PERSPECTIVE

Enterprise mobile management – a need or an option?

Payal Patel, Jagdish Vasishtha (Jags)

Even as native platforms are growing tighter with security features, the enterprise mobile management solutions market is booming. If BYOD has to be enabled at SMB companies, with inbuilt solutions from Google and Apple, enterprises would need to support their mobility apps to withstand security threats and other mobile management needs.

Infosys
be more

Introduction

The release of Android 'L' at Google I/O 2014 and iOS 8 at Apple WWDC 2014, were the two major announcements in the mobility world this year. Both had a lot of surprises for consumers, developers, and enterprises alike.

Other parts of the mobility industry were buzzing with the boom of the mobile device management (MDM) market that is expected to be worth US$3.94 billion by 2019.

EMM is not just limited to MDM or MAM now. With reference to Gartner Magic Quadrant Report on Enterprise Mobility Management Suite, June 2014, EMM offers much more than just device and application security.

So what bodes well for enterprise mobile management (EMM) from both releases?

- Security is becoming more matured with newer OS version releases in terms of hardware and software.
- Core security features from these platforms were optional. Some of them were left to the end user to enable / disable the same. However, these are enforced by default now.
- Developers can build secured apps and solutions with the help of native platform APIs without relying on external MDM / MAM and other BYOD products.

This PoV talks about:

- Native platforms' focus on security features
- EMM industry happenings and what it means to the industry

Native platforms become more secured with every new OS release

Along with every main OS release, Google and Apple also update security features. Apart from this, several security patches are applied as part of interim OS updates.

Android 4.0

- Device administration
- Password protection
- File system encryption
- Permission-based model

Android 4.2

- Always-on VPN
- Certificate pinning
- Installed hardening
- OpenSSL cryptography

Android 4.3

- SELinux to reinforce Sandbox
- KeyStore provision
- KeyChain is BoundKeyAlgo
- Restrict setuid from APPS

Android 4.4

- OS hardening
- Per user VPN
- SELinux enforcing mode
- Device monitoring warnings

Android L

- Default data encryption with keys not stored off-device
- Enforced Google Play services to get security firmware updates
- Android for Work powered by Divide acquisition and Samsung KNOX features
- Universal data controls

iOS 5

- Data protection improvements
- New features for MDM providers
- Email forwarding control
- S / MIME

iOS 6

- Controlled installation of configuration profiles and certificates
- Auto removal of user profiles after a certain period
- Single app mode and global HTTP proxy
- Geo-fence use notification

iOS 7

- Touch ID fingerprint authentication
- Per application VPN
- Enterprise single sign-on
- Third-party app data protection
- Open in management and extended MDM

iOS 8

- Default data encryption with user passcode for all personal data
- Data management and content filtering
- Improved and more powerful device management capabilities
- Extended data protection with user passcode for pre-built apps such as Contact, Calendar, and Notes
- Greater security control for PPIM apps

EMM collaborations on the rise

Some significant acquisitions have taken place in the last one year.

This justifies two things: Realization for every industry to consider mobile-first strategies, and traditional security tech vendors to include mobility safeguards.

May 2013: Citrix made a strategic acquisition of Zenprise, one of the top five MDM vendors (as per Gartner's Magic Quadrant report), to provide device management capabilities. Citrix already had mobile market offerings through CloudGateway and ShareFile.

November 2013: IBM acquired FiberLink, maker of the popular MaaS360 EMM service, and then made a deal with MAM vendor Apperian two weeks later.

November 2013: Oracle acquired Bitzer Mobile, a MAM vendor, to support the growing need of BYOD. Blitzer offers BYOD purely in the form of application management without controlling much on the device side.

December 2013: Even though a late entrant, Dell offered MDM, MAM, MCM, and end-point management after acquiring KACE, Wyse, SonicWALL, and Quest Software. Dell had a cohesive strategy in place with the plan of massive integration amongst these products.

January 2014: Airwatch, one amongst the top five EMM vendors, got acquired by VMware for US$1.54 billion, making it the largest acquisition in the history of enterprise mobility.

February 2014: Good technology, one of the biggest MDM/MAM vendors, acquired BoxTone to bolster its security needs.

October 2014: Siris Capital acquired one of the very few network-approach-based EMM products – Junos Pulse, from Juniper Networks and incorporated this joint venture in the name Pulse Secure, LLC.

October 2014: Pulse Secure acquired the Israeli-based BYOD startup MobileSpace for US$100 million. MobileSpace is a new entrant in the EMM industry with its unique approach of managing in-house and public enterprise applications on Android. This can make BYOD more acceptable beyond iOS devices.

The latest Gartner Magic Quadrant report 2014 on mobile device management, suggests that big players such as Airwatch, Mobileiron, Citrix Solutions, SAP, Good Technology, IBM, Symantec, Microsoft, Sophos, and Soti are making this space difficult for SMB vendors. However, every enterprise has its own needs and one size does not fit all.

Is EMM a need or an option? – Facts to consider

Extended mobility

- The number of wearable units will be about 111.9 million by 2018, according to the IDC worldwide wearable survey. Many of these devices would have custom OS and would interact with native platforms as extended communication or with their stand-alone applications that can also have custom OS. How would it be possible for enterprises to manage them with only native OS offerings?
- With mobiles connected with auto, gears, entertainment, payment systems, and other embedded devices the need for massive data sharing and storage would increase. Enterprises would have to think about security and management in this connected world.

Native platform offerings

- To compete with other platforms, native platforms keep releasing new features. This brings changes at a framework level. For instance, a closed network of Apple has introduced features such as data sharing across applications, touchID authentication usage access at the application level, handoff feature to access work from any connected iOS devices, and access for external keyboard applications. Some of these features can open doors to further security threats.
- Android still remains very far from being considered a safe device for enterprise usage. While, Google attempts to address fragmentation, it also leads to more security issues. Android for Work covers only main OEMs such as HTC, Sony, Samsung, Motorola, and LG. When this platform gets populated with other manufacturers and models, how would they address security concerns?

Development perspective

- Do developers follow best coding security practices while developing apps on platforms?
- Are architects and developers able to visualize security threats?
- Do all enterprises have a security framework that integrates seamlessly with all apps and ensures IT-defined security?
- All security frameworks have to go under revisions of development changes and testing with every new native OS version. Without an external EMM vendor, how many enterprises have a dedicated workforce to execute this?

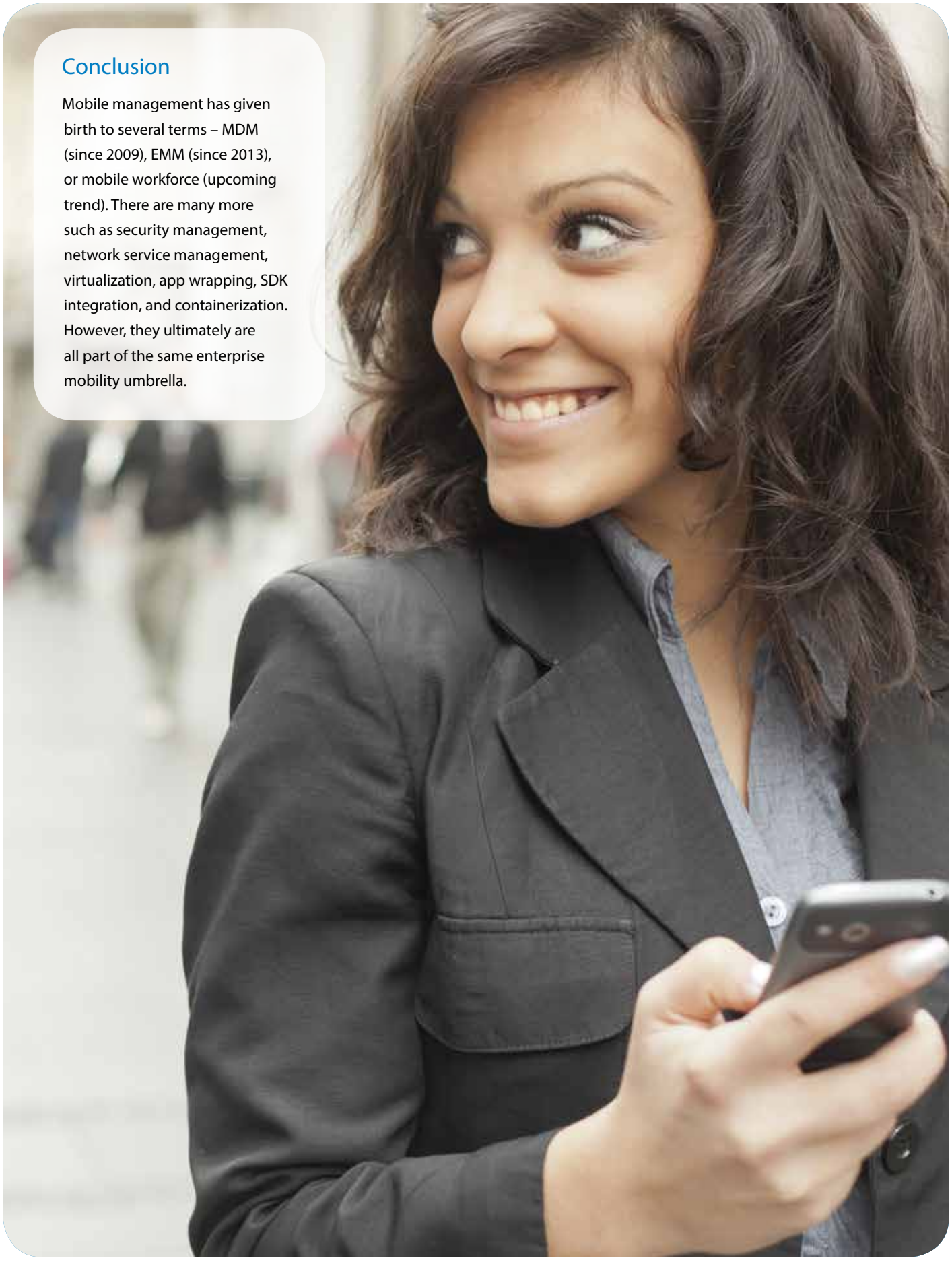
EMM offerings

- EMM does not help resolve BYOD but offers features such as:
  - Multiple user support per device
  - Runtime profile push to device
  - Attack corporate data on device
  - Inject enterprise policy changes to apps
  - Devices and users tracking
  - Application usage detection
  - Crash analytics

Uniformity in features, applying policies, defining security profiles and management console accessibility by administrators and IT departments would be possible only with EMM products and not through native platforms' mobile management offerings. Imagine if enterprises have to enable BYOD for iOS, Android and Windows mobile devices without external EMM solutions, they would have to select Google to manage Android devices, Apple to manage iOS devices, and Microsoft to manage Windows devices. Even if Google supports other platform devices, it will secure and control those devices, only if those devices use GApps.

Conclusion

Mobile management has given birth to several terms – MDM (since 2009), EMM (since 2013), or mobile workforce (upcoming trend). There are many more such as security management, network service management, virtualization, app wrapping, SDK integration, and containerization. However, they ultimately are all part of the same enterprise mobility umbrella.



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