Gartner.

Magic Quadrant for Enterprise Mobility Management Suites

3 June 2014 ID:G00261703

Analyst(s): Terrence Cosgrove, Rob Smith, Chris Silva, Bryan Taylor, John Girard, Monica Basso

VIEW SUMMARY

The mobile device management market has evolved into the enterprise mobility management suites market. EMM is growing quickly, and the vendor landscape has changed significantly, which will impact IT leaders' choices.

Market Definition/Description

This document was revised on 4 June 2014. The document you are viewing is the corrected version. For more information, see the Corrections page on gartner.com.

Enterprise mobility management (EMM) suites consist of policy and configuration management tools and a management overlay for applications and content intended for mobile devices based on smartphone OSs. They are an evolution from previous-generation mobile device management (MDM) products that lacked application and content management. IT organizations and service providers use EMM suites to deliver IT support to mobile end users and to maintain security policies.

EMM suites provide the following core functions:

Hardware inventory

Application inventory

OS configuration management

Mobile app deployment, updating and removal

Mobile app configuration and policy management

Remote view and control for troubleshooting

Execute remote actions, such as remote wipe

Mobile content management

Executing these core functions through MDM represented the early implementation of these functions. MDM tools have evolved to incorporate advanced mobile application management and mobile content management.

Mobile application management applies management and policy control functionality to individual applications, which are then managed by the EMM console. This capability is necessary when the OS (e.g., iOS, Android, Windows Phone) does not provide the required management capability or when organizations elect not to install an MDM profile on the device. There are two basic forms of mobile application management:

Preconfigured applications: These generally include a secure personal information manager (PIM) for email, calendaring and contact management, as well as a secure browser provided by the EMM provider or a third party. These tools are configured to be managed and secured by the EMM system.

Application extensions: These apply policies to applications through the use of a software development kit (SDK) or by wrapping. This capability is necessary when the OS does not provide the required management capability or when organizations elect not to install an MDM agent on the device.

Mobile content management enables users to access content from their mobile devices. The mobile content management function within EMM suites has three fundamental roles:

1. Secure Container — A client-side app that enables a user to store content securely on a mobile device. The EMM can enforce policies such as authentication, file sharing and copy/paste restriction. Content comes from three primary sources:
   Email (attachments)

   Content pushed by the administrator or another internal person

   Content accessed from a back-end repository

2. Content Push — Push-based document delivery. Some specific functions are:
   Control document versions

   Alert a user of new files

   Flag content expiration date

3. Content Access — A connection to a back-end repository where users can pull content to their devices. Specific capabilities are:
   Support for specific back-end repositories (SharePoint, Documentum, etc.)

   Restrict downloads while roaming

EVALUATION CRITERIA DEFINITIONS

Ability to Execute

Product/Service: Core goods and services offered by the vendor for the defined market. This includes current product/service capabilities, quality, feature sets, skills and so on, whether offered natively or through OEM agreements/partnerships as defined in the market definition and detailed in the subcriteria.

Overall Viability: Viability includes an assessment of the overall organization's financial health, the financial and practical success of the business unit, and the likelihood that the individual business unit will continue investing in the product, will continue offering the product and will advance the state of the art within the organization's portfolio of products.

Sales Execution/Pricing: The vendor's capabilities in all presales activities and the structure that supports them. This includes deal management, pricing and negotiation, presales support, and the overall effectiveness of the sales channel.

Market Responsiveness/Record: Ability to respond, change direction, be flexible and achieve competitive success as opportunities develop, competitors act, customer needs evolve and market dynamics change. This criterion also considers the vendor's history of responsiveness.

Marketing Execution: The clarity, quality, creativity and efficacy of programs designed to deliver the organization's message to influence the market, promote the brand and business, increase awareness of the products, and establish a positive identification with the product/brand and organization in the minds of buyers. This "mind share" can be driven by a combination of publicity, promotional initiatives, thought leadership, word of mouth and sales activities.

Customer Experience: Relationships, products and services/programs that enable clients to be successful with the products evaluated. Specifically, this includes the ways customers receive technical support or account support. This can also include ancillary tools, customer support programs (and the quality thereof), availability of user groups, service-level agreements and so on.

Operations: The ability of the organization to meet its goals and commitments. Factors include the quality of the organizational structure, including skills, experiences, programs, systems and other vehicles that enable the organization to operate effectively and efficiently on an ongoing basis.

Completeness of Vision

Market Understanding: Ability of the vendor to understand buyers' wants and needs and to translate those into products and services. Vendors that show the highest degree of vision listen to and understand buyers' wants and needs, and can shape or enhance those with their added vision.

Marketing Strategy: A clear, differentiated set of messages consistently communicated throughout the organization and externalized through the website, advertising, customer programs and positioning statements.

Sales Strategy: The strategy for selling products that uses the appropriate network of direct and indirect sales, marketing, service, and communication affiliates that extend the scope and depth of market reach, skills, expertise, technologies, services and the customer base.

Offering (Product) Strategy: The vendor's approach to product development and delivery that emphasizes differentiation, functionality, methodology and feature sets as they map to current and future requirements.

Business Model: The soundness and logic of the

Audit logging to track who accesses/downloads files

Return to Top

Magic Quadrant

Figure 1. Magic Quadrant for Enterprise Mobility Management Suites

Source: Gartner (June 2014)

Return to Top

Vendor Strengths and Cautions

Absolute Software

Absolute Software is a publicly traded company based in Vancouver, British Columbia, Canada. The company provides EMM functionality as an extension of its device-tracking and client-management products. It has a strong presence in education, state and local governments, and healthcare. Its product Absolute Manage provides diverse coverage, supporting iOS, Android, Windows Phone, Mac OS X, and Windows 7 and Windows 8 (Windows 7/8). The product is offered via an on-premises offering or SaaS model.

Strengths

Absolute Software provides a compelling offering for midsize organizations seeking to manage Macs, PCs and mobile devices from a single tool.

Absolute Software has a persistence technology, which embeds an agent in the firmware of certain devices (e.g., Samsung Galaxy tablets and smartphones) for location and theft tracking.

Absolute Manage's support for Mac OS X is very strong.

Cautions

Application management features are rudimentary and lack advanced SDK and wrapping capabilities.

Absolute Manage lacks a self-service portal for users to locate, track, wipe and manage their own devices.

Absolute Manage lacks strong device and content management for Windows Phone.

Return to Top

AirWatch

VMware is a publicly traded company based in Palo Alto, California. In February 2014, VMware completed its acquisition of AirWatch. VMware plans to use AirWatch to build a workspace aggregator, complementing its desktop virtualization and SaaS application management technologies. However, AirWatch will continue to operate as a separate business unit and is branded as AirWatch by VMware. The product suite, offered via SaaS or on-premises, consists of all the standard components of an EMM product plus an application reputation service and basic management for PCs and Macs. AirWatch's offering has comprehensive EMM functionality, which

---

allows it to frequently win deals. The mobile application management and mobile content management components sometimes lack stability and usability, resulting in customers mainly using the MDM features. AirWatch is a good fit for organizations that require a comprehensive EMM feature set on a broad range of platforms.

Strengths

AirWatch has proven large-scale deployments across every vertical market.

There is a good administrative console with embedded training videos, links and a wizardlike approach to help new administrators become productive quickly.

AirWatch continues to push innovation with being only one of two leading vendors to support the latest release of iOS on the same day, and was one of the first to support key technologies such as the Apple Volume Purchase Program and Samsung Knox.

Cautions

AirWatch's vision is to be the solution for all of an organization's mobile needs; however, we have had numerous reports of problems in the Secure Content Locker and Inbox email applications, causing customers to use AirWatch only for MDM and mobile application management.

With the latest release, 7.1, AirWatch released the software only to cloud customers. Therefore, if immediate software updates is a selection criterion, consider only the cloud offering.

On-premises AirWatch customers have reported app wrapping issues with support and stability.

Return to Top

BlackBerry

BlackBerry is a publicly traded company based in Waterloo, Ontario, Canada. BlackBerry Enterprise Service (BES) is used primarily by organizations that support BlackBerry devices. BES10, the current version of the product, is provided via an on-premises offering or a SaaS model. BES offers the best support for BlackBerry 10 devices. However, the company announced that it will open BlackBerry 10 to be managed by other EMM providers. BlackBerry reduced and simplified its BES10 pricing, and created an EZ Pass program, allowing customers to update BES 5 and BlackBerry OS licenses to BES10 licenses for BlackBerry 10, iOS and Android devices. BES10 provides support for other platforms, such as iOS and Android, but Gartner has not seen substantial uptake of BES on those platforms. While BlackBerry continues to lose ground in the mobile device space, the lack of mature alternatives that offer similar security capabilities has given the company a little bit of extra breathing room. BlackBerry is a good fit for organizations committed to supporting BlackBerry devices.

Strengths

BES10's MDM support for BlackBerry devices is the strongest in the market, including the ability to audit and log SMS messages.

BlackBerry has a mature customer support program, with several tiers of support subscriptions, depending on customer preference.

BlackBerry has the potential to have a differentiated EMM offering, leveraging assets such as QNX, and identity and access management (IAM) to control access to Web applications.

Cautions

BES10 lacks broad mobile platform support for handset-specific Android — for example, Samsung for Enterprise (SAFE), Samsung Knox, Windows Phone, Windows 8 and Mac OS X.

The depth of iOS and Android support is incomplete, lacking comprehensive MDM and certificate management, as well as multiuser support.

BES10's mobile content management is provided only on BlackBerry devices today, but the company plans to expand platform coverage.

Return to Top

Citrix

Citrix is a publicly traded company based in Santa Clara, California. Citrix entered the EMM space following the acquisition of Zenprise in January 2013. Zenprise added to Citrix's mobile app management and mobile app technologies, as well as to Citrix ShareFile and Citrix NetScaler. In May 2014, Citrix announced Workspace Suite, which combines desktop virtualization and EMM to deliver access apps and content to any device through a combination of physical and virtual mechanisms. XenMobile is available via an on-premises option or through a SaaS model. XenMobile MDM supports iOS, Android, Windows Phone, BlackBerry (via BES) and Windows 8. Citrix MDX Toolkit supports iOS and Android. Citrix is a good fit for organizations that are looking to deliver a secure workspace comprising Windows, Web and mobile applications, as well as organizations that use ancillary technologies, such as XenApp, XenDesktop and NetScaler.

Strengths

Citrix has developed strong point applications in its Worx Mobile Apps suite and related third-party applications in the Worx App Store. These integrations improve the experience of using multiple enterprise mobile apps.

Citrix ShareFile is among the most complete and feature-rich mobile content management capabilities among EMM vendors.

Citrix gets high marks from customers for support and on-site consultative assistance.

Cautions

There are fewer large XenMobile deployments (i.e., over 10,000 users) compared with other leading EMM vendors. Gartner's reference checking found relatively low adoption of the product.

The WorxMail 1.0 app, introduced last year, is still in development and has had issues with battery drain and app crashes. Citrix plans to release improvements in battery usage in the XenMobile 9.0 release.

XenMobile's separate consoles (MDM, AppController, NetScaler) for administration lack integration, making the overall administrative experience complex. Integration is planned for later in 2014.

Return to Top

Globo

Globo, a new vendor in this Magic Quadrant for EMM Suites, is a publicly traded company. Its main offices are in the U.S., U.K. and Greece. GO!Enterprise, offered via SaaS or on-premises options, provides MDM support for iOS, Android, Windows Phone and BlackBerry (via enterprise application software [EAS]). Its mobile application management module supports iOS, Android, Windows Phone and BlackBerry (for apps BlackBerry built with Globo's mobile application development platform [MADP]). Unique among its peers in this analysis, Globo includes MADP as part of the license for its EMM tool. The GO!Enterprise license includes a core set of Secure PIM, collaboration and productivity applications, and a secure content container under a single license. Globo is a good fit for organizations looking for a single product that provides MADP and EMM.

Strengths

Globo is one of the few vendors offering an EMM suite with supplemental app development tools.

Depth of platform support across all major mobile platforms, including BlackBerry, at relative parity is an attractive feature of this offering and makes it appropriate for diverse environments.

Globo includes Secure PIM applications, such as email, calendar, contacts and messaging, as well as a secure content management application in its core offering; adjuncts are additional cost add-ons from many competing solutions.

Cautions

At present, the Globo solution for EMM does not provide a facility to display an end-user license or agreement prior to device enrollment, relying instead on a postenrollment email. This may be a concern for some organizations interested in recording explicit user consent prior to device enrollment.

Globo has solid MDM support, but still lags the leading vendors in some areas, such as certificate management.

Globo provides a set of off-the-shelf mobile apps, which can be managed by GO!Enterprise. However, GO!Enterprise's mobile application management does not provide support for a long list of public app store apps.

Return to Top

Good Technology

Good Technology (Good) is a privately held company based in Sunnyvale, California. Good is best known for its containerized PIM functionality through the Good for the Enterprise (GFE) product. Good has expanded with mobile application management and mobile content management, and with the BoxTone acquisition. BoxTone strengthens Good's MDM capabilities and provides mobile service management, which enables administrators to monitor and manage the performance of the mobile environment. One of Good's priorities for the next 12 to 24 months is to further integrate these technologies. GFE MDM supports iOS and Android. Good Dynamics (a mobile application management module) supports iOS, Android and Windows Phone. GFE and Good Dynamics are currently available only via an on-premises architecture, but Good offers its enterprise app stores and stand-alone MDM as SaaS options. Good plans to add a SaaS option for GFE and Good Dynamics later in 2014. Good Technology is a good fit for organizations bound by stringent data security regulations, and that require a strong PIM client and strong mobile application management.

Strengths

Good's Secure PIM (i.e., email, calendar, contacts) is the most mature in terms of features among the EMM vendors offering proprietary PIM clients.

Support had historically been an issue with Good; but, in 2013, the company implemented a more rigorous support model. References have noted that support is now a strength for the company, particularly with GFE.

The Good Dynamics mobile application management SDK provides the most comprehensive security capabilities for public and private app store apps among vendors in the EMM market.

Cautions

Good's historic focus on mobile application management places it behind leading EMM vendors in MDM support, particularly for Android and Windows Phone.

Windows 8 and Mac OS X MDM support is weaker than that of leading EMM vendors.

Good's EMM offering provides strong Secure PIM and mobile application management, but can be time-consuming to deploy, as noted by customers and partners.

Return to Top

IBM

IBM acquired Fiberlink in December 2013 and has positioned MaaS360 as a major component of its enterprise mobility solutions. MaaS360 brought IBM a much-needed EMM cloud solution, as well as a new on-premises offering that had just been completed for more conservative buyers. MaaS360 MDM supports iOS, Android, Windows Phone, Windows 7/8 and Mac OS X. Its mobile application management module supports iOS, Android and Windows Phone. MaaS360 is housed under the

same management group as other IBM endpoint management products, laying the ground for a broader management portfolio. MaaS360 is a good fit for organizations looking for a SaaS-based product and those who use IBM collaboration, productivity and security technologies.

Strengths

IBM (Fiberlink)'s mature shared-processing multitenant architecture is the best-in-class cloud among ranked EMM vendors. It can support thousands of installations per day for large accounts.

Reference customers consistently praise MaaS360 for ease of use at the end-user and administrator levels. Installations can be readily personalized to meet a company's needs, and extensive self-help is available for individual users.

MaaS360 provides good laptop management functionality, based on its long-standing client management product and MDM, which provides basic MDM policy management for Windows 8.1 devices and, to a lesser extent, Mac OS X.

Cautions

IBM's vision for mobility is large, broad and complex. IBM has much work to do to fully rationalize the elements of its MobileFirst offering. Buyers of MaaS360 should look for new capabilities, but also must monitor for product and service continuity.

MaaS360 has an issue in which records of inactive devices are not deleted automatically. Administrators need to set up rules to have these devices removed from views, rules and reports.

Administrators can customize the alert settings based on roles and compliance requirements; however, the default console alert presentation doesn't help the administrator prioritize urgent tasks according to relevant factors, such as effort and impact.

Return to Top

Landesk

Landesk EMM products Mobility Manager and Avalanche originate from the Landesk 2012 acquisition of Wavelink. The two products share the same code, but Mobility Manager has tight integration with Landesk Management Suite (LDMS), a strong client management tool. Avalanche is offered via an on-premises offering and a SaaS model. Both EMM products support iOS, Android, BlackBerry (via EAS), Windows Phone 8, Windows 7/8 and Mac OS X. Landesk offers user-based licensing that enables organizations to license Mobility Manager, LDMS, Landesk Security Suite and Landesk Service Manager with a single license. Landesk is still behind in the EMM market, and has not been getting significant uptake outside customers that use the broad set of Landesk products. Landesk recently acquired LetMobile, a secure mobile gateway vendor. Landesk also has been building a workspace aggregator, Landesk Fuse, which will provide a portal for users to obtain apps and content. Landesk is a good fit for organizations looking to combine strong client management (LDMS) and EMM.

Strengths

Landesk has one of the strongest offerings for converged endpoint management.

Mobility Manager is one of the few products in the market to offer integrated EMM and service desk.

Mobility has a mature management console with strong role-based access control (RBAC) and language support.

Cautions

MDM support is incomplete, lacking full iOS policy and certificate management, as well as limited support for Android handset MDM APIs.

Mobile content management is limited to content push and storage on the device. Mobility Manager does not provide access to back-end content stores or file share and sync.

Application management features are rudimentary and lack advanced SDK and wrapping capabilities.

Return to Top

MobileIron

MobileIron's strategy is to provide an EMM offering that is agnostic to the applications and devices an organization uses. This differs from EMM vendors that combine a proprietary Secure PIM and EFSS product with their EMM tools. The company continues to innovate its EMM offering, and to seek and receive patents for its mobile technology. MobileIron is available via an on-premises offering and a SaaS model. The MDM product supports iOS, Android, Windows Phone, Windows 8 and Mac OS X. Its mobile application management module supports iOS and Android. MobileIron filed its Form S-1 in April 2014, demonstrating its intent to pursue an initial public offering (IPO). This is necessary, as MobileIron continues to compete with larger and well-funded vendors. MobileIron is a good fit for organizations that adopt a best-of-breed strategy for mobile applications, such as file share and sync, email and app reputation. MobileIron's approach is to integrate with vendors and products that are strongest in their respective areas.

Strengths

Customer support receives high marks in nearly all reference interviews with a consistent refrain offered by users that the company, while maturing, still offers the responsiveness and dialogue on product enhancements typical of a startup.

Although a common feature, MobileIron's Federal Information Processing Standard (FIPS) 140-2 compliant mobile application management, server gateway and client apps stand apart as having received third-party validation of its appropriate implementation and function.

MobileIron is the only vendor in the EMM market that demonstrates real-time remote-view capabilities on iOS.

Cautions

> MobileIron's infrastructure is appliance-based and more difficult to monitor for availability and performance than many other competitive products.

> MobileIron has more limited Android manufacturer API support than many other leading EMM vendors.

> The MobileIron administrative console is supported in English only, while reporting and end-user communications have broader language support.

Return to Top

SAP

SAP Mobile Secure is a suite of products that includes Afaria (MDM), SAP Mobile App Protection by Mocana (for mobile application management) and SAP Mobile Documents (for mobile content management). Mobile Secure is offered via an on-premises offering and a SaaS model. Afaria supports iOS, Android and Windows Phone. SAP Mobile App Protection by Mocana supports iOS and Android. Mobile Secure benefits from SAP's breadth of assets, including SAP Business Intelligence (BI) to deliver a unique administrator dashboard experience. SAP is likely to further leverage other SAP assets, such as the SAP Mobile Platform, SAP Hana and SAP BI to augment Mobile Secure. However, expect Mobile Secure likely to follow a tactical path, as shown by its track record, following the market and showing few differentiating factors over the leading EMM competitors. Mobile Secure is a good fit for companies that own SAP products and value the extension of those products within a single vendor's offering, although the product does not require an existing SAP back end.

Strengths

> SAP Mobile Secure provides a scalable architecture, demonstrated through large customer references, and specific product capabilities, such as allowing components to be spread across multiple servers.

> Mobile content management has broad back-end content repository support, including SharePoint, Documentum and IBM connections.

> SAP has a large set of global partners to help with sales and implementation. This enhances SAP Mobile Secure's overall viability.

Cautions

> SAP has a track record of supporting releases of mobile OSs (the OSs and new features available in the release) later than the competition.

> MDM capabilities are incomplete, with weaknesses in areas such as certificate management and multiuser device support for iOS and Android.

> SAP Mobile Secure has a history of unstable releases requiring administrators to implement work-arounds and rework.

Return to Top

Sophos

Sophos is a privately held company based in Oxford, U.K. Sophos Mobile Control (SMC) MDM supports iOS, Android, Windows Phone and BlackBerry (via BES). It is also the only vendor to feature a form of digital rights management (DRM) as a core component to its mobile content management application. Enterprises and small or midsize businesses (SMBs) looking for an easy-to-implement solution that combines desktop and mobile protection should look at Sophos' Complete Security Suite, but should be aware that it is currently available only as an on-premises-based solution; however, SMC is available as a hosted offering. Gartner frequently sees SMC deployments with SMBs, but rarely in large enterprise customers' sites. Sophos is a good fit for organizations looking for integrated EPP and EMM from the same console.

Strengths

> Sophos' mobile content management transparently encrypts files leaving a PC or mobile device to prevent data leakage. This integrates with third-party file storage providers and enables companies to securely use low-cost third-party storage.

> Sophos is only one of two endpoint protection platform (EPP) vendors to qualify for inclusion in the EMM Magic Quadrant. Customers can leverage their relationship with Sophos for support, and potentially improve its user-based pricing by combing multiple solutions.

> SMC directly integrates with Unified Threat Management (UTM) gateways from Sophos and Check Point for easier enablement of remote access.

Cautions

> Sophos' ability to innovate with the latest advancements in mobile technology is slower than the leading vendors' technology; the most notable missing functionality is Samsung Knox support.

> Companies that require trusted certificates should note that Sophos currently supports only Microsoft Certificate Services.

> Sophos offers no app wrapping functionality. Therefore, organizations looking to deploy in-house-developed apps must build in additional security that other EMM vendors provide as a core portion of their products.

Return to Top

Soti

Soti is a privately held company based in Mississauga, Ontario, Canada. Soti offers a strong, general-purpose EMM solution suitable for mainstream use cases, but has its roots in the ruggedized space, where it has been a dominant player for a number of years. MobiControl is delivered via an on-premises offering, as well as a SaaS model. MobiControl supports iOS, Android,

Windows Phone, Windows 8 and Mac OS X. Its core differentiator lies in the MobiControl Android+ technology, which allows MobiControl to manage Android devices with a high degree of control and configuration management capability. Soti is a good fit for organizations that require broad EMM capabilities, especially those making a heavy investment in Android special-purpose mobile devices.

Strengths

MobiControl has strong remote support capabilities, with full remote control for Android devices and remote viewing for SDK-enabled iOS apps.

Soti has a large customer base with significant investments in Android, and has deep experience and excellent feature/functionality support for this platform.

Soti enables users to customize the End User License Agreement (License) presented at enrollment time through policies that can key off any combination of specific Lightweight Directory Access Protocol (LDAP)/Active Directory attributes, allowing companies to automate the presentation of different Licenses to different types of users, rather than presenting a cumbersome, monolithic document.

Cautions

Soti relies on partnerships for most mobile application management functions (e.g., Secure PIM, secure browser and app wrapping). This reduces Soti's influence and control of product road maps for these functions.

Soti just recently launched a premium support offering, involving a designated technical account manager, and does not have the demonstrated track record in this area as other vendors.

MobiControl's MDM enrollment capabilities are limited. Soti provides several options for Android, but automated iOS and Windows Phone enrollments are limited to email.

Return to Top

Symantec

Symantec is a publicly traded company based in Mountain View, California. Symantec Mobile Management Suite (MMS) consists of Symantec App Center, Symantec Mobile Management and Symantec Mobile Security. MMS is provided via SaaS and an on-premises offering. The suite supports iOS, Android and Windows Phone. Although MMS is a strong product offering, Symantec has executed weakly in terms of mind share and market presence in EMM, and is rarely on shortlists or proposals that Gartner sees. Symantec recently acquired Secure PIM vendor Nitrodesk, which will immediately strengthen its EMM offering. Symantec is a good fit for organizations that require strong mobile application management and that use Symantec for endpoint security.

Strengths

MMS provides app wrapping capabilities that allow apps to be dynamically updated without rewrapping.

Symantec has integrated strong security features for mobile data loss prevention (DLP) and IAM.

Symantec is only one of two EPP vendors to qualify for inclusion in the EMM Magic Quadrant. Thus, EPP customers can leverage their relationship with Symantec for support, and potentially improve, their user-based pricing by combing multiple solutions.

Cautions

MMS currently lacks several leading features, including Samsung Knox support.

With its broad offering, Symantec is well above the median price for similar EMM solutions.

Due to Symantec's large product portfolio, MMS has experienced difficulties in building mind share from end customers and from Symantec internally.

Return to Top

Tangoe

Tangoe is a publicly traded company based in Orange, Connecticut. Tangoe offers EMM as a stand-alone product or a companion product with its telecom expense management (TEM) and help desk outsourcing services. MatrixMobile is provided via a SaaS model or an on-premises offering. MxSecure provides MDM capabilities for iOS and Android, and integrates with BES for management of BlackBerry devices. It provides limited support for the Windows Phone platform. Its MxApp module provides mobile application management capabilities and Secure PIM through a partnership with Divide, and is included with MxSecure. The product is capable, but lacks some of the more advanced app policies available with leading mobile application management products. Tangoe is a good fit for organizations looking to extend EMM from TEM functionality.

Strengths

Tangoe's self-service procurement, asset management and activation capabilities are among the best in class.

Tangoe offers global 24/7 support coverage that gets high marks from customers.

Tangoe offers well-regarded consulting and advisory services for mobile and bring your own device (BYOD) strategy development.

Cautions

Many of the most compelling aspects of Tangoe's product set, such as MyMatrix Mobile, are designed to deliver best results in the context of a comprehensive MMS play, where adjacent products and services can be integrated.

Windows Phone is weakly supported in the mobile application management and mobile content management areas.

MatrixMobile EMM offering relies on several third-parties to complete its EMM offering: Divide for Secure PIM, Acronis for mobile content management, SAP Afaria for Knox support.

Vendors Added and Dropped

We review and adjust our inclusion criteria for Magic Quadrants and MarketScopes as markets change. As a result of these adjustments, the mix of vendors in any Magic Quadrant or MarketScope may change over time. A vendor's appearance in a Magic Quadrant or MarketScope one year and not the next does not necessarily indicate that we have changed our opinion of that vendor. It may be a reflection of a change in the market and, therefore, changed evaluation criteria, or of a change of focus by that vendor.

Added

Globo

Dropped

Kaspersky Lab did not have sufficient mobile content management to be included.

McAfee did not have sufficient mobile content management to be included.

Trend Micro supported only two mobile OSs (iOS and Android).

BoxTone was acquired by Good Technology.

Fiberlink was acquired by IBM.

Inclusion and Exclusion Criteria

More than 100 vendors offer EMM functions. We developed inclusion criteria involving a combination of business metrics and technical capabilities. Vendors in the Magic Quadrant must meet the following criteria:

$8 million in 2013 EMM revenue.

1,500 EMM customers.

500,000 EMM licenses in customer environments.

Five references using the EMM product in production.

MDM support for at least three mobile OSs (i.e., iOS, Android, Windows Phone 8, BlackBerry).

The EMM product must be able to manage policies and control data sharing for mobile applications.

The EMM product must provide a device resident container to store and manage content.

Many EMM products provide functions beyond those already listed. Some features were considered optional and not necessarily critical criteria for comparison. For example:

Support for Mac OS X and Windows 8

Advanced mobile content management that provides connectivity to back-end file stores

Advanced mobile application management that manages PIM, browsers and other applications

Remote view, or control of mobile devices or mobile applications

Evaluation Criteria

Ability to Execute

The Ability to Execute axis measures the vendors' ability to meet the current needs of EMM buyers, as well as their ability to succeed in this market by gaining market share and achieving revenue growth.

Product/Service: What features are supported and how is EMM delivered?

Overall Viability: This criterion evaluates the size of the vendor and its financial performance. We also evaluated the size and growth of the vendor's EMM business.

Sales Execution/Pricing: This criterion was influenced by the frequency of the vendor's appearance on buyers' shortlists. We also evaluated the degree to which the vendor has a presence in North America, Europe, Latin America and the Asia/Pacific region.

Market Responsiveness/Record: We evaluated execution on delivering products consistently and in a timely fashion, the agility to meet new market demands, and how well the vendor received customer feedback and quickly built it into the product. We looked at the vendor's ability to meet promised timelines.

Marketing Execution: This is a measure of brand and mind share through client references and channel-partner feedback. We evaluated the degree to which customers and partners have positive identification with the EMM product, and whether the vendor has credibility in this market. We also used search hits on gartner.com for the vendor and product as a measure of brand recognition and market awareness.

Customer Experience: We assessed the vendor's reputation in the market based on customer feedback regarding customers' experiences working with the vendor, whether they were glad they

chose the vendor's product and whether they planned to continue working with the vendor.

Operations: This refers to the ability of the organization to meet its goals and commitments. Factors include the quality of the organizational structure, including skills, experiences, programs, systems and other vehicles that enable the organization to operate effectively and efficiently on an ongoing basis.

Table 1. Ability to Execute Evaluation Criteria

Evaluation Criteria	Weighting
Product or Service	High
Overall Viability	High
Sales Execution/Pricing	Medium
Market Responsiveness/Record	Medium
Marketing Execution	Medium
Customer Experience	High
Operations	Medium

Source: Gartner (June 2014)

Return to Top

Completeness of Vision

The Completeness of Vision scale provides an aggregate measure of a vendor's likelihood of future success in the EMM market. We evaluated vendors' statements about product direction, the degree to which current capabilities map to future demands, and the vendor's focus on EMM requirements.

Market Understanding: This criterion evaluated vendor capabilities against future market requirements. It takes into consideration the evolution of the buyer for EMM suites, and whether the vendor will remain focused on meeting the buyer's needs.

Marketing Strategy: This criterion considered how EMM technology and value is positioned. The marketing strategy must be aligned with the evolution of the EMM buying center and its requirements.

Sales Strategy: This criterion evaluated the vendor's route to market (e.g., direct versus indirect sales) and the strength of the offerings that go to market with the vendor's EMM tools (e.g., file share and sync, desktop virtualization, endpoint security, endpoint management and desktop virtualization). We also evaluated the vendor's pricing models and whether they map to customer requirements.

Offering (Product) Strategy: This describes the degree to which vendors have plans to deliver differentiated functionality and have a timely road map to provide that functionality.

Business Model: This considers the vendor's business model for its EMM product and whether it ensures future investment and success in the EMM market.

Innovation: This evaluated the vendor's plans to meet customer needs that extend beyond conventional EMM technology.

Geographic Strategy: This refers to the vendor's strategy to direct resources, skills and offerings to meet the specific needs of geographies outside the vendor's home or native geography, either directly or through partners, channels and subsidiaries, as appropriate for the geography and market.

Table 2. Completeness of Vision Evaluation Criteria

Evaluation Criteria	Weighting
Market Understanding	High
Marketing Strategy	Medium
Sales Strategy	High
Offering (Product) Strategy	High
Business Model	Medium
Vertical/Industry Strategy	Not Weighted
Innovation	High
Geographic Strategy	Medium

Source: Gartner

Return to Top

Quadrant Descriptions

Leaders

Leaders have the highest product revenue in the EMM market, several years of proven customer implementations, customer mind share, and extensive partnerships with channel and other technology providers. They have the most complete products in the EMM market. Leaders also demonstrate commitment to the EMM market. Their companies are aligned with the trends of the EMM market. They possess product road maps, which (if executed upon) would establish continued differentiation in the market. Overall, they have a strategy that creates a high likelihood of success in this market.

Return to Top

Challengers

Challengers possess a strong ability to execute, demonstrated by high product revenue and a large customer base. The vendor's considerable resources ensure long-term viability. Challengers may have solid products, but lack the product commitment to lead the market. They are not as closely aligned with the most important EMM market trends, and do not have a road map that demonstrates compelling differentiation from other EMM products.

Return to Top

Visionaries

Visionaries have unique capabilities in certain aspects of EMM. They address a particularly important issue, such as Android support or data loss prevention, in a differentiated way. They meet the requirements of customers that place a high priority in certain critical EMM areas. They may not have the product completeness, support capability, business performance, mind share or track record compared with leading vendors.

Return to Top

Niche Players

Niche Players are often excellent choices for organizations. Niche Players do not have the product completeness, revenue, mind share and track record of Leaders or Challengers. Their product road maps typically represent a strategy of following the market, rather than leading it. In some cases, this is due to a lack of a vendor's resources. Often, many of the niche EMM products are extensions of other management, security or mobility products from those vendors. If a customer does not require best-of-breed capability, it may be best served by a Niche Player that may have an easier or less expensive way to meet EMM requirements, compared with Leaders or Challengers, for example.

Return to Top

Context

There are distinct differences in vendor strategies in the EMM market. In many cases, the EMM tools are designed to work with specific functions from the vendor (such as file share and sync), and specific mobile applications, client management tools and endpoint protection tools. We note these strategies in our analysis of each vendor in this research. IT leaders should base their decision in part on their need to combine EMM with these functions or whether they need an EMM tool that is independent of these technologies.

EMM product requirements change as mobile platforms change. Keep abreast of these changes; engage Gartner analysts regularly to understand the changing mobile device landscape and the implications on mobility management.

Best practices are:

Create your requirements first, and then form a list of vendors.

Consider all the possible mobile scenarios you may have in your organization, such as BYOD, and use cases specific to your organization.

Do not choose vendors simply on the basis of their position in the Magic Quadrant.

Many vendors were considered for the Magic Quadrant, but did not qualify because they did not meet the business metrics or the technical capabilities required for inclusion.

Microsoft did not meet the business metrics necessary for inclusion. Microsoft's Enterprise Mobility Suite is a combination of Windows Intune (for MDM and mobile application management), Microsoft Azure Rights Management and Microsoft Azure Active Directory Premium. The offering has promise, but Microsoft must drive adoption and demonstrate that it can meet enterprise requirements.

Other vendors considered, but that did not qualify, include Acronis, Apperian, CA Technologies, Centrify, Cisco, Cortado (formerly ThinPrint), Dell, Excitor, FancyFon, Fixmo, Ibelem, Kony, MobileSpaces, Seven Principles and The Institution.

Return to Top

Market Overview

The EMM market is evolving rapidly. CIOs see the potential to leverage mobility to better run, grow and transform their organizations. Indeed, the CIOs represented in our 2014 CIO survey ranked mobility among their top three technology priorities. As enterprises' use of mobility becomes increasingly complex, their requirements to protect data and support users will become more complex as well.

Organizations usually adopted MDM to help enable mobile users. As requirements broadened to more applications and access to more sources of content, MDM evolved into a broader set of technologies, which is now commonly referred to as EMM. The technology is at an adolescent stage, and has significant room to improve. Innovation around the EMM space in mobile application management, mobile data management, IAM and mobile security may alter the way organizations

approach these challenges, as well as broaden the technologies in the EMM toolset.

Return to Top

The EMM Buyer Is Moving to End-User Computing

Several important trends will bring about change in the EMM market. The most important trend is the movement of EMM into the end-user computing (EUC) operations group. Three factors are driving this change:

> Enterprise mobility is evolving from a special-purpose IT discipline into a general-purpose IT practice. Organizations initially chose an EMM solution based on how well it supported their email and calendaring needs, how well it worked with a certain mobile application, or its suitability to manage a particular device. Consequently, the buyer for the EMM tool was often someone in messaging, applications or telecom. However, organizations have evolved their mobility practice to serve many purposes, not only messaging, but also collaboration, productivity and business process optimization. This has led to the EUC group, which is charged to look holistically at enterprise computing requirements, to take ownership of mobility management.

> Because of current limitations in mobile platforms, there is a need to combine applications and their management capabilities, broadly referred to as "containerization." Smartphones and tablets operate in a sandboxed architecture (see "Learn the Taxonomy of Mobile and Endpoint Management Architectures"), which means management tools can exert only controls allowed by the OS. If the OS does not provide the necessary management capabilities, the capabilities must be built into the application. This means organizations may have to buy a specific EMM tool to support a specific application. This has also forced EMM vendors to build email applications with management capability not yet present in OS platforms, such as iOS and Android. This is a suboptimal situation. It means not all applications can be supported, and it has resulted in many management tool vendors stepping outside their core competency into developing messaging, productivity and other applications.However, the situation is improving. Mobile OSs are maturing their management and security capabilities. Apple made many device and application management improvements in iOS7. Hardware players such as Samsung and Intel that support Android are building platforms to better support enterprise needs. This will continue to reduce the need to integrate management functionality into applications. This means organizations will be able to choose EMM tools that support broad enterprise needs across multiple platforms and device types, rather than those that support a specific purpose.

> Endpoint platforms have become similar, with smartphones and tablets becoming more powerful and PC platforms adopting mobile computing architectures. Windows 8 and Mac OS X are adding MDM capabilities that will increasingly determine the way platforms are secured and managed. The convergence of the mobile and PC architectures logically drives an IT organizational convergence.

These changes will have a major impact on the management tool vendor landscape. Because the buying center for EMM tools is shifting to the EUC group, successful EMM vendors will have credibility and mind share with this IT role. Vendors that already have this credibility and mind share have a distinct advantage. Vendors that do not will have to earn it or move into other markets, such as collaboration or mobile applications, or be acquired.

Return to Top

Mobile Application Management Helps Maintain Order Amid Chaos

While mobile application management as a security technology will become less necessary, several factors will ensure its short-term necessity:

> First, while mobile platforms improve their management capabilities, these improvements will not meet all the security requirements (e.g., single sign-on, app timeout policies) for some organizations. Thus, mobile platforms will remain indefinitely necessary to embed these management functions into applications.

> Second, mobile platform providers (i.e., Apple, Google, Microsoft) do not inform customers of upcoming changes to their OSs. Therefore, embedding management capabilities into the app assures the organization that security policies will be maintained for the foreseeable future. This also reduces the IT organization's obligation to test every new version of the OS, because IT is concerned only with supporting the application.

> Third, containerizing applications through mobile application management reduces the complexity of supporting a multi-OS environment. This is particularly important on Android, where each variant of Android has its own support model.

> Finally, mobile application management provides, at least ostensibly, a less-intrusive way of delivering apps to users. This is particularly important in BYOD scenarios.

The maturity of the platform providers' management capabilities will be one of the most important aspects of enterprise mobility to watch over the next five years. Organizations may, in the end, still decide to use mobile application management, even when the necessary management functions are enabled by the OS. However, these decisions will increasingly be based on the functionality and usability of the apps, and not on the unique management capabilities they provide.

Return to Top

SaaS Helps Organizations Keep Up

SaaS has been widely embraced in the EMM market. Part of this is due to timing. Organizations have become more open to SaaS, in general, in recent years. However, part of this acceptance is due to unique characteristics of mobile technology. To keep up with the new features and mobile OSs as they become available, leading EMM vendors release software patches at least once a month and major releases once a quarter. If an organization runs its EMM tool on-premises, the IT staff is obligated to manage frequent updates to the server infrastructure. Consequently, Gartner has seen a significant percentage of organizations that previously would not consider a cloud-

based solution instead choose a SaaS model to maximize support for the latest technology. SaaS represents just over 20% of the market. This market share will continue to grow over the next several years.

Return to Top

The EMM Focal Point Will Shift to Data and Identity

Data protection is the greatest concern organizations have with respect to mobility. Organizations manage the device and applications as a means toward protecting the data. Increasingly, organizations will focus more closely on protecting the data through technologies such as DRM and IAM. EMM vendors will provide DRM technologies or integrate with third-party DRM tools. It's unlikely that the EMM and IAM markets will converge, but the two technologies will begin to work more closely together to enable organizations to better manage access to Web applications. EMM vendors will provide IAM capabilities that can federate with an IAM system.

in the short term, synergies between EMM and IAM will come to market. For example, if the EMM detects that the device is jailbroken or in a particular location, it could trigger the IAM system to revoke access to SaaS applications. Enterprises will demand that data be protected even when it flows outside the enterprise to parts unknown by way of unassuming employees who move information to places of convenience, albeit not places that are considered secure.

Return to Top

Unified Endpoint Management

As the IT role responsible for EMM continues to move to the EUC operations group, the inclination to use a common set of tools for mobile devices and PCs will grow. We believe that there are three waves of mobile and client management convergence, ultimately culminating in unified endpoint management (see "Managing PCs, Smartphones and Tablets and the Future Ahead"):

> The first wave involved largely separate tools for mobile and client management; this is where most organizations are today.

> The second wave will include more options for organizations to use a single vendor's tools for PCs and mobile devices. There will be more options, because mobile devices are making the management of their platforms easier, which will allow more vendors to offer sufficient EMM capabilities. Many organizations have an entrenched client management tool, which involved significant investments in training and implementation. Because their client management vendor may not meet their EMM needs, many organizations will skip Wave 2.

> Wave 3 will represent true convergence, we believe five to seven years out for most organization. The organization will no longer need legacy client management tools, because they have removed their dependence on legacy Windows applications. At this point, a single tool for all endpoints will be feasible.

Eventually, mobility will not represent a distinct set of platforms with their own management requirements. Mobile devices will be one of many components in a user's personal cloud. IT's job will be to manage access to and policy for each user's personal cloud.

Return to Top

About Gartner | Careers | Newsroom | Policies | Site Index | IT Glossary | Contact Gartner