IDG

Good

Evaluating Approaches to Mobile Security

What you should know about MDM, Containerization and EMM

MOBILITY HAS TAKEN ENTERPRISES BY STORM, increasing collaboration and spurring productivity. But device management by itself has been a headache for administrators—especially when it comes to balancing the organization's need for security and control over applications and data with end-user desires for a positive mobile experience and assurance of personal privacy.

Increasingly, enterprises are opting for new enterprise mobility management (EMM) capabilities that complement device management by mobilizing and containerizing business apps and content. In fact, according to technology market research firm IDC, the number of enterprise applications optimized for mobility will quadruple by 2016, and IT organizations will dedicate at least 25 percent of their software budget to mobile application development, deployment, and management by 2017.

IT, though, may find this evolution challenging. For example, IDC states, "Difficulties linking mobile platforms to existing databases will cause 45 percent of mobile enterprise app initiatives to be delayed or go over budget in 2015."

For many organizations, realization of the full potential of mobility still lies over the horizon. They are often held back by device-centric management strategies that ultimately result in compromises on security and corporate data protection and, worse, blur the lines between personal and company data.

Moving mobility beyond the basics

In the past, mobility strategies were fairly straightforward: Businesses issued company-owned Blackberry phones and laptops to employees. IT was able to tightly control data and applications. But the proliferation of smartphones and tablets ripped the management fabric apart, often at the behest of top executives who wanted to be able to use an iPhone or iPad.

"There was some hesitance initially, but mobile device management was a nascent technology that IT was able to bring into the enterprise to enable executive leadership to get email on their cool new iPhones," says Jeff McGrath, senior director of product marketing with Good Technology, a supplier of secure mobility solutions since 1996.

Mobile device management (MDM) leverages device-level controls that are made available by the mobile OS vendors. MDM solutions were broadly implemented to bring devices under the control of the enterprise when configuring basic services such as email and Virtual Private Network (VPN) access.

Then, adds McGrath, “users throughout the enterprise started demanding the same thing, but that created even more expectations.” No longer satisfied with simple email access, users now want to use mobile devices to access business applications to work from anywhere without lugging around and firing up a laptop.

The availability and lower-cost of consumer-focused mobile devices meant mobility was available to all employees. The burgeoning consumer market fueled an explosion of readily accessible applications and eventually cloud-based services that anybody could download to a mobile device, regardless of whether it was company or personal property.

The proliferation of devices and apps, along with frequent operating system upgrades exposes the limitations of MDM, according to Brian Reed, Chief Mobility Officer with Good Technology. “MDM can configure how a device connects and what type of passcodes need to be on the device, but there is nothing in MDM that is actually security technology; it is just configuring whatever security may already be available on that device. And, it does little to secure applications.” says Reed.

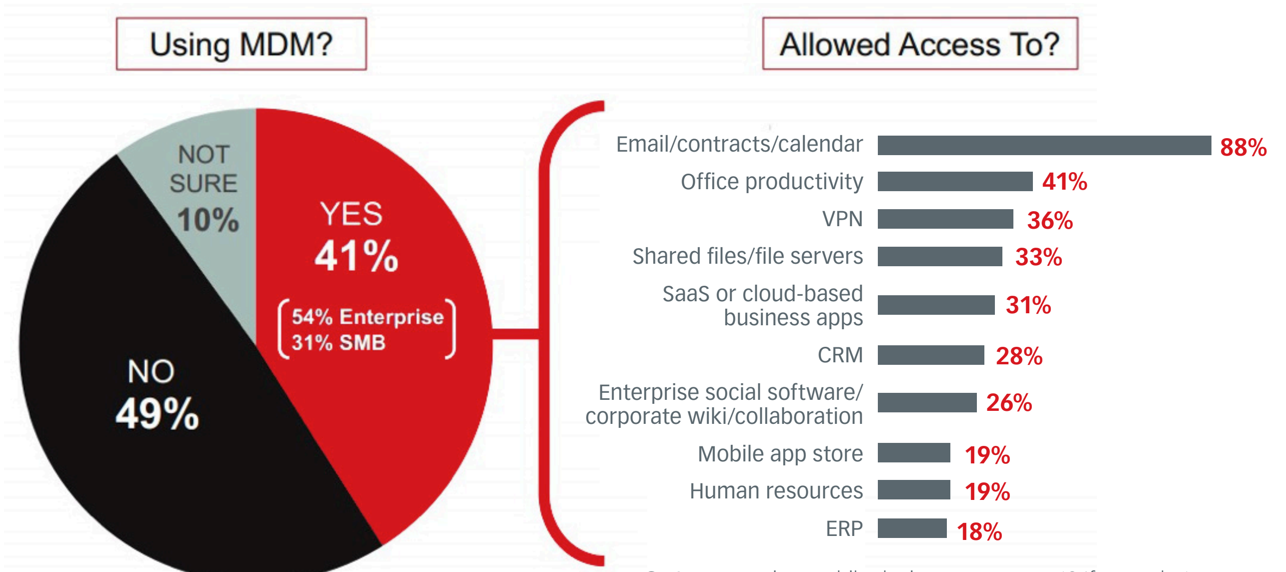
MDM also raises a host of personal privacy issues that may concern workers. The solutions generally allow IT to remotely “wipe” a mobile device if it is lost or stolen, or when an employee leaves for another job opportunity, but that includes wiping personal data and apps in the process. Additionally, the ability of MDM to detect “jail breaking” of iOS devices and “rooting” of Android devices, is dependent on location-based tracking services, which raises additional privacy concerns, can drain batteries and cause sluggish performance.

Conversely, with MDM, IT has little control over users’ ability to copy data from a business application into a consumer application, or a cloud file sharing service. To control such misappropriation of data, many companies using MDM are limiting user capabilities. According to the Computerworld Forecast 2015 survey of IT leaders, most companies using MDM allow user access only to email, contacts, and calendar functions, while just 41 percent let users connect to office productivity apps, and even fewer allow mobile remote access to VPN, shared files and file servers, or cloud-based business applications.

Adjusting to the app-centric reality

MDM by itself doesn’t provide separation between business applications and personal apps on a mobile device. That often leaves IT struggling to meet the needs of workers without having to compromise between data security and user experience. For

Limited Mobile Access Granted for Company Resources



Q: Are you using mobile device management? If yes, what company resources are you allowed to access from their mobile devices?

SOURCE: *Computerworld* 2015 Forecast Study

“Mobile device management tools are transforming into enterprise mobility management (EMM), which includes app and data security, among many other things.”

SOURCE: *Computerworld* 2015 Forecast Study

example, enabling a complex device passcode to protect corporate apps on the personal device forces users to enter that code—even if it’s just to make a phone call, text or listen to music—all in the name of corporate security policy.

“With MDM there are very limited ways for administrators to control business data on the device,” says McGrath. “For example, if I’m getting email on my device, any attachments that contain proprietary information could be moved to a personal cloud, like Dropbox, or the information opened into personal apps I may have downloaded just to be more productive, like a document editor or some other tool.”

As a result, IT has little ability to ensure that data remains within the corporate security umbrella. Proprietary information may find it’s way to personal file sharing services that can’t be wiped, or even detected if a worker takes a job with a competitor. Corporate legal staffs aren’t able to fully execute electronic discovery requirements because they don’t have access to data stored within personal apps or personal cloud services. The ability to manage and monitor workflows and business processes may be very limited.

Meanwhile, users want more from mobility and are increasingly interested in progressing beyond email to collaboration and mobilizing existing business processes, but MDM does little to enable those goals.

“What makes mobile work is the apps on the device, the data and back end applications they can access, and the tasks users can accomplish. MDM might configure a device and connect it to the network, but it doesn’t really do anything to enable the applications,” Reed says.

A key driver for collaboration is the frequent use of documents sent as email attachments spurring demand for document editing as well as access Microsoft SharePoint, file shares, and intranets to document-based workflows can be completed on their mobile devices. These capabilities are not inherently part of MDM and may require the organization to purchase additional solutions.

Clearly MDM is not sufficient to meet the needs of the enterprise. As *Computerworld* reported, “Mobile device management tools are transforming into enterprise mobility management (EMM), which includes app and data security, among many other things.”

In fact, according to the 2015 *CIO* magazine Tech Poll: Tech Priorities, 48 percent of respondents say their companies already have EMM in pilot, in production at the business unit or division level, or in production enterprise wide. Furthermore, 52 percent are increasing spending on EMM while 33 percent say their spending in this area will stay constant.

In 2014, according to *Network World,* Gartner upset more than a few solution providers when it overhauled its mobility management Magic Quadrant to focus on Enterprise Mobile Management, rather than MDM. “According to [Gartner], EMM suites provide core functions that include hardware as well as application inventory; OS configuration management; mobile app deployment and configuration; remote view and control for troubleshooting; the ability to execute remote actions, such as remote wipe; and mobile content management.”[1]

Key components for a more robust EMM suite include MDM along with:

- **Mobile application management (MAM),** enabling IT to manage business applications with the security controls, administration, and monitoring capabilities expected of other information systems.
- **Mobile content management,** so users can access content repositories in SharePoint or other document management systems, file servers, web apps, and portals.
- **Mobile service management,** to monitor quality and performance of mobile services, including applications, in real-time across backend systems, mobile servers, NOCs, carrier networks, and devices
- **Application deployment** and management capabilities

Containers emerge as MAM technology of choice

EMM expands mobile security capabilities beyond the device to encapsulate the applications themselves. “By Gartner’s definition,” *Network World* reports, “EMM content management includes a ‘secure container’ that lets the user store content securely on a mobile device; ‘content push’ that allows for push-based delivery; and ‘content access’ as a connection to a back-end repository where users can pull content to their devices.”

App containerization technology provides each managed app, and its data, with its own secure runtime container. Containerization, typically

[1] www.networkworld.com/article/2361467/wireless/gartner-magic-quadrant-shifts-focus-from-mdm-to-enterprise-mobility-management.html

delivered via a mobile app security platform, causes an app to transform in multiple ways: the app data is encrypted and segregated from all other apps; native OS runtime system calls are replaced with equivalent secure versions; and secure back end connectivity and app-to-app secure workflows are enabled.

Some solution providers offer alternatives to containerization such as virtualization to provision secure enterprise applications. But virtualization requires compromises that fracture the mobile user experience; for example, they require an always-on connection to be effective and essentially seek to recreate the office desktop environment on a much different mobile form factor.

“Virtualization solutions were developed primarily for Windows apps and desktops, and the applications are designed for PC screens and navigation using a mouse and keyboard, so users are generally not very satisfied with the mobile experience,” says McGrath.

Another alternative is the dual-persona approach, which creates two completely separate and different environments on the mobile device — one for business and one for personal activity and apps. The problem with this approach is that the user has to completely exit one environment and then launch the other environment to access its applications.

“With a dual persona solution, I’m forced to basically have a different phone within my phone just for business,” says McGrath. “If I’m working on my document editing app for work, for example, I have to exit my business persona and return to my personal environment to utilize my texting capability.”

Mobile motivation

Many companies adopted MDM as a means to solve an immediate problem. Today, organizations are looking to move beyond problem-solving and utilizing mobile as a key element in their business strategies.

The motivation may be as basic as adapting key business processes such as a Salesforce opportunity entry or Microsoft Word document editing. In many cases the driver is improving client engagement in the field with instant-on devices and apps, or mobilizing the remote workforce. Others have identified specific job functions they can better accomplish with a tablet or smartphone.

“The key issues in determining an enterprise mobile management strategy are identifying the roles that are being mobilized, determining what tasks they need to be able to do with a mobile device, and finding a way to securely provide the mobile apps that will enable tasks and workflows on mobile devices,” says Reed.

Mobility shouldn’t have to be about compromising security and risk management to enable business innovation, user satisfaction, and operational productivity. Leveraging secure mobile app containers makes it possible to drive user productivity and satisfaction without having to compromise.

GOOD™ to GO

With secure app containerization, as implemented in the Good Technology platform, the core look and feel of a user’s device stays the same, while business applications themselves are secured. Users may place each secured business app wherever on the springboard they choose so they have complete control.

Good Technology provides a suite of core secure productivity applications with its EMM solution to simplify access to email, calendar, contacts, enterprise instant messaging, Intranet access, CRM, and document access and editing. Good also has an ecosystem of ISV partners with over 100 apps available built on the Good platform to extend Good’s application set. These apps already incorporate Good’s next-gen containerization that includes secure data sharing between any Good-secured app as well as app-level encryption independent of the device used.

Beyond basic collaboration apps, enterprises and ISVs can utilize the Good platform technology to build secure containerized apps with enterprise-level policy controls leveraging SDKs available for iOS, Android, and Windows Phone as well as a plug-in for hybrid apps A simple wrapper for pre-compiled apps is also available.

For example, in 2015, Microsoft introduced Dynamics CRM for Good, a Good-secured version of Microsoft’s flagship CRM solution.

Good Technology delivers the world’s most comprehensive secure mobility solution, and continuously develops new innovations for mobile security, manageability, scalability, and usability. For more information on creating an enterprise mobile mobility platform, please go to **https://www1.good.com/about/why-good.html**.