TechTarget

E-Guide

iOS7: 3rd party or platform-enabled MAM?

Taking a look behind the scenes with Jack Madden

Contents

Get ready for iOS7 by looking at the difference between 3rd party and platform-enabled MAM

Jack Madden

You're probably well aware that one of the hottest topics in enterprise mobility management right now is iOS 7. More specifically, you might also know that that iOS 7 is going to natively include mobile app management features that are currently strictly the province of third-party vendors. (This was a big topic last week at BriForum, too.)

Since we're going to be talking about this topic a lot—iOS 7 isn't due for at least another month or two—I want to take some time to make sure we're all on the same page about the different types of mobile app management (MAM) we're talking about.

The two types of MAM I'm talking about are:

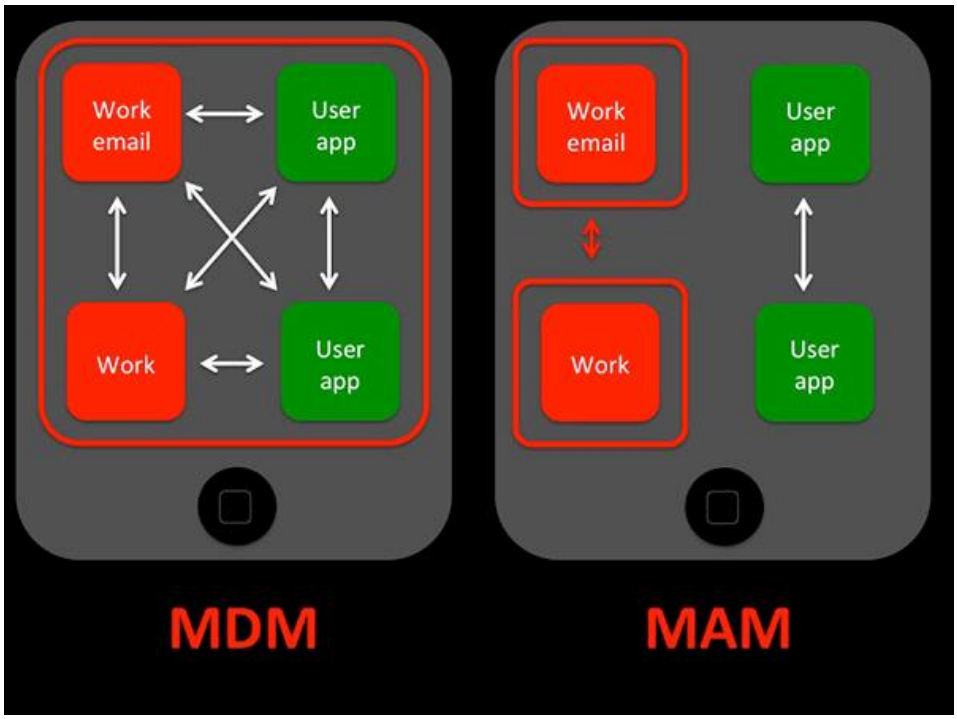
- External, operating system-enabled MAM (anything that goes on outside of an app)
- Internal, third-party-enabled MAM (anything that happens inside of an app)

Why MAM?

Many of you are probably familiar with mobile app management, but before we get to the different types, I want to first reframe it in sort of a generic way. So here I'm not talking about any specific technology, like SDKs, app wrapping, mobile virtualization, or anything related to a particular platform. Rather, for now just consider MAM to be anything at all that can take management policies, security features, etc, and apply them to individual mobile apps. The result is much more granular control than is possible with

Contents

device-level management, a must when multiple parties have interests on the device (i.e. when users mix personal and corporate apps on the same device). See Figure 1, below:



(Fig. 1: Device-level management and MAM. The red boxes represent the boundary of corporate management policies, and the arrows represent inter-app communication. Notice that on the MDM side, the work and personal apps can communicate freely, an obvious security and compliance risk. The personal apps are subject to to management, as well. On the MAM side, there's more control over how the work apps communicate with the personal apps, and the personal apps are unaffected by policy. Now certainly this can get tricky, especially when you're talking about apps that users might use for both personal and work tasks, or when you're talking about email, but that's a conversation for another time.)

Internal MAM

For the last year or so, when we were talking about MAM, most of the time we were talking about internal MAM from third-party EMM vendors. Internal

Contents

MAM influences the way apps themselves behave, regardless of status of the device they're running on. In other words, all the features we care about are built into the app itself, and there's no need to manage the device to get them to work. There are several ways we get these types of apps, all of them involving third party sources:

- SDKs
- App wrapping—you might think that since app wrapping is external MAM since it involves pre-existing apps, but since you have to have special access to the app itself (which is difficult or impossible with public app stores) and the resulting wrapped app has all the MAM features built in, it's internal MAM.
- Apps that EMM vendors provide
- Apps that ISVs create through partnerships with EMM vendors (such as Good Dynamics apps, Citrix Worx apps, Symantec Sealed apps, MobileIron apps, AppSense apps, and others)

The advantage to this type of MAM is that you don't have to worry as much about the device. (This is especially important with Android, where fragmentation makes things difficult.) Also, MAM features from third-party vendors can go way beyond what's provided by the device. (For example, different types of encryption, support for different types of VPNs, geofencing—the sky's the limit!)

The disadvantage is that the apps have to be specially built (or modified) to have these MAM features. See articles about MAM standards, difficulties around acquiring MAM-capable apps, and difficulties distributing them.

External MAM

Now with iOS 7, people are excited that many MAM features will be enabled directly in the operating system. iOS certainly isn't the first platform to have this, but it has the most significant impact because iOS doesn't have to deal with fragmentation, and it will be the largest install-base of any operating

Contents

system-enabled MAM when it comes out. Other examples of external MAM include:

- Samsung KNOX
- iOS 5 and 6—they do have some capabilities to deploy and manage corporate apps, it's just not nearly as extensive as in iOS 7.
- BlackBerry Balance
- Some forms of mobile virtualization
- Corporate app stores—sort of. While this isn't a device thing, by controlling access to apps based on the identity of the user, a degree of external MAM is achieved.

Here are the advantages with external, operating system-enabled MAM:

- It can work with any app. All those concerns around app ecosystems, vendor lock-in, how to wrap apps, and so on are much less significant.
- The platform vendor (i.e. Apple in the case of iOS 7) can have special access to built in apps like the iOS mail app (and we know that email is a big sticking point with MAM).

These are both a really big deal. But there are disadvantages, too:

- All this requires a specific device running a specific version of an operating system. (This can be troublesome for Android—there's that fragmentation again. This is also why people are more excited about iOS 7 than KNOX or anything else that has come out for specific Android devices.)
- You'll need to have some sort of control over the device to ensure that the MAM features are supported. So if you wanted to do MAM to get out of the business of managing devices, this might not work for

you.

- This type of MAM is limited to whatever features happen to be enabled in the device, so if you want features that go beyond what's in the OS, you'll need a third-party

Contents

Conclusion

App-level management (MAM in general) is becoming a very important part of enterprise mobility management. iOS 7's MAM capabilities will be a big deal, but it's important to keep in mind the differences between internal and external MAM. (And of course all of this is important for conversations around Samsung KNOX, mobile virtualization, and other platform-enabled MAM, too.) Clearly there are places for all types of MAM.

Keep tuned for more on iOS 7 and MAM in general—there's lots more to talk about!

Contents

Free resources for technology professionals

TechTarget publishes targeted technology media that address your need for information and resources for researching products, developing strategy and making cost-effective purchase decisions. Our network of technology-specific Web sites gives you access to industry experts, independent content and analysis and the Web's largest library of vendor-provided white papers, webcasts, podcasts, videos, virtual trade shows, research reports and more —drawing on the rich R&D resources of technology providers to address market trends, challenges and solutions. Our live events and virtual seminars give you access to vendor neutral, expert commentary and advice on the issues and challenges you face daily. Our social community IT Knowledge Exchange allows you to share real world information in real time with peers and experts.

What makes TechTarget unique?

TechTarget is squarely focused on the enterprise IT space. Our team of editors and network of industry experts provide the richest, most relevant content to IT professionals and management. We leverage the immediacy of the Web, the networking and face-to-face opportunities of events and virtual events, and the ability to interact with peers—all to create compelling and actionable information for enterprise IT professionals across all industries and markets.