Revised Edition

Mobile Application Delivery: The Next Frontier

With the influx of mobile devices and applications entering enterprises, IT departments have a new mandate: to securely and efficiently deliver reliable applications to end users.

TechTarget®

App Delivery Poses Mobile Management, Security Challenges

THE CONSUMERIZATION OF IT, including the bring your own device trend, has forced enterprises to reexamine how they provide access to corporate applications and data. Employees are more comfortable finding and using apps and storing data in the cloud, but IT administrators still need to maintain proper control and regulatory compliance.

Application and desktop virtualization, BYOD and the cloud all promise to make admins' lives easier, but IT must first determine how applications will be delivered, how mobile apps and devices will be managed, and how to maintain security amid a diversifying IT landscape. This updated handbook looks at the best approaches to take when delivering mobile applications.

In our first article, consultant Robert Sheldon examines options for mobile application delivery. App stores, private clouds, Web apps and desktop virtualization each offer different pros and cons, but you'll have to weigh ease of management and security for your own environment.

Colin Steele, executive editor of SearchConsumerization, breaks down the differences between mobile device management and mobile app management in our second article. Understanding these differences can help admins focus on where to apply more granular controls for mobile app delivery.

Finally, security expert Lisa Phifer examines specific methods for secure delivery of mobile apps. Even in combination, security approaches such as encryption and remote device wipe still need to be used alongside proper network security. ■

EUGENE DEMAITRE
Associate Managing Editor
Data Center and Virtualization Media Group
TechTarget

Assessing Four Mobile Application Delivery Options

As mobile devices continue to pervade the workplace, IT must find ways to deliver and manage the applications and services that employees need to conduct business. Some organizations might use existing consumer services to meet their business needs, such as Dropbox for file storage and sharing. In that case, workers simply go to Google Play, Apple's App Store or another public marketplace to download the Dropbox app to their mobile devices.

The challenge with this approach is that it puts sensitive company data at risk and provides little way, if any, for IT to control and monitor how employees use those services for business. In fact, public apps and services can be so risky that many organizations ban them outright. True, some consumer services now offer enterprise-level alternatives, such as Dropbox for Business, but even these might not address all of IT's security and administrative concerns.

For this reason, many organizations are looking to other approaches for delivering and managing mobile apps and services, including implementing an enterprise app store, delivering mobile services via a private cloud, building Web-based apps or implementing virtual mobile desktops.

1. ENTERPRISE APP STORES

Enterprise app stores provide a mobile app delivery platform that lets users browse and download IT-approved apps. But an app store is much more than an online catalog. Normally, it's part of a larger mobile application management (MAM) strategy that helps IT secure apps and oversee issues related to compliance, data governance, bulk purchasing and licensing. Such a solution also provides a forum for user feedback and quality control, much like consumer app stores.

Creating a private app store is no small task, however. The store must be able to control and monitor the entire application lifecycle, which includes app delivery, usage tracking, removing outdated apps and controlling which versions workers use. Implementing and maintaining this type of system can require a significant investment in resources.

In some cases, an organization can tie into a public app store, but there are limitations to these programs. For example, Apple's App Store supports only iOS devices and doesn't give IT the same degree of control available to a homegrown system. That said, a private app store should still be able to interface with the public ones, if that service is necessary.

Organizations have several options for implementing an enterprise app store. One is to build their own using such development tools as StrongNode and Titanium Studio. They can then host the app store in-house or with a cloud-based provider that offers Platform as a Service (PaaS) hosting.

On the other hand, organizations can purchase an out-of-the-box MAM solution, again, hosting it either in-house or with a PaaS provider. Companies such as Symantec, MobileIron and App47 all offer MAM software packages. In addition, all three also offer cloud-based services that let an organization set up a virtual private enterprise app store (VPEAS). In fact, numerous companies now offer VPEAS services, including BMC, FullArmor, Salesforce and Apperian.

2. PRIVATE CLOUDS FOR MOBILE APP SERVICES

Delivering apps to employees' mobile devices is only part of the challenge IT faces. More often than not, business apps need access to corporate resources, and systems need to be in place to support that access.

In some situations, business apps can interface with existing systems, such as a customer relationship management (CRM) product, in which case, the app merely taps into the available application programming interfaces (APIs) and uses the existing infrastructure.

Quite often, however, an organization must not only deliver mobile apps to its employees, but also implement a system for providing the services that support those apps. At the same time, users expect to be able to work with data in a cloud-like manner. They expect to be able to access data from multiple devices, update the data from any of those devices and have those updates automatically synced across devices. Users also expect to share and collaborate on that data with other users.

> *Taking a PaaS approach might be easier or cheaper to implement, but that means losing control over how and where sensitive data is stored.*

Many consumer apps already provide these capabilities. And that's where the private cloud comes in. A private cloud facilitates the type of data exchange users have come to expect with their consumer apps, without the risks associated with public cloud services.

To implement a private cloud, an organization can build its own or purchase one from a vendor such as Hewlett-Packard or Microsoft. Another option is to build a virtual private cloud hosted on one of the many PaaS services that have shot up in recent years, such as Amazon's Elastic Compute Cloud (EC2).

However, any option an organization chooses is likely to require a significant investment. Taking a PaaS approach might be easier or cheaper to implement, at least at first, but that means losing control over how and where sensitive data is stored.

Developing an in-house service offers IT more control, but it also means investing in the resources necessary to develop, implement, house and maintain that system across multiple mobile platforms.

Despite the costs, supporting mobile apps with cloud services offers a great degree of flexibility and provides a central access point from which to conduct and manage business.

3. WEB APPS FOR MOBILE DEVICES

Until recently, Web-based apps were considered an unrealistic strategy for providing services to mobile users, but better processors, faster connectivity and the latest generation of the Hypertext Markup Language, HTML5, have altered the landscape forever. HTML5 has been particularly instrumental in this transformation. Web apps can now better deliver multimedia and graphical content as well as support offline operations through local storage capabilities, without requiring special plug-ins.

Unlike native mobile apps, users access Web apps through their browsers, making the apps more compatible across a variety of devices. IT can develop, deliver, maintain and upgrade Web apps more easily than native apps, and it doesn't need to build multiple versions or provide a distribution system or private cloud.

Browsers are also delivering more native-like capabilities within their interfaces. In the iOS version of Safari, for example, you can make interface elements disappear as you scroll through the page content.

But Web apps still pose many hurdles for IT. For instance, whenever application-state data—the data stored in memory during a session—must be updated, a screen refresh is required. If the user's connection is less than optimal, this refresh can affect performance.

Mobile device browsers are also limited when it comes to functionality. For example, pop-ups and multiple windows are not available on mobile devices, which makes displaying alerts and error messages more difficult.

Another issue to contend with is that Web apps, unlike native mobile apps, can't take full advantage of device features such as cameras. One way to get around this is to create hybrid Web apps. The core of a hybrid app is still Web-based, but it is wrapped in a native app that can interface with other device features. This approach lets developers reuse code and create apps whose core remains platform-agnostic, which reduces development time and costs while taking advantage of the flexibility of Web apps.

IT can develop, deliver, maintain and upgrade Web apps more easily than native apps, and it doesn't need to build multiple versions.

As the Internet world continues to solidify around HTML5, we'll likely see a steady growth in the number of mobile Web apps. So promising is this technology, in fact, that even Amazon is now accepting HTML5 Web apps for their Android and Kindle Fire customers.

4. MOBILE DESKTOP VIRTUALIZATION

Desktop virtualization delivers a traditional PC environment to any endpoint, from a desktop or laptop to a smartphone or tablet. With mobile desktop virtualization, users connect to secure in-house computers that run the operating systems and applications needed to conduct business. These computers can either be servers set up for this purpose, or they can be the users' own desktops.

On the mobile device, a remote access app acts as a thin client that connects to the target computer via the Internet in order to render the virtual desktop.

Remote access services and technologies that support mobile desktop virtualization are popping up every day. Microsoft Virtualization Desktop Infrastructure, for example, lets IT deploy remote desktop services for access to Windows desktop environments and their applications.

In addition, services such as LogMeIn, GoToMyPC and Splashtop make implementing remote access from supported mobile devices fast and easy wherever they're connected to the Internet.

One of the biggest advantages of desktop virtualization is that sensitive data remains within the organization's secure environment and is never stored on the device itself, unless the remote-access service specifically supports file transfers and those transfers are permitted. Desktop virtualization also makes it easier for IT because there are no special apps to develop or app stores to implement.

For desktop virtualization on mobile devices to work, however, the user must have reliable network connectivity. Some products support offline desktops, but consistent connectivity is the key to an effective user experience.

In addition, apps that are delivered virtually don't always translate well to mobile devices, particularly on small smartphone screens. And any app that relies on intensive keyboard input and mouse actions can be particularly challenging for mobile workers. Not surprisingly, desktop virtualization is much more effective on tablets than on smartphones.

Despite the limitations of desktop virtualization, the remote-access services sector is a fast-growing market, and apps are constantly improving, providing features such as zoom capabilities and mouse-like controls.

At this point, though, these services and their apps are still used primarily to augment existing infrastructures and provide quick and easy access to desktop resources when needed. But the industry still has a long way to go before virtual desktops deliver the level of ease and productivity found through native apps.

PICK AND CHOOSE

Native apps aren't going away, which makes the app store a useful alternative for controlling mobile app delivery. However, Web-based apps and cloud-based services, as well as virtual desktops, provide flexible alternatives that will only improve as they mature.

Determining which mobile app delivery method to use is no easy choice, and the options are changing rapidly. New products and technologies come along frequently, and old ones are evolving all the time. Whatever you decide, you must remain flexible and willing to shift strategies as new technologies emerge.

—*Robert Sheldon*

Distinguish Between Mobile Device and Mobile App Management for Control

MOBILE DEVICE MANAGEMENT and mobile application management are two of the more popular technologies for enabling secure smartphone and tablet use in the enterprise. They have different use cases, but some of their features overlap, and more vendors are combining the two technologies into single products.

That means mobile device management vs. mobile application management isn't necessarily the discussion you should be having in your IT department. Instead, take into account your users' needs, your organization's security and compliance requirements, and other factors. Then you can decide which technologies will best help you meet those objectives. It may be one technology or the other, but it may also be a combination of both.

KEEPING MDM AND MAM STRAIGHT

- **Mobile device management** (MDM) takes a full-device approach to securing and controlling smartphones and tablets. IT can secure access to the device by requiring the use of a passcode and keep sensitive data out of the wrong hands by remotely wiping a lost or stolen device. Other basic features of MDM tools include the ability to enforce policies, track inventory and perform real-time monitoring and reporting.

The problem with MDM is that the full-device approach can be too heavy-handed in an era where employees, not their employers, own their smartphones and tablets. Users may wonder, "If I only use my phone to check email at night, why do I have to enter my work password every time I want to use the phone?" or, "If I lose my phone, why does my IT department want to remotely wipe pictures of my dog?"

- **Mobile application management** (MAM) offers more granular controls. MAM gives IT the ability to manage and secure only those apps that were specifically developed to work with a particular MAM product. In the example above, IT could wipe or cut off access to the employee's corporate email without deleting his dog photos. In fact, IT wouldn't even know the device contained dog photos. Admins can also use MAM to deploy apps and limit the sharing of corporate data among apps.

But MAM has its own challenges as well. Because every app requires unique coding to work with each individual MAM product, the availability of apps for a specific platform can be limited.

COMBINING MDM AND MAM

MDM takes care of basic security and controls, but mobile application management tools allow organizations to unlock the full potential of mobile devices. With MAM, IT can enable workers to get more real work done on their smartphones and tablets—which is what they want in the first place.

Some mobile device management tools can integrate with MAM to automatically deploy and update mobile apps. Others also offer mobile document management features that can tie in nicely to server-based applications such as SharePoint.

The general perception is that MDM is more of a security play, while MAM focuses on enablement. But don't sell MAM's application security capabilities short. Admins can use MAM products to create a catalog of safe, approved apps for employees to download, which supplements the blacklisting and whitelisting features found in most MDM products.

MORE MDM VS. MAM RESOURCES

- **Mobile device management pros and cons:** Understanding the pros and cons of mobile device management can help set proper expectations. MDM accomplishes some pretty important security tasks, but it can be expensive, and it doesn't protect against every kind of data leak.

- **What to get out of MDM:** All MDM products are different, especially now that the line between MDM and MAM products is blurring.

You won't need every feature offered, but knowing what's available and how it can (or can't) meet your objectives is important. With this MDM checklist, nothing will slip through the cracks.

■ **Controlling consumerization with enterprise app stores:** One of the most common MAM features co-opted by MDM vendors is the ability to build and maintain enterprise app stores. Like their consumer counterparts, such as the Apple App Store and Google Play, enterprise app stores let users pick and choose the software they want to download to their devices. Enterprise versions take extra steps, however, giving IT the power to limit users' options and make available corporate apps that aren't found in public app stores. —*Colin Steele*

Home

Editor's Note

Assessing Four Mobile Application Delivery Options

Distinguish Between Mobile Device and Mobile App Management for Control

Mobile Applications Require a Secure Foundation

Mobile Applications Require a Secure Foundation

Ultimately, mobile applications are only as secure as the foundation on which they are built—that is, the mobile devices and operating systems on which they run. So it's imperative to understand the inherent risks associated with mobile devices, the native security measures built into mobile operating systems and the best practices for mitigating risks.

UNDERSTANDING MOBILE RISKS

Lost or stolen smartphones and tablets pose a significant risk to sensitive data. Phone theft is rampant. Employers are right to be concerned, since forensic analysis of resold devices can often recover some of a previous user's data. If no security is applied, a lost or stolen device can easily lead to a breach of stored business data, including email messages, contacts, customer records, passwords and more.

Moreover, missing mobile devices enable intrusion into corporate networks and services. A smartphone configured for corporate email, Wi-Fi or VPN access can be an unlocked back door into otherwise secure systems, bypassing perimeter security. While the same can be said for laptops, users lose smartphones and tablets far more often. Lost devices almost always contain saved passwords and are less likely to verify user identity with two-factor authentication.

These data and network risks are exacerbated by mobile malware. According to Nielsen, the average U.S. smartphone has 41 user-downloaded apps. While most apps come from reputable sites such as Apple's App Store and Google's Play Store, mobile malware is growing fast—especially for the open source Android OS.

Even legitimate apps often have access to sensitive data and services such as contacts and location. A device running a malicious or overly inquisitive app, combined with access to corporate data, networks, or services, poses substantial business risk.

In fact, malware spreads by exploiting mobile OS and application vulnerabilities. Mobile ecosystems lag well behind established desktop/laptop patch infrastructure. When malware writers find a new Android bug to exploit, a fix must work its way first through Google, then device manufacturers, and then cellular network operators before being offered to mobile users. As a result, IT has little effective control over mobile vulnerability management.

Perhaps the biggest risk of all is the human hand that holds a smartphone or tablet. End users often ignore suggested updates, permission warnings and passcode prompts. According to the Information Defense Corporation, 71% of chief information security officers say that mobile devices have contributed to security incidents, largely due to careless employees who lack security awareness. User behavior poses an even greater risk given the under-secured, mixed-use bring your own device (BYOD) trend.

BEST PRACTICES FOR SECURING MOBILE DEVICES

Fortunately, many of these risks can be managed by instituting native security measures. When smartphones first emerged, they offered little built-in security. With its native encryption and over-the-air device management, RIM BlackBerry was a noteworthy exception and fostered broad business adoption, leading to emulation by other manufacturers.

When the Apple iPhone debuted, for example, it had no encryption or IT management hooks. Today, every Apple iPhone and iPad comes with an encrypted file system, can be locked with a long, complex passcode, and supports more than 150 IT-configurable policies. Although such native capabilities vary by device make and model, all four major mobile OSes—Apple iOS, Google Android, RIM Black-Berry, Microsoft Windows Phone 8—support those best practices and more.

- ***PIN or passcode.*** The first line of defense against the unauthorized use of a lost or stolen device is a robust PIN or passcode. All four OSes support numeric PINs and alphanumeric passcodes. The primary challenge is enforcing long, complex passcodes that users must re-enter frequently. Pairing shorter passcodes with secondary user authentication to open every sensitive business application is a practical way to reduce risk.

- ***Remote find and wipe.*** Most employers also want the ability to remotely locate lost or stolen devices and, when warranted, remove all corporate data from them. Again, all four OSes support remote find and wipe, but effectiveness varies.

For example, wiping an iOS device renders all personal or corporate encrypted data inaccessible. By contrast, wiping an Android device simply resets it to factory-default settings, which, in many cases, leaves recoverable data behind. Pairing remote wipe with applications that rigorously encrypt their own data makes remote wipe more effective.

- ***Stored data encryption.*** As noted, stored data encryption has become an enterprise must for mobile devices that store business data, including temporary files, message attachments, screen snapshots, cached Web pages, and other data that "leaky" applications generate. Full device encryption is widely supported, though noteworthy exceptions include Android 2.x and Windows Phone 7. Further, some devices can't encrypt everything, even if the OS supports it. And even an encrypted device exposes data to a thief with a cracked PIN.

Try pairing full-device encryption with software encryption by each application. To avoid leaks, application developers must be careful to rigorously encrypt everything written to flash storage and to safeguard their encryption keys. Emerging trends include sandboxed applications that create their own safe (authenticated, encrypted) operating environments and secure data containers that safely store IT-managed documents for offline access.

- ***Over-the-air encryption.*** Employers also worry about data in motion, or the continuous stream of traffic to and from always-connected wireless mobile devices. All four OSes natively support Transport Layer Security (TLS)-encrypted email and Web traffic, WPA2-encrypted Wi-Fi traffic, and virtual private network-encrypted network access.

Unfortunately, related settings and certificates are too complicated to rely on end-user configuration. In addition, requiring secure Wi-Fi on-site doesn't prevent users from exposing data at public Wi-Fi hotspots, and VPN configurability varies by device make and model. As a result, application developers should use TLS to encrypt their own traffic, independent of network or VPN security.

- ***Antimalware.*** The security measures described above focus on data, but they can also deter malware—preventing Android malware from grabbing files on removable storage accessible to all applications, for example. In addition, mobile OSes "sandbox" applications to insulate them from one another and require users to grant each application permission to access device features or shared data. Unfortunately, users often accept those requests without understanding the consequences. Apple's App Store policies have deterred iOS malware, but the same can't be said for Google or Microsoft stores. Even BlackBerry users can install applications from less-trustworthy sources (a risky behavior known as "sideloading").

Deterrents for mobile malware are still emerging, but they include monitoring for blacklisted applications or compromise, routing mobile traffic through cloud services that scan for malware, and running malware scanners on mobile devices. Application development best practices include self-protection of data, testing for exploitable vulnerabilities, and requesting only essential permissions.

- ***Mobile device management.*** IT can gain visibility into and control over smartphones and tablets with mobile device management (MDM). Methods include using Microsoft Exchange ActiveSync to require a PIN and encryption to using third-party MDM tools to configure and continuously enforce security policies. Supportable security policies vary by mobile OS/version, device make/model, and MDM tool, but centralized security policy management is necessary for PIN/passcode, remote find/wipe, encryption and even antimalware protections without depending on end users to always do the right thing.

- ***Mobile application management.*** Increasingly, MDM tools also provide mobile application management, letting IT inventory, deliver, install, update and remove applications. However, application developers need to understand how applications can be packaged, deployed and updated for each mobile OS, as well as the distribution rules imposed by each manufacturer and app store. Those rules have security implications—all four mobile OSes require applications to be signed, for example—but they differ as to who issues the signing certificate and how that affects application permissions. The best practice here is developer education.

- ***Data backup.*** To ensure that data can be restored after a device is damaged, wiped or lost, use the data backup capabilities supported by each mobile OS. Native capabilities typically include writing backup files to a laptop or desktop and routinely backing up data to cloud storage such as Apple iCloud or Google Drive.

  Potential defenses include passcode-protecting access to backup files and cloud storage, encrypting those backups wherever possible and preventing business data from being backed up to personal storage areas. Mobile application developers may want to take advantage of native backup capabilities, but they also need to consider the security implications of doing so.

As indicated, many mobile security best practices use native mobile device and OS capabilities as a starting point, strengthened by combining those with application-specific security measures. Building security into each mobile application not only reduces risk but also levels the still-uneven playing field of mobile platforms. Mobile OS security and management hooks will continue to improve, and new mobile devices will emerge with new vulnerabilities.

Furthermore, although we have focused here on mobile device and OS security, mobility involves many other components that must also be secured by IT, including the wireless networks, mobile messaging servers and cloud storage accessed by mobile users. Understanding all of these mobile risks and looking for ways to mitigate them during mobile application development is an investment that will pay dividends for years to come. —*Lisa Phifer*

ABOUT THE AUTHORS

Home

Editor's Note

Assessing Four Mobile Application Delivery Options

Distinguish Between Mobile Device and Mobile App Management for Control

Mobile Applications Require a Secure Foundation

ROBERT SHELDON *is a technical consultant and freelance technology writer.*

COLIN STEELE *is executive editor of SearchConsumerization, and he oversees four other TechTarget sites: SearchEnterpriseDesktop, SearchVirtualDesktop, SearchServerVirtualization and SearchVMware.*

LISA PHIFER *owns Core Competence Inc., a consulting firm specializing in business use of emerging Internet technologies. Phifer has advised many companies about safe networking requirements, technologies and best practices, and she has written extensively about these topics for various publications.*

TechTarget

Mobile Application Delivery: The Next Frontier
is a SearchConsumerization.com e-publication.

Margie Semilof | *Editorial Director*

Phil Sweeney | *Managing Editor*

Eugene Demaitre | *Associate Managing Editor*

Laura Aberle | *Associate Features Editor*

Linda Koury | *Director of Online Design*

Neva Maniscalco | *Graphic Designer*

Rebecca Kitchens | *Publisher*
rkitchens@techtarget.com

TechTarget
275 Grove Street, Newton, MA 02466
www.techtarget.com

About TechTarget: TechTarget publishes media for information technology professionals. More than 100 focused websites enable quick access to a deep store of news, advice and analysis about the technologies, products and processes crucial to your job. Our live and virtual events give you direct access to independent expert commentary and advice. At IT Knowledge Exchange, our social community, you can get advice and share solutions with peers and experts.