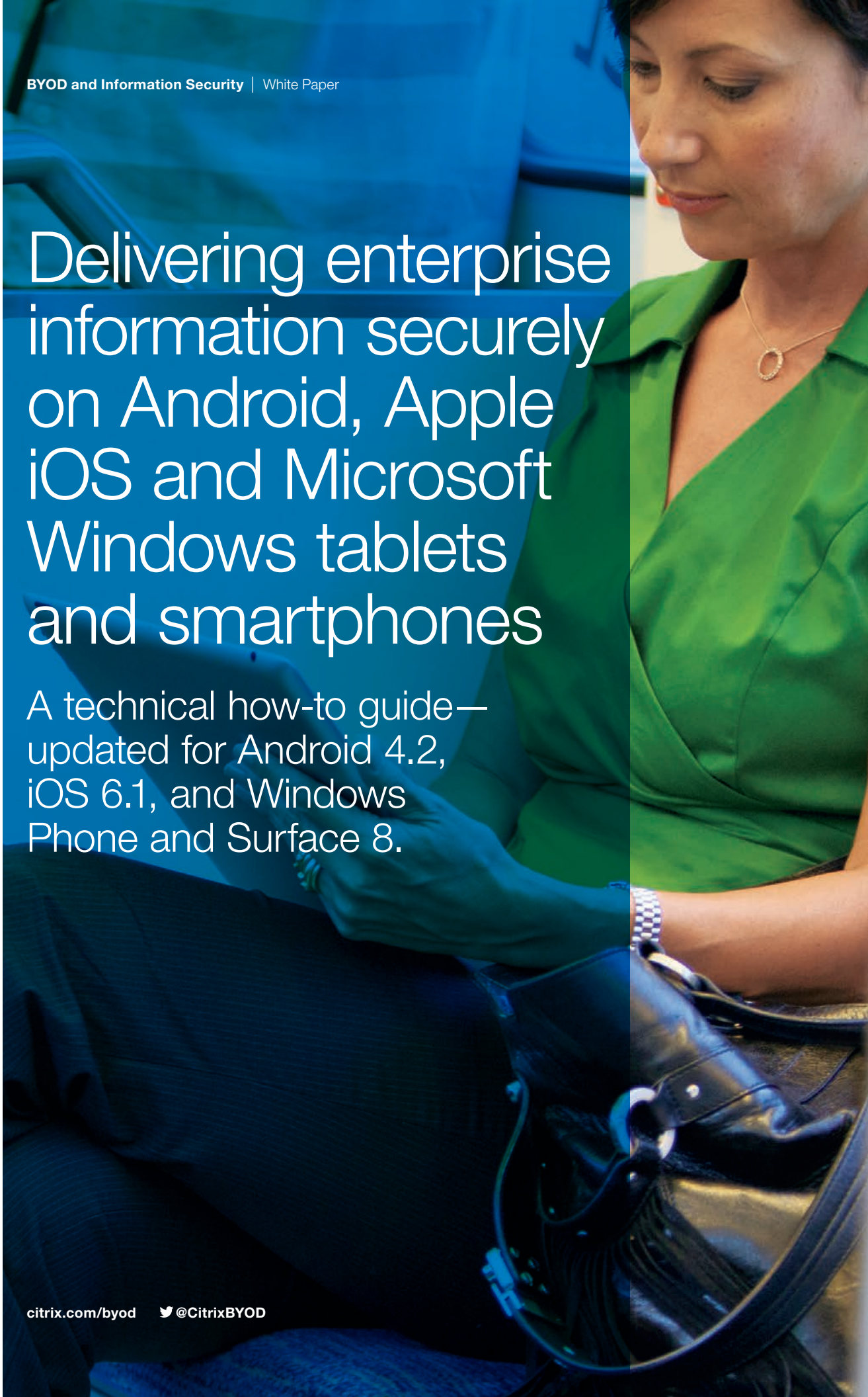
Delivering enterprise information securely on Android, Apple iOS and Microsoft Windows tablets and smartphones

A technical how-to guide—updated for Android 4.2, iOS 6.1, and Windows Phone and Surface 8.



CITRIX®

citrix.com/byod @CitrixBYOD

Android, iOS and Windows-based mobile devices—including smartphones, tablets and everything in between—play an expanding role in 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. This paper describes these issues and explains how they can be addressed effectively with solutions from Citrix.

Two competing desires are increasingly at odds with each other: expanding mobility to leverage productivity gains—and controlling mobility to combat significant risks. While IT may want to return to the days of two distinct devices, one dedicated to work and one for personal use, today's mobile users clutching consumer devices have successfully rebelled against this stance in most enterprises, never to return.

At the intersection between the evolution of mobility and the revolution of mobile users is bring-your-own device (BYOD). The bring-your-own movement, which can involve everything from devices to applications, has forever transformed computing. While BYOD is often viewed through the lens of productivity and freedom, a closer look reveals the imperative for a simple and effective BYO-focused security model. To embrace BYOD successfully requires focusing on a deeply individual and situational balance of usability and risk management.

Enterprises and individuals seek unified mobility solutions that are powerful, easy to use and always available, while also protecting privacy and providing appropriate security. These mobility solutions combine devices, operating systems, networks, applications, data and policy—but the OS is really the heart and soul of mobility.

The choice of mobile OS determines everything from hardware and apps to support, jailbreak ability, expandability and accessories, while discretely impacting enterprise management, support, privacy and security. Security features are either inherent in the mobile OS or enforced through measures and policy controlled by the mobile OS. This means that the proper configuration and maintenance of mobile OS security features are imperative to protect both the enterprise and the individual. In addition, innovative uses of mobile technology such as tablets in the boardroom are pushing the boundaries of the secured mobile experience—and screaming for security innovation.

In this paper we look at three major mobile OS platforms, security issues and features unique to each, and enterprise guidance for making it easy for mobile OS users to do the right things to protect privacy and security.

Android powered devices enable a wide variety of hardware manufacturers to offer a similarly wide variety of differentiated devices. As an open platform with roots in open-source software, Android has become a key operating system in the quest for increasing mobility. Features and benefits that are targeted at both consumers and enterprises make Android an attractive choice for both individuals and organizations. However, organizations must ensure that specific measures are in place to ensure the security and privacy of enterprise information. While device and OS security features continue to impress, issues of OS version fragmentation and a lack of upgrade capabilities on carrier-controlled devices continue to be problematic for Android security.

Apple iOS-based mobile devices such as the iPhone and iPad have been marketed as consumer devices, but have found themselves at home enabling mobility in many enterprises. The proprietary iOS operating system is tightly controlled, resulting in a consistent experience across applications and devices. In addition, iOS has a broad ecosystem of software and hardware that tightly integrates with Apple devices. Apple sets the bar for user experience, consistency and overall control from hardware to applications. The walled garden approach to security reduces vulnerabilities, but simultaneously limits traditional enterprise security options.

Microsoft Windows 8 operating system based mobility solutions include Windows Phone and Surface. These systems promise the greatest compatibility with Microsoft environments, including the Office suite of applications. With advanced built-in security features that include secure boot, BitLocker device encryption, anti-malware, firewalling and information rights management, Windows Phone and Surface present a strong security foundation. The relatively newly refreshed mobile Windows platforms may become an IT security favorite, especially as legacy Windows security technologies are well-understood and managed by most IT departments.

As part of a commitment to creating a world where people can work and play anywhere on any device, Citrix has developed technologies and best practices designed to unlock the full value of the latest mobile devices for both personal and enterprise computing. Citrix bring-your-own-device (BYOD) solutions enable people, including employees, contractors, partners and outsourcers, to use their tablets and smartphones seamlessly in the course of their work while providing IT with the control to ensure security and protect confidential business information.

This white paper describes, from an IT perspective, the issues that arise when allowing Android, iOS and Windows-based tablets and smartphones into both enterprise and consumer networks—and the steps IT must take to maintain control while encouraging productivity and mobility. The discussion includes the security considerations, risk mitigation options and the architecture required to support tablets and smartphones as consumer-grade devices accessing sensitive business information.

The paper also outlines how Citrix enables tablet and smartphone usage within the enterprise by giving people secure access to their enterprise applications, data and desktops on Android, iOS and Windows-based mobile devices. Citrix Receiver, a lightweight software client, makes it simple for people to access the enterprise app store from any device they choose, personal or corporate-owned. Citrix XenMobile provides for mobile device management (MDM) and mobile application management (MAM) to return governance and visibility over mobility to IT. Citrix XenDesktop enables IT to centralize Windows applications and desktops within the datacenter for delivery as an on-demand service and Citrix ShareFile enables managed data sync and sharing. 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. Citrix Receiver, XenMobile, XenDesktop and ShareFile, are complemented by Citrix GoToMeeting and Citrix Podio for easy online collaboration, and Citrix GoToAssist for remote support.

What's the latest? The following tables summarize the user benefits and the IT security impact of the latest features in Android 4.2 Jelly Bean, Apple iOS 6.1 and Windows Phone and Surface 8 for tablets and smartphones.

New and notable in Android 4.2		
Android 4.2—Jelly Bean—introduces multiuser capabilities, simplifies the permissions model and improves control over many security-related features. The following notable features and their impact are discussed in this paper.		
Jelly Bean feature	**Device user benefit**	**IT impact**
Application vetting	Android now includes a service based on Bouncer that works with all apps, not just those on Google Play. For example, it can check apps you download on the Amazon Appstore, or from third-party sites.	Apps installed from enterprise app stores and personal apps will be scanned for signs of malicious code. Enterprise users should still be encouraged/ forced to use only sanctioned application sources.
Multi-user	New multi-user support for tablets lets different users have their own separate, customizable spaces on a single device. Three users can be active at a time, and they can all sync data like email at the same time and even reuse apps if another user has them installed.	People who share devices with their family can finally keep the kids away from work apps and email. This feature will also be a benefit to consultants and healthcare professionals who work for multiple organizations.
Daydream	A new display mode, Daydream, allows apps to display interactive screensavers such as a photo album or a Currents stream when the device isn't being used.	Cameras are often used to record images for later transcription. Work-related pictures, including images of sensitive data on whiteboards can be inadvertently displayed.
SMS firewall	A warning is issued before an app tries to send SMS messages that may cost money.	Malicious apps will look to new vectors for generating income.
In addition to features supplied as part of the Android operating system, device manufacturers, carriers and partners are constantly enhancing Android with new features.		

New and notable in iOS 6.1		
Building on iCloud, Apple has expanded cloud connectivity and control for mobile devices. The following notable features and their impact are discussed in this paper.		
iOS feature	**Device user benefit**	**IT impact**
Security and iCloud enhancements	iOS includes behind-the-scenes updates to advance device security and extend the utility of iCloud.	Many enhancements only apply to iPhone 3G and above, effectively sunsetting earlier platforms.
Privacy settings	To guard your privacy, apps requesting location information or data from Calendar, Contacts, Reminders, and Photos must first get your permission.	This helps thwart information leakage through control of shared application services. Be sure to also enable Limit Ad Tracking.
Shared Photo Stream	Share photos with people you choose. Friends using Apple devices get the photos delivered immediately within native apps, with the ability to like individual photos and make comments.	Photos of work-related activities, including whiteboard images may be inadvertently shared with a wide audience. Location tracking can pinpoint work locations.
Offline Reading List	Full web pages—not just links—are saved in your Reading List.	This utility can leak business info as the Reading List is synced between personal devices via iCloud.
Facebook integration	Users can share a photo to Facebook from within camera or photo apps and post their location right from Maps. Facebook events are integrated into Calendar and Facebook friends' profile information is integrated into Contacts.	Users are told, "you need to sign in to Facebook only once, and you'll be off and sharing." While that may be personally convenient for users, instant sharing via social media is an IT security risk.

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.

Consumer devices present security challenges to enterprises

As mobility and workplace flexibility transform the way today's organizations operate, consumer devices have surged in popularity within the enterprise. Tablets and smartphones provide new flexibility and convenience for people to choose the right kind of device for each task and location, helping the organization increase workforce productivity, mobility and agility. However, as a significantly different type of device than the traditional enterprise endpoint, the embrace of tablets and smartphones requires a thoughtful, fully informed approach by IT. This includes everything from their mobile operating systems to their hyper-mobility to the way people are accustomed to interacting with them.

For organizations to maximize total value of ownership for these devices, IT must address several challenges. One is to incorporate them into a culture of self-service from any device; in this scenario, people can choose their own enterprise applications for a truly customized workspace, rather than being constrained by traditional rigid IT control over resources, which greatly limits workforce mobility. IT must also ensure that people can access and sync all their enterprise files on-demand and collaborate securely, from any device or location, and enable effective data management, sharing and backup in the cloud. Most fundamentally, IT must deal with several new concerns about protecting security and access to enterprise applications. These include:

- **Increasing demand** – With the consumerization of IT and bring-your-own-device adoption, people—including employees as well as contractors and other third parties—are demanding access to their business resources using tablets, smartphones and other devices that enable mobility and productivity. This is especially true for executives and younger generations, who often need multiple devices and readily adopt the latest and greatest technology. People in general rarely understand the technical issues or security concerns that prevent IT from providing immediate access from consumer devices.
- **Proliferation of unmanaged devices** – Most organizations' application, networking, systems and security architectures are not designed to support tablets, smartphones or any other unmanaged device on the enterprise network. Traditional infrastructure and security models assumed end-to-end ownership and device control, so IT fears security breaches and loss of control of the infrastructure as new, privately-owned devices connect to enterprise networks. For example, while the security infrastructure is set up to detect attacks over the Wi-Fi controlled by the organization via IDS and IPS, with Bluetooth and P2P Wi-Fi in place, this assumption is broken as smart devices build Bluetooth and other peer-to-peer networks.
- **The use of consumer cloud services** – Consumer-focused cloud services can be a tremendous boon to productivity, freeing people from mundane tasks such as backups and the synchronization of information across devices. But it also causes security concerns as enterprise data that resides on the device could be backed up in a consumer cloud, where it can be shared with an endless tapestry of cloud-connected endpoints and is thus out of the company's control and in violation of its policy.

- **Rapid business change** – The business climate has changed substantially in recent years. Traditional project cycles, budget priorities, connectivity and access to information have all evolved rapidly. Security must evolve to meet the changing needs of both people and the business.

To balance regulatory security requirements and user demands for more functionality, organizations need a mobility-centered IT architecture that focuses on data control instead of overdependence on device ownership. The good news is that by enabling a security architecture centered on mobile applications, desktops and data, and complemented with virtualization, IT can solve longstanding security problems and protect sensitive data regardless of access method, device type, network connection, device ownership or location.

Unmanaged devices and BYOD challenge traditional security policies

In tandem with consumerization, many leading organizations have created or are considering BYOD initiatives, which encourage people to bring their personal devices to work in order to increase mobility and productivity. BYOD initiatives also free IT from burdens of device ownership and management while giving people the freedom to choose personal devices such as tablets and smartphones to optimize their productivity. A recent Citrix survey showed that the current average number of devices connecting to the corporate network is 5.18 per knowledge worker—4.43 devices across all workers—and predicted to rise to almost six devices by 2020.[1]

BYOD sounds like an attractive proposition—until you factor in security. Unmanaged devices represent a threat to enterprise networks, including the potential for security lapses that expose confidential business information or sensitive data—not to mention possible damage caused by malicious insiders. For this reason, enterprises have long been wary of allowing anyone, outsiders or employees, to plug unknown devices into their networks.

Allowing tablets, smartphones and other unmanaged devices onto the network requires a new way of thinking about security. This includes coming to terms with a shift in the concepts of inside and outside. Many people now connect to enterprise systems over networks that are not under enterprise control, such as those in airports, hotels, coffee shops and at home. With people more mobile than ever, organizations need a new concept of data boundaries that transcends traditional network boundaries. The system must seek to establish trust and verification for all sensitive data access, instead of immediately granting access based on whether IT owns the device or whether it is plugged into an internal network. The best way to protect truly sensitive data while supporting the needs of internal and external users is through a trust-but-verify security model where all devices and users are considered as outsiders. The challenge of this model is to provide a seamless user experience in a cost-effective way.

Today's threats against confidential business information and sensitive information

To enhance the security model to support mobile devices such as tablets and smartphones, it's worthwhile to review the challenge at hand: protecting and securing sensitive data at all times while allowing unfettered access to public data. With more personally owned and managed mobile devices tapping into enterprise IT resources, information security becomes highly dependent on situational information, such as security of the device, its location, the user, and the network and the applications being used.

Malware is a familiar and critical threat, encompassing additional risks including viruses, Trojans, spyware, root kits and other attacks that are top-of-mind concerns for IT. However, malware is not the primary or the only challenge to mobile information security. Any data use policy that allows access to sensitive data by unmanaged and highly mobile endpoints will need an enhanced security architecture to protect against all of these threats, including:

- **Data exfiltration** – the unauthorized movement of data outside the control environment and general data loss
- **Data tampering** – the unintended or unauthorized modification of data
- **Data unavailability** – the unavailability of data when it is needed

These security issues correspond to business risks surrounding the confidentiality, integrity and availability of resources. Organizations must protect against any attack that would compromise these business mandates. Control measures begin with a well-architected security architecture that includes enterprise mobility management, Windows application and desktop virtualization and data sync and sharing, and further specifies configuration steps to protect individual data elements.

How the security of mobile devices is different from the security of a legacy PC

A security architect tasked with securely allowing iOS devices in the enterprise has to approach the issue from the standpoint of data protection—not from the perspective of current and familiar control measures. For example, insisting on mapping existing control measures such as 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.

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 model 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	Unavailable	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 rooting	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
- Android application framework with robust implementations of common security functionality such as cryptography, permissions and secure IPC
- Technologies like ASLR, NX, ProPolice, safe_iop, OpenBSD dlmalloc, OpenBSD calloc and Linux mmap_min_addr to mitigate risks associated with common memory management errors
- 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 that 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 new Bouncer scanning feature will also 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 it is world readable. This implies that if any file is to be shared between applications, the only way to do it is 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 Menu/Settings/About/System Upgrades—to determine if the platform can be upgraded. Also, check whether the carrier has installed CarrierIQ in the build for support. CarrierIQ can be configured to capture sensitive information and should be disabled. BitDefender has an application that will show if CarrierIQ is installed.

Support for active content, including Flash, JAVA, JavaScript, and HTML5 allow 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, rogue apps that unknowingly subscribe to nefarious services, sending personal information—eroding privacy and even remotely controlling the device. This is especially true for applications from rogue app stores, which have not been security-reviewed and vetted. While features in Jelly Bean promise to significantly reduce these vulnerabilities, it's recommended that Android devices are hardened to provide a more robust security posture.

The iOS security architecture overview

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:

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.

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 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.

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:

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 that 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 should reduce the likelihood of this, but the platform is too new for in-depth real-world data.

Without much experience in the new platform, issues such as version upgrades–especially across hardware generations—is still mostly unknown. As with other mobile platforms, this could leave a Windows user with an otherwise viable device from being able to install the latest OS and security patches.

The default user runs as Administrator, giving much too much access for normal day-to-day work. It's recommended that a separate user is 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.

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, and enterprise data sync and sharing)

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 datacenter 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
Data loss	• Loss of device • Unapproved physical access • Application vulnerabilities	• Managed data on device • Device encryption • Data encryption • Updates and patching

Threats and corresponding mobile security measures (with enterprise mobility management, Windows app and desktop virtualization, and enterprise data sync and sharing)		
Threat	**Threat vector**	**Mobile security measure**
Malware	• OS modification • Application modification • Virus • Rootkit	• Managed operating environment • Managed application environment • Architecture*

* 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. XenMobile and XenDesktop can be configured to keep highly sensitive data in the datacenter and never copied to a mobile device. Citrix Receiver will enforce those policies on the mobile device. Data that must be mobilized can rely on ShareFile, which gives people access to their files and IT the flexibility to remotely wipe them from mobile endpoints. Applications that must be mobilized and controlled can utilize XenMobile MDX technologies for app containerization. Access to enterprise email, intranet and web apps are automated and secured through the WorxMail and WorxWeb features of XenMobile. Any device that would benefit from the strong control environment of mobile device management can utilize XenMobile MDM.

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 Receiver serves as the unified app store on the mobile device, enabling access to both productivity and business apps as well as enterprise data via ShareFile. Beyond providing access to apps and data, Citrix Receiver serves as the remote access mechanism for centrally hosted applications and Windows desktops delivered by XenDesktop. By providing remote mobile access to centrally hosted resources, IT can keep sensitive data in the datacenter, where it can be kept safe and secure. Citrix Receiver, with data sync and sharing powered by ShareFile, can also be used to enable offline data access on mobile devices. IT can use ShareFile to enable access to non-sensitive data or configure ShareFile via XenMobile to containerize sensitive data and implement a host of data control policies to block user leaks. When configured to containerize data, ShareFile can be used to remotely wipe the data contained on the device at any time, or in an automated fashion based on an event such as device jailbreak. Whether an organization keeps sensitive data in the datacenter, contains it on the device, or allows it to go mobile, IT can execute and enforce these policies through Citrix Receiver, ShareFile and XenMobile.

Citrix Receiver and Citrix-secured mobile apps take advantage of Citrix NetScaler Gateway for strong authentication and encryption of network traffic. The NetScaler Gateway SSL/VPN complements the XenMobile app-specific VPN, offering enterprise mobile and web apps backend access for application specific networking security. Citrix Receiver also serves as an integral component of XenMobile for 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 Receiver protects configuration data, screen bitmaps and the user workspace. Citrix Receiver utilizes native mobile platform functionality to encrypt data at rest and in motion through Wi-Fi and 3G/4G network interfaces.

How Citrix XenMobile helps protect apps and devices

XenMobile provides mobile device, app and data freedom. People have quick, single-click access to all their mobile, web, SaaS and Windows apps from a unified app store, including secure productivity apps that seamlessly integrate to offer a great user experience. 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/stolen devices. 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. With XenMobile, IT can:

- **Unify control over remote access to apps and data.** Citrix's 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—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 the enterprise bubble being wiped in the event of a problem—not the entire device. Enterprise email and contacts are isolated, protected and controlled by the bubble, not by the device. This is a more appropriate approach for BYOD. Work and personal email are also separated through the sandboxed approach, which helps keep email and contacts separate.

How ShareFile helps protect data and files

In addition to robust managed data sharing and syncing capabilities, and integration with XenMobile and Citrix Receiver, ShareFile 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 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** with the ability to mark entire folders in addition to individual files for offline access on mobile.
- **Increase availability** through offline access to entire folders, complemented with support for document editing.

ShareFile also integrates easily with XenMobile to support role-based provisioning and de-provisioning of the service, two-factor authentication, policy-based controls and real-time application monitoring. In addition, ShareFile has adopted Health Insurance Portability and Accountability (HIPAA) Security Policies and Procedures (HIPAA Security Policy) intended to comply with the requirements of the Security Standards for the Protection of Electronic Protected Health Information and the Health Information Technology for Economic and Clinical Health (HITECH). The solution is certified under the U.S./E.U. Safe Harbor Program.

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 for allowing consumerization and BYOD strategies in a safe and controlled manner. Citrix recommends the following user and administrator guidelines when using Citrix Receiver with Android, iOS and Windows tablets and smartphones.

Recommended user actions

Users have a responsibility to protect their organizations' sensitive business information. They can control device set-up and configuration, have good daily use practices, use XenMobile, Citrix Receiver and ShareFile 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

Device setup and configuration	
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 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 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 SkyDrive
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

Device setup and configuration	
Network and Wireless	Utilize only trusted networks, ensure network encryption and utilize a VPN or micro-VPN to provide encryption regardless of underlying network capabilities; the WorxWeb feature of XenMobile enables application-specific 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

* 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.

Device setup and configuration	
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
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

Device setup and configuration	
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 SkyDrive accounts, which are tied to sensitive data.

Citrix Receiver use

- Log out of Citrix Receiver when finished working with truly sensitive data.
- Use Citrix Receiver to connect to applications and data that are most accurately viewed in their native application.
- Disable client drive mapping for mobile device file system when local storage of enterprise information is not desired.

Additional Considerations

- 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 configure it via XenMobile to contain sensitive data.
- 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).

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.
- 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.
- 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 the allowed NetScaler Gateway authentication methods from the following:
  - No authentication
  - Domain only
  - RSA SecurID only

– Domain + RSA SecurID

– SMS authentication

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, which is a sandboxed, user friendly mail client, can be used to control email and its attachments with granular data control policies.

Conclusion

Consumer devices are enabling new usage models for the enterprise—models that force organizations to adapt to the new security challenges of rising IT consumerization and BYOD initiatives, mobility and changing demands on IT from the business. Citrix Receiver, with more than 10 million downloads to date and one of the top free business applications in the respective application stores, enables Android, iOS and Windows tablet and smartphone users to work and play from anywhere with full access to enterprise applications, data and desktops. With a centralized approach to security that protects sensitive enterprise data and confidential business information, Citrix offers 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—and confidently say yes to enabling personally owned and enterprise-issued Apple, Android, Blackberry and Windows-based consumer devices across the entire organization.

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 Citrix Receiver, XenMobile and ShareFile in addition to enterprise mobile application management security features.

For a demonstration of Citrix Receiver capabilities, simply download Citrix Receiver for Android from the Google Play store, the iOS version from the iTunes App Store or the Windows version from the Microsoft store. Additionally, you can try Citrix Receiver for mobile devices with a Citrix-hosted cloud environment and be up and running in minutes, whether or not your company runs a Citrix environment.

Version statement: This document is current for Android 4.2, Apple iOS 6.1 and Windows 8.0 as of April, 2013.

For additional information, about Citrix BYOD solutions and secure-by-design technology, please visit www.citrix.com/byod and www.citrix.com/secure or read our related papers.

Additional Resources

- 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
- Citrix Receiver: How It Works
- Try Citrix Receiver

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
- iOS security

Android

- Jelly Bean, Android 4.2 features

Windows Phone and Surface

- Windows Phone 8 security and encryption

1 Citrix, Workplace of the Future: a global market research report, September 2012

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 the cloud company that enables mobile workstyles—empowering people to work and collaborate from anywhere, easily and securely. With market-leading solutions for mobility, desktop virtualization, cloud networking, cloud platforms, collaboration and data sharing, Citrix helps organizations achieve the speed and agility necessary to succeed in a mobile and dynamic world. Citrix products are in use at more than 260,000 organizations and by over 100 million users globally. Annual revenue in 2012 was $2.59 billion. Learn more at www.citrix.com.