Eight steps to fill the enterprise mobile application gap

Mobile devices and applications are quickly becoming as important and widespread in the enterprise as PCs and traditional business apps. Thanks to the consumerization of IT and bring-your-own-device (BYOD) programs, the workplace has expanded beyond the office and even the home to wherever the user happens to be. Traveling executives and Millennials alike expect to communicate, collaborate and access their important work applications and data from anywhere on whatever device they choose.

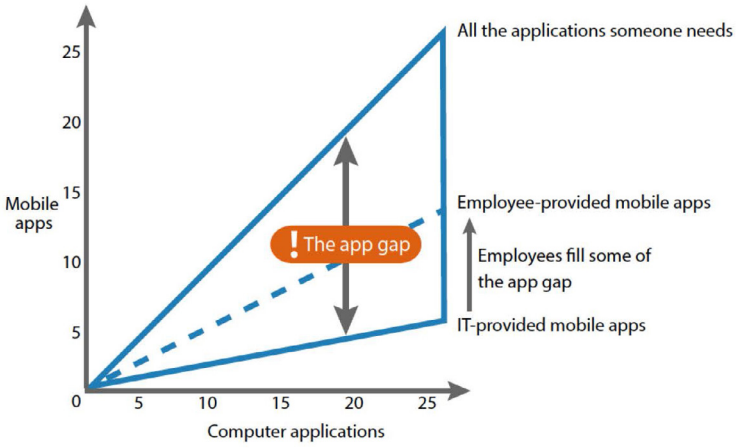
CITRIX®

Mobile agility is not just a convenience for employees, however. Mobile working and BYOD initiatives help enterprises hire the best of the younger generation and boost productivity and innovation for everyone. A recent survey of enterprise mobile users by Cisco's Internet Business Solutions Group highlighted the positive effects of BYOD on driving employee innovations that transform business processes and enhance productivity and competitive position. Most of these innovations involve mobile applications for business use.

Enterprises have caught on and are taking action. In a 2013 Enterprise Mobility Exchange survey and report entitled Global State of Enterprise Mobility for the Past, Present and Future, mobile applications were cited as a priority investment by 48 percent of enterprise practitioner respondents, followed by BYOD at 43 percent, with 70 percent citing increased productivity as the principal reason behind their mobility management investments. The report describes practitioners as mobility project owners and direct influencers of investments. 43 percent cited mobile security as a priority investment for the next 18 months, vs. 20 percent for the past 18 months.

In the meantime, many employees have been forced to use their own personal mobile applications and cloud services to fulfill their work needs. According to a 2013 Forrester report, Workforce Personas and the Mobile App Gap, 29 percent of global information workers work from multiple locations on multiple devices with many applications, and 25 percent compensate for missing IT-supported mobile applications by bringing their own applications and cloud services. Dropbox, Evernote and Skype are a few apps reported by Forrester to be used by a large percentage of mobile workers.

Result: The App Gap



Source: October 2013, "Workforce Personas And The Mobile App Gap"

Figure 1: The "App Gap" is created when employees bring in apps unsanctioned by IT.

Most use of personal applications and cloud services is unsupervised by IT, presenting a host of management and security issues. For example, cloud file-sharing and synchronization services such as Dropbox, Box and Google Drive were created with the consumer in mind, yet enterprise users harness these services regularly to store and share documents and other files containing corporate data that is sensitive or subject to stringent security and compliance requirements. Without enterprise policy controls or data leakage prevention measures, the enterprise runs a risk of data theft, particularly when personal devices are lost or stolen or when users attach files to personal mobile email or leave the organization with sensitive files still on their devices. Unsupervised use of personal applications also raises the risk of malware accessing the network when the user connects with an infected personal device.

Mobile users are also hard pressed to access preferred Windows applications when they are out of the office and limited to personal Android- or Apple iOS-based mobile devices. Much of the mobile application development effort in the enterprise is aimed at mobile versions of Windows software.

How can enterprises quickly fill this application gap with secure, managed alternatives to users' personal solutions? The first step is identifying a manageable number of mobile use cases, (email, line-of-business apps, etc.) and then creating a list of top-priority applications and other solutions for each. Then organizations can harness Citrix® XenMobile®, Citrix XenApp® and Citrix XenDesktop® to fulfill productivity needs rapidly and ensure airtight security and centralized management, even when people run these apps on the same devices they use for their personal life.

Step 1: identify mobile application use cases

The breadth of mobile application capabilities that users seek can be overwhelming for IT, particularly with the variety of mobile devices, operating systems and user roles in the average enterprise. To prioritize mobile applications and focus on those that bring the maximum return in the shortest amount of time, it helps to divide an organization into a manageable number of mobile use cases. A careful analysis of the workforce and consultation with mobile-enabled business units can help IT organizations build these use cases and set mobile application priorities.

Forrester divides mobile workers into *mobile professionals* and *mobile practitioners*, each having different mobile needs. Mobile professionals tend to be executives, managers and knowledge workers in departments such as product development, marketing and IT. They spend a lot of time at the office but also tend to work at home and on the road. They often require smartphone and tablet apps that maintain their productivity and collaborative capabilities when they're away from the office. These include email, file syncing and sharing services such as Dropbox, and Microsoft Office-type applications for creating and presenting content. They may also need occasional access to enterprise applications that are typically PC based and run on Windows.

By contrast, mobile practitioners tend to be field workers, salespeople or others who are away from the office most of the time and use their mobile devices for task-oriented applications that access and manipulate backend applications and data. For example, salespeople access CRM and ERP applications and cloud services to stay up-to-date with customer and inventory data and product information. They enter sales, expenses and other information into these enterprise apps directly from their mobile devices. Field workers may also access backend applications for scheduling information, job reporting and data entry. Full support from IT is necessary for applications that access backend databases. However, the number of mobile applications used by practitioners tends to be lower than those used by professionals.

Forrester also defines *dedicated professionals* and *practitioners* who tend to be desk bound office workers but who will likely require mobile applications in the future. For now, they tend to need some mobile collaboration and process capabilities but are not as dependent on them as their mobile professional and practitioner counterparts.

Keeping these categories in mind can help your organization define its use cases in conjunction with representatives from various business units such as sales, marketing and human resources.

Step 2: build your mobile application strategy

Once you have identified your use cases, you can start prioritizing mobile application requirements for each and developing a strategy to fulfill them. Essential to this strategy is determining where these applications can be obtained: licensed from third-party developers or off-the-shelf or native solutions; provided by cloud services; developed internally; or delivered virtually, either temporarily or permanently, through solutions such as XenApp and XenDesktop. Developing applications internally is usually the most expensive, resource-intensive option and is considered a last resort by most organizations.

Third-party applications and cloud services can usually cover mobile professionals' requirements for enterprise email, file sharing, and other collaborative capabilities. However, be sure you can provide the security and management features the organization requires to protect sensitive information.

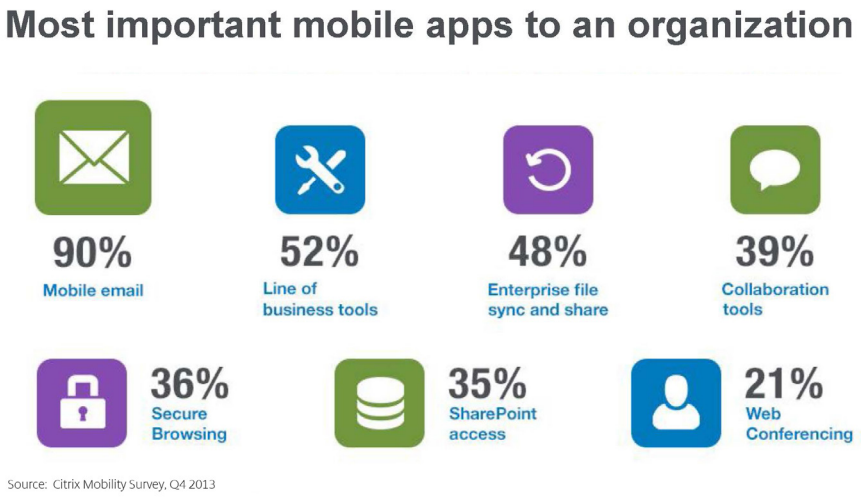


Figure 2: This is data from a recent mobility survey done by Citrix. A list of the most important mobile apps for an organization, with mobile email and line-of-business apps as the most critical.

Cloud services are worth considering for their low upfront investment, quick deployment and reach, particularly if your users travel globally. Just make sure they provide secure solutions geared to enterprises with stringent management and security requirements.

Mobile practitioner applications that conform to a specific business process are more likely to have special requirements that require custom development.

In making these decisions, organizations should analyze each mobile application from a security and policy perspective, drawing up requirements for each use case. A priority for security-sensitive organizations deploying a BYOD program is likely to be the ability to protect sensitive enterprise applications from data theft and malware and containerize them from personal applications and information on employee devices.

Citrix XenMobile: enterprise mobility management to address device, app and data security

Citrix XenMobile is a complete mobile device and application management platform that allows organizations to develop and apply policies to mobile applications and data in an enterprise BYOD or other mobility environment.

With XenMobile, IT organizations can register, provision, manage and secure thousands of enterprise mobile users, applications and devices throughout their lifecycle. Users can self-enroll their new devices for quick deployment and instantly receive enterprise policy profiles. XenMobile also includes full mobile application and data management capabilities.

XenMobile enables IT to apply a host of policies to users, groups, applications and data, including separating sensitive enterprise from personal applications and data on the device in a secure mobile container; providing application-specific VPN connections and data encryption; and preventing data leakage by controlling users' ability to cut, paste, email and print sensitive enterprise information.

Many of these policies can be applied to just about any mobile application with the Citrix Worx SDK, using as little as a single line of code. Even simpler, XenMobile provides its own highly secure mobile email, browser and file-sharing apps, and a large marketplace of Citrix-approved third-party enterprise applications that already offer the security and policy protections provided by the Worx SDK.

Finally, XenApp and XenDesktop, together with the Citrix Receiver™ client, can be used to virtualize Windows applications and deliver access from any device running just about any mobile operating system. With Citrix solutions, enterprises can develop and implement a comprehensive strategy for filling the mobile applications gap quickly and methodically, with all the security and management features they require.

Step 3: create policies for users and groups using XenMobile MDX technologies

The next step in mobilizing enterprise applications is to configure application policies using XenMobile MDX technologies. MDX provides the secure mobile container that keeps enterprise applications and data separated from personal applications and data on mobile devices and ensures they will not be visible to any user who is not included in the Active Directory groups authorized by XenMobile. MDX also lets users access a secure, unified interface to public and private app stores containing enterprise-approved applications, as well as SaaS and virtualized Windows applications.

With MDX, IT can configure policies that require enterprise authentication and endpoint analysis before permitting users to download enterprise applications and install them on their devices. Once a user installs approved enterprise mobile applications, the XenMobile Worx Home mobile application ensures that all configured IT policies are enforced.

Policies IT can configure with XenMobile MDX include:

- Permitting, blocking or restricting cut, copy, and paste operations from an enterprise mobile application. Restricting allows clipboard data to be placed in a private clipboard available only to other Worx-enabled applications.
- Permitting, blocking or restricting an application's document exchange operations. Restricted documents can only be exchanged with enterprise-approved Worx enabled applications.
- Preventing an application from using a device's GPS or network location services components.
- Preventing applications from using the device's onboard camera or microphone.
- Preventing the application from sending email messages directly.
- Requiring local database encryption
- Preventing, permitting or redirecting application network activity, such as requiring an application VPN connection to the enterprise network
- Requiring enterprise logon and authentication for application use
- Requiring re-authentication after a configured time period
- Locking applications when the device is jailbroken

Step 4: use XenMobile to provision mobile users with Citrix ShareFile® for content sharing and synchronization

One way to dissuade mobile employees from using unmanaged, unsecured cloud file-sharing and synchronizations services is to provide a secure, managed alternative such as Citrix ShareFile, part of the XenMobile solution. ShareFile offers users full, secure access to their most current files from any device while providing tight security and control over sensitive corporate information. All shared files are stored securely on the device using AES-256 encryption and all files are sent over wireless or wired networks using SSL3 encryption.

IT can also apply a host of policies to ShareFile data such as disabling copy and paste and preventing the opening of files in non-Worx-enabled applications and emailing sensitive enterprise documents. All ShareFile data can be locked or wiped remotely if the device is lost or stolen or if the user leaves the organization. ShareFile user accounts can be created and deleted using Active Directory rules, and enterprise file storage zones can be configured on-premise or via a ShareFile managed cloud.

Step 5: consider WorxMail and WorxWeb applications for managed, secure email and browsing

Many organizations begin their mobile deployment by configuring ActiveSync access to enterprise email via the native Android or iOS email application and allowing users to use the native browser. However, these native mobile solutions may not provide sufficient security for sensitive enterprise data with strict compliance

requirements. By deploying WorxMail™ and WorxWeb™ applications, part of the XenMobile solution, enterprises can offer users a native-like email and browser experience while ensuring email and web content are containerized and secured with the same policies as other Worx-enabled applications.

With WorxMail, all enterprise email, contacts and calendar items are stored separately on the device from personal applications and are inaccessible to them. All attachments are encrypted and IT can create policies to prevent users from opening, editing and saving attachments in non-Worx applications or cutting and pasting company information into other documents. IT can also require secure, encrypted connectivity to the enterprise email data store via an app-specific VPN.

WorxMail integrates with WorxWeb so all web links are opened in a secure, sandboxed environment, which prevents malware from being downloaded from insecure websites and infecting the enterprise network.

Aside from secure attachments, WorxMail enables links to ShareFile as an alternative that can provide secure file access and storage savings, without having to forward large attachments to multiple Exchange accounts.

Step 6: take advantage of the Worx App Gallery to provide users with secure, enterprise-ready applications

In addition to WorxMail and WorxWeb, the Citrix Worx App Gallery offers more than 100 Worx-enabled third-party enterprise mobile applications from more than 70 ISVs. All applications have been certified by Citrix as offering the same security policy controls and containerization as WorxMail and WorxWeb and easy integration with other parts of the Worx environment. You may find one or more secure third-party applications that can fulfill certain user requirements immediately, without any additional development required. IT admins can investigate the Worx App gallery first, to see what apps may securely fulfill employees' mobile application needs.

Step 7: Worx-enable approved third-party and internally developed applications with the Worx SDK or MDX Toolkit

Even if you can't find the applications you need in the Worx App Gallery, XenMobile allows you to Worx-enable any internally developed or third-party application with the Worx SDK or MDX toolkit using a few simple steps. Users can then download and install the applications on their mobile devices from the Worx Home screen or the mobile device springboard.

The MDX toolkit is available on the Worx Mobile Apps section of a Citrix customer's MyCitrix site and runs on a Macintosh with Mac OS X 10.7 (Lion) or 10.8 (Mountain Lion) installed. For iOS apps you need the iOS app IPA file and iOS Distribution Provisioning Profile and Distribution Certificate to sign the app for distribution. For Android apps you need the Android mobile app APK file, the Java Development Kit (JDK) 1.7, Android Software Development Kit (SDK) and a key store for signing Android mobile apps installed on your computer.

After downloading and installing the MDX toolkit, the IT admin is prompted to provide the app name, supported minimum operating system versions and a list of devices to exclude from running the app. Then you simply save a new Citrix MDX file the tool creates with MDX logic and policies to your computer and upload the file to XenMobile App Controller, which you can then use to configure app details and policy settings.

Developers can also integrate their apps with the MDX app container technology by importing a "WorxEnable.h" header file in the app's precompiled header file. For custom app behavior or further integration with the XenMobile infrastructure, developers can take advantage of Worx SDK APIs written in Object-C.

Step 8: mobilize Windows applications with XenApp or XenDesktop

For organizations that seek to provide quick mobile device access to Windows business applications, either while Android or iOS alternatives are being developed or for just a few users, Citrix offers XenApp and XenDesktop application and desktop virtualization solutions. These work together with Citrix HDX™ technologies and a Citrix Receiver client installed on the device to deliver a mobile device-friendly Windows user experience.

HDX intelligent redirection capability examines mobile client screen activity, application commands and device, network and server capabilities to determine instantly how and where to render an application or desktop activity. With its native interface control channel, it can reconfigure the Windows application interface for a mobile experience and take advantage of smartphone and tablet features such as multi-touch gestures, native menu controls, GPS capabilities and embedded camera.

Many native touch features are available for Windows apps without any application source code modifications. Other capabilities can be added using the HDX Windows Mobile Application SDK, which includes more than 50 APIs for controlling how buttons function on the device, refactoring apps to use available resolution and horizontal layout and integrating mobile device capabilities such as the camera, SMS or GPS with Windows application workflows.

XenApp is used to virtualize individual Windows applications, while XenDesktop can virtualize the

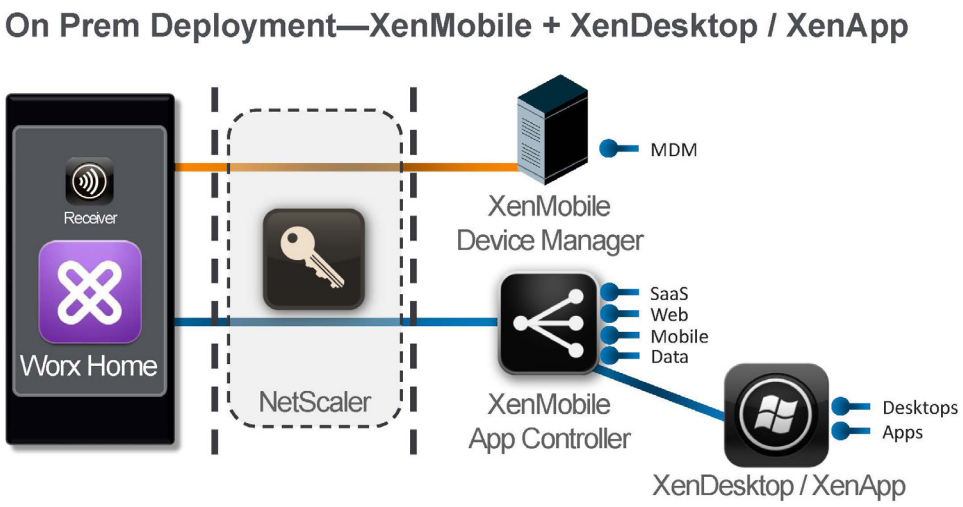


Figure 3: XenMobile + XenDesktop/XenApp architecture diagram, showing easy integration for existing XenDesktop/XenApp customers.

entire Windows desktop. Virtualized Windows applications run on XenApp or XenDesktop servers in the datacenter or the cloud.

Finally, application delivery is secured, accelerated and scaled using the Citrix NetScaler® application delivery gateway, which fulfills the most stringent enterprise needs for fast, controlled, scalable and mobile access to all Windows, SaaS and internal web applications and enterprise content from any device. One NetScaler appliance can handle up to 65,000 mobile devices and 8 million concurrent connections. It provides mobile users with advanced, secure single sign-on and authentication using Kerberos and PIN-based certificates so they don't have to remember multiple passwords. It also gives IT secure, fine-grained application access control with more than 60 application-specific policies, as well as highly granular data-level access control based on user role and device type.

Conclusion

Providing mobile users with all the mobile applications they need in a secure, managed fashion can be a steep challenge for IT. By harnessing the mobile application management and security capabilities of Citrix XenMobile, XenApp and XenDesktop together with a methodical strategy, organizations can close the mobile application gap efficiently and effectively in a short time without overspending their IT budgets.

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