Deployment Best Practices and Guidelines to Deliver Any App to Mobile Users

As organizations embrace smartphones, tablets and mobile applications, they are moving beyond simply providing mobile email and browser capability to offering mobile access to Windows-based and other corporate applications. Access to corporate applications allows mobile workers to be more productive, responsive and informed when serving customers or collaborating with peers, helping to achieve business goals such as improved customer satisfaction and faster time to market for new products and services.

CITRIX®

There are many ways to provide enterprise application access on mobile devices:

1. Deploying third-party mobile applications and services
2. Porting Windows applications to the mobile platform for each device
3. Writing brand-new, platform-specific code
4. Developing mobile web-based applications
5. Creating hybrid HTML 5 applications that also provide low-level, platform-specific access to hardware
6. Virtualizing Windows applications

When taking into account user experience, ease of deployment and maintenance and flexibility, each of these strategies has advantages, disadvantages and target use cases. There are also serious management, security and privacy issues to address in a wide open mobile world where employees use multiple personal devices for work.

Deploying third-party mobile applications

Perhaps the easiest way to provide an enterprise app for mobile devices is to wait for a third party to develop one for your target mobile platforms. This is the ideal solution for organizations that lack a skilled development staff. Even for those with such a staff, deploying a third-party application saves a lot of resources that would otherwise be spent on application development, maintenance, and updates. Third-party applications are likely be optimized for the look, feel and performance users expect on each platform.

The obvious drawback is the possibility of waiting months for such a solution to become available. Further, when it does hit the market, the application may not include all the features you need and may not support all the mobile operating systems used in your organization. You may have to purchase and deploy additional software products with different features and interfaces for other mobile devices and operating systems, if these are available at all. However, if developed properly, third-party mobile applications can deliver the best, most optimized solution for your users.

Porting applications

If a third-party mobile application is not available, porting a legacy application is one of the simplest, least resource-intensive ways to make it available on mobile devices—certainly easier than developing an entirely new mobile version of the application from scratch. In theory, if the application is written in a portable language such as C++, you can just rewrite the sections of code that are machine dependent and then recompile the program for each mobile platform. Porting is also a way to make a version of an application developed for one mobile platform, such as iOS, usable on another such as Android. Unfortunately, porting in practice is not as simple as it is in theory.

A mobile-savvy developer might be able to port a Windows application to a mobile platform successfully. However, porting is a potentially perilous path fraught with unintended consequences. In practice, it usually involves a lot more than rewriting some code and reworking the interface for a smaller screen.

Why? PC applications are geared to keyboards, mice, plentiful memory and storage, and fast processors and internal connections, none of which are typical features of smartphones or even tablets. Windows users are willing to spend a lot of time at their desks in return for a rich feature set, while mobile users are more likely to want fast access to some basic features as they're walking down the street or drinking coffee at a coffee bar. That's why simple porting may give you a poorly performing application ill suited to your users and their devices. If not skillfully recoded to provide a good user experience on a small screen, the mobile interface might require excessive pinching and zooming, making it annoying at best, and at worst, causing users to miss essential alerts, buttons and other necessary components that are at times out of visible range.

Finally, you may have to port the application to several mobile platforms, requiring even more development resources that could better be applied elsewhere.

However, if your users don't have to depend on the application to perform like the rest of their mobile apps, porting might be a viable way to save money and provide the access to corporate applications that users need.

Native application development

If a third-party mobile version of an app won't be available for a long time, and porting is not likely to provide the right experience for your mobile users, developing a native mobile application is worth considering, particularly if it is essential to your organization's mission and you have the requisite development resources.

Developing a native mobile version of an application using tools provided by the vendor offers the opportunity to rethink and optimize the GUI, display, connectivity, memory and special features such as touch and location awareness for each platform. You can include all the functions users need to be productive while leaving out those they don't. If planned and developed intelligently, a native application has a good chance of providing the best performance and most satisfying user experience. Also, it can incorporate the security features you need, including those native to each mobile platform.

The obvious disadvantages are the considerable time, complexity, expense and resources required for planning and development. For reasons of cost or skills, small or medium-sized organizations may be unable to develop native mobile applications. Some organizations may have the resources to develop to one mobile platform, but not the multiple platforms common in a BYOD environment.

In addition, in the time it takes to develop the application, your users may have selected new devices or added new requirements, making your efforts obsolete. Plus, your IT organization will have to devote additional resources to application updates and maintenance. Still, if you have the resources and face the strategic need to supply a high-performing, mission-critical application with specific features, going native might be the best solution.

Mobile web applications

For an organization with several different mobile platforms in use, developing an application that runs on a website geared to mobile devices can kill several birds with one stone. A single, mobile, web-based application theoretically will work across mobile devices and platforms, saving considerable development resources in a BYOD environment. It could be developed either as a web site or an application that fires up the browser page. Any

changes or upgrades are made once to the website and are then available to all users. Web-based applications can either be provided internally or through third-party SaaS solutions.

The drawback is that a web-based application will likely not be optimized for a single device and so will have to sacrifice performance and functionality in the process. Development will also involve tailoring it to all the mobile browsers in use.

Browser-based applications also bring up a number of security issues, particularly if people are using the same browser for personal surfing. Websites infected with malware can also infect user devices and end up on your network. Further, if you place some of the backend functionality of the web application in the corporate DMZ for easier access, these components could provide a path into the network for hackers and malware.

HTML 5 hybrid

HTML 5 provides a unique opportunity to integrate some of the cross-platform advantages of web development with the platform-specific advantages of native applications. With such a hybrid, large parts of the application can be developed in HTML 5 to work across mobile platforms, while other parts are developed separately for each platform to take advantage of their unique hardware and operating system specifications.

The HTML 5 mobile specification includes a JavaScript API to a number of lower-level features provided by individual mobile platforms. Applications developed to this specification may be able to take advantage of hardware features such as a device camera or platform features such as geo location or a haptic touchscreen. A number of third-party JavaScript libraries can provide more of these device-specific capabilities.

Performance with a hybrid application is likely to be better than with a web-only application, since this method has more hardware specificity. Development and subsequent updates will be less time-consuming and resource-intensive than for a native application developed for each of several mobile platforms. However, a hybrid HTML 5 application will likely not perform as well as a native application built solely for a particular device and will not be as customizable. Security is also likely to be tighter and easier to build into a native application as there will be better access to the advanced security features and encryption of each platform. Of course, developing natively will likely give you access to more device-specific features.

A solution that works for many organizations is to develop a native application for the most widely used or most important mobile platform and use the HTML 5 hybrid approach to cover the rest.

Virtualized desktops and applications

One of the easiest and quickest ways to provide mobile access to internal applications, regardless of their operating system, is virtually. Citrix® XenDesktop® and Citrix XenApp® are mature desktop and application virtualization platforms for virtualized access to enterprise Windows applications. Apps centrally stored in the datacenter can be accessed over the network or the application interface can be streamed and held locally on the mobile device on a secured, encrypted file system with strict enterprise policy enforcement. Administrators can even configure application streaming to provide several hours of offline application access, so that users can continue to be productive when they're out of reach of an Internet connection.

Citrix offers a set of tools for adjusting the virtualized application experience to the individual mobile device and operating system, including adding appropriate touch capabilities.

The principal advantages of virtualization are cost-effectiveness, ease of deployment, appropriateness for multiple mobile platforms and security, particularly if applications run in the datacenter. It also requires few application development resources. Performance is excellent, even over low-bandwidth connections.

However, the user experience is not as customized as that of a native application built from scratch. When only a native or third-party mobile solution will do, virtualization provides an excellent temporary solution.

Managing and securing applications

Regardless of which type of mobile application development solution you choose, Citrix offers a solution to manage and secure it.

Citrix XenMobile® is a comprehensive enterprise mobility management (EMM) platform that IT can harness to discover and manage all mobile devices and applications in the enterprise, whether native, third-party, web-based or hybrid. With XenMobile capabilities, administrators can configure mobile management servers via a web-based administrative console and import user groups and accounts from Microsoft Active Directory. Users can then self-enroll their mobile devices quickly, after which the devices are configured automatically with IT-provisioned policies and applications. Users can also download other approved applications via a single enterprise app store, similar to iTunes, and IT can limit installation of unapproved applications through application blacklisting and whitelisting policies.

Securing dual-purpose personal and work devices and their business applications and data is essential, as personal applications and Internet use pose a serious security hazard, to applications and sensitive data stored on the device, or located on the enterprise network. Not only may users inadvertently download malware-laden applications or make sensitive data available to unauthorized users via their mobile applications, but hackers can use unprotected mobile devices, browsers and applications as a path into your enterprise network. Mobile devices are also frequently lost or stolen, potentially making sensitive enterprise data and applications available to unauthorized users.

With XenMobile, IT can configure devices easily with role-based enterprise authentication and access policies, and implement application restrictions that can prevent corporate applications—including native, ported and third party—from sharing sensitive data or interacting in any way with any vulnerable personal applications on the same device. With Citrix ShareFile®, which is integrated into XenMobile, organizations can provide mobile users with a secured, encrypted file and data-sharing solution similar to less- protected consumer services such as Dropbox.

The Citrix Worx SDK can add extensive mobile policy definition and enforcement to any enterprise-developed or third-party line of business applications, including ported Windows applications. With Worx, IT can enforce data encryption and password authentication and provide an encrypted, application-specific micro VPN for secure enterprise access. IT can also set up and enforce policies for restricting or preventing data sharing among mobile device applications and prevent users from cutting and pasting data from one application to another, including email.

You can apply the SDK either during application porting or development or afterward as an application wrapper that adds these capabilities in as little as a single line of code.

XenMobile users can jump-start the delivery of secure, managed mobile applications with the Citrix Worx App Gallery, an online marketplace of Citrix and third-party Worx-enabled mobile applications. The Worx App Gallery contains more than a hundred third-party Worx-enabled applications that provide scores of useful mobile functions. All Worx-enabled mobile apps come with enterprise level security, policy and provisioning controlled by XenMobile. Administrators can simply select the Worx apps most useful for employees and deploy them to the enterprise app store for download.

In the event a mobile device is lost or stolen, or the user leaves the organization or changes roles, XenMobile enables IT to lock the device and wipe sensitive applications and data remotely.

Enterprises can deploy and require users to use the Citrix WorxWeb™ mobile browser. WorxWeb ensures that all links, including enterprise web- or HTML 5-based applications or third-party SaaS services, are opened in a secure, sandboxed browser environment that prevents hacking and introduction of malware into the enterprise application environment.

The Citrix NetScaler® application delivery controller gives mobile users remote access to web-based and virtual applications using highly granular IT-configured controls that prevent the wrong users from accessing applications and sensitive data. NetScaler can provide encrypted SSL connections to the enterprise network, as well as application-specific encrypted micro VPNs when necessary. NetScaler is also a powerful application load balancer that maintains reliable performance even during peak use periods, ensuring a positive user experience rather than the frustratingly slow or uneven performance that sometimes characterizes web applications. NetScaler allows enterprises to deploy their web applications securely behind the firewall, rather than in the less-secure enterprise DMZ.

Enterprises have multiple options for providing enterprise application access on mobile devices in a BYOD environment. Each has strengths, weaknesses and best use cases. However, any enterprise that needs to protect its sensitive data and comply with data privacy regulations will have to deploy solutions for managing and securing all its mobile devices and applications. No matter which enterprise application access option you choose, Citrix provides the most comprehensive solution for managing and securing devices, users, applications and data.

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.