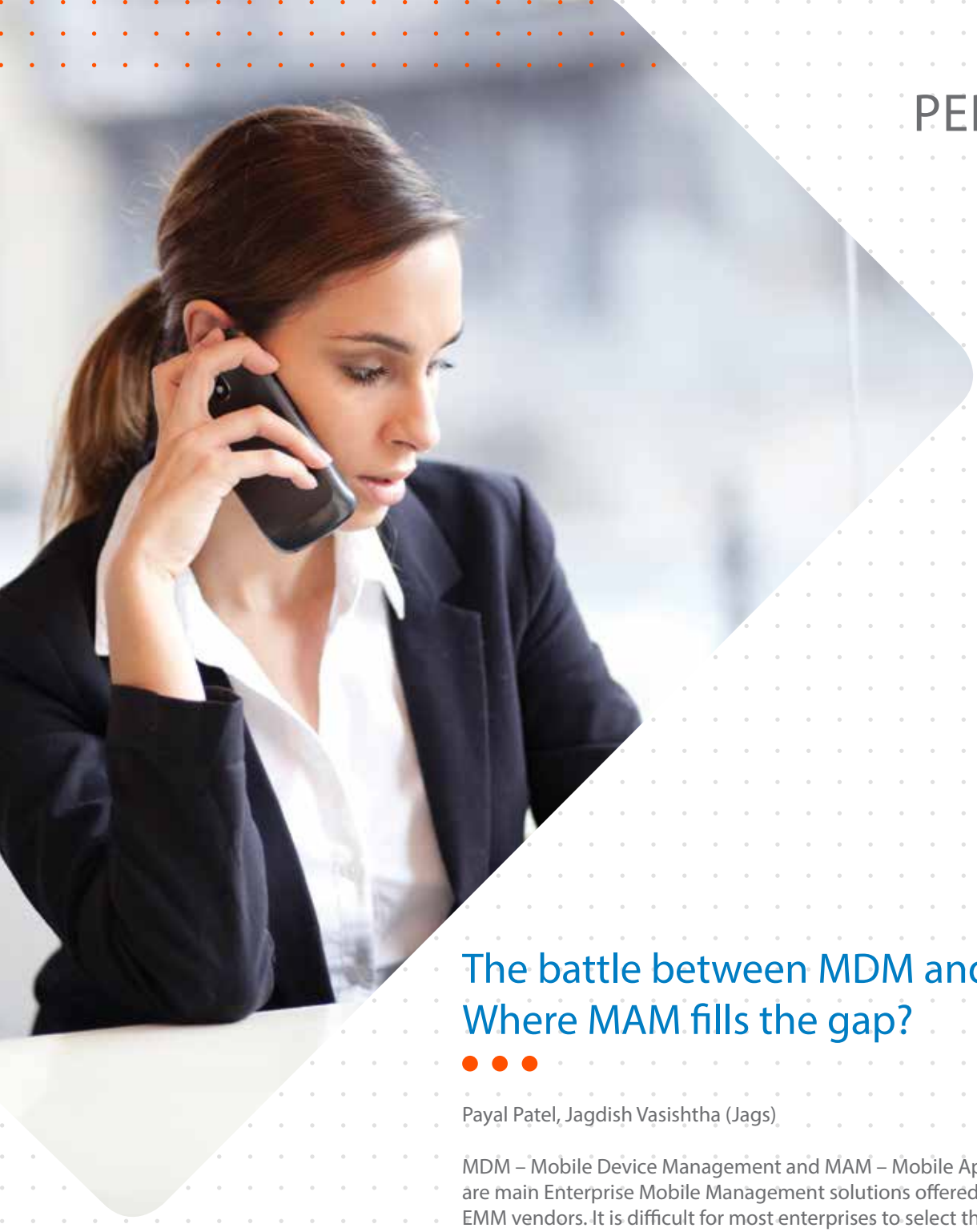
PERSPECTIVE



The battle between MDM and MAM: Where MAM fills the gap?

Payal Patel, Jagdish Vasishtha (Jags)

MDM – Mobile Device Management and MAM – Mobile Application Management are main Enterprise Mobile Management solutions offered by mobile security/ EMM vendors. It is difficult for most enterprises to select the right products for their security needs. This paper provides a comparison of two top security mobile management solutions – the MDM, which acts as a device guard, and MAM, which acts as an application spy.

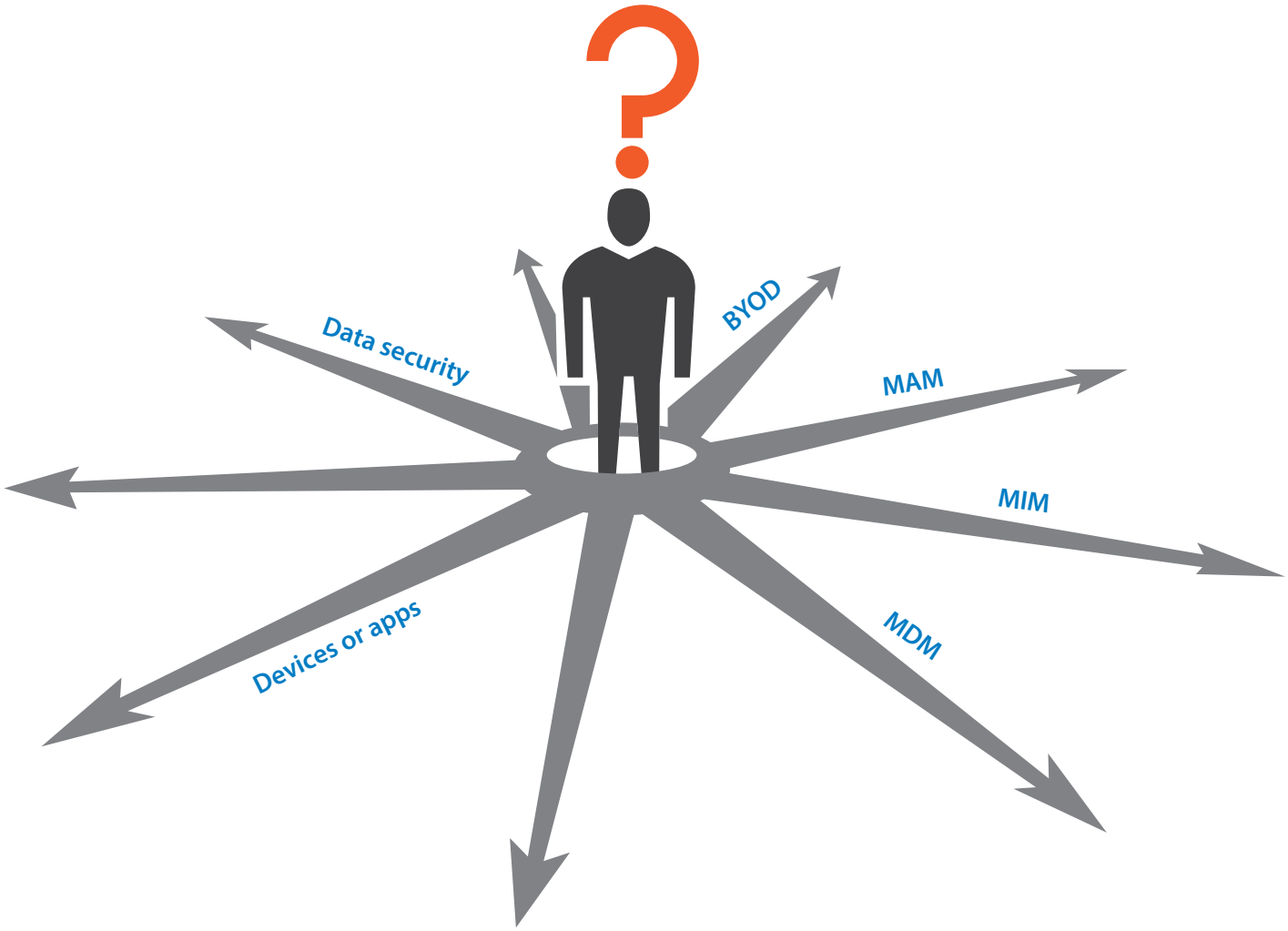
Infosys
be more

Context

In spite of the advent of smartphone technologies and a new set of security features provided by native OS platforms with every release, the landscape of Mobile Management products is large and dynamic. According to CIO insights, almost 45 percent of the world's enterprises who adopted mobility are planning to spend at least $500,000 on mobility projects over the next 12–18 months, of which at least half of will be invested on mobile devices and applications management.

The capabilities that each mobile management service provider offers vary from vendor to vendor, mainly in terms of approach and cost. Each vendor considers their approach to be the best and sometimes they support more than one approach to provide the solution. This makes it difficult for IT security to decide which one to go with.

With the influx of mobile devices, apps, mobility use cases, and data security threats, enterprises are compelled to take mobile management seriously. Currently, MDM, MAM, and MIM are the top choices for effective mobile management. Out of these four solutions, MIM (mobile information management) is achievable with both MDM and MAM. So, which of the two makes a better choice? Let's look at the strengths and limitations of both solutions.



Brief on MDM

MDM was evolved mainly to manage iOS, Android, and Windows-based handhelds after they gained ground over Blackberry to become enterprise devices.

MDM takes the approach of managing and controlling the entire mobile device and all enterprise-registered applications within the device. Of all EMM solutions, MDM is the most powerful since it provides the highest control at device level. However, do enterprises want to allow BYOD (bring your own device)? Are the employees ready to let a solution manage their entire device? They are right to be concerned about compromising on privacy while using corporate specific apps. Also, B2C apps cannot claim control to monitor end user devices. Consequently, enterprise mobility adoption to BYOD and COPE concepts as well as security concerns related to B2C applications presented a strong need for another solution called MAM.

Brief on MAM

MAM stands for Mobile Application Management. The MAM application resides mainly at the top of the device in the form of an application guard layer that manages, secures, and monitors single or multiple applications within its layer. Although MDM has more reach and power to fetch special API-level access at OS level, MAM has its own strength in terms of offering granular control and analytics at a single app level.

What MDM offers

A list of basic and advanced features of MDM is available through hundreds of blogs and articles on the internet. Therefore, the information is not repeated here.

Why MDM is not the preferred mobile management solution

MDM acts like another super user on the mobile device and plays an important role after the native OS. Existence of this spy rootkit on the device was accepted till the time enterprises had device ownership.

- Employees carrying their personal devices to work and enterprises allowing them access to organization-specific applications and data gave a boost to BYOD.
- Both in B2E and B2C scenario, where the devices are owned by end users, enterprises enforcing security policies and control at device level is not accepted by end users.
- In case of lost or stolen devices, triggering remote data wipe for the entire device can delete users' personal data, including personal contacts, media, personal device settings, and application configurations.
- Every time while operating the device even for personal use, why should the end user type complex passwords or patterns as enforced by MDMs?
- MDM being operated at device level can continuously monitor the user's current location, read private information from applications like contacts, calendar, etc., in case the same apps are being used even for work purposes. Only based on some MDM approaches where they enforce custom native apps, isolation of personal and official data is possible but again at the expense of performance and usability issues with custom apps against native.
- What if the same device should be used between multiple users? Would MDM be able to manage multiple user profiles on the same device and control them differently based on user persona? No.
- MDMs enforce the device OS version upgrade enforcement to end users. What if the user is comfortable in using all his favorite apps (which might not be compatible with the next version) with the current device OS version? Is there an option left for the user there?
- With a majority of the approaches, MDM enables access to multiple enterprise applications via VPN-based model. Every time while switching between personal and professional space on the same device, the device retriggers authentication which is performance intensive. Also it brings user experience issues.
- Enterprises may wish to push specific policies and profile configurations based on security and analytics need at application level. With MDM, where things are governed and watchdog is the security guard at device level, this is challenging.

How MAM can address the challenges raised by MDM

End user acceptance for BYOD

Containerization is possible on both MDM and MAM to control and manage a group of applications running on a device without having full control at device level. Now, with rising BYOD in B2E / B2B and growing consumer apps in B2C industry, end users want privacy and native user experience across personal and professional workspace on their mobiles. IT control policies are not acceptable at device level, anymore. MAM is the right fit to address these issues.

Enterprise app store

With thousands of business and productive apps in public app stores and with the VPP initiated by Apple, many enterprises wanted to offer public apps usage to employees. This sets up a coherent offering from the MAM bucket called enterprise app store. As opposed to MDM's approach to configuration, control, and locking down the data at device level, MAM stands out for installing, updating, and validating access for B2E and B2C from devices remotely. Secured application distribution to users devices based on their organizational profile and device properties is a good feature as a part of the enterprise app store.

Version upgrade at app level

The user must have the liberty to choose the device OS version she is most comfortable with. That's why even Google and Apple never allow remote silent installation of OS upgrades on end users' devices. Users' consent and network preference are required from the end user before doing so. MAM agrees, and gives optional and mandatory version upgrade alert for select applications only.

Dynamic and custom policies and configuration

With intelligent approaches such as app wrapping and app integration with security SDK provided by MAM, it is possible for organizations to enforce different configurations such as network, WiFi, app level VPN, allowed users profiles, and enterprise policies to different applications. This makes sense even in a scenario where enterprises want to allow B2C apps access by employees.

Granular application and data control

Ultimately in any security solution, the main objective is to protect data. While MDM can encrypt data, remote wipe at the device level or for the data stored on default path for applications, MAM has more control over application encryption, deletion, and protection at profile, or particular data file level.

Business based on app and user persona

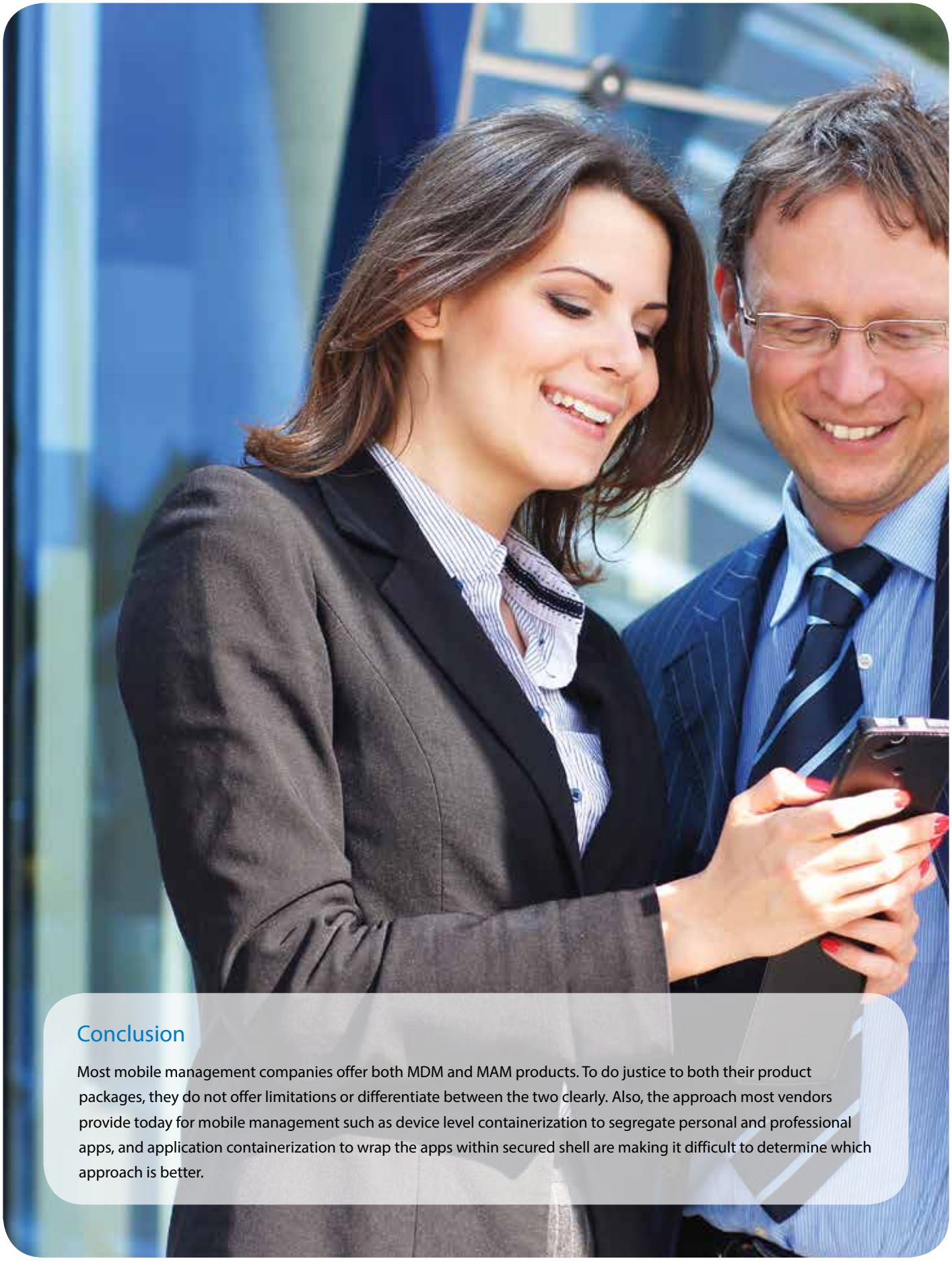
The most important things achievable only with MAM are as follows:

- Geo fencing-based policies and context injection
- Application accessibility based on the user's profile, for example, role, department, and group, and change in the same way even when any of these entities change for user
- Alerts and notifications based on the user and device profile
- Pilot roll out of specific application for set of users

Business strategy revision based on usage analytics

Unlike MDM, MAM can provide the statistics at single application level based on the following:

- Overall app usage by particular user or groups
- App usage based on mobile platform, platform version, device manufacturers, etc.
- Selective application version usage across users or groups
- Application crash scenarios
- Most frequently used features of the application



Conclusion

Most mobile management companies offer both MDM and MAM products. To do justice to both their product packages, they do not offer limitations or differentiate between the two clearly. Also, the approach most vendors provide today for mobile management such as device level containerization to segregate personal and professional apps, and application containerization to wrap the apps within secured shell are making it difficult to determine which approach is better.

Feature support	MAM	MDM
App level two-factor authentication		
User- or data-specific remote wipe		
BYOD solution to end users' privacy concern		
Multi-users profile management for same application		
App configuration change without the need for version upgrade		
Remote content injection based on user and application persona		
Application feature specific usage analytics		
Network Security based on app-level VPN		
App level usage monitoring		
Device jail break and root detection		
Managing and securing B2C applications		
Data loss prevention		
Data at rest and data in motion security		
Application distribution based on configuration		
Whitelisting and blacklisting of device, user, and applications		
Managing and securing B2C applications		
App and device inventory management		
Remote data wipe at device level		
Full device data encryption		
Enforcing set password policies		
Remote installation and uninstallation of apps without user's consent		
Control data sharing options at device level, e.g., WiFi, camera, Bluetooth, and 3G		
Control mobile peripherals such as printers and scanners		

In conclusion, enterprises can choose the appropriate solution based on their security requirements, device ownership, faster time-to-market, and cost factor, by considering the following:

- MDM and MAM are not substitute solutions.
- Both MDM and MAM can co-exist on the same device
- While MDM is the security at the physical layer of the device, it provides utmost level of security and control which again affects performance based on various approaches, and user experiences and limits the number of OEMs/handset models. Now when COPE (Corporate Owned, Personally Enabled) and BYOD (Bring your own Device) are on the rise, solutions are more preferred to govern and to secure applications and data with minimal or no control at device level.
- While MAM can be a solution for application provisioning, de-provisioning, and controlling app access, it can also be the right feedback channel for enterprises to receive the ratings, event- or feature-specific popularity, and furnishing the next mobility roadmap based on the same by meeting BYOD and COPE models. Also, for B2C mobile apps, MAM can be considered a preferred solution over MDM.

About the Authors

Payal Patel,

Senior Technology Architect, Infosys

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

Jagdish Vasishtha (Jags)

AVP and Head – Enterprise Mobility Solutions, Infosys

Jagdish Vasishtha (Jags) is responsible for all intellectual assets business of the unit. Overall he has 20+ years of experience in IT and Telecommunications.

For more information, contact askus@infosys.com

Infosys be more