

Take Charge With MDM

In a complex mobile world, MDM (mobile device management) solutions provide companies a way to secure and maintain a plethora of devices.

The increasing popularity of mobile devices has created a number of challenges for information technology departments. While desktop systems are generally easy to track, manage, and maintain and in most cases use some flavor of the Windows operating system, mobile devices present a variety of headaches for the IT staff. The devices are small and easy to lose, staff may be using a mix of personal and company-owned hardware in the field, and companies have deployed a wide variety of devices across applications that may include a mix of ruggedized computers, laptops, and smartphones, all using different operating systems.

“We often refer to enterprise mobility as ‘death by a thousand cuts,’” says Alan Dabbieri, chairman at AirWatch. “IT must configure and secure each device, ensure constant compliance with any industry-specific and/or governmental regulations, mitigate any business and legal risk posed by device usage, provision the device’s software and keep it current, and then support each individual end user on a 24/7 basis. These tasks multiplied by thousands of devices can quickly overwhelm even the best IT team.”

IT departments may struggle with securing mobile devices (particularly personal smartphones, that may just show up in the enterprise because an employee wants to access corporate data on their own device), supporting the various operating systems, provisioning new devices, and managing software upgrades. Because of this complexity, companies have increasingly relied on MDM software solutions to streamline these management activities and increase security.

The Role Of MDM Solutions

According to IDC, the worldwide MDM market is expected to experience a compound annual growth rate of 7.6% over the next five

years, reaching \$382.7 million in 2014. In multiplatform environments, these solutions provide visibility across the entire mobile device fleet and the ability to parse that visibility and control depending on the user’s role and title.

“With a good device management solution that supports devices from multiple vendors, IT administrators don’t need to know the low-level detail for each type of device,” says Jay Cichosz, VP of marketing at Wavelink. “The device management platform can take care of that for them. They can use one common interface to set up security policies and user profiles that are pushed out across the enterprise to different types of devices instead of requiring IT to try and understand how to do it on each one.”

By using a robust MDM solution, IT can more easily compile an asset registry, automatically provision software during off hours, perform remote diagnostics, and lock down or wipe devices remotely if they are lost. These capabilities go far beyond simple asset management.

Users should select a scalable solution that can not only grow with the number of mobile devices deployed in the enterprise, but that is also flexible enough to support new device platforms as they are introduced, as well as other types of mobile equipment. “End users also tend to forget to take into account everything in the ecosystem,” Cichosz says. “For example, they look at their mobile devices but don’t think about their mobile printers or access points. All of these share the same common network, so if their management solution is not compatible with their printers and they want to do security upgrades, it can create problems.”

Enterprises should also consider solutions that allow them to employ different approaches to managing different classes of mobile



Alan Dabbieri
chairman,
AirWatch



Jay Cichosz
VP of marketing,
Wavelink



Ron Hassanwalia
director of sales
and marketing,
SOTI

devices. “Mobility solutions, such as push email, mobile phones, and simple document sharing (e.g. SharePoint), are very different from form-based mobility solutions, real-time job delivery, proof of delivery, and terminal emulation,” says Ron Hassanwalia, director of sales and marketing at SOTI. “For example, it is a mistake to cluster 200 technicians who conduct repairs in the field with 800 enterprise employees who access email on their mobile phones. Adopting one system to manage all mobile devices actually reduces the efficiency of managing line of business (LOB) applications for technicians and reduces the mobility ROI due to downtime.”

Smartphones Present Complex Challenges

One of the biggest changes in the mobile space has been the adoption of smartphones within the enterprise. Employees at most companies use a mix of both personal and corporate assets, and the variation among operating platforms (Windows, iPhone, Android, BlackBerry) has added to the complexity of managing and securing these devices. “For their first several years, BlackBerry’s market dominance, their ability to manage only emails, and the devices’ price points limited their use to the executive and management ranks,” Dabbiere says. “As price points began to fall, mobile app development took off, and competitors entered the market. In the last several years, with the rise of iPhones and Android, these two devices have also flooded into enterprises of all sizes.”

MDM vendors have added support for these devices, and wireless carriers are even offering solutions. Recently, AT&T announced a smartphone management solution, the MobileIron Virtual Smartphone Platform, to help manage phones on multiple operating systems within the enterprise.

But while rugged mobile devices and laptops provide extensive functionality to allow users to easily provision, secure, and manage devices, those capabilities may be limited when it comes to smartphones. “If the company owns the device, it’s a corporate-liable [CL] device, and it’s easier for the company to dictate usage restrictions,” Cichosz says. “But if the devices are individual-liable [IL], the user considers them their own, and they don’t want company intrusion on them. But they are still getting corporate data on them, which needs to be secured.”

The Android and iPhone platforms have posed a particular challenge, because initially they were not easily supported within third-party management solutions. “Businesses will need to understand that, unlike Microsoft, Apple and Google are fairly new to the enterprise space having specialized and effectively captivated the consumer space,” Hassanwalia says. “Fueled by great success in millions of devices sold worldwide, both platforms continue to transition toward meeting enterprise demands.”

Things are already starting to improve. With the release of

iOS 4, which includes Apple’s MDM service, the company has made its devices more conducive to enterprise usage, and all of the major MDM suppliers now support the phones.

“We are able to support both iPhone and Android and provide management of the devices, but the big thing we are missing right now is the ability to do full help desk support with remote control,” Cichosz says. “The facilities provided in Android and iPhone make real-time screen scraping and control more difficult than in other platforms, such as Windows Mobile. [The] devices can be managed, but there are still some improvements that can be made on their part to allow a management solution to interact with the device.”

MDM Solutions Ease Device Upgrades

Many enterprises are now deploying their second or third generation of mobile devices, presenting their IT departments with even more challenges as they migrate from one vendor or platform to another. For these transitions to be smooth, IT has to have a clear understanding of the end users’ needs, their role in the application, and how the new device should be configured to optimal performance in that context.

“Before embarking on any type of large-scale mobile deployments or upgrade, a vast majority of companies need to first document and communicate the specific needs of each type of mobile user,” Dabbiere says. “Many companies also fail to define, document, communicate (and then overcommunicate) IT’s policies and procedures regarding device usage. End user education and training on correct/approved device usage and IT’s policies must be part of the onboarding process and should include a detailed explanation of how the organization intends to enforce these policies.”

Again, the MDM platform can provide a valuable resource when moving from one platform to another. “When you switch to a different device type, you have to work with a whole new interface and make sure you are able to provide the same level of security, particularly if you are using certificates or other advanced forms of security,” Cichosz says. “But if you use an MDM solution that is designed to allow for seamless transition between devices, then there really isn’t any major impact. We have customers that do this all the time, and it really demonstrates the value of MDM.”

By utilizing a flexible, scalable MDM solution, enterprises can better manage their current fleet of mobile devices, while positioning their IT departments to be prepared for new platforms and the security threats that go along with those new devices. With an MDM system in place, IT administrators can improve efficiency and security, while reducing downtime, all of which can improve the return on investment of the company’s mobile initiatives. ●