Organising to choose Enterprise Mobility Management

MDM is no longer sufficient

By Charles Brett, June 2014

Originally published by

Mobile Device Management (MDM) is only one part of the broader Enterprise Mobility Management (EMM) jigsaw, albeit it a starting point. Now that Microsoft has joined heavyweights like CA, Dell, Good/Boxtone, Fujitsu, IBM, SAP, Symantec and VMware in offering more than MDM for enterprises organisations will need to identify which vendors offer what that enterprise requires, for not all will need the same from EMM.

This consideration will apply across two dimensions:

- What the individual enterprise needs now, and will need
- Which of the major vendors can deliver against this.

Of two things we can be sure. Not all EMM 'suites' have been created equal. Furthermore not all will remain equally competitive.

Within EMM there are already at least six primary categories to consider, and within each there are subcategories. The primary ones are:

- Mobile Device Management (MDM)
- Mobile Content and App Management
- Integration tools for connecting to back end systems
- Mobile Development (including both front and back ends)
- Mobile App and Device Performance Evaluation
- Identity, Security and Risk Management.

As its name suggest MDM focuses on the device. Most obviously this is about the enterprise knowing what the characteristics are of those devices that the enterprise knows about. This can range from determining which OS and version a device is running through to locking or wiping devices if they are lost or stolen through to black and white listing of apps. Device specific as well as user and role specific policies are an integral part of automating as much as possible of device management which almost always now includes elements of self-service and self-support. In practice, while there are significant differences in how different vendors deliver parts of MDM, the practical functionality is becoming ever more similar.

Whether ever increasing similarity explains a part of why EMM has emerged or whether enterprise customers realized that they needed more than MDM could provide is moot. Today's reality is that vendors who wish to succeed in the enterprise mobility need differentiation. This has led the majors to expand their visions, most notably in refocusing:

- Away from the device itself
- Onto what each device can and should be allowed to do.

Mobile App and Content Management is the first part of this broader view. Content management focuses on matching content to the consumer of that content and to the enterprise's policy for classes of content. In effect the sensitivity of the document determines who can view on a mobile device or download it to a mobile device or copy (or send) it to someone else. App management has similar characteristics: the objective is to match apps to authorized users as well as to ensure that enterprise IP-sensitive apps cannot leave a mobile device. A third variant within this category is corporate email, still the most used of applications but one which requires specific controls and considerations. All the major EMM vendors provide capabilities here.

Somewhat different is integration to existing IT apps and data. This embraces, for example, the ability of mobile devices to work with ERP or customer support or data warehouses and other corporate resources. This varies from access being enabled via by browser-like sessions through to interworking embedded within mobile apps running on mobile devices. In some instances specialized tools, that are not complete apps, may be used – for example from business intelligence suites. Then there are tools like SAP's SUP which facilitate device to ERP connectivity where integration to existing apps and data (usually) presumes that the apps and data remain in the enterprise data centre with constrained access from the mobile device.

Mobile Development relates to the creation of new apps for use on mobile devices. The scope is broad with many aspects ranging from the development of a mobile app through DevOps/Lifecycle management specifically aimed at mobile through distribution of these apps out to the field. One of the most difficult areas in developing for mobile devices is their variety (think of the many form factors plus OS variants -- from iOS to multiple Android versions, to Windows Phone and Blackberry and others). CA and IBM currently are making much noise in this category (others will catch up) which is mainly applicable to those enterprises which believe that they have or will need to develop their own mobile apps and app/application combinations.

Mobile App and Device Performance Evaluation is a new category. It is not one that is particularly well served. IBM bought TeaLeaf to enhance its offerings and has also introduced Mobile QA wherein users can provide feedback and how-they-use-the-app data which can be analysed so that apps can improve. In contrast Symantec talks about an app rating service. Boiled down Mobile App and Device Evaluation embraces the capability to understand how mobile apps are used in practice. It can vary from being able to step through what a user does (and does not do) to seeing where in a process a customer stops buying. A second variant assesses apps for their acceptance, usability or even vulnerability to outside attack (which, arguably, is an only a mobile-relevant extension of what traditional application performance management vendors like Compuware have been doing for a long time). A third is to offer 'wrapping services' to third party app developers so that their apps can achieve a form of enterprise certification. In this last category IBM and Symantec seem to have capabilities here today though it is likely that others will follow.

Identity, Security and Risk Management bring together a cornucopia of enterprise issues -- from Single Sign On, User as well as Device Authentication, conventional security and pro-active security. All of security involves Risk Management and its assessment, which is vital when mobility for the enterprise is introduced into the equation. By their very nature mobile devices are easy to steal or lose or access. Ensuring that appropriate controls exist and are implemented is one imperative. A second is to think about pro-active security where some vendors are able to supply early warnings of possible threats because they have the research depth and competence to anticipate threat patterns. The good news is that most of the major EMM vendors have proven strengths, or good alliances, to deliver mobile security at levels an enterprise needs. The larger challenge, however is to operate this enhanced security as invisibly to users as possible while still ensuring that corporate requirements are met.

Besides the six primaries outlined above there is one other important factor: EMM integration. While it is possible to acquire most of the capabilities described from multiple vendors, and self-integrate, too much of this is probably not desirable, partly because of the expense and partly because of the potential to leave unintended 'holes'. While not all enterprises will need all the primary capabilities, enterprises should weigh the degree of integration across what they do decide they need. Insufficient EMM integration runs the risk of creating those unintended weak spots.

Mobility and the enterprise are increasingly intertwined. MDM is established but is no longer sufficient for the future. Enterprises envisaging significant mobile adoption should now begin to consider how to define what their needs are for Enterprise Mobile Management and then start to investigate which vendors might be candidate suppliers, especially for when existing MDM contracts expire.

About Freeform Dynamics

Freeform Dynamics is a research and analysis firm. We track and report on the business impact of developments in the IT and communications sectors.

As part of this, we use an innovative research methodology to gather feedback directly from those involved in IT strategy, planning, procurement and implementation. Our output is therefore grounded in real-world practicality for use by mainstream business and IT professionals.

For further information or to subscribe to the Freeform Dynamics free research service, please visit www.freeformdynamics.com or contact us via info@freeformdynamics.com.