Citrix XenMobile Technology Overview | White Paper

Citrix XenMobile technology overview

The bring your own (BYO) device movement, the proliferation of smartphones in the workplace, and enterprise tablet initiatives have made mobility a top priority among CIOs. Today, the average employee uses three devices a day to get work done, and on average, owns at least one of them. At the same time, there has been an explosion in the number and type of applications created for and used on these devices. In a recent survey, Citrix found that most enterprises today support more than 200 applications in their increasingly diverse portfolios. In the near future, half of these are expected to be web, SaaS and mobile applications. In addition, most employees use personal cloud-sharing services to store files outside the corporate firewall. Collectively, these trends have prompted IT departments to seek a way to support employees who choose where, when and how they want to work, all the while securing corporate data and protecting the network from mobile threats.

What businesses need is a solution that supports these new devices, applications and data with appropriate security and policy controls. Specifically, IT wants to: manage and configure corporate and BYO devices throughout their lifecycle with enterprise-grade mobile device management (MDM); provide users key secure productivity apps like email, browser, and data sharing; secure and control custom or third-party apps in a consistent, centralized way; make any app available on any device with a unified app store; make access simple for users and give IT access control with identity management, single sign-on and scenario-based access controls. Most solutions either focus on device management with little regard to apps and data, or address the latter two without providing foundational MDM. Moreover, most solutions optimize for IT needs without factoring in the user experience. An effective solution allows employees to choose their devices, get access to the apps and data they need to get their jobs done, and all the while give IT the ability to secure corporate data and protect the network. This solution is Citrix® XenMobile.

Citrix XenMobile is a comprehensive enterprise mobility management solution that includes:

- **Enterprise MDM**
- **Secure email, browser and data sharing**
- **Mobile app containers**
- **Unified app store**
- **Identity management, SSO and scenario-based access control**

As depicted in Figure 1, XenMobile is part of the Citrix end-to-end enterprise mobility management solution, which also includes Citrix Receiver™ and Citrix ShareFile®.

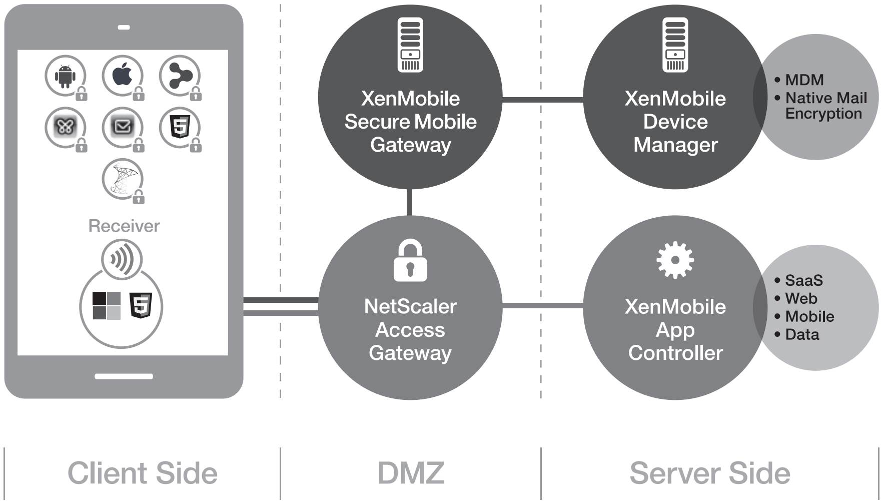

Figure 1: End-to-end enterprise mobility management architecture

The following sections detail how Citrix XenMobile, together with Citrix XenDesktop® and XenApp®, delivers the aforementioned features and benefits.

XenMobile MDM Edition

XenMobile™ MDM is the MDM component within Citrix XenMobile. It 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 jailbroken or out of compliance and block their ActiveSync email access and do a full or selective wipe of a device that is lost, stolen or out of compliance. XenMobile MDM delivers the following features:

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 an LDAP-compliant directory such as Microsoft® Active Directory® (AD) to import groups, user accounts, and related properties. Note that LDAP 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-premise products sit in the DMZ and cache LDAP data in the product.

Administrators can also configure XenMobile MDM to make certificate 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 does this by acting as a client to Microsoft Certificate Services and requesting certificates on behalf of users with enrolled devices. For non-Microsoft CA 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 six-step wizard-based configuration workflow in the administrative console. They can specify which devices can enroll and receive policy profiles (e.g., based on operating systems, OS versions, and patch levels), designate device ownership 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 self-service enroll their devices. They select the enrollment mode and method to push the enrollment invitation to users—email or SMS. They can send out an invitation URL, enrollment PIN, or enrollment password, or any combination of the three. They can also specify whether users can use the self-help portal. Users can self-service enroll either by downloading the agent or upon receiving an invitation from the administrator. The user downloads the agent, accepts the terms and conditions, and goes through a wizard-based series of profile and certificate acceptances. If users are provisioned access to the self-help portal, they can access it via a web-based console and can do basic functions such as enroll, locate, lock and wipe a device.

Secure

Besides configuring device security settings, IT can take further security action in the event of loss, theft or user departure. This includes the ability to locate, track and geo-fence devices, lock devices if they're lost, wipe devices if they're stolen and selectively wipe a BYO device if the user leaves the organization. The solution keeps 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. This includes the ability to view 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. They can also integrate with log management and security information and event management systems by exporting logs in syslog format to those systems. IT uses this integration to pull mobile 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, replaced or upon user departure in a secure fashion. The admin can do this either from the dashboard for a group of devices, or for a single device in the devices tab. When a device is fully wiped, it is turned back to its factory settings and ready to be recommissioned. When it is selectively wiped, the corporate profile and all of its associated apps are removed (such as corporate email and apps that have been pushed or made available via the corporate unified app store). 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 if they want to prevent admins from accidentally wiping a device.

Receiver

Citrix Receiver comes in two different forms.

Receiver for Web is browser-accessible and hosted by the StoreFront server. It facilitates the user's initial session until a native Receiver is installed and activated. Receiver for Web is also used for ongoing sessions on platforms that do not support a native Receiver, or when it cannot be installed for some reason.

In contrast, native Receiver is installed client software that can be launched from a user's start menu (or equivalent) and is designed to take advantage of platform-specific capabilities to deliver the best possible user experience.

Essentially a portable workspace for Windows apps, Receiver provides a consistent user interface across all client platforms. For mobile and web apps, Receiver has evolved to serve as a control point on mobile devices, so it serves as the initial delivery mechanism (unified app store), but doesn't force the user to access mobile, web, and SaaS apps via its interface on an ongoing basis. It also incorporates the Citrix ICA® client engine and other technologies needed to communicate directly with backend resources, such as StoreFront and XenDesktop.

Receiver delivers the following key features when used with XenMobile:

- **Unified app store** – Supported by StoreFront enumeration capabilities, Receiver 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 may be accessed within or outside of Receiver 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 StoreFront 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).
- **One-click setup** – The system automatically generates a configuration file. The user clicks on a button to activate and implement it.
- **Zero-touch update** – In the background, Receiver periodically checks for new policies, configuration changes and updates, most of which are implemented transparently.

Citrix NetScaler Gateway

With a few minor exceptions, Citrix NetScaler Gateway™ serves as a front end to facilitate and secure mobile sessions.

One minor difference is support for a new call-back feature, whereby the Store service within StoreFront confirms that NetScaler Gateway is indeed the source of the aforementioned remote flag, which is delivered via Receiver for Web. This is similar to a pre-existing call-back used for configurations where NetScaler Gateway, rather than StoreFront, serves as the initial point of authentication. The purpose of both call-backs is to help prevent man-in-the-middle attacks.

In addition to providing an authenticated, encrypted tunnel and multiple access modes to enable secure access by remote users, a major contribution of NetScaler Gateway is the SmartAccess feature set. SmartAccess performs endpoint analysis of the client device, such as the device type, configuration settings, and the presence, operational status and version of available security software. These properties are then evaluated against policies governing access to backend resources.

The verified information is communicated back to the Store service as part of the NetScaler Gateway response to the remote flag call-back. This information is subsequently consumed by content controllers (e.g., AppController), XenDesktop, and XenApp to determine which specific resources a user should be allowed to access and at what level, given the degree of trust associated with the user's actual operating conditions. Trust levels and corresponding security policies are defined by IT administrators, and available resources can be filtered down to the granularity of individual virtual channels (e.g., to control client drive, printer and clipboard mapping).

AppController

AppController manages and enables access to an organization's mobile, web and SaaS apps and ShareFile data resources.

With AppController, the single-factor authentication and enumeration processes and associated network communications with StoreFront are the same as between StoreFront and XenDesktop. As noted previously, however, the launch process is a bit different for web and SaaS apps. Upon receiving a launch request from StoreFront, AppController verifies that there is a credential mapping for the user/app pair in question. Assuming the mapping exists, AppController transparently authenticates the user to the requested app, effectively providing a single-click, single sign-on user experience. This is followed by a 302 redirect that establishes a direct connection between the user's browser and the desired service. XenMobile is not in the communication path.

Single sign-on access is just one of AppController's powerful identity management capabilities. Following are descriptions of other AppController core services:

- **Federated SSO** – Single sign-on is set up for a given app simply by selecting, configuring and activating a corresponding SSO connector from the extensive AppController catalog. Connector types include Formfill (where credentials from a local encrypted store or designated directory are submitted via an HTTP form post) and Security Assertion Markup Language (SAML), the increasingly popular XML-based open standard for exchanging authentication and authorization data between security domains.
- **Automated provisioning** – Most applications with an SSO connector also have corresponding provisioning connectors. These utilize a combination of APIs, web services, Service Provisioning Markup Language (SPML) and SAML to support a range of tasks, such as creating new user accounts, enabling/disabling existing accounts, resetting user passwords, unlocking user accounts and deleting user accounts. Individual tasks can be initiated either as part of an administrator-defined workflow or automatically based on periodic synchronization of AppController with an authoritative data store.

The latter option works by first establishing application-to-group mappings in AppController (e.g., the application Salesforce is mapped to the directory group Salesforce Users). With these mappings, when users are added to a group in the directory service, AppController detects this change and automatically provisions a new account for the user. Similarly, when a user is removed from the directory service group, the user account is automatically removed from the application. In this way, users can be provisioned/de-provisioned and receive immediate access to the apps they need (or in the case of off-boarding, be precluded from doing so) with no manual intervention or delay. From a security perspective, administrators can also define the user ID and password rules that must be adhered to when creating new accounts or resetting passwords.

App request and automated workflow

In some instances, applications will be included in the Receiver list of available apps—for example, based on the user's role—even though the user does not yet have accounts for those apps. Such apps will be accompanied by a Request button in the Receiver interface. Clicking on the button triggers an administrator-defined workflow that routes the app account request to designated approvers, captures their responses, reports progress to StoreFront and if appropriate, leverages the automated provisioning capability of AppController to create a corresponding user account.

Configuring these workflows is simplified by integration of AppController 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, whether approvers are mandatory, to whom a task should be delegated when a primary approver is on leave and how often task reminders should be sent.

Mobile app management

As noted previously, AppController also serves as the content provider/controller for an organization's iOS®, Android™ and HTML5 native mobile applications (including homegrown 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 Receiver alongside all of the user's virtualized Windows, web and SaaS apps.

Additional new AppController capabilities account for other unique characteristics of native mobile apps. For example, the enumeration process includes making Receiver 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 to mobile apps. It can be applied pre-compile via an SDK delivered to the app developer. In this case, it would entail the developer adding two additional lines of code that allow the AppController to deliver a configurable policy wrapper that the IT admin can configure to intercept app system calls, thereby enforcing policy at run-time. Alternatively, it can be applied to the app post-compile, which would create a new app. For practical purposes, the former approach is most 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.

AppController is powered by Citrix 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 allows IT to secure any custom developed, third-party or BYO mobile app with comprehensive policy-based controls, including mobile DLP and the ability to remote lock, wipe and encrypt apps and data. The three capabilities of MDX are: **MDX Vault**, which separates business and personal apps and data in a secure mobile container; **MDX Interapp**, which ensures all MDX-enabled apps can communicate with each other; and **MDX Access**, which provides Micro VPN, or an app-specific VPN so apps can get access to backend resources without full-bore VPN. The 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 user logon via Receiver 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
- **Jailbroken policy** – specifies whether or not 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, e.g., copy/paste.

Interaction between Receiver and MDX-enabled apps

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

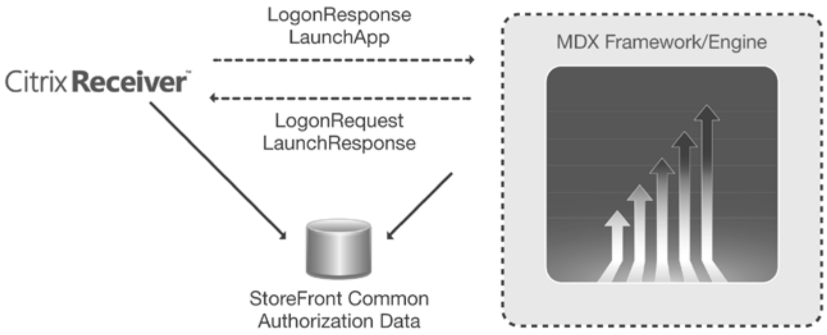

Figure 2: Mobile application delivery via Receiver

Secure mobile email and browser applications

Citrix @WorkMail™ and @WorkWeb™ are native mobile apps that are included in the XenMobile. Both apps can be wrapped and provisioned with an enterprise certificate from AppController. These apps provide users with a secure native email, calendar and contacts solution as well as a secure browser that can be encrypted and used based on IT-defined policies. @WorkMail and @WorkWeb give IT the assurance that corporate email, web content and user data are secured within the MDX Vault, a secure 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 intranet connectivity for both @WorkMail and @WorkWeb.

Citrix offers multiple email options. While @WorkMail is the most secure option because it is fully contained, Citrix also offers the ability to encrypt attachments in the native email client. IT can specify which file types are to be encrypted for example, they can specify encryption only for Excel spreadsheets. This option works best for organizations that want to secure specific documents but don't have a need to secure and contain all email, calendar and contacts.

Microsoft SharePoint integration

XenMobile also includes secure Microsoft® SharePoint® integration. IT centrally configures SharePoint document library access (folders and sub-folders) and the control policies that are tied to the documents in each based on AD group. Besides tying policies to folders, IT can also tie policies to content metadata, making it content-aware. Once resources are configured and data control policies specified, IT provisions a mobile app to users on iOS or Android devices that allows them to access the content based on the policies specified. The app has been secured with a Micro VPN and data vault for secure connectivity and data leakage prevention. It also supports document annotation. Beyond data control policies that dictate whether users can email, copy/paste, sync and take other actions on the content, IT can also set policies for automated actions to occur based on a status or event. For example, they can set a policy that will wipe the vault clean of content after a specified number of failed logins or if the device becomes jailbroken or rooted.

ShareFile integration

ShareFile, which seamlessly integrates with XenMobile, is a solution that enables organizations to securely store, sync and share data, both 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 user benefits include:

- **Easy single sign-on access** to corporate applications and data with Receiver.
- **Ability to access and edit data** with editors available on the device or with Windows applications hosted by XenApp for a rich content editing experience.
- **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 gives IT robust reporting functionality that enables comprehensive logging of user activity, download 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 datacenters.
- **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 one of seven datacenters 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 datacenters.

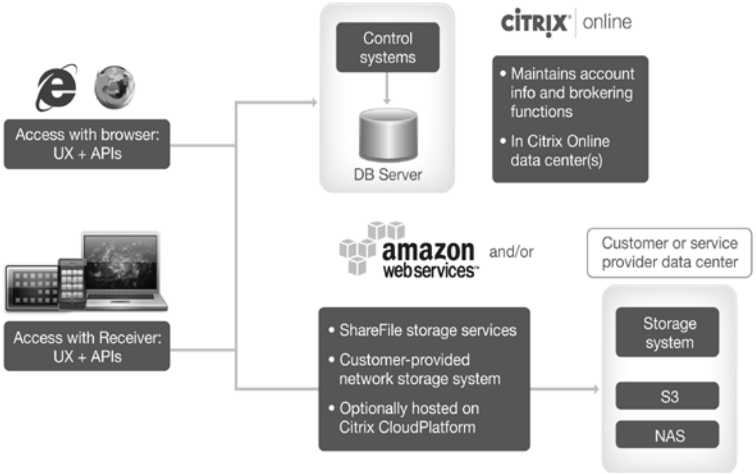
Access with browser: UX + APIs
Access with Receiver: UX + APIs
Control systems
DB Server
citrix online
• Maintains account info and brokering functions
• In Citrix Online data center(s)
amazon webservices
and/or
Customer or service provider data center
• ShareFile storage services
• Customer-provided network storage system
• Optionally hosted on Citrix CloudPlatform
Storage system
S3
NAS

Figure 3: ShareFile architecture with StorageZones

Using ShareFile with XenMobile

While ShareFile and XenMobile are separate products, there are substantial benefits to leveraging the integration between them to deliver a mobile, collaborative and secure enterprise. Most importantly, using ShareFile with XenMobile provides IT with AD 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 Receiver with their usual credentials (single-factor or multi-factor) and access to all their documents, in addition to their apps, in a single place.

StoreFront

StoreFront provides a set of service interfaces for use by Receiver that enable access to AppController (which controls and delivers mobile, web and SaaS apps and ShareFile data resources) and XenDesktop (which controls and delivers virtualized Windows desktops and apps). StoreFront is an optional component that extends a customer's existing XenDesktop/XenApp environment and integrates directly with AppController.

StoreFront is modularized for maximum flexibility and easier updates to various functions—effectively future-proofing the deployment, as depicted in Figure 4.

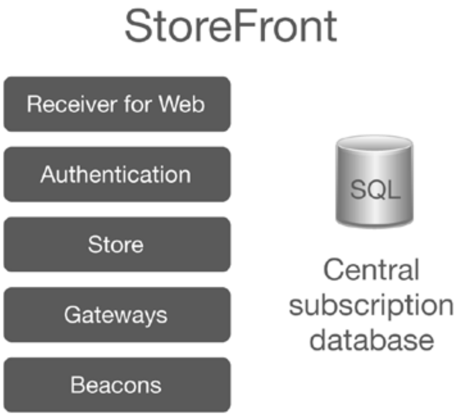

Figure 4: StoreFront modular architecture

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 not lost when upgrading to a new version.

Following are more details on each StoreFront element:

- **Receiver for Web** – this hosted 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., AppController 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 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 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).
A different launch process is used for resources managed by AppController and is explained in the AppController section below.

- **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 Receiver configuration files). This approach provides greater flexibility than previous Web Interface deployments, including the ability to support configurations using multiple gateways.

- **Beacons** – the beacons “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 or not the ICA file generated in response to a launch request should include gateway information.

Native Receivers use the provided beacons. If 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 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

Citrix XenMobile is an enterprise mobility management solution that securely delivers mobile, web and Windows® apps and data to any device, including BYO. XenMobile provides employees access to all of their business apps and data while offering IT complete control over this business content.

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

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.