MOBILE APP MGMT

- MAM vs. MDM
- Making the Best Use of Mobility
- Think Ahead
- Flexible Data Protection
Solve your enterprise’s mobile management puzzle.

Energize and Enable your organization with Mobile Enterprise Management from AT&T.

Leverage AT&T network assets and organic IT knowledge banks.

Protect your intellectual property, remotely or in the cloud, across devices and carrier networks.

With the expertise to develop and manage game-changing applications, AT&T can assist in driving productivity for your organization while serving as your trusted partner from end to end.

Enterprise is on the move with mobility. And AT&T can get you there.

For more information, visit us at www.att.com/mobilemanagement

© 2012 AT&T Intellectual Property. All rights reserved. AT&T and the AT&T logo are trademarks of AT&T Intellectual Property.
According to the results of an Apperian survey, only 10.3% of mobile workers said their company has a combined mobile device management (MDM) and mobile application management (MAM) solution in place, while 22% have an MDM solution, just 8% have a MAM solution.

A full 42% of respondents said their company has no mobile management solution in place at all. This illustrates that deciding what kind of management solution to deploy is so challenging, nearly half of companies haven’t done anything yet despite the fact that mobile devices are affecting nearly every business large and small.

BUILDING TOWARDS APPLICATION MANAGEMENT
Mobeen Khan, Executive Director of Advanced Mobility Solutions at AT&T Business Solutions, says most companies initiate a mobile deployment by just
looking for a basic level of control and security. “And that’s where device management comes in,” he says. “All they’re interested in on day one when they start to roll out mobility is, ‘What kind of devices and rate plans do I have, and how do I make sure that they’re secure and do some basic policy management?’”

It’s at the next level, Khan says, that mobile application management (MAM) comes into play. “The next step is, ‘How can I start to leverage these devices and mobility to empower my employees, or to extend my desktop or web applications into a mobile environment?’” he says. “And that starts to get into a whole other layer of policy management and control that you need to have at the application layer — and that’s really what mobile app management is about.”

The point is that app management and device management are often inseparable, with app management as step two in a logical process. “App management means that you have some content or application that you want to manage for your employees or for your customers — and if you’re doing that, especially in an employee setting, you almost always will have some sort of a device control element in it,” Khan says.

**MAM vs. MDM**

John Marshall, CEO of AirWatch, says that at the most basic level, MDM is about enablement and security, while MAM is about business productivity. “The best strategy is usually a hybrid of the two,” he says. “Usually, it involves some app management, maybe some app wrapping, and use of an SDK, linking in some cases to MDM and in some cases separate from MDM.”

Still, Marshall says there are some scenarios where MAM on its own may be the best fit — consider a retailer that just wants to build an app to allow its employees to schedule their work hours. “You don’t necessarily want to manage 100,000 of your store workers’ devices simply to get some app-level information and interaction down to those devices,” he says.

The same would be true for an airline that wants to build an app to allow its cabin crew to select their routes for the next month. “That doesn’t mean you want to manage the devices for all of your cabin crew,” Marshall says. “So that’s an easy scenario where standalone app management is a great solution. You’re providing a convenience that could otherwise be done on a PC, but not as conveniently — and it’s making the lives of your workers easier and more productive.”
WHERE DEVICE MANAGEMENT FITS
On the other hand, Marshall notes, a retail point-of-sale device that tracks inventory and collects credit card data will require more traditional MDM. “That’s a scenario where you’ve built an app, and you still have app management to be able to push out updates and all the scenarios around the app, but you absolutely have to have an integrated MDM approach for that scenario,” he says.

There’s also a third scenario, Marshall says — a company that allows senior executives, who need access to sensitive corporate data, to bring in their own iPads. “They want to be able to access the corporate intranet; they want to be able to connect to a file share; and they want to do some type of business intelligence,” he says. “So now you’re in a scenario where it’s bring your own device (BYOD), but it has more high-value, highly sensitive information.”

In that case, you’ll still need MDM. “That’s not just for security, to ensure that there’s a passcode on it, but to truly enable those workers so IT doesn’t have the overhead of having to help somebody connect to a VPN or a VLAN,” Marshall says. “If you want to use a business intelligence app, and if you want to make sure that you’re meeting some basic security and governance policies, then you probably need to allow MDM so that the app can be managed, and if somebody leaves the company, it can be removed. So that’s where MDM and app management tend to coexist really well.”

MANAGING APPS
Keith Katz, Vice President of Management Products at Kony, says it’s worth noting that most device management solutions entered the market when companies first began looking beyond BlackBerry devices. “When you start to use an iPhone or Android or Windows device, you find that you’re missing all the normal management security tools that you had from a BlackBerry server,” he says. “So, MDM fills in those gaps.”

But that doesn’t provide a business with any significant value beyond the basics, Katz says, like enabling mobile email. “If you want to create your own internal app, then you need some sort of efficient, secure way to get it down to your end users, and then be able to regulate what they can do with that data so you don’t end up with inadvertent leaks,” he says. “And that moves you squarely into the app management side of the world.”

What’s more, Katz says it’s often much easier to deploy app management than device management. “If you want to enroll your device against the device management server, you’re going to have to put in credentials, and you’re going to go through eight to 10 screens, some with big scary warnings on them — and users don’t like it,” he says. “With application management, you open the app, put in your user name and password, hit yes, and that’s it — you’re done.”

And Marshall says it’s important to note that MAM has evolved far beyond Most device management solutions entered the market when companies first began looking beyond BlackBerry devices.
simply maintaining an enterprise app store. “You have the whole workflow of developing, testing and distributing applications; you have change management; you have compliance — making sure that people have the latest apps out there — if there’s regulatory or compliance issues where they must have a specific version, you need to make sure that’s there,” he says. “And you have the social and feedback element, which you didn’t used to have. Think about five years ago — when did you ever rate one of your internal apps and have an opportunity to get feedback directly to the developer or to the application group? That never happened before.”

**BYOD VS. CORPORATE-OWNED**

Robert Fenstermacher, director of product and solutions marketing at Aruba Networks, suggests a very simple way to look at the difference between MAM and MDM — while MDM is an excellent solution for corporate-liable devices, he says, MAM is a perfect fit for bring your own device (BYOD).

“So it depends on the organization, whether they want to employ both approaches or just one,” Fenstermacher says. “And I’ve talked to a lot of organizations that are saying, ‘You know what, I want to get out of the device management business completely, even if it is a corporate-owned device — all I really care about is the content that sits on that device. I don’t care about managing it completely.’”

For BYOD in particular, Fenstermacher says, MAM controls what matters, leaving the users in control of the devices they own. “And there are additional controls that you can put in place with MAM to ensure that the secure sandbox or container stays secure,” he says. “You can restrict things like cut and paste functionality between the two environments, and you can require a passcode to get into that environment.”

**MAKING THE BEST USE OF MOBILITY**

John Herrema, Senior Vice President of Product Management at Good Technology, says it’s crucial to keep in mind that this is all ultimately about securing and managing mobility. “And a narrow focus on one thing to the exclusion of another — managing only devices but not paying attention to applications, or focusing solely on app distribution but not actually paying attention to how the applications work with one another — and you’re going to end up with a solution that’s maybe secure in certain cases and not in others,” he says. “So the big shift we see with our customers is that they’re increasingly focused on the app, because that’s where the value comes from.”
In the insurance business, for example, a company can count on the fact that every one of its independent agents and brokers will have a smartphone, and many will have both a smartphone and a tablet. “And so now the really cool thing is, I have an opportunity to extend business processes to them and apps to them in a way that just wasn’t possible three or four years ago,” Herrema says. “And all I have to be able to do is to deliver a secure, managed and controlled app, or combination of apps, down to that device, and now I can implement a workflow that gets my business partner and my end customer and my employees all more closely connected in real time.”

And that, Herrema says, is what’s really exciting about MAM. “It’s all about how companies can use mobility to create entirely new workflows and optimize business processes in ways that simply weren’t possible a few years ago, because you didn’t have this ubiquitous medium out there in terms of mobility and these smart devices,” he says.

COMPONENTS OF APP MANAGEMENT
Ultimately, Khan says, any MAM solution will generally cover three key areas — content management, group management and policy management. “The content management piece is about, ‘What content am I going to put in it, how do I provide authorized access to that content, how do I update that content, how do I provide version control of that content,’ and so on,” he says.

The second part, group management, is about controlling who sees what data. “You don’t want to have financial content and applications accessible by your salespeople — so it’s about how you divide up the world of your content and provide, perhaps, some sort of a tiered or containerized access to the content and applications,” Khan says.

The third piece, then, is policy management. “In the case where you have multiple apps rolled out, how do you control the policies around a lost device? It’s not only about wiping the device clean of data, but also perhaps locking content, locking access to apps, and so on,” Khan says.

THINK AHEAD
In considering a MAM solution, Herrema says it’s important to look not just at what you need today, but also at what you’re likely to need down the road. “It’s critical to know that what
Pernix Therapeutics

The pharmaceutical company Pernix Therapeutics has a field sales force of approximately 130 people, all of whom use iPads. “It’s a great tool for doing a presentation to a doctor, and also for using CRM software to record the details of the call,” says Clay Hilton, the company’s director of IT.

Because Pernix provides samples of highly regulated narcotics, Hilton says, the company needs to ensure that those samples are tracked in a reliable manner — which means that any updates or bug fixes for its CRM application have to be pushed out to all iPads at the same time, with confirmation that those updates have been successfully installed.

Hilton says Pernix chose Fiberlink’s MaaS360 solution for mobile application management because it’s fully hosted. “Fiberlink as a service checked all of the boxes, but we didn’t have to fool with the back end,” he says.

Pernix uses Concur for expense reporting, which Hilton says is also managed via MaaS360. “Even though it’s an App Store app, we can still push out an update and say, ‘Hey, this is here for you to install’ — and all they have to do is one click, and it installs for them,” he says. “Then we can generate a report — 75 people have clicked on it; 45 haven’t” — and we can automatically email the 45 that haven’t.”

So far, Hilton says, there’s hasn’t been any need to do anything more intrusive, like blacklisting specific applications. “A lot of that has to do with the stability of the Apple iOS platform,” he says. “We’ve been able to let our representatives install various productivity applications, and because we have reporting on network usage and we’re able to set usage thresholds and do alerts, we don’t have to worry a whole lot about them installing Netflix and watching movies over their 3G connection.”

Hilton suggests that any other company seeking a similar solution run a trial with several different providers. “Look at the major players and make a short list for what functionality you have to have,” he says. “We’ve been happy with Fiberlink, but there’s lots of opportunities to sample what’s out there — so I would highly recommend doing that.”

Different lines of business or divisions often move forward in building their own apps without giving any thought to app management.
technologies in silos. There are a lot of solutions out there today that can really address all of the different aspects of the problem with one product — and that’s going to make life a lot easier.”

That type of holistic approach, Fenstermacher says, also allows you to use information from one technology area and apply it to another. “For instance, if I know from MDM that my device has been jailbroken, I can now apply that outside of just the device,” he says. “If I just had MDM and I knew that the device was jailbroken, I could only lock or wipe the entire device, whereas if I have MAM in the same solution, I can use that event of a device being jailbroken to lock individual apps. I can also use it to make a decision on the network. I can actually quarantine the device if I know that it’s jailbroken.”

FLEXIBLE DATA PROTECTION
Herrera says the most important feature to consider in evaluating a MAM solution isn’t the ability to distribute and manage apps — it’s the ability to manage sensitive business data. “One of the key things to think about is, do I have an ecosystem of secure and trusted business applications where I know that, as my data’s flowing between them, I can be productive, and I can give the user what they want — which is the ability to move a document from an internal application over to a secure email application over to a secure document reader — but I shouldn’t be allowing that document to end up in iCloud or a personal Dropbox account,” he says.

Still, Katz says it’s crucial to be flexible in doing so. “One document may be a confidential document that you need to keep completely isolated on the device, but the next document may not be — it might be a marketing brief that a sales guy wants to distribute,” he says. “So you have to have a solution that can regulate both of those, based either on content or on the repository you’re pulling them from — and something that feels seamless to the end user, so they don’t feel like you’re putting a burden on them.”

And Jonathan Dale, Director of Marketing at Fiberlink, recommends making sure that any solution you’re considering is a good match for your own specific use cases. “The worst thing to do is to start looking at solutions and be swayed by features that you may never use, or that may never be applicable to your environment,” he says. “But if you have those use cases already defined, and you know what your needs and must-haves are, it makes quicker work of evaluation.”

Ultimately, Dale says, that can mean actually trialing the solutions themselves. “Most providers today have online trials available, and they’re extremely quick to set up — some take just a few minutes to get set up and running,” he says.

With enterprise security on the line, and considering that MAM is an investment in the future, a “few minutes” of set up, a few times is certainly worthwhile.
Thank you to our sponsor

*TITLE SPONSOR*
Mobile Enterprise Management from AT&T simplifies the complexity of mobility. From delivering network security and device control, to content distribution, workspace management, governance, and through the entire life-cycle of application development, AT&T leverages best practices and proven frameworks to address nearly every enterprise mobility challenge. For more information - [www.att.com/mobilemanagement](http://www.att.com/mobilemanagement)