, spyware, and other malicious software in real time.	Native antivirus and anti-malware is a welcome addition to mobile platforms.
SmartScreen	SmartScreen Filter in Internet Explorer helps protect users from phishing and malware attacks by warning users if a website or download location has been reported as unsafe.	IT policy needs to enforce that users heed the SmartScreen warnings.
Data loss prevention	Information Rights Management (IRM) allows content creators to assign rights to documents that they send to others. The data in rights-protected documents is encrypted so that it can be viewed only by authorized users.	Requires Windows Rights Management Services (RMS) and Windows Phone.
Firewall	A personal firewall protects inbound and outbound application and network connectivity.	Configuration of the firewall should be specified and controlled by IT.

How today's mobile devices protect sensitive data

Mobility models shift traditional IT security responsibilities from tightly defined organizational standards to a collection of standards that involve a myriad of devices, operating systems and policies. There is no one-size-fits-all approach to mobility, and the unique aspects of device ownership, device capabilities, data location and application needs all factor into the security picture.

However, familiar control measures such as enterprise-controlled antivirus protection cannot be installed and maintained on all mobile devices. Organizations must consider the efficacy of specific mobile security measures in the context of their own requirements and seek the recommendations of their own enterprise security architects. For more information on how enterprise mobility management, Windows app and desktop virtualization, and enterprise data sync and sharing counter potential mobile security threats, review the table below.

Threats and corresponding mobile security measures (with enterprise mobility management, Windows app and desktop virtualization, enterprise data sync and sharing, and networking)

Threat	Threat vector	Mobile security measure
Data exfiltration	Data leaves organization Print screen Screen scraping Camera Copy to removable media Loss of backup Email	Data stays in the data center or is encrypted and managed on the device App/device control Restrict removable media Encrypted backups Email not cached in native app Restrict screen capture
Data tampering	Modification by another application Undetected tamper attempts Jail-broken device	Application/data sandboxing Logging Jailbreak detection Mutual authentication Micro-app VPN
Data loss	Loss of device Unapproved device and access Mistakes and configurations Application vulnerabilities	Managed data on device Device encryption Data encryption Updates and patching

Malware	OS modification	Managed operating environment
	Application modification	Managed application environment
	Virus	Architecture*
	Rootkit	

*While mobile OS architectures can be hardened against malware, latent PC-based viruses can be passed through infected documents. It is recommended that anti-malware capabilities are available for all host environments that the mobile device connects to, especially email.

With personally owned devices in the enterprise, it's prudent to keep the most sensitive business information off of the device to reduce vulnerability. Highly sensitive data should, by default, be accessed remotely from the datacenter and never copied to a mobile device. Data that must be mobilized should be secured through measures such as encryption and the ability to remotely wipe them from mobile endpoints. Applications that must be mobilized and controlled can be containerized to prevent interaction with non-enterprise apps.

See what you're missing

Mobile applications don't always display content in the same way as native apps on a PC. Here are some of the problem areas:

- Videos that are not in native mobile-supported formats won't play (e.g. WMV, Flash)
- Email apps often have issues with properly displaying graphics, are misconfigured for security certificate support, don't encrypt data, and don't handle recall notices and other special features
- Calendar can't view free/busy status and has problems with multiple updates to events and events that are not current
- Presentation apps don't always show all graphics, fonts and layouts as they appear in PowerPoint
- Word processing apps don't show when Track Changes is enabled and don't display comments and notes, so edits are not displayed and key updates may be missed

Securing enterprise information accessed on tablets and smartphones with Citrix

Citrix provides a unified app store on the mobile device, enabling access to both productivity and business apps including data managed via ShareFile. ShareFile can be used to enable offline data access on mobile devices. ShareFile and XenMobile help IT protect sensitive data stored on mobile devices through containerization, encryption and comprehensive data control policies to block user leaks. Containerized data on the device can be remotely wiped by IT at any time; this can also be triggered automatically by specified events such as device jailbreak. The Citrix unified app store delivers mobile apps as well as centrally hosted Windows applications and desktops via XenApp and XenDesktop. By providing remote mobile access to centrally hosted resources, IT can keep restricted data in the datacenter, where it

can be kept safe and secure. Whether an organization keeps sensitive data and applications in the datacenter, contains it on the device, or allows it to go mobile, IT can execute and enforce these policies through XenMobile and ShareFile.

Citrix-secured mobile apps take advantage of Citrix NetScaler Gateway for strong authentication and encryption of network traffic. The NetScaler Gateway SSL/VPN gateway provides micro-app VPNs to enable backend access for enterprise, mobile and web apps, acting as a network policy enforcement point to enable application-specific networking security. Micro-app VPNs only run specified, business data through the enterprise, helping to manage traffic better and secure end-user privacy at the same time. XenMobile offers unified management and control over all types of applications, including mobile, web, SaaS and Windows, as well as over data, devices and users.

Encryption in Citrix protects configuration data, screen bitmaps and the user work-space. Citrix utilizes native mobile platform functionality to encrypt data at rest and in motion through WiFi and 3G/4G network interfaces.

How XenMobile helps protect apps and devices

XenMobile provides mobile device, app and data freedom. XenMobile provides identity-based provisioning and control for all apps, data and devices, as well as policy-based controls such as restriction of application access to authorized users, automatic account de-provisioning for terminated employees, and selective wipe of device, apps or data stored on lost or stolen devices. The solution's secure container not only encrypts application data but also separates personal information from business information. In this way, organizations can give people device choice while giving IT the ability to prevent data leakage and protect the internal network from mobile threats.

OS-level protection
XenMobile Device Manager ensures that the necessary OS hooks are in place to enforce and manage OS-level features including:

- Device-level password protection
- Encryption
- WiFi
- Device inventory
- Application inventory
- Full/selective wipe
- Specific device manufacturer APIs (Samsung, HTC, etc.)
- Automated configuration of WiFi
- Restricting access to device resources including app stores, camera and browser
- Support for Samsung SAFE and KNOX security controls

Encryption and security

XenMobile gives IT the ability to prevent copy/paste or only allow it to happen across authorized applications. Through Worx Mobile Apps, features such as AES-256 encryption and FIPS 140-2 validation protect data at rest for key business data. Open-in controls let you specify that certain documents can be opened only in specified applications. Even links to web sites can be forced to open in a secure browser.

In transit, data is protected through a micro-app VPN capability, which allows secure access to enterprise resources for apps, intranet and email. Micro-app VPN tunnels are unique per-application and encrypted to be protected from other device communication or other micro-app VPN communication.

Jailbreak detection

XenMobile detects jailbreak and root status through proprietary methods including API availability and binary inspection.

Geo-location policies

Location services enable IT to establish a geo-perimeter to control where devices or specific apps can be used. If the device leaves the perimeter, its contents can be fully or selectively wiped.

Mobile application management (MAM)

MAM controls the usage, updates, networking and data security for applications. Each application on the device can receive its own SSL-encrypted tunnel that can only be used by that application. When an employee leaves the company, IT can remotely, selectively wipe all enterprise data from the managed application containers without touching any personal apps or data on the device. XenMobile also provides a single, secure storefront for mobile devices to access both public and private apps.

Secure productivity apps

Built-in Citrix productivity apps include a secure web browser, a mail/calendar/contact container and ShareFile, a secured file sync and sharing service. This makes it possible for people to seamlessly browse intranet sites without the need for expensive VPN solutions that open the company network to all applications on the device. With Worx Mobile Apps, any developer or administrator can add enterprise capabilities, such as data encryption, password authentication or a micro-app VPN.

Worx Mobile Apps include:

WorxMail – WorxMail is a full-featured native iOS and Android email, calendar and contacts app that functions and manages data entirely within the secure container on the mobile device. WorxMail supports Exchange ActiveSync APIs and offers security features such as encryption for email, attachments and contacts.

WorxWeb – WorxWeb is a mobile browser for iOS and Android devices that enables secure access to internal corporate web, external SaaS and HTML5 web applications while maintaining the look and feel of the native device browser. Through a micro-app VPN users can access all of their websites, including those with sensitive information. WorxWeb offers a seamless user experience in its integration with WorxMail to allow users to click on links and have the native apps open inside the secure container on the mobile device.

Worx Home – Worx Home is the central control point for all XenMobile-wrapped applications as well as content stored on the device. Worx Home manages the user experience springboard for authentication, applications, policy management and encryption variable storage.

Together, these and other XenMobile features enable IT to:

Unify control over remote access to apps and data. The Citrix unified enterprise app store securely aggregates virtualized Windows applications and desktops; web, SaaS and native mobile applications; and data into one place to manage and control the policies and accounts that apply to user services.

Isolate and secure enterprise email. One of the biggest advantages of WorxMail is that it keeps enterprise email in a sandbox or container—not co-mingled with the device. Contrast this with using ActiveSync and the native mobile email app, where an admin needs to take some control of the device and the user needs to consent to the device being wiped if there's a problem. Access, encryption and profile info are all tied to the device. In addition to this, the sandboxed approach provides encryption of both the email body and any attachments.

Avoid interfering with personal content on mobile devices. Using WorxMail, the user needs to only consent to business information stored in the WorxMail container being wiped in the event of a problem—not the entire device. Enterprise email and contacts are isolated, protected and controlled by the container, not by the device. Work and personal email are also separated through the sandboxed approach, which helps keep email and contacts separate.

XenMobile and Samsung SAFE and KNOX

XenMobile supports Samsung SAFE and KNOX security controls, including the management of the KNOX container. Tight integration between Worx Mobile Apps and the secure KNOX container ensure that sensitive enterprise data—including email subject to retention regulations—is never exposed to malware that might reside on the OS, or to unmanaged applications in the personal partition. In addition, the solution also supports audit trails to verify data integrity for compliance and regulatory considerations. XenMobile also enables additional security features and controls for KNOX including secure inter-app communication, geo-fencing control, intelligent network traffic control and secure content management. (Note, additional licenses for Samsung Knox may be needed.)

XenMobile and iOS 7.x

XenMobile supports and extends iOS native controls with added security features. For both iOS 7 and KNOX, XenMobile provides the following enhancements:

XenMobile Feature	Details
Enterprise app store	Single-pane access with the ability to provision mobile, SaaS, web and Windows apps directly to device springboard
Enhanced SSO	One-click access to mobile, SaaS, web and Windows apps

Ecosystem of business-ready apps	Largest ecosystem of apps with Worx App Gallery
Network control	Control app usage based on WiFi networks
Authorized SSID control	Granular control of which internal networks apps work with
Geo-fencing control	Enhanced security to lock, wipe or notify based on device location
Online/offline access	Restrict app to online access or determine length of offline usage
Inter-app communication	Control communication between managed apps
Easy provision and de-provisioning	Enable/disable access
Secure mail	Sandboxed email integrated with corporate contacts and calendar with contact availability visibility
Secure browser	Fully functional HTML5 browser for secure content and corporate intranet sites
Secure content management	Access, annotate, edit and sync file from any device
Full suite of EMM apps	Apps to address every EMM use case and critical capabilities that include ShareFile, GoToMeeting, GoToAssist, and Podio

How ShareFile helps protect data and files

ShareFile provides robust managed data sharing and syncing capabilities, fully integrated with XenMobile. The solution also allows IT to store data on-premise or in the cloud, and helps mobilize existing investments such as network shares and SharePoint. Integrated rich content editing capabilities within ShareFile enable people to meet their mobility, productivity and collaboration needs from a single, intuitive app. With ShareFile IT can:

Secure data with comprehensive device security policies. ShareFile provides extensive capabilities to ensure data security on mobile devices. ShareFile provides remote wipe and poison pill features that remove access to sensitive data in the event of a security breach. IT can also restrict modified mobile devices and enable passcode lock to leverage the mobile device's encryption capabilities.

Boost user productivity with rich content editing on mobile devices. Users can create, review and edit Microsoft Office documents within the ShareFile app and edit them with similar tools that are available from their desktop Microsoft Office applications.

Restrict third-party applications and improve data security on mobile devices. IT can restrict the use of unauthorized third-party applications to open and edit ShareFile data. A built-in editor makes it possible for IT to restrict the use of third-party editors that employees may be using, and thereby prevent employees from storing copies of sensitive data within those apps.

Retain folder and sub folder structure on mobile devices. You can mark entire folders in addition to individual files for offline access on mobile.

Increase availability. Offline access to entire folders, complemented with support for document editing, helps people be fully productive anywhere.

Track, log and report on user file access, sync and sharing activity. IT gets comprehensive tracking over the date, type, place, and network address of each user event. Multiple versions of files can be stored to create full audit trails of editing activity. If a remote wipe is initiated, IT can track file activity that occurred on the device from the time the wipe was initiated through its successful execution, and will receive a notification indicating whether the wipe has succeeded.

Streamline administration and security. IT can easily leverage role-based provisioning and de-provisioning of the service, two-factor authentication, policy-based controls and real-time application monitoring through ShareFile integration with XenMobile.

ShareFile allows you to choose where you store your data. With the ShareFile StorageZones feature, organizations can manage their data on-premises in customer-managed StorageZones or choose Citrix-managed StorageZones (secure cloud options available in multiple worldwide locations) or a mix of both. With customer-managed StorageZones, IT is able to place data in the organization's own data center to meet unique data sovereignty and compliance requirements.

For those who choose to store their data in the cloud, the datacenters that host the ShareFile web application and databases are SSAE 16 accredited and the data centers that host the file storage application are SSAE 16 and ISO 27001 accredited. Citrix implements and maintains commercially reasonable and appropriate physical, technical and organizational complimentary controls to protect customer data.

ShareFile is PCI-DSS compliant and will enter into a HIPAA business associate agreement. Citrix also offers ShareFile Cloud for Healthcare—a secure enclave within a private cloud where IT can upload, store and share patient heath information (PHI) and meet strict HIPAA compliance laws. ShareFile Cloud for Healthcare supports compliance with the HIPAA Security Rule.

How XenDesktop and XenApp help protect apps and data

XenDesktop and XenApp provide secure remote access to centrally hosted virtual Windows desktops, apps and associated data that remains protected within the datacenter. Although devices—and the people who use them—are mobile, the data itself stays secure and protected within the datacenter. XenDesktop and XenApp also provide an easy, efficient and secure way to deliver third-party and internally developed Windows apps to a mobile workforce.

How NetScaler helps protect data and files

NetScaler provides secured connectivity for mobility, enabling single sign on (SSO), strong multi-factor authentication, encryption and micro-app VPN functionality. The use of NetScaler automates network security, freeing the device owner from having to enable/disable VPNs or remember how to securely log into web and cloud applications. NetScaler benefits security and compliance officers by assuring that all required authentication, encryption, logging and networking protective measures are enforced.

Best practices for mobile security

To ensure effective security and control, organizations should complement the security capabilities inherent in Citrix technologies and mobile devices with comprehensive best practices for both people and IT. Every member of the organization must share responsibility for following these measures, which are vital to enable enterprise mobility and BYOD in a safe and controlled manner. Citrix recommends the following user and administrator guidelines when using Citrix with Android, iOS and Windows tablets and smartphones.

Recommended user actions

Users have a responsibility to protect their organization's sensitive business information. They can control device set-up and configuration, have good daily use practices, use XenMobile, ShareFile, XenDesktop and XenApp to help ensure security, and take several other recommended actions. Administrators can ensure that users employ these best practices by enforcing them automatically by policy in XenMobile. Best practices for users are outlined here.

Device setup and configuration	
Platform	Don't jailbreak or root your device if used within enterprise environments, and deny requests to install third party certificates **Android:** If you must share, use different user accounts for kids and other guests on a shared device **iOS:** No configuration necessary **Windows:** Create a separate account for Administrator and use an unprivileged user account for daily work

Authentication	Utilize a passcode lock to protect access to the mobile device—use eight character non-simple passcode **Android:** Configure Lock screen to set passcode or PIN security, set Lock automatically for timeout, and set Lock instantly with power key **iOS:** Set Require Passcode to Immediately and thwart passcode guessing by setting Erase Data to ON. Enable Auto-Lock and set to one minute. Use TouchID, if available on your device **Windows:** Set an account password and require a password after the display is off for x minutes
Encryption	Encrypt the device and backups, and control the location of backups **Android:** Encrypt device **iOS:** Set a passcode or passphrase to encrypt the device and encrypt backups in iTunes and iCloud **Windows:** Configure BitLocker
Cloud Services	Configure services so that sensitive enterprise data is not backed up to the consumer cloud; this includes documents, account information, wireless passwords, settings and messages **Android:** Disable personal Backup to Google Account **iOS:** Disable personal iCloud **Windows:** Disable personal OneDrive
Bluetooth and Sharing	Disable data transfer for untrusted connections; for example, disable the transfer of your contacts and phone book while using Bluetooth for phone calls or playing music in a rental car **iOS:** Turn off Sync Contacts **Windows:** Turn off Sharing
Network and Wireless	Utilize only trusted networks, ensure network encryption and utilize a VPN or micro-app VPN to provide encryption regardless of underlying network capabilities; the WorxWeb feature of XenMobile enables micro-app VPN connectivity **Android:** Configure wireless to provide Network Notification **iOS:** Configure wireless to Ask to Join Networks **Windows:** In advanced sharing settings under Control Panel, turn off network discovery for Guest or Public networks and turn on password protected sharing

Email	Since email is commonly used for sharing (and leaking) sensitive data, use ShareFile to keep sensitive attachments out of email and use WorxMail with XenMobile when a managed email container is desired **Android:** Configure email access to always use a secured connection **iOS:** Ensure that Use SSL is On for all supported accounts and use S/MIME, if configured **Windows:** Configure accounts to support SSL
Device Upgrades / Device Loss	Know how to back up all data for transfer to a new device and how to securely erase an old device as well as the procedure for contacting your IT organization to report a lost or stolen device **Android:** Use native Backup my Data and settings or a third-party backup solution, and use Factory Data Reset to erase personal data **iOS:** Consult your IT organization on whether or not a mobile device management (MDM) solution is in place that would allow them to remotely locate and wipe your device should it be lost or stolen; if MDM is not being used, configure Find My iPhone and utilize it to wipe a lost or stolen device* **Windows:** Use File History or a third-party backup solution and remove everything and reinstall Windows to erase personal data
Privacy	Prevent inadvertent display and sharing of personal and sensitive information **Android:** Disable the collection of Diagnostics and Usage Data under Settings/General/About **iOS:** Turn on Limit Ad Tracking in General/About/ Advertising and configure Notifications to only display information in the Notification Center from apps that won't erode privacy **Windows:** Configure Notifications to Show App Notifications on the lock screen only for trusted apps; disable Let Windows Save My Searches as future search suggestions; turn on Do Not Track in Internet Explorer; delete search history in Windows; disable Let Apps Use My Name and Account Picture; and disable Help Windows Store by sending URLs for the web content that apps use

* The Find My iPhone app, a free download on the App Store, lets people easily locate a missing device on a map and have it display a message or play a sound. People can even remotely lock or wipe data from a lost device to protect privacy.

Diagnostics and Developer Features	Disable features used by developers that can erode security and privacy **Android:** Disable Developer Options and USB debugging **iOS:** Disable the sending of Diagnostics and Usage Data under Settings/General/About/Diagnostics and Usage **Windows:** Run as an unprivileged user, not as Administrator, to disable access to administrative and system diagnostics
Applications	Only install apps from known-good sources–enterprise app stores and official platform app stores **Android:** Don't accept applications that require excessive permissions and ensure Device Administration/Unknown sources is not selected **iOS:** Utilize apps from the Apple App Store **Windows:** Utilize apps from the Microsoft Store
Updates	Apply software updates when new releases are available **Android:** Go to About Device/Software Update for OS updates and the Play Store app for app updates **iOS:** Go to General/Software Update to check for iOS updates and check the App Store application for app updates **Windows:** Use Windows Update for OS updates and Store for app updates
Security Software	Configure included security software and features, including firewall and run an anti-malware solution if required **Android:** Search the Play Store for security applications that meet personal and enterprise security needs **iOS:** No special configuration necessary **Windows:** Configure the Windows firewall; Windows Defender anti-virus is pre-installed

Daily use

- Press the power button to lock the device whenever it is not in use.
- Verify the location of printers before printing sensitive documents.
- Report a lost or stolen device to IT so they can disable certificates and other access methods associated with the device.
- Use a self-service portal to lock and locate lost devices.
- Consider the privacy implications before enabling location-based services and limit usage to trusted applications.
- Manage access to iTunes AppleID, Google and OneDrive accounts, which are tied to sensitive data.

Additional Considerations and Best Practices

- Keep unmanaged sensitive data off of shared mobile devices. If enterprise information is locally stored on a device, it's recommended that this device not be openly shared. Ask your IT department how to use Citrix technologies to keep data in the datacenter and keep personal devices personal.
- If you must have sensitive data on a mobile device, use ShareFile and XenMobile to contain sensitive data and track where enterprise data moves and sits.
- Utilize the additional authentication and encryption features of ShareFile and XenMobile as mitigation to Lock Screen bypass vulnerabilities.
- Configure location services to disable location tracking for applications that you don't want to know your location information.
- Configure notifications to disable the ability to view notifications while the device is locked for applications that could display sensitive data.
- Configure AutoFill – Auto-fill Names and Passwords for browsers to reduce password loss via shoulder-surfing and surveillance (if desired and allowed by enterprise policy).

Additional responsibilities of mobile device owners accessing enterprise email communications

Android, iOS and Windows tablets and smartphones natively support Microsoft Exchange and other email environments. XenMobile can be used to configure email policies on the device, as well as to block access if the device becomes non-compliant.

For highly secure environments, WorxMail, a sandboxed, user-friendly mail client, can be used to control email and its attachments with granular data control policies.

Recommended administrator actions

Administrators are responsible for implementing and enforcing the policies set by security leaders, IT and business executives. Key recommended actions are listed here.

- Publish an enterprise policy that specifies the acceptable use of consumer- grade devices and personally owned devices in the enterprise. Make sure users are aware of these policies.
- Publish an enterprise policy for cloud services, especially file-sharing tools.
- Enable security measures such as antivirus to protect data in the datacenter.
- Implement policy that specifies what levels of application and data access are allowable on consumer-grade devices, and which are prohibited.
- Specify a session timeout through NetScaler Gateway that is consistent with enterprise policy.
- Specify whether the domain password can be cached on the device, or whether users must enter it every time they request access.
- Enable SSO for commonly used mobile apps for both security and ease-of-use.
- Determine and configure the allowed NetScaler Gateway authentication methods.

Conclusion

Enterprise mobility and BYOD call organizations to adapt to new security challenges. Citrix enables a centralized approach to security that protects sensitive business information without hindering productivity, giving enterprises an effective way to meet the needs of an increasingly mobile workforce. With Citrix, the enterprise can adopt a more effective and modern approach to information security.

This document is not intended to be a complete guide to Android, iOS and Windows enterprise mobile security. Citrix recommends an overall strategy assessment that includes XenMobile, ShareFile, XenDesktop, XenApp, and NetScaler.

Version statement: This document is current for Android 4.4, Apple iOS 7.1 and Windows 8.1 as of April 2014.

For additional information, about Citrix BYOD solutions and secure-by-design technology, please visit http://www.citrix.com/byod and http://www.citrix.com/secure or follow us on Twitter @CitrixBYOD and @CitrixSecurity.

Additional Resources

- 10 essential elements for a secure enterprise mobility strategy
- Best practices to make BYOD simple and secure
- Enterprise mobility management: Embracing BYOD through secure app and data delivery
- The 10 must-haves for secure enterprise mobility

For more device-specific information about securing iOS, Android and Windows Phone and Surface devices in the enterprise, please visit:

Apple iOS

- iPad in Business – IT Center: Security
- iPhone in Business – IT Center: Security

Android

- KitKat, Android 4.4 features

Windows Phone and Surface

- Windows Phone 8 security and encryption

Corporate Headquarters
Fort Lauderdale, FL, USA

India Development Center
Bangalore, India

Latin America Headquarters
Coral Gables, FL, USA

Silicon Valley Headquarters
Santa Clara, CA, USA

Online Division Headquarters
Santa Barbara, CA, USA

UK Development Center
Chalfont, United Kingdom

EMEA Headquarters
Schaffhausen, Switzerland

Pacific Headquarters
Hong Kong, China

About Citrix
Citrix (NASDAQ:CTXS) is a leader in virtualization, networking and cloud infrastructure to enable new ways for people to work better. Citrix solutions help IT and service providers to build, manage and secure, virtual and mobile workspaces that seamlessly deliver apps, desktops, data and services to anyone, on any device, over any network or cloud. This year Citrix is celebrating 25 years of innovation, making IT simpler and people more productive with mobile workstyles. With annual revenue in 2013 of $2.9 billion, Citrix solutions are in use at more than 330,000 organizations and by over 100 million people globally. Learn more at www.citrix.com.

0414/PDF

citrix.com/byod **citrix.com/secure**