Unlocking the Power of Mobile Device Management

Mobile device management (MDM) is about more than technology—it’s also about skillful strategic resource management. It’s about making the right business and management decisions to truly optimize the functionality and security of a mobile communications network while minimizing cost and downtime.

This supplement combines information about the latest MDM tools available from vendors with real-world advice on how enterprise business managers can best put these tools into practice. It features top tips and advice for enterprise end users on how to turn MDM tools into productivity powerhouses.
The proliferation of new mobile devices on the market is having a profound impact on enterprise mobility deployments. Devices that once targeted consumers are beginning to infiltrate businesses as more and more employees are using their personal devices on the job. Smartphones and tablets are increasing in popularity and power, making them the device of choice for many industries.

“I don’t think it’s any secret that one of the biggest drivers in the diversification of mobile devices has been Apple,” says Tim Williams, product manager, lifecycle management for Absolute Software. “I can’t remember a device ever being adopted as rapidly as the iPad has in the last year.”

Brian Reed, chief marketing officer and VP of products for BoxTone, is also seeing more organizations employing tablet computers at the point of use in retail, healthcare, distribution, and transportation as workers interact with patients, customers, and clients.

To successfully manage the influx of these mobile tools and address both security and policy concerns related to their use in the business environment, enterprises are paying closer attention to mobile device management (MDM) software. In fact, Gartner supports the notion that the MDM market is growing quickly with the advent of new devices. According to the research company, MDM revenue (excluding revenue for messaging, security, etc.) for year-end 2010 is estimated at $150 million, and it is forecast to increase at a compound annual growth rate (CAGR) of 15% to 20% over the next three years.

Vendors are responding accordingly with a range of hosted and non-hosted solutions to fit every need and budget. “The intention of implementing an MDM solution is to truly optimize the functionality and security of a mobile communications network,” points out Oscar Rambaldini, director of product development for SOTI Inc. “Businesses need employees to be connected and productive, but the current surge in personal devices entering the corporate network compounds many security risks and accessibility issues. This trend quickly prioritizes the need for a flexible and reliable MDM solution.”

According to Gartner, MDM revenue for year-end 2010 is estimated at $150 million, and it is forecast to increase at a CAGR of 15% to 20% over the next three years.

“OS and device proliferation are certainly driving the core need along with employee-liable challenges, but it’s really about the apps,” says John Marshall, CEO of AirWatch. “As enterprises develop more applications that require deeper access to corporate resources and proprietary information out in the field, MDM will continue to play a critical enabling role.”

According to VDC Research Group, another factor driving the adoption of MDM software is cost savings. The company’s research indicates that the use of an MDM solution can save an organization more than $230 per device per year in support costs.

“For a 1,000-unit deployment, this translates into savings of more than $1.1 million over a five-year period,” notes Rambaldini. “Moreover, MDM solutions are responsible for substantial savings in hardware and infrastructure investment, incredible reduction in maintenance costs and time, resulting in increased efficiency, productivity, and hence, ROI.”
“In many cases the corporation may realize an increase in support costs when managing employee-
liable devices as it cannot control what is loaded on the device, how the device is used, who uses it, the operating system chosen by the user, and what the user support needs may require,” explains David Boatman, COO of Ovation Wireless Management, Inc. “Ultimately the corporation cannot leverage device and application synergies in order to reduce the per device cost for the company without a sound MDM approach.”

The right MDM model
Before enterprises determine what type of MDM solution to deploy, they need to take a careful look at their mobile operations. “Recognize that mobile should be viewed as a new strategic platform or a new strategic service that IT needs to deliver to its end users,” advises Reed. “Companies need to look at how all their existing people and processes and technologies are going to extend to make mobile successful in the enterprise. You’ve got network and PC administrators that need to get involved with mobile. You have applications developers that are going to need to build mobile applications or mobile versions of applications. Your data center team needs to get involved because these devices are going to be connecting to applications and services in the data center, and you need financial and procurement teams to procure the technology and track the assets and asset utilization.”

“MDM is a strategy and not a product,” explains Boatman. “The right MDM strategy begins with a combination of identifying the needs of the company from many perspectives including expense control, information security, government imposed regulations, and legal protection elements of company confidential data.”

Marshall agrees. “MDM enables companies to focus on the strategic aspects of their mobility investments and not worry about tactical day-to-day management of devices and apps,” he says. “It increases productivity and efficiency across end users and IT departments and reduces the total cost of their mobility investment.”

Some enterprises discover that they lack the expertise or they are ill equipped to handle the influx of new devices. In these instances, enterprises may opt to outsource their MDM solution. “Customers are coming to us because of the complexity of dealing with mobility,” says Bobbie Ramsey, senior manager of managed services for Intermec. “Companies are overwhelmed with it because of the diversity of devices, platforms, and rapidly changing technologies. There are short product lifecycles and regulatory issues to take into consideration, so companies are overwhelmed by MDM, but at the same time realize they have to do it and do it quickly.”

Last year, Intermec launched a service that allows customers to outsource mobile device management, giving them access to technical experts that can remotely track assets, control devices, run diagnostics, download and update applications, and remotely fix the device should a problem occur. This year, Intermec acquired Enterprise Mobile, a provider of lifecycle services for mobile devices, thereby expanding the company’s portfolio of MDM offerings for both rugged and non-rugged devices.
“One of the first things we talk about with customers is their technical expertise,” says Ramsey. “You have some customers that have very large IT departments and have technological and mobility experts in house. Customers like that can use the Enterprise Mobile team to evaluate the business and determine what the best MDM software solution is. Then you have another customer segment that may or may not have an IT department; however, they don’t have that mobility expertise, so now they can outsource that service to us.”

Along with determining the best MDM model for their business, enterprises need to define their objectives and policies. “Sometimes companies don’t think through the implementation and understand what their objectives are,” says Doug Louie, Smith Micro’s senior director of product marketing enterprise. “Since [MDM tools] offer new control that they didn’t have before, companies will have to look at what it is they want to enforce and whether there are certain applications they want to blacklist. If they just put in a system without any control, then they’re not really mitigating any risk. Companies need to identify what their policies are and educate their employees on how to effectively take advantage of these new tools.”

“First, determine the business drivers, platform, and priorities,” says Marshall. “Start simply and quickly with basic privacy, legal, and HR policies, and you’ll certainly learn where to add depth.”

**Employee-liable devices**

One of the most important policies companies need to consider when implementing MDM solutions is security—and the mobile user is often the most vulnerable point of entry when it comes to security threats. Allowing employee-liable devices into the enterprise can place the business at serious risk if such policies are not clearly defined and enforced.

“We’ve seen quite a large amount of interest from enterprises, particularly around security and control, as they wrestle with whether to allow employee-liable devices and how to manage these resources to support these devices as well as maintain the policies in the company,” says Louie.

IT departments are being forced to give up some measure of control when allowing employee-owned devices on the network, but they must strive to find a balance if MDM tools are to be implemented successfully in managing these devices, including any security threats they may pose.

“Most new smartphones are designed for the consumer,” says Rambaldini. “This is a compromise to the business value of such individual-liable devices as the enterprise is unable to ascertain ultimate control and security. Such individually owned smartphone devices require user interaction to manage, which may contradict the policies and requirements of the enterprise.” Furthermore, Rambaldini notes that employees with individual-liable devices may express strong feelings about giving up control of their own devices.
When implementing MDM software, companies first need to decide what level of security they want to enforce on employee-owned devices, says Reed. “You have to decide what security means to your enterprise,” he notes. “What policies should be in place? For example, things like high password complexity, expiring passwords, rotating passwords, encryption of data on the device or over the air, and the ability to remotely wipe a device—to selectively wipe certain parts of the device versus the entire device.”

This can be further complicated by the diversity of devices and operating systems coming into the enterprise. “Not all devices are created equal, so you need to account for the fact that whatever device and applications you choose, you may have slightly different capabilities on each of the different platforms,” says Reed. “For example, users might be asking me to include Android in my standards policy; however, I may have a corporate security policy that requires all data on my mobile devices to be encrypted. And today, you cannot encrypt all your data on an Android device. Part of the challenge is navigating the complexity matrix of what’s technically possible or not and how to blend that with the rules and policies you want to have, recognizing you’re going to have to make some tradeoffs in certain areas because the functional level of different devices or applications is going to vary,” he says.

According to Williams, companies can find a way to adapt to the tradeoffs that come with allowing employee-liable devices to infiltrate the business, provided they have a flexible enough MDM platform. “If I’m managing your computer, which I gave you, I have total control, and that’s what IT’s used to,” says Williams. “If you’ve got your iPad, I’m not going to have total control because it’s yours, and it’s the nature of the operating system. So there’s a bit of a balancing act, and I think it goes beyond the technology. People have to accept that if they’re going to be allowed to use their devices at work there are rules they’re going to have to follow. Some of those rules can be enforced through configuration profiles. So for example, it’s perfectly legal to jailbreak your device, and we can’t stop people from doing that, but we can identify when they have and remove some of their privileges. It has to do with balancing tradeoffs. As a company, I want people to be happier with the devices they use, but I don’t want to put the organization’s resources and data at risk. As an end user, I want the freedom to choose the device I want, but I need to have access to the company resources.”

“In the same way that IT administrator has active directory security groups that allow or deny access to resources, MDM should do the same,” explains Marshall Geyer, director, Mobility Managed Services at Dell. “Any of the policies that can be created must be able to be apportioned to a segment of the population.”

Having a profile-based management solution that can be easily removed from devices is an important principle of MDM software, says Williams. “Again, you’re never going to have 100% control on mobile devices like you do on computers, so you need to have the flexibility to grant privileges and restrictions but also to remove them in a nondestructive way.”

“If your MDM solution has a rules-based framework and event management, the opportunities are immense,” says Geyer.
In addition to security concerns, enterprises will need to decide who pays for what when allowing employee-liable devices on the network. “We’re seeing hybrid models where the user gets a stipend of $100 every three years to buy a new device, and if they want a fancier model they pay the difference,” says Reed. “Maybe the user gets a $50 stipend toward their monthly voice and data expenses, or they’re allowed to expense their monthly bill, or they go onto a master billing system.”

Companies also need to figure out who is going to support the user: “Are you going to have help desk support?” asks Reed. “Do you call a special number? If it’s an employee-owned device, do you call the carrier first? Maybe you only want user self-service, so you establish a Web-based user self-service portal. These questions will help you lay out your policy. You’ll use MDM to help you enforce your decision, but separate from that you need to get yourself organized on what those policies actually are.”

### Security and beyond

Regardless of whether a mobile workforce uses employee-liable devices, corporate-owned devices, or a combination of the two, there are common security controls as well as other policies that companies need to address when implementing MDM solutions.

“The IT manager needs to secure the network and mitigate the risk of data loss while giving the workforce the technology needed to engage in the mobile world,” explains Geyer.

“Companies need to have some boundaries, controls, and processes in place for an MDM program to be successful,” agrees Rambaldini. “To facilitate MDM, businesses must implement policies around the secure and appropriate use of mobile devices by employees. This would include the need for complex device passwords to be set and enforced frequently, corporate e-mail to be authorized and controlled, and secure network connection access to be granted and revoked at any needed time. IT administrators need to be knowledgeable about mobility security risks and the complexity of managing personal and corporate devices on the same network.”

“MDM solutions that leverage OS features—especially with iOS—can easily segregate corporate and personal settings, e-mail, and applications,” explains Marshall. “Enterprises can quickly decide where to draw the line in terms of access to corporate resources. It’s all about the policy decisions.”

### Takeaway

**Security Matters:** Security controls and policies are key parts of a complete MDM solution.

A good MDM solution must be able to manage passwords remotely. “The ability to enforce password restrictions on the device is very important,” says Williams. “Most companies have some type of password standards, so MDM software needs to be able to enforce those same standards on the mobile devices. That also entails a responsibility for IT to be able to reset that password remotely should an employee forget it.”

Another critical function of MDM software is the ability to disable stolen or lost devices remotely. “Simple e-mails and contact databases on a phone are potentially damaging for any company should they get into the wrong hands, no matter what industry you’re in,” says Louie. “The reality is most people don’t even lock their phones, so they’re just leaving their address book open for anyone to see.”
And with the proliferation of tablets being used in healthcare to collect patient information, the impact to a business should those devices be lost or stolen can be financially devastating. “Healthcare providers now have employees collecting data on iPads as they go from patient to patient,” says Louie. “If that device isn’t automatically uploaded then and there, and that information is still resident on that device, losing that one device could cost them upward of $150,000 per incident.

“I’ve not yet heard of a major loss, but I believe we’re close to a tipping point where all it’s going to take is one sensationalized case, where someone’s going to leave a phone or iPad in the back of a cab and some sensitive data is going to make the front page of The Wall Street Journal. People are losing devices all the time, and with the amount of devices and the amount of data on those devices it’s only a matter of time before we see that headline.”

To mitigate these risks, enterprises can use MDM software to perform a remote lock and wipe in the event a device is lost or stolen. “Customers are looking at MDM for additional layers of encryption and security for their data and devices in the form of a lock/wipe feature that can be used agnostically,” says Jay Gordon, VP sales, Enterprise Mobile. “So they can use a single console to perform a lock/wipe feature when a device is lost or stolen for any platform regardless of the manufacturer.”

Additionally, the software’s ability to access geolocation information can help the enterprise locate the missing device prior to initiating a lock and wipe. “If a device is lost or stolen, we can locate that device and make better decisions,” says Williams. “So for example, if my employee says they don’t know where their iPad is, and the last time they had it was at Starbucks, we can look on the map, and if it’s still at Starbucks we can lock it and send a message to the device that reads ‘if you find this, please call this number.’ On the other hand, if the device is in a cab moving down 5th Ave. away from Starbucks, we probably want to take different action at that point and wipe the device out, even if that means losing the employee’s Little League pictures.”

To avoid deleting employees’ personal files unnecessarily, MDM software can also perform a selective wipe: “If a device is lost or stolen, you can use the MDM tool to do a selective wipe, which will only kill the business end of the device, so you’re not wiping someone’s personal photos or their applications,” says Gordon.

To ease the burden on IT, enterprises can choose to relinquish control to the employee if their device is missing. “We provide a portal to the end users so they can register their device,” says Louie. “The solution will automatically download the application and recognize the device. Also, by giving them that portal access, should the employee ever lose that device, they don’t have to call IT. They can go back to the Web site and use the portal to help locate the device. If they can’t find it, they can wipe it without involving IT. So the user can take that first step before IT moves in and has to commit resources.” Smith Micro is also rolling out a feature that will allow employees to activate the camera on a misplaced phone to help them remember where they last left it.
While one of the most important functions of MDM software is to secure mobile devices, Ahmed Datoo, chief marketing officer for Zenprise, warns enterprises to look beyond devices when choosing an MDM vendor to protect their business.

“To protect the mobile enterprise, you’ve got to be able to secure more than just the device,” says Datoo. “Any good security solution is going to have a multilayered approach, and that means protection not only on the device but in the network and protection for applications, because recently these devices are all about apps.”

“Flexible delivery models are critical to adoption,” says Marshall. “Enterprises are increasingly putting e-mail, SharePoint and CRM in the cloud, so it often makes sense to leverage a SaaS offering for MDM.”

Additionally, companies have to allow for an always-on architecture, says Datoo. “That means if your server goes down, you have to have a back-up server that immediately takes over, because if the server you’re using to protect the enterprise goes down, then the whole enterprise is at risk.”

Finally, companies must have the ability to move beyond pilot deployments: “It’s great if you’re managing five or 10 devices as part of a pilot,” says Datoo, “but if you decide to move it across the entire enterprise, you need to be able to protect the entire enterprise.”

Marshall agrees. “When possible, it’s important to consider a global solution capable of advanced grouping or multi-tenancy for autonomy across regions or P&Ls but some level of centralized control and asset management.”

SMBs can benefit from cloud solutions as well. “The cloud offering could be a better solution for smaller organizations that do not have an IT department to take on this infrastructure responsibility or perhaps are facing other internal resource constraints,” explains Boatman.

“MDM solutions are maturing quickly and leveraging SaaS or cloud-based solutions allows enterprises of all sizes to access the same tools in a matter of hours or days,” says Marshall.

With the diversity of mobile devices and applications flooding the enterprise, customers are looking for MDM tools that offer robust application and content management features in addition to security features. A good solution should manage and support mobile applications, including deploying, installing, updating, deleting, or blocking applications as needed.

“Companies need to be able to use the MDM tool to create an MDM application store that’s specific to the organization,” says Gordon. “So for instance, on an iPad there’ll be an icon that says ‘xyz company app store,’ and in there they can publish content, media, videos, and applications that would allow the user to pull those onto their device from that hosted app store.”
Another advantage of MDM software is the ability to export certificates to mobile devices for remote authentication. “A lot of applications that come through Apple have a one-year certificate expiration, so every year a new certificate needs to be sent to that application for it to work,” explains Gordon. “Once a device is deployed, it’s costly and time-consuming to have users ship all their devices back just to have that certificate updated. That’s where an MDM tool really comes into play: to be able to push that certificate out to the device before it expires.”

In addition to the challenges inherent with employee-liable devices, enterprises are focusing on finding MDM tools to help them manage connectivity issues. “Companies are wrestling with connectivity as they deal with Wi-Fi, 3G to 4G, and also hotspot management and the security around that,” says Louie. “Managing connection policies when people are roaming, for instance, or trying to manage the data costs when they’re roaming, is a big challenge. Or just ensuring your employees on the road can make sure they’re securely connected, whether it’s 3G, 4G, or to the Wi-Fi network at Starbucks, has always been a concern. Going to 4G is going to increase the amount of sensitive data that’s potentially at risk.”

Reed encourages companies to consider the lifecycle of the mobile devices in use and how MDM software will integrate with existing enterprise system capabilities.

“There’s a misnomer in the market that MDM is a ‘set it and forget it’ kind of model,” says Reed. “You have to think about the full lifecycle of that employee with that device, those applications, and that corporate data. An employee with a mobile device is not unlike an employee with a PC. Over that lifecycle, there’s a set of policies and services that the enterprise employs to enable you to use that PC and give you rights to access applications and manage that PC in the background.

“What the enterprise needs to do is recognize that a smartphone and a tablet are just like a PC, and they need to make sure they can manage the entire lifecycle of that device and all the applications over that employee’s experience,” Reed continues. “Take those existing systems and processes and make sure you pick an MDM vendor that integrates with them so those processes and techniques for security, compliance, and provisioning all work the same for mobile devices as they do for PCs and laptops.”

Datoo echoes this sentiment: “The MDM tools are only as good as the processes you put around them,” he says. “So you really need to think through how you roll this out, and how you audit users to make sure they’re not sneaking devices on the network. Make sure you have tools in place to enforce the policies you’re setting up. At the end of the day, if you don’t have clearly defined policies and procedures up front, the tools become meaningless because you don’t know what to enforce.”

“Find the right balance between minimizing risk and waiting for the perfect solution,” concludes Marshall.
AirWatch is a global leader in mobile security, mobile device management, and application management software. AirWatch simplifies enterprise mobility with a single console for device activation, configuration, security, management, application distribution, end user support, and full lifecycle management of all smart devices and mobile computers. www.air-watch.com

The power to do more

Organizations today are experiencing the largest ever transformation in client computing. Unprecedented growth and diversification of mobile devices and supported applications has increased the complexity and cost for enterprise IT organizations, making security and manageability a key issue. Learn how Dell’s Enterprise Mobility Solutions address these pain points – and more. http://marketing.dell.com/mobility-solutions

OVATION Wireless Management specializes in complete Mobile Lifecycle Management and partners with industry-leading MDM providers to evaluate and implement each client’s MDM strategy. Ovation brings unmatched wireless industry experience to help enterprises address mobility challenges by supporting, securing, and monitoring the proliferation of smartphones, while optimizing expenses and increasing the productivity of each end-user. www.OvationWireless.com

SOTI Inc. develops industry-leading technology that solves the unique challenges involved in deploying, managing, securing and supporting remote mobile and desktop computing devices. 80,000+ customers around the world in retail, manufacturing, health care, government, logistics and other industries rely on SOTI to reduce the costs associated with supporting mobile field-forces. www.soti.net

Sybase, an SAP company, delivers enterprise software to manage, analyze and mobilize information. We are recognized globally as a leader, proven in the most data intensive industries across all major systems, networks and devices. Our mobility management solution, Afaria, delivers power and flexibility for application and device management for iOS, Android, Windows and more. Contact us at 1-800-8SYBASE.