The Truth About Enterprise Mobile Security Products

Presented by Jack Madden at TechTarget Information Security Decisions 2013

Welcome to my enterprise mobile security product session! Instead of printing out the slides, this handout contains notes about everything I'll be covering in my session.

Abstract

Mobile security products and enterprise mobility management solutions are flooding the market today. CISOs and device administrators have all been exposed to these products and are wondering the same things: Are they effective? What do they actually protect users from? This session will compare the approaches taken by mobile security suites and enterprise mobility management (EMM) solutions (including mobile device management (MDM) and mobile app management (MAM) tools) to give attendees a better grasp on the current state of mobile security and what the real challenges are today. Attendees will learn the validity of deploying mobile security products and enterprise mobility management solutions in their organization and will leave ready to make a more informed decision about the mobile security posture of their organization.

Part 1: Why are we here?

Mobility is a big deal right now. There's little else we need to say—you're here in this mobility session, after all, so you probably agree. The only other thing we can say is that no matter what technologies we use—mobile device management (MDM), mobile app management (MAM), desktop virtualization, security suites, anti-malware apps, whatever—the future of dealing with end user computing will mean dealing with devices that don't always have mice and keyboards, and that don't always run Windows.

Anyway, imaging that your boss comes to you and says, "We need to secure our phones!" "Let's do BYOD." "Let's secure our BYOD." Or even, "Wait... do we have BYOD?" Since this is a security conference, we'll assume that one of the first thoughts that comes up is to go to one of the well-known security vendors and order one copy of their "Mobile Security Suite." Done!

But wait, there's also a crop of new enterprise mobility management (EMM) vendors, and some of them are hot startups getting lots of attention. Think along the lines of AirWatch, MobileIron, Fiberlink, Citrix, and Good Technology. (By the way, generally the term EMM is used as a way to collectively refer to MDM, MAM, and other associate technologies.)

What's the difference between the two categories of vendors? The traditional security vendors put out reports about mobile malware threats, anti-malware products, and their products have "security" in the name. The EMM vendors talk about MDM and MAM (or argue about MDM versus MAM), and talk about things like "app wrapping" and "containerization."

Those are just rough generalizations, though. It actually gets a little more confusing. Some of the security vendors talk about MDM, too (and even MAM). The EMM vendors, on the other hand, almost never talk about malware. And then there's all this stuff about BYOD... Yikes! How are you supposed to figure out what which way to go and what to do?

That's what this session is for. I'm not here to tell you which vendor to pick. I am here, though, to talk about the overall enterprise mobility landscape, and where EMM vendors, security vendors, and malware threats fit into that landscape.

We'll start out by getting an overview of enterprise mobility.

Part 2: What do you really need to worry about in mobility?

Enterprise mobility used to be easy. For many people it was just BlackBerrys, with the vertically-integrated BlackBerry Enterprise Server right there to manage it all. But then the iPhone and Android devices and later iPads came along. These things were cool, but at first they were completely unmanageable—in short, a headache for IT. That didn't last too long, though. In 2010, several new innovations (over-the-air configuration profiles for iOS and the Device Administrator API for Android) meant that these devices could come a lot closer to being locked-down, corporate-controlled devices. Modern MDM had arrived.

Did modern MDM solve all of the problems with iPhones and Android? No way! While users were falling in love with their new devices, they were also starting to work in completely new ways, too. This was also around the time we started talking about the consumerization of IT. The result is that old BlackBerry-style management doesn't cut it for the way people really like to use their devices.

Today, users like to have a wide variety of exciting personal apps on their phone, along with their work email. They also want to be able to do real work tasks (more than just email) on their phones. And finally, they don't want their phones to be locked down, and they don't want to feel like Big Brother is watching. (Phew! Dealing with all this stuff is a tall order!)

Here's the problem: mobile devices were made so that certain types of data can very easily be shared from one app to another. That sharing is great when you want to post a picture of your cat on Facebook, but when it comes to enterprise data, all that sharing is really just leaking! MDM isn't very good at controlling this. By having a corporate Exchange account synced to a phone's built-in email client, there are all sorts of ways data can leak. The only way for MDM to deal with this is to lock down the device so that all those risky personal apps aren't on there. But do you think users will like that? Again, that's no longer acceptable. (And if you try to say no, just wait and see how "creative" your users become!) Another problem is that while MDM can provide email access, there are probably a lot of other work tasks users want to do on their phones and tablets.

How do we solve this? Virtual desktops and web apps have been proposed, but for everyday apps like email, users just have to have a native app. Mobile app management is gaining ground as a solution. Since MAM provides more granular management than MDM, you can also have better control over how apps share data (and keep corporate data out of personal apps). For the past few years, MAM has involved apps that are specially created or modified to have built-in management features that don't rely on the device. More recently, iOS 7 and some specialized versions of Android have started to include basic MAM features built directly into the operating system. These can work with any app.

It's important to know that any form of MDM or MAM will require some sort of compromise between security and accessibility (and of course that problem is as old as time itself). I'm a strong believer that a consumerization-friendly way of approaching MDM and MAM is to give users a choice for how the compromise is made, when possible. For example, some users might prefer to have work email be just a third-party app, and not have their whole device be managed. Other users might prefer a better email experience and want to use the built-in client, and accept device-level management policies.

These issues are far from being 100% solved, but we can see that one of the biggest issues in enterprise mobility today is providing secure, managed access to resources, in user-friendly way. If we don't do that, users will figure it out on their own, and we can be sure that won't be as secure!

Part 3: What about security products and malware?

So what about these hard core security issues? And what about threats from malware?

Regarding mobile security, the good news is that there are many things in place that help us out. Mobile devices have features such as:

- Permission-based mobile OSes
- Sandboxed apps
- Well-define inter-app sharing frameworks
- Code-signing requirements
- Curated app marketplaces
- User-controlled permissions for sensitive data

However, malware is definitely still an issue. Plus we have a host of vulnerabilities that security professionals have been dealing with for decades:

- Physical device access
- Network-based attacks
- Phishing
- Social engineering
- End users themselves

Of course, mobile devices amplify some of these issues, because mobile devices are:

- Mobile! (They can get lost easily!)
- Always connected
- Very personal

However, I'm not really here to comment on these general security issues. I'm here to sort through the range of EMM and mobile security products. So back to malware and anti-malware. Like I was saying, this is an interesting issue because some vendors talk a lot about it, and some vendors hardly at all.

There are two different types of malware: there are apps with malicious intent, and then there's malware that is only in the eye of the beholder.

Apps with malicious intent sometimes exploit weaknesses in mobile OSes or other apps, or take advantage of devices that are rooted or jailbroken. However, many malicious apps work completely in the user space, without taking advantage of any exploits. In addition, these apps can come from curated app stores (like Google Play or the Apple App Store) too! So the mobile malware threat definitely exists, even if it seems like some of those reports over-emphasising it.

The second category of malware comprises apps that are not necessarily outright malicious, but behave in ways that IT administrators would rather they not. This could be anything—social media apps, Path, Dropbox, and so on. Remember that when it comes to enterprise data, sharing equals leaking, so any app that deals with contacts, calendars, photos, attachments, cloud file syncing, location data, Facebook, Twitter, or iCloud in a way that threatens enterprise data can be considered malware. (Really, this is almost every single app, ever!)

How do we deal with this second category of malware? This is where something called app reputation comes in. App reputation can look at a ton of different factors, including:

- Static and dynamic code analysis
- Malicious and unexpected behaviours (Think—why does this flashlight app need access to my contacts?)
- App store reviews
- Reputation of the app creator and other apps they offer
- URLs the app connects to
- Ad networks used in the app
- Permissions requested
- Phone calls and SMS
- Terms of service

But there are still some difficulties with this:

- An anti-malware app is just another app. A jailbroken or rooted device could lie to it.
- App reputation services for iOS often require the use of MDM on client devices.
- The mechanics of using MDM to blacklist apps is difficult.
- How do you begin to decide what apps or app behaviors to block?
- It's difficult to get in between the user and the app store during the install process.
- Blacklisting a user's favorite app will lead to "creative" workarounds, not to mention really annoy them.

One final note: there are a lot of other security measures that mobile security products take. Many of these are readily available through MDM and MAM as well. These measures include:

- Location tracking
- Password protection
- Device encryption
- Remote wiping
- VPN
- Secure browsing and other secure versions of apps.

Part 4: What do we need to do to put this all together?

Now we know the stakes that we're dealing with in mobility. We know that these are the things we have to deal with:

- Providing access to corporate resources; consumerization and the way users work today; work and personal data and apps together on the same devices.
- EMM technology: policies to protect our resources, implemented through MDM and MAM.
- Mobile malware

So what do we figure out first?

- Access to resources
- Management policies on devices and/or apps, with MDM and MAM
- How sensitive is our data? How strict does the separation need to be?
- How to make this all user friendly?

Great, so then what's the role of anti-malware and app reputation? That all depends on how you're managing mobility. How do you decide that? This is a big topic of debate in the EMM space, but really it doesn't have to be. Here's a quick side note about that whole topic:

EMM scenarios really just boil down to how you decide to manage email. Why? For pretty much any resource other than email, you have to deploy an app, so you probably have to do some sort of MAM. But email is a special case, since every device out there has a built-in email client. It's the experience that users prefer, but securing it means you have to manage the whole devices. So forget about MDM versus MAM, forget about dual persona or containers, even forget about BYOD. All that matters is that you have two options:

- *Option 1: Email in the native client with device-level policies. Users have to put up with management but get a better email experience.*
- *Option 2: Email in a third-party client with no device-level management. Users are free to use the rest of the device as they please, but the email experience won't be as good*

There are a range of in-between options, but they essentially boil down to variations on these two.

Anyway, the role of anti-malware will probably depend on the management state of the devices. For managed devices, anti-malware would be more expected, as well as app reputation-type services. The implementation of app reputation policies will vary widely depending on the scenario. For unmanaged devices, it's probably a lot less likely that you'll be doing anything about anti-malware or app reputation.

One final note on anti-malware and app reputation: How are you going to decide which apps to block or build policy around? Good luck with that! Seriously, this is all so new that there aren't any best practices yet. Some products out there can link into MDM, so that real-time policies can be built around specific issues or classes of behaviors. There are also some vendors that have templates that can be used to build policies based on specific regulatory compliance scenarios, but this is still pretty new and wide open.

Part 5: Back to the vendors. What's the difference?

We've looked at the landscape, talked about what we have to deal with in mobility, examined malware, and even looked at where to start. There's just one final step:

What about all those vendors we talked about in the beginning?

Sure, we can make some generalizations, for example that vendors with products with the word "security" in their name emphasize anti-malware and and publish reports about how much of it there is, and that EMM vendors don't talk about malware very often.

However, we can also observe that many security products also incorporate MDM (some even have forms of MAM), and many MDM and MAM vendors provide app reputation or anti-malware through partnerships.

So which way to go? Remember our requirements:

- Access to resources
- Management policies on devices and/or apps, with MDM and MAM
- How sensitive is our data? How strict does the separation need to be?
- How to make this all user friendly?
- And under certain circumstances, anti-malware and app reputation

If you start out with just a security-oriented approach (comprising anti-malware, plus basic policies like passwords, encryption, tracking, wiping, etc) and don't include other elements of EMM (access to resources, consumerization, work/personal separation), then you will have overlooked many serious issues.

In other words, your first overall priority should be fulfilling EMM requirements—like finding a vendor that can satisfy your needs for MDM, MAM, and other apps. Then there will be places where anti-malware and app reputation can be fit into your deployment.

At this point, we can also note that there is actually quite a bit of overlap between the two different camps ("Security vendors" and "EMM startups.")

I'll bring this whole session to a close. This isn't really a new lesson—we've seen that it's necessary to:

- Be aware of the landscape
- Determine your requirements
- Then, as the final step, choose a vendor that can satisfy those requirements.

With this session, the first step is done!

About the presenter

Jack Madden writes about everything related to enterprise mobility management at BrianMadden.com. He is the co-creator of the Consumerization Nation podcast, and has spoken at BriForum, Citrix Synergy, VMworld, and other events in the US and Europe. Jack was is co-author of "The VDI Delusion," and author of "Enterprise Mobility Management: Everything you need to know about MDM, MAM, & BYOD."

To contact Jack:

Email: jmadden@techtarget.com

Twitter: @JackMadden