XenMobile Technology Overview

Mobility is a top priority for organizations. Why? Because more employees than ever before are demanding access to the apps and data that will make them productive on the go. But this isn't as easy as it was in the past.

CITRIX®

Employees want access to apps and data from any mobile device, including their own personal devices. In addition, the apps that people need to get their jobs done have expanded beyond mobile email to include Windows, datacenter, web and native mobile apps. However, for IT, allowing users to access all of their apps and data from untrusted devices raises significant security and compliance concerns.

Until now, there have been two main options for meeting users' mobility requirements. IT could either secure and manage all those devices, apps and data with a complex array of point solutions, creating management headaches and security silos, or require people to use different devices for different activities, leading to user frustration. Enterprises needed an integrated approach that would allow people to be fully productive while addressing security and management concerns. Such a solution would enable IT to secure and manage mobile devices, apps and data from one centralized point, and set app and data policies based on device ownership, status or location. Users would be given secure access to email, web and documents, and the ability to self-select the rest of their apps from a unified corporate app store—all with a beautiful user experience on any device. This solution is XenMobile.

XenMobile is a comprehensive solution for managing and protecting mobile devices, apps and data, and giving users the freedom to experience work and life their way. Its features include:

- Mobile device management (MDM) for configuring, securing, provisioning and supporting mobile devices
- Mobile app management (MAM) for complete management, security and control over native mobile apps and their associated data
- Sandboxed apps including email, browser, file sharing and editing, note taking, task management, and collaboration
- Multi-factor single sign-on (SSO)
- Shared devices - i.e. the ability to share apps and data among multiple users with MDM and MAM control

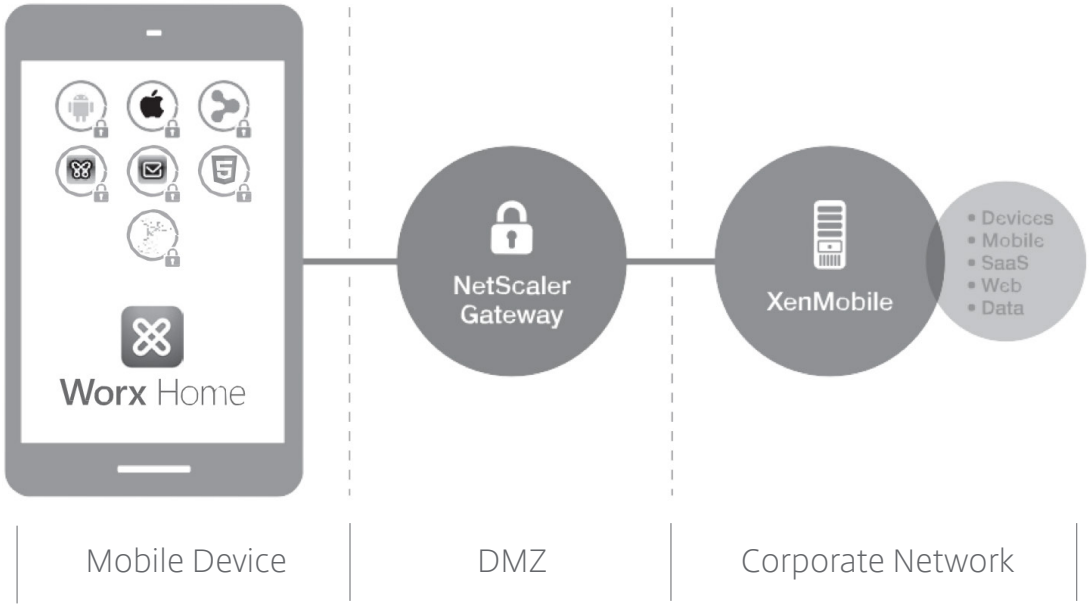


Figure 1: End-to-end enterprise mobility management architecture

The following sections detail how XenMobile delivers these features and benefits.

Mobile Device Management

XenMobile MDM provides role-based management, configuration and security of corporate- and user-owned devices. IT can enroll and manage devices; blacklist or whitelist apps; detect devices that are jail broken or out of compliance and block their ActiveSync email access; and perform a full or selective wipe of a device that is lost, stolen or out of compliance.
With XenMobile MDM, IT can perform the following actions:

Configure

Administrators configure both the server-based solution and devices through a web-based administrative console. They can create groups directly or configure the solution to read Microsoft® Active Directory® to import groups, user accounts and related properties. Note that Active Directory integration is direct, meaning that each device-server interaction (e.g., device authentication, policy

deployment) prompts a query to the directory. This is unlike solutions whose on-premises products sit in the DMZ and cache Active Directory data in the product.

Administrators can also configure XenMobile MDM to make requests to a central certificate authority such as Microsoft Certificate Services to enable certificate-based authentication for Wi-Fi, VPN and Exchange ActiveSync profiles. The solution acts as a client to Microsoft Certificate Services and requests certificates on behalf of users with enrolled devices. In other environments, the administrator can accomplish this through the solution's Universal PKI mechanism, which will make a web services call to the PKI server.

Administrators configure devices via a wizard-based configuration workflow in the administrative console. They can specify (based on operating system type, or version and patch levels, for example) which devices are permitted to enroll and receive policy profiles; designate devices as corporate- or user owned (and, if they choose, upload corporate asset metadata from an asset or configuration management database); and configure platform- or OS-specific device settings such as passcodes, encryption, ActiveSync email, Wi-Fi, VPN and PKI. If they choose, they can also deploy a certificate to the device for automatic access to Wi-Fi and other enterprise resources. IT can also restrict default apps and device resources, as well as blacklist or whitelist apps.

Provision

Administrators can provision access to users by finalizing and scheduling delivery of the profiles they create during the configuration process. They can make it easy for users to enroll their devices using self-service. They select the enrollment mode and method (email or SMS) to push the enrollment invitation to users. They can send out an invitation URL, enrollment PIN, enrollment password or any combination of the three. They can also specify whether users can use the self-help portal. Users can self-enroll either by downloading Worx Home, a combined MDM and MAM agent, or upon receiving an invitation from the administrator. The user downloads the agent, accepts the terms and conditions and completes a wizard-based series of profile and certificate acceptances. If given access to the self-help portal, users access it via a web-based console and can perform basic functions such as enroll and locate, lock and wipe a device.

Secure

Besides configuring device security settings, IT can take further security actions in the event of loss, theft or user departure from the organization. These include the ability to locate, track and geo-fence devices, lock a device if it is lost, wipe a devices if it is stolen and selectively wipe a BYO device if the user leaves the organization. The solution maintains an audit trail of administrator actions and integrates with security information and event management systems for threat correlation, forensic analysis and compliance reporting.

Support

IT can provide help desk functions, remote support and troubleshooting for mobile users. These

include viewing mobile alerts and information via a one-click, interactive dashboard. IT can drill down into and remedy device issues individually or by group.

Monitor and report

IT can monitor and report on device and app inventory, device status and security, and compliance status. IT can also integrate log management and security information and event management systems by exporting logs in syslog format to those systems. This integration can be used to pull mobile evidence into the threat picture during real-time network event analysis as well as for after-the-fact auditing, such as reporting on administrator actions like device wipes.

Decommission

IT can decommission devices when they are lost, stolen or replaced, or upon user departure, in a secure fashion. The admin can do this either from the dashboard for a group of devices or in the devices tab for a single device. When a device is fully wiped, it is turned back to its factory settings and ready to be re-commissioned. When it is selectively wiped, the corporate profile and all associated apps (such as corporate email and other apps that have been pushed or made available via the corporate unified app store) are removed. Besides being secure, this process is fully auditable for compliance purposes. IT can identify inactive devices, fully wipe corporate devices and selectively wipe BYO devices. IT can also disable the full device wipe function to prevent accidental wiping of a device.

Worx Home

Available for any mobile device, the Worx Home app allows IT to enforce mobile settings and security while providing access to a unified app store and live support services. Worx Home provides a consistent onboarding and app access experience across all platforms. XenMobile communicates with Worx Home to deliver device-specific policies and Worx-enabled app policies.

When used with XenMobile, Worx Home delivers the following key features:

- **Single app for MDM and MAM enrollment –** Worx Home is the single app that connects to XenMobile for all MDM and MAM policies and app delivery. Using this single app, IT can secure and manage devices and corporate apps installed on the device.
- **Unified app store –** Worx Home displays all Windows, web, SaaS and mobile apps and data resources available to each user, subject to access policies (e.g., role within the organization, device type and status, and network conditions). Mobile, web and SaaS apps can be accessed within or outside Worx Home on the device springboard.
- **Self-service and "follow-me" apps –** Users subscribe to individual resources by selecting them from the "available" list. This selection causes corresponding application icons to appear in their workspace. In addition, because subscriptions are indexed in the XenMobile database rather than a client-side cookie, they are fluidly maintained as a user migrates from one device to the next (i.e., "follow-me" apps).

- **Integrated support service** – GoToAssist customers benefit from integration with Worx Home to provide mobile users a critical lifeline to request live support. Users can initiate service desk tickets and chat sessions instantly from a mobile device. They can also transition to full remote support sessions with their help desk team. Support technicians can retrieve rich user account and device diagnostic information to troubleshoot problems with mobile devices and apps. Technicians can also remotely view and control devices, where allowed by the device OS, for mobile support.
- **One-click setup** – Users simply enter their email address, user ID and password, and the Worx Home app is automatically configured.
- **Zero-touch update** – In the background, Worx Home periodically checks for new policies, configuration changes and updates, most of which are implemented transparently.

NetScaler Gateway

NetScaler Gateway is a secure application and data access solution that gives administrators granular application- and data-level control while empowering users with remote access from anywhere. It provides a single point for managing access control and limiting actions within sessions based on both user identity and the endpoint device, leading to better application security, data protection and compliance. NetScaler Gateway also provides per app micro-VPN, and class-leading network security and access control.

Mobile Single-Sign-On

XenMobile manages and enables access to an organization's mobile, web and SaaS apps and ShareFile data resources, without the need to constantly reauthenticate. Single- and multi-factor methods of authentication are supported.

SSO access is just one of the powerful identity management capabilities of XenMobile. Following are descriptions of its other core services:

- **Federated SSO** – SSO is set up for a given app using Security Assertion Markup Language (SAML), the increasingly popular XML-based open standard for exchanging authentication and authorization data between security domains.
- **On-demand provisioning** – Most applications with an SSO connector also have corresponding provisioning connectors. These utilize a combination of APIs, web services and SAML to support Provisioning. Provisioning tasks can be initiated on demand by subscribing to the App from Worx

Store. From a security perspective, administrators can also define the user ID and password rules that must be adhered to when creating new accounts.

App request and automated workflow

In some instances, applications will be included in the Worx Home list of available apps — for example, based on the user's role — even though the user does not have accounts for those apps. When a user subscribes to an app, the request triggers administrator-defined workflow, An app account will be created upon workflow approval, and the user will get seamless SSO to the app.

Configuring these workflows is simplified by integration of XenMobile with an authoritative data store (e.g., Microsoft Active Directory) to discover details about users, such as their titles, roles and relative positions in the organization's hierarchy. Administrators can then leverage this information to define approvers based on name, title or role, and establish an approval sequence. They can also specify parameters such as the total number of approvals required.

Mobile app management

As noted previously, XenMobile also serves as the content provider/controller for an organization's mobile applications (including homegrown apps and those sourced from third parties). From a XenMobile perspective, this means that the SSO, app enumeration, user self-service and follow-me app capabilities will work for native mobile apps just as they do for a user's other resources. For instance, mobile apps will be displayed in Worx Home alongside all of the user's virtualized Windows, web and SaaS apps.

Also, XenMobile MAM can operate entirely independently of MDM, making it ideal for bring-your-own-device (BYOD) environments. MDM enrollment is not required in order for XenMobile MAM policies, such as local encryption and data leakage protection (DLP), to be enforced.

Additional XenMobile MAM capabilities account for other unique characteristics of native mobile apps. For example, the enumeration process includes making Worx Home aware of essential information related to the specified app, such as relevant policy data, the URL for package download and min/max platform and device type requirements. Candidate apps are also "wrapped" before being published. This wrapping process injects the code required to support management tasks and policy enforcement into mobile apps. It can be applied before compiling via the Worx App SDK delivered to the app developer. In this case, the developer would add two lines of code that allow XenMobile to deliver a policy wrapper that the IT admin can configure to intercept app system calls, thereby enforcing policy at runtime. Alternatively, it can be applied to the app after compiling, which would create a new app. The former approach is more practical for third-party apps offered on public app stores, while the latter is better for non-public custom apps that have already been developed.

XenMobile MAM is powered by MDX technologies, which enable complete management, security and control over native mobile apps and their associated data. With MDX, corporate apps and data reside in a container, separated from personal apps and data, on the user's mobile device. This containerization allows IT to secure any Worx-enabled application, such as custom developed, third-party or BYO mobile apps, with comprehensive policy-based controls, including mobile DLP and the ability to remote lock, wipe and encrypt apps and data. The Worx App SDK with MDX allows IT to:

- Separate business and personal apps and data in a mobile container where they can be secured with encryption and other mobile DLP technologies and can be remotely locked and wiped by IT.
- Provide seamless integration between Worx-enabled apps while controlling all communication policies, such as ensuring that data only is accessible by Worx-enabled apps.
- Provide granular, policy-based controls and management for all HTML5 and native mobile apps, including an application-specific micro-VPN for accessing an organization's internal network. A micro-VPN avoids the need for a device-wide VPN that can compromise security.

Following are examples of the control that can be exerted at common checkpoints during the lifecycle of the app (e.g., start-up, transition from background to foreground):

- **Authentication** – forces logon via Worx Home if the user is online and is not already logged on, or at the end of the application's lease when operating offline
- **Authorization** – checks for user entitlement prior to app launch; wipes data and locks the app if the user is not entitled to it
- **Offline lease policy** – controls duration (typically days) that an app can be used offline before the user must re-establish a connection with the app store
- **App update policy** – forces an available app update to be performed or allows it to be deferred for a specified time
- **Jail broken policy** – specifies whether an app is allowed to run on a jailbroken device
- **Data control policy** – controls what users can and can't do with data resident in the app, such as copy/paste
- **GeoFencing Policy** - controls app access based on the location of the device
- A **kill pill** capable of erasing managed applications and data that does not require the device to be online in order to be triggered
- **Biometric authentication** that leverages Touch ID for authentication

Interaction between Worx Home and Worx-enabled apps

The Worx App SDX library is loaded by the Worx-enabled application to enforce the management tasks and policies listed above. Communications between the wrapped app and Worx Home are as shown in Figure 2. Both the Worx-enabled app and Worx Home share information, such as app policies, through the common authorization data store. This data is refreshed by Worx Home after each successful app enumeration, and remains persistent across reboot of the device.

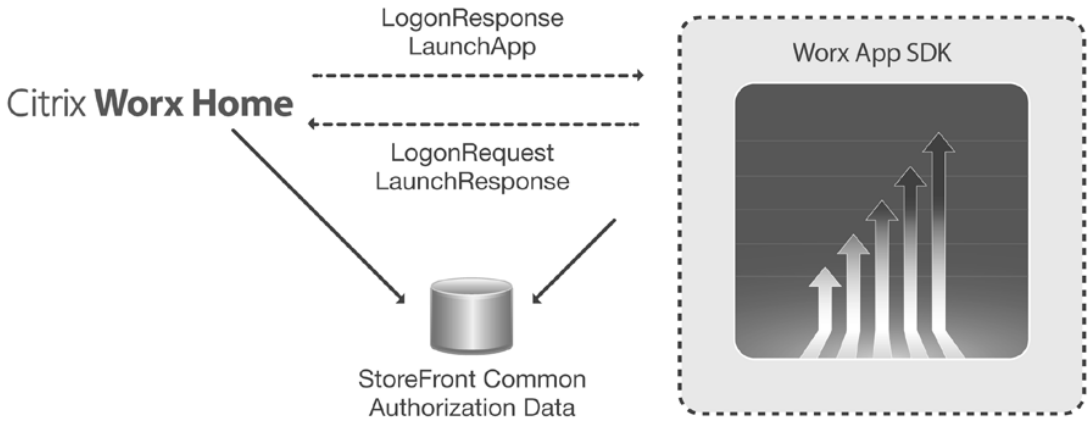


Figure 2: Mobile application delivery via Worx Home

Secure productivity applications

The suite of Worx mobile productivity apps are included in XenMobile Advanced and Enterprise Editions. These apps provide users with secure native email, calendar and contacts, a secure browser that can be encrypted and used based on IT-defined policies, file sharing and editing, note taking, task management, and collaboration. Together the Worx apps give IT the assurance that corporate content and user data are secured within a mobile container on the device and can be wiped remotely at any time. The Microsoft Exchange servers that are used are not exposed for any other type of client, and an app-specific micro-VPN facilitates Worx app intranet connectivity.

ShareFile integration

ShareFile, which is included and seamlessly integrated with XenMobile, enables organizations to securely store, sync and share data within and outside the organization. Using ShareFile with XenMobile provides IT with enterprise directory (e.g., Active Directory) integration capabilities for easy, enterprise-wide provisioning and deployment of user accounts. The combined power of XenMobile and ShareFile enhances authentication and data security while giving users the freedom and flexibility to access, share and sync data on multiple devices.

Additional ShareFile user benefits include:

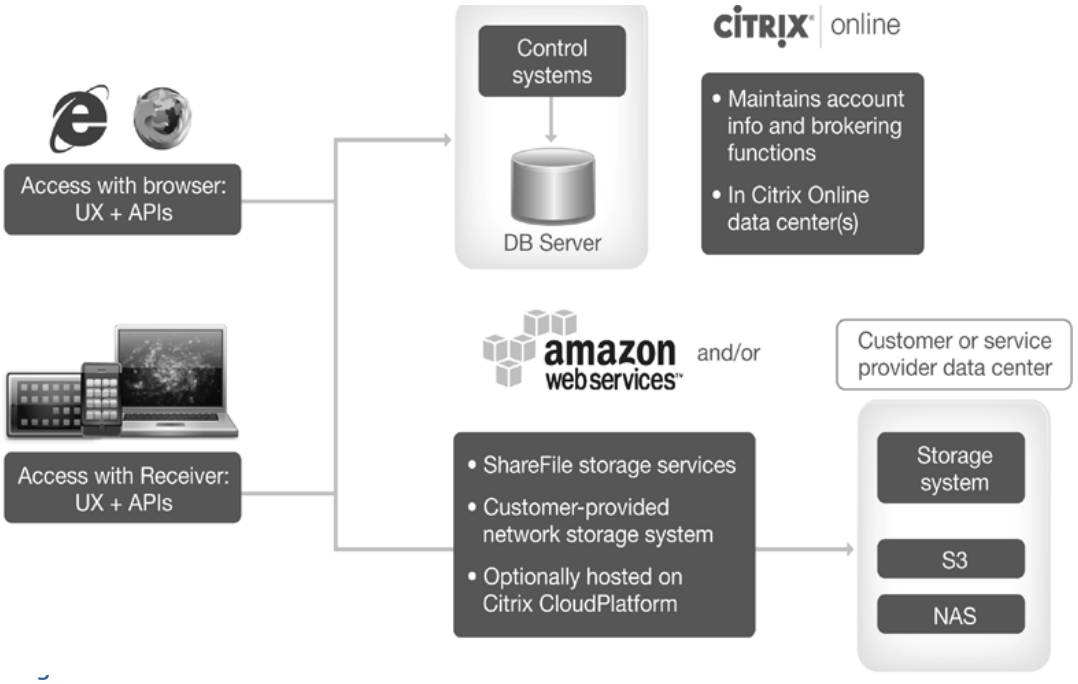
- **Easy SSO access** to corporate applications and data with Worx Home
- **Ability to view, edit, and annotate content** with editors available on the device or with Windows applications hosted by XenApp for a rich content editing experience
- **Seamless mobile access** to enterprise data in the cloud or on premises, including in corporate network shares and Microsoft SharePoint
- **Complete mobility** with offline access to corporate data

How ShareFile works

ShareFile is an IT-managed, secure data sharing service that delivers enterprise-class capabilities. ShareFile provides robust reporting functionality that enables IT to perform comprehensive logging of user activity, downloads and usage notifications, as well as granular folder permissions to control and monitor how data is accessed and shared.

The secure product architecture (Figure 3) is comprised of two components:

- **Control system** – This system is responsible for maintaining user account information and brokering functions. This information is completely protected, encrypted and stored in Citrix-managed data centers.
- **Storage system** – This is where the data is hosted. The innovative ShareFile StorageZones feature gives IT the control and flexibility to securely store data on premises, in the cloud or a mixture of both. Cloud-based storage is hosted on Amazon Web Services (AWS) with an option to use any of seven data centers in the United States, Ireland, Brazil, Japan and Singapore. The storage servers run on Amazon EC2 while the backend storage resides in Amazon S3. All files are encrypted in transit and at rest via SSL. The on-premises option allows IT to store data locally (entirely or partially) to meet unique compliance requirements, enhance performance by storing data in close proximity to the user and to build the most cost-effective solution. With the on-premises option, Citrix can support any CIFS or NFS-based network storage system and enable access to existing on-premises file stores, such as Windows network shares and SharePoint, to eliminate the need for data migration. Regardless of the customer's choice of StorageZones, the control system resides in highly secure Citrix-managed data centers.



While ShareFile and XenMobile can be sold separately, Citrix is delivering increasing levels of ShareFile functionality with each XenMobile edition. Using the two together delivers a mobile, collaborative and secure enterprise. Most importantly, using ShareFile with XenMobile provides IT with Active Directory integration capabilities for easy enterprise-wide provisioning, management and de-provisioning (including remote wipe) of ShareFile accounts and data. Additionally, users can log in to Web, Home with their [illegible] credentials (single sign-on, multi-factor authentication) and access [illegible]. ShareFile Enterprise is included

Receiver that enable access to desktops and apps). StoreFront nDesktop/XenApp environment.

s to various functions, effectively

Figure 4: StoreFront modular architecture

This modular architecture is reflected in the StoreFront administrative console, which uses the same five tabs (Receiver for Web, Authentication, Store, Gateways and Beacons) as the starting points for configuration. Under this framework, customizations are retained when upgrading to a new version.

- **Receiver for Web** – This hosted Citrix Receiver separates the display logic for browser-based users from the remaining StoreFront services.
- **Authentication** – This service provides a single-factor authentication experience for users. Submitted credentials are not only validated but also provided to other services and components as needed to keep users from having to enter them again.
- **Store** – A primary function of the Store service is the enumeration of resources available to a given user. To accomplish this, it queries designated content providers (i.e., XenMobile Server for mobile, web and SaaS apps and XML Broker for associated XenDesktop farms), aggregates the returned responses and makes adjustments to account for the "subscription" information stored in its local database. This information is then made available directly to native Citrix Receiver or via Receiver for Web for browser-based users.

The Store service is also responsible for processing user requests to launch applications. For virtualized Windows resources, this happens as it has in the past. Based on information obtained via the corresponding XML Broker, an ICA file containing the necessary details is prepared and forwarded to Citrix Receiver so that it can connect either directly to an appropriate resource server (in the case of an internal user session), or via NetScaler Gateway (for external user sessions).

- **Gateways** – This is actually not a service, but rather a dedicated container for maintaining essential gateway objects and settings and making them available for consumption by other services as needed (e.g., to generate ICA and Citrix Receiver configuration files). This approach provides greater flexibility than previous Web Interface deployments, including the ability to support configurations using multiple gateways.
- **Beacons** – The beacon's "container" stores objects used to help automatically determine whether a user is operating within the corporate network or externally. This distinction is needed to indicate whether the ICA file generated in response to a launch request should include gateway information.

  Native Citrix Receiver clients use the provided beacons. If Citrix Receiver can ping an internal beacon—a server with an address that is only accessible from within the organization—then it knows it is operating within the corporate network.

If Citrix Receiver cannot reach the internal beacon, but can reach an external beacon (e.g., www.google.com), then it knows to signal StoreFront that it is operating externally.

For browser-based users leveraging Receiver for Web, the internal/external distinction is established by a "remote" flag in the HTTP header of a user's initial connection that indicates whether the traffic is coming in via NetScaler Gateway

Conclusion

XenMobile is a comprehensive solution for managing mobile devices, apps and data. Users receive single-click access to all of their mobile, SaaS and Windows apps, including seamlessly integrated email, browser, data sharing and support apps, from a unified corporate app store. IT gains control over mobile devices with full configuration, security, provisioning and support capabilities. In addition, XenMobile securely delivers Worx Mobile Apps, which are built for business using the Worx App SDK and found through the Worx App Gallery. With XenMobile, IT can meet compliance and control needs while users enjoy the freedom to experience work and life their way.

To learn more about how Citrix helps organizations balance employees' desire for flexibility and a consistent experience with the security and control requirements of IT, access additional XenMobile resources on our website: www.citrix.com/xenmobile

Corporate Headquarters
Fort Lauderdale, FL, USA

Silicon Valley Headquarters
Santa Clara, CA, USA

EMEA Headquarters
Schaffhausen, Switzerland

India Development Center
Bangalore, India

Online Division Headquarters
Santa Barbara, CA, USA

Pacific Headquarters
Hong Kong, China

Latin America Headquarters
Coral Gables, FL, USA

UK Development Center
Chalfont, United Kingdom

CITRIX®

About Citrix
Citrix (NASDAQ:CTXS) is leading the transition to software-defining the workplace, uniting virtualization, mobility management, networking and SaaS solutions to enable new ways for businesses and people to work better. Citrix solutions power business mobility through secure, mobile workspaces that provide people with instant access to apps, desktops, data and communications on any device, over any network and cloud. With annual revenue in 2014 of $3.14 billion, Citrix solutions are in use at more than 330,000 organizations and by over 100 million users globally. Learn more at www.citrix.com