Enterprise Mobility Management
Solution to Manage, Analyze and Control the Mobile Devices, Applications and Content

This paper highlights what is the need of Enterprise Mobility Management for enterprises, and how an enterprise can choose right Solution to Manage, Analyse and Control their Device, Application and Content based on business requirements.
Need for Enterprise Mobility Management

The challenge

The mobile device is fast becoming the preferred medium of accessing the internet, enterprise data and also personalized information. According to Gartner in their report titled: “Tablet Market And Smartphones Market: Global Database & Forecast (2010 – 2015),” by 2014, 1.3 billion smartphone & tablet devices would be sold worldwide.

The deluge of devices and apps written for them is fast becoming a nightmare for Enterprise IT to manage and maintain. The devices also bring in security and access related issues with them.

For example, when users are bringing their personal devices to work, they are also bringing in their own network. Through personal devices, employees can create a wireless hotspot, and by tethering their mobile devices to laptops or other corporate devices they can put corporate data and information at risk. The usage of corporate data and applications usage on such ad hoc networks cannot be monitored. This means that IT policies should be framed for network access also. If this is done then the mobile devices become part of security issue for enterprises.

The diagram below shows some challenges faced by enterprises, IT departments and end users in industry.

The solution

The solution to the problem lies in ability to manage Devices, application and content within the enterprise. Such solutions are commonly available under the banner of Enterprise Mobility management (EMM)

However as each business is unique, so are its needs for mobile enablement. While certain businesses would require stringent control on Device, Application and Content, for others, control on Application and Content would suffice.

Depending on the specific nature of requirements, the enterprise will need to tailor its EMM Solution.

Next question is what if only 'D', 'A' or 'C' matters for business requirement? Answer is complex and objective now.

There are 4 main flavors of EMM solutions in market viz.

- Mobile Device Management
- Mobile Application management
- Mobile Content management
- Bring your own device (BYOD)

It is up to enterprise to evaluate which solution to choose out of this A (MAM), B (BYOD), C (MCM) & D (MDM).
The following sections will look at each of the solution in detail.

MDM

- MDM (Mobile Device Management) is about controlling the device to manage, secure and control the devices.

- MDM Capabilities usually include security management, device configuration management, policy management, enterprise network integration, remote data wipe, blacklisting/whitelisting of apps/devices and many more but mainly at device level.

- MDM solutions create agent on the device which runs as a daemon and monitors under all enterprise policies. To access native platform offerings, in some cases, MDM vendors may have to get devices preconfigured through OEMs also.

When it is not perfect EMM solution?

- Employees have to carry two devices – personal and professional, in order to ensure segregation between enterprise and personal data.

- MDM is mainly suitable for enterprise owned devices as it controls the device as a whole which may not be accepted for BYOD (Bring your own device) as well as for B2C where users own their own devices for corporate work also.

- MDM can execute intelligence based on the enterprise policies configured at the device level. It is not suited for scenarios where enterprise policy or rule has to be applied on selective applications or to application specific data. Since the agent runs as a daemon process at device level, it cannot control and monitor health and performance of each application at individual level.

- In addition to device procurement cost, the operational and capital cost for MDM solution deployment does not make it cost effective.

MDM Solution vendors

Some of the popular MDM solutions available in the market include SAP Afaria, Mobile Iron, Good technology, Citrix, AirWatch, Kony, BoxTone etc…

MDM Research

As per Gartner and Forrester reports on MDM, here is their recommendation and evaluation for top MDM service providers in the world.
BYOD
• BYOD (Bring your own Device) is a new popular concept in enterprise mobility management where enterprises allow employees to bring their own devices to work. This enables enterprises to mobilize their business in a more cost effective manner by not doing any device procurement at all.

When it is not perfect EMM solution?
• BYOD secures the number of applications for enterprise mainly by providing container approach within which all enterprise apps can work. However, most of the time, transitioning out of this container to personal space of device becomes a problem as policies don’t allow using both spaces of device at the same time.
• End user uses the same device for professional and personal use, which implies that there is always a security threat to the corporate data, as it can be shared across personal apps, until comprehensive BYOD strategy is implemented by IT department.
• Enterprises that support BYOD would need to create applications on multiple platforms each of which need to be enterprise approved.
• In scenarios where, organizations have to contend with user’s privacy concerns by letting them allow private apps like contacts, emails while allowing them access to corporate data at the same time, puts this sensitive info on security risk,
• In BYOD, all the applications have to be run under same enterprise policies irrespective of the app security level
• BYOD is trend which is getting popular and on high demand by enterprise in mobility. However, unlike hundreds of vendors in MDM, BYOD is still evolving.

BYOD solution Vendors:
MobileIron, GOOD, AirWatch, Kony, AmTel, Symantec, Citrix (Zenprise), Cisco, Juniper, etc…

MCM/MIM
• MCM (Mobile Content Management)/MIM (Mobile Information Management) is analogous to a bank locker where enterprises can safely deposit their secure and sensitive data. Irrespective of MDM, MAM or BYOD, the main concern of the enterprises or end users boils down to data security.
• User authentication, data access/ wipe as per Policy configuration, Data security over the air and data at rest, data sharing protection, data version update, and data modification detection and sync content between device-server are the main features of MCM solution.

When it is not perfect EMM solution?
• From technical perspective, it has to do with persistent memory of a device which is accessible only through native APIs. Hence, native mobile apps are must to implement MCM/MIM.
• Limited platform support. E.g. iOS and android only are supported by MIM solutions,
• Solution focus is around corporate data only. Hence, does not manage or control devices or applications.
• Very few vendors support the MIM / MCM.

MCM Solution Vendors:
Air Watch

MAM
• MAM (Mobile Application Management) is glue between MDM and BYOD strategies. It is the solution to manage the lifecycle of a mobile application.
• MAM is the EMM solution which can rightly fit the enterprise MAC (manage, analyze & control) needs in B2C, B2B or B2E industry segments unlike MDM which is preferably most likely to be the solution for B2E apps for corporate owned devices.
• When MAM has to offer the solution at application level, it still has more power to offer more at enterprise policy and configuration management at each application level. Thereby it offers more integrity with app specific data and its security.

When MAM is not a perfect EMM solution?
• Unique policy management and IT specific configuration cannot be offered at device level unless the containerization approach is followed.
• Control can be at container or individual app level only.
• Version upgrade for the agent or SDK becomes difficult since this is bundled along with application. Entire application has to be upgraded to support an agent or SDK upgrade. However, this is only in case of container based approach.
• Validation and certification of private applications to detect the malicious code and malware third party app/ code integration is complex task. This is similar to deployment process which has to be followed before uploading an application to public app stores like apple app store.

MAM Solution Vendors
Afaria, Good, MobileIron, Mocana, Apperian, AirWatch, Kony, AppBlade, BoxTone etc…
What should Enterprise look for in EMM Offerings?

A good EMM solution will have multiple features. These include

**Application Deployment**
- For B2E & B2B, applications are provided through enterprise app stores. As a part of EMM, enterprise app stores define the process like app validation, certification and provisioning the same to valid users on allowed devices.
- App stores developed as a part of EMM solution assure the accessibility of certified applications to valid users on authorized devices which is not the case with public app stores.

**Device Authentication**
- Device identification and validation to check if the device is owned by enterprise or end user.
- Registration of the users on valid devices based on multi factor authentication like OTP (One Time Passcode).

**User Authorization**
- Application access and usage for users based on the status of enterprise registration, location or defined policies.

**Version Control Management**
- Application version upgrades notification based on the device OS compatibility check.
- Disabling the app access in case of mandatory upgrade to address security flaws.

**Geo/Location based authentication**
- Allowing or disallowing application or data access based on user’s location is a good feature for enterprises that want to track their employees’ location for on field operations.

**Push Notifications**
- Dashboard or portal operators can push the data or event notifications like version updates, remote data wipe, configuration updates or policy updates to application when the app is not connected to the server.

**Data Security**
- Data protection policies should be configured to secure any sensitive data.
- DAR (data at rest) should be in encrypted mode using a dynamic encryption key.
- Disable any data sharing applications or utilities on device e.g. personal email, messenger apps, camera, Bluetooth, 3rd party apps integration etc…
- Confidential documents to be deleted from device based on “time to live” certificates.
- Provide data security in transport layer with encrypted data communication on top of SSL protocol offerings.
- Provide transport layer security by implementing asymmetric encryption key algorithms.
Statistics & Reports

- Real time customized reports to help enterprises plan and revise their mobile strategies. For example, reports like application usage vs. platform, app vs. platform versions (especially for android platform), application vs. device OEMs (in case of B2C), application vs. locations, apps distribution vs. enterprise etc… can be good measurement parameters.

Dashboard

- Login management and Role based access to web console operators.
- Configuration of policies at enterprise and application level dynamically.
- Generate statistics and reports on predefined and customized types.
- Accessibility to block/unblock, deregister, data wipe, version update feature injection through web console at device, user or app level.
- Easy and effective user interface to provide Support activities.

Policy Management

- Policy can be static or dynamic and is a set of rules applied at user, device or application level based in many conditions. Few examples are:
  - App provisioning only to certified OEMs devices.
  - Blacklist malware apps installation or usage on any device.
  - Disallow jailbreak or rooting the devices which are owned by enterprises.
  - Allow enterprise app access only during working hours
  - Disable application access in case of unauthorized location.
  - Selective data wipe in case of multi users accessing same device.
- Full data wipe in case of blacklisted device or user.
- Block particular version of an application based on security flaw or major bug found.
- Push notification for version update to be sent to executive or privileged customers first.
- Restriction on number of login attempts in offline mode & disable app access if it exceeds.
- Disable device or app access unless lost or stolen device is recovered.
- Disable app access in case device operating in offline mode since N days

Remote Data Wipe

- In case of device gets lost or stolen or gets blacklisted due to any enterprise defined policy, wipe the data at application or container level. Data wipe should be supported in offline mode.
- Types of remote data wipe which can be preferable for MDM/MAM/BYOD based on enterprise requirement
  - Factory reset ---- MDM
    - Removes all the downloaded apps, personal data, settings and all the changes user has made to device after purchase. Device resets to new handset state.
  - Enterprise Device wipe --- MDM/BYOD
    - Wipe only enterprise email account and profiles, messages, corporate contacts, policy configuration.
    - This option does not affect personal data like Gmail account mails, public apps, media files or personal downloaded data.
  - Container wipe --- MAM/BYOD

Solution Integration Effort

- After evaluating for the features offering by EMM vendors, next biggest challenge is deployment and integration effort to adapt the solution to the needs of the enterprise.
- How much code repacking needed, whether it is different per platform, version upgrade for enterprise private apps vs. version updates in vendors device agents are important factors.
- Enterprise apps installed within secured data container will be removed along with all associated data. Again the option is offered as Full or Partial data wipe where partial wipe is offered either at user profile level or at personal-official data partitioning on the device.
- Selective Application wipe --- MAM
- Uninstallation of application from device along with data, configurations, and settings wipe for that app only.
EMM Solution Approaches

1. Device Centric Approach:
   • Solution runs as a daemon process in device. This would be native application.
   • Mainly an MDM approach which controls and monitors at device level
   • Vendors: Sybase Afaria, McAffee, Symantec etc…

2. Containerization with SDK:
   • Solution is provided through SDK/library which should be integrated with mobile application.
   • Many MAM and BYOD go with this approach due to more control and security at app and data level.
   • There are containerization approaches where multiple applications are executed in single container environment to create virtual data partitioning between personal and enterprise apps on device.
   • Advanced features like data sharing between enterprise apps, persona based app and data management, custom app specific policies etc. is possible.
   • Vendors: Mobile Iron, Good, Sybase Afaria, Kony, AirWatch, Zenprise, Symantec etc…

3. Containerization without SDK:
   • Solution is to wrap the application with secured container without any code integration or source code changes which is the main advantage of this approach.
   • Many MAM and BYOD solution providers prefer this approach.
   • Executable of mobile application just needs to be deployed at the vendor’s on-premise enterprise network or on a secure cloud environment.
   • There can be some limitations with this approach like advanced features like allowed data sharing between enterprise apps, supporting multi user profiles, scenario based authorization etc. may not be possible.
   • Vendors: Good Dynamics, Mocana MAP & all partners like BoxTone, Apperian.

4. Remote Streaming:
   • This approach creates virtually separate space on mobile for application where app is isolated from device specific settings, configurations and interaction with other apps in any means.
   • Solution delivers applications on users’ devices through application streaming from hosting servers in the datacenter.
   • This solution is more generic in terms of device types (handheld devices, desktops, printers & other peripherals), operating system/platform type or nature of an application (native or thin client).
   • Vendors: Citrix XenApp

5. Network Based:
   • This unique approach gathers the real-time contextual information from the network, devices (either laptop or handheld or any other non-telephonic devices) and users.
   • It runs more on network measurement and instrumentation out of IP packets traversing on network between device and enterprise server wall.
   • This provides security framework for any wireless devices, desktops or even wired/wireless peripheral devices like printers since they detect data at network layer like SSL/VPN/WLAN.
   • Limitation lies in the fact that approach has huge dependency on the infrastructure.
   • Vendors: Cisco, IF-MAP, Juniper Junos Pulse

EMM Deployment Architecture

There are two distinct approaches available to deploy Enterprise Mobility Management solutions viz.

1. On-premise deployment
2. Hosted on secure cloud data center.

Following is on-premise deployment view of most of the solution providers in mobile management space. It can change based on enterprise backend infrastructure and deployment requirement.
Infosys Mobile Application Management (iMAM) Solution

Infosys offers a comprehensive mobile application management solution to meet the needs of enterprises to manage their mobile app deployments.

- With the explosion of B2C mobile apps, there is a strong need in the market for Enterprises to control the application version, security, data, etc. This is particularly needed in case of applications like Banking, Payments, Loyalty, where critical personal information/data is being stored/transacted from the Mobile device.
• The main challenge with B2C mobile application is posed when the device on which the app installation is to be done is not owned or controlled by the enterprise. The architecture and pricing of other MAM solutions in the market is such that it is not suitable for large scale deployments in B2C context.

• Infosys MAM Solution is a lightweight Mobile Management solution which allows enterprises to have accessibility, manageability, and control over the applications for right users on right devices.

• Infosys Mobile Application Management Solution helps enterprises manage their mobile application's life cycle in the following way:

   - Submit
   - Deploy
   - Govern
   - Provision
   - Retire

   - Add app
   - Validate app
   - Certify for deployment

   - Deregister
   - Remote wipe
   - Decommission

   - Control
   - Monitor
   - Secure

   - Pilot/Alpha release
   - Configure rule engine

   - OTA install/Upgrades
   - Device compatibility check

   - Pilot/Alpha release
**Conclusion**

More than 100 solutions in the market to manage more than 1 billion mobile devices loaded with millions of public-private apps. There is no one size fits all solution.

<table>
<thead>
<tr>
<th>BYOD</th>
<th>MDM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Employee personal device UX better</td>
<td>Complete monitoring &amp; control of enterprise device possible</td>
</tr>
<tr>
<td>Enhances business productivity</td>
<td>Limited choice of devices</td>
</tr>
<tr>
<td>Reduces enterprise infrastructure cost</td>
<td>UX is very poor for end user</td>
</tr>
<tr>
<td>Security threat for enterprise data</td>
<td>Factory resets the device</td>
</tr>
<tr>
<td>IT process modifications must</td>
<td>Costly for enterprises</td>
</tr>
<tr>
<td>It is BYOD, Not BAD</td>
<td></td>
</tr>
<tr>
<td>Heavy on employee pocket</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>MCM</th>
<th>MAM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secure content locker</td>
<td>No interference to UX</td>
</tr>
<tr>
<td>Auto/manual Data sync</td>
<td>MM solution for B2C &amp; B2B</td>
</tr>
<tr>
<td>Worth deploying only for B2E</td>
<td>Application level control</td>
</tr>
<tr>
<td></td>
<td>Mobile OS agnostic solution</td>
</tr>
<tr>
<td></td>
<td>IT rule modifications not needed</td>
</tr>
<tr>
<td></td>
<td>Perfect glue between MDM &amp; BYOD</td>
</tr>
</tbody>
</table>

<p>| |</p>
<table>
<thead>
<tr>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Secures mainly data/content</td>
</tr>
<tr>
<td>Achievable with effective data manage module of other MM solutions also</td>
</tr>
<tr>
<td>Complete monitoring &amp; control of enterprise device possible</td>
</tr>
<tr>
<td>Limited choice of devices</td>
</tr>
<tr>
<td>UX is very poor for end user</td>
</tr>
<tr>
<td>Factory resets the device</td>
</tr>
<tr>
<td>Costly for enterprises</td>
</tr>
<tr>
<td>No device level control</td>
</tr>
<tr>
<td>Portioning can affect application performance</td>
</tr>
</tbody>
</table>
Finally organizations who need to get mobility management should decide upon a solution based on:

- What is main business objective? Target users are B2C or B2E?
- Who owns the device?? BYOD or COPE (Corporate owned personally enabled)?
- Are there public or private applications?

- Both MDM and MAM can resolve BYOD issues. What level of control required?
- Does enterprise already have one MDM in place? Both MAM and MDM can coexist.
- Least cost of Ownership and easy to use / deploy.
- Is solution meeting NFRs on scalability, availability, multi tenancy, multi device-multi user mapping?
- Operation management for device procurement or reimbursement for data
- Platform and Device Diversity support
- Cost & Support provided by vendor.

About the Author

Payal Patel

is a Senior Technology Architect with Infosys. She has over 9 years of experience in Mobile related technologies and her interests and expertise include Mobile Management technologies.