CITRIX®

White Paper

7 best practices to securely deploy enterprise-grade apps to mobile users

Give your teams the apps they need to be productive — anytime, anywhere, on any device.

Table of contents

To get the most of out of mobility, organizations need to go beyond simply supporting email and browser capability. They also need to give employees a choice in the types of apps and devices they use, and securely deliver enterprise-grade applications — like Microsoft Office, legacy desktop apps, SaaS, and web apps — so their employees can be productive anywhere, anytime.

Here are seven best practices for deploying enterprise-grade apps:

1. Evaluate and build a mobile strategy based on your needs

There are a lot of different ways to provide enterprise application access on mobile devices. Before implementing new technology, assess your application needs and what systems currently support those needs. Understanding the bigger picture will help you create a solution that works well across the board.

When evaluating your mobility needs, determine whether or not you need to:

- Deploy third-party mobile applications and services
- Port Windows applications to the mobile platform for each device
- Write brand-new, platform-specific code
- Develop mobile web-based applications
- Create hybrid HTML 5 applications that also provide low-level, platform-specific access to hardware
- Virtualize Windows applications

Also remember to factor in user experience, flexibility, and ease of deployment and maintenance. Each of these strategies has advantages, disadvantages and target use cases, as well as serious management, security, and privacy issues to address in a mobile world where employees use multiple personal devices for work. Once you've taken stock of your varying needs and risks, you'll be better equipped to build a mobile strategy that addresses the greatest number of concerns.

2. Save resources by deploying third-party mobile applications

Perhaps the most efficient way to provide an enterprise app for mobile devices is to wait for a third-party to develop one for your mobile platforms, especially if you lack a skilled development staff. Even for organizations with such a team, deploying a third-party application saves a lot of resources that would otherwise be spent on application development, maintenance, and updates. What's more, third-party applications are likely already optimized for the look, feel and performance your users will expect on each platform.

Of course, there are sometimes drawbacks. Often, when using a third-party app, organizations need to wait months for such a solution to become available. When it does hit the market, the application may not include all the features you need, or it may not support all the mobile operating systems used in your organization. In that case, you'll likely have to purchase and deploy additional software products with different features and interfaces for other mobile devices and operating systems (if they're available at all). However, if developed properly, third-party mobile applications can deliver the best, most optimized solution for your users.

3. Port applications when third-party options are not available

Porting a legacy application is one of the simplest, least resource-intensive ways to make apps available on mobile devices. It is 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 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 usable on another. For example, an iOS becomes usable for one like Androids.

Like many things in life, 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 tablets.

Another factor when using third-party applications is user experience. 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 more likely to be working while on the go or at a remote site. Keeping your end user in mind is crucial for successful third-party app implementation because simple porting may give you a poorly performing application ill-suited for the situation. In that case, skillful recoding will be required to ensure users have a good experience on a small screen, and that the mobile interface doesn't have shortcomings — like requiring excessive pinching and zooming (which could cause users to miss essential alerts, buttons and other necessary components that are at times out of visible range). And, if you have to port the application to several mobile platforms, even more development resources could be required — and those resources could better be applied elsewhere.

However, if your users don't have to depend on the application to perform as smoothly as 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. Finding a solution that supports management and oversight to ensure IT maintains control of the ported app.

4. Develop native applications when necessary

If a third-party mobile version of an app won't be available for a long time, and porting isn't likely to provide the right experience for your mobile users, developing a native mobile application is worth considering — particularly if it's essential to your organization's mission and you have the requisite resources. Developing a native mobile version of an application using tools provided by the vendor offers the opportunity to rethink and optimize things for each platform, like:

Developing native applications also give you the ability include all the functions users need to be productive while leaving out those that don't. If planned and developed intelligently, a native application has a good chance of providing the best performance and most satisfying user experience. It can also incorporate the security features you need, including those native to each mobile platform.

But developing native apps has some disadvantages. It can be time-consuming, complex, expensive, and require a lot of planning and development resources. For reasons of cost or skills, small or medium-sized organizations may be unable to develop native mobile applications. And while some organizations may have the resources to develop to one mobile platform, they don't always have resources needed to develop the multiple platforms common in a bring-you-own-device (BYOD) environment.

What's more, in the time it takes to develop the application, your users may have upgraded to 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 need for a high performing, mission-critical application with specific features, going native is often the best solution.

5. Harness the benefits of mobile web applications

For an organization with several different mobile platforms in use, developing a web-based application that runs on a website geared to mobile devices can have multiple benefits. A single, mobile, web-based application will, theoretically, work across mobile devices and platforms, saving considerable development resources in a BYOD environment. Whether developed as a website or an application that fires up the browser page, any changes or upgrades can be made once to the website, and then be pushed out to all users. This saves on time and management costs. 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. As a result, performance and functionality may be sacrificed in the process. Browser-based applications also bring up a number of security issues, particularly if people are using the same browser for personal surfing. One very important example is that of websites infected with malware. They can also infect user devices and as a result, end up on your network. Further, if you place some of the backend functionality of the web application in the corporate perimeter network for easier access, these components could provide a path into the network for hackers and malware, so it's crucial that you have a solution that encompasses a layer of security as well as the flexibility to support mobile web applications.

6. Adopt HTML 5 hybrid to take advantage of different platforms

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 geolocation or a haptic touchscreen. Many 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 app 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 app for the most widely used or most important mobile platform and use the HTML 5 hybrid approach to cover the rest.

7. Get the most out of 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. A good workspace solution will offer mature desktop and application platforms for virtualized access to enterprise applications, such as Windows. Apps centrally stored in the data center can be accessed over the network or the application interface; they 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.

Another benefit of embracing virtualization is the ability to adjust the application experience to the individual mobile device and operating system, including adding appropriate touch capabilities. What's more, virtualized workspaces are often ideal because they are:

- cost-effective, as they require few development resources
- easily deployed and secure, especially when apps are run in the datacenter
- excellent in performance, even over low-bandwidth connections

While the user experience is not as customized as that of a native application built from scratch, the overall benefits outweigh concerns. And even if only a native or third-party mobile solution is required, virtualization provides an excellent solution until the native or third-party app can be created.

A complete solution to manage all aspects of app delivery

Regardless of which type of mobile application development solution you deploy, Citrix Workspace helps you simplify deployment, management, and security.

Management

The mobile component of the Citrix Workspace Solution allows your IT teams to discover and manage all mobile devices and applications in the enterprise, whether native, third-party, web-based, hybrid, virtual or SaaS.

Managing mobile solutions is made easy for end users and IT alike. Administrators can configure mobile management servers via a web-based administrative console and import user groups and accounts from Microsoft Active Directory or from Azure. Your 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.

What's more, workspace users can jump-start the delivery of secure, managed mobile applications with an app gallery, an online marketplace containing more than a hundred third-party applications that provide scores of useful mobile functions. And they all come with enterprise-level security, policy, and provisioning so users can quickly and efficiently get the apps they need.

Security

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 devices or located on the enterprise network. Not only do many 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 exposing sensitive enterprise data and applications to unauthorized users.

A software development kit (SDK) can add extensive mobile policy definition and enforcement to any enterprise-developed or third-party line of business applications, including ported Windows applications. As an important feature of the workspace, 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. This SDK can be applied 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.

Another protective ensures 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 Workspace, this mobility component is integrated into a file sharing solution so organizations can provide mobile users with a secured, encrypted file and data-sharing solution similar to less-protected consumer services such as Dropbox.

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

Citrix Workspace also has a solution for a secure mobile browser that can ensure 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 the introduction of malware into the enterprise application environment.

All of the security features are only part of the package. An application delivery controller (ADC) 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. With a robust networking solution, Citrix Workspace provides encrypted SSL connections to the enterprise network, as well as application-specific encrypted micro VPNs when necessary. This powerful ADC solution also functions as an application load balancer, maintaining reliable performance—even during peak use periods. This ensures a optimal user experience rather than the frustratingly slow or uneven performance that sometimes characterizes web applications. The networking component allows enterprises to deploy their web applications securely behind the firewall, rather than in the less-secure enterprise demilitarized zone (DMZ).

Bringing it all together

Enterprises have multiple needs, challenges, and options, for providing enterprise application access on mobile devices in a BYOD environment. Each has strengths, weaknesses, and unique use cases — but every enterprise needs a solution to simplify deployment and management, as well as secure sensitive data and comply with data privacy regulations. No matter what your unique application delivery needs, Citrix Workspace Solution provides the most comprehensive solution for managing and securing your apps and data across devices, users, networks, and clouds — all while delivering an exceptional user experience.

Find out how to give your teams the enterprise-grade apps they need.
Visit citrix.com/workspace.

Enterprise Sales
North America | 800-424-8749
Worldwide | +1 408-790-8000

Locations
Corporate Headquarters | 851 Cypress Creek Road Fort Lauderdale, FL 33309, United States
Silicon Valley | 4988 Great America Parkway Santa Clara, CA 95054, United States