Gartner

Magic Quadrant for Mobile Device Management Software

23 May 2013 ID:G00249820

Analyst(s): Phillip Redman, John Girard, Terrence Cosgrove, Monica Basso

Interest and adoption in mobile device management continues to grow at a fast rate, with companies looking for enterprise security and mobile optimization and enablement. Strong offerings go beyond policy to support enterprise mobile management.

Market Definition/Description

Enterprise mobile device management (MDM) software is: (1) a policy and configuration management tool for mobile handheld devices (smartphones and tablets based on smartphone OSs), and (2) an enterprise mobile solution for securing and enabling enterprise users and content. It helps enterprises manage the transition to a more complex mobile computing and communications environment by supporting security, network services, and software and hardware management across multiple OS platforms and now sometimes laptop and ultrabooks. This is especially important as bring your own device (BYOD) initiatives and advanced wireless computing become the focus of many enterprises. MDM can support corporate-owned as well as personal devices, and helps support a more complex and heterogeneous environment.

Magic Quadrant

Figure 1. Magic Quadrant for Mobile Device Management Software

Vendor Strengths and Cautions

EVIDENCE

[1] Gartner Webinar, "Best Practices in Mobile Device Management," 18 December 2012

NOTE 1
OTHER NOTABLE MDM VENDORS

A number of vendors assessed for this Magic Quadrant were not included because they did not meet our criteria. However, many of them offer some type of MDM software or service. These include:

- Amtel
- Apperian
- AppSense
- Aruba Networks
- AT&T (Toggle)
- Bitzer Mobile
- Capricode
- Centrify
- Cortado
- Dell Kace
- Excitor
- Fixmo
- ForeScout Technologies
- Globo Mobile
- Ibelem
- Juniper Networks
- Kony
- Cicso-Meraki
- Microsoft
- Mobile Active Defense
- MobileFrame
- MobileSpaces
- Mobiquant
- Notify Technology
- Novell
- OpenPeak
- Portsys
- Samsung SDS
- Seven Principles
- SilverbackMDM
- Smith Micro Software
- The Institution
- VMware

NOTE 2
DECISION CRITERIA FOR CHOOSING MDM SOFTWARE

Although the Magic Quadrant is the tool to use to help make a purchase decision, many clients ask what are the main criteria when deciding whether to purchase an MDM at all. Note 3 looks at the criteria for moving away from the use of EAS, but there are some additional criteria to consider when choosing an MDM solution. These include:

- Internal resources for management — Most MDM purchases are 500 devices or fewer. The size of the company doesn't really matter here as much as the internal resource capabilities to manage devices. From our research, 47% of MDM sales are for fewer than 100 seats, so many SMBs are purchasing MDM software.
- Complexity of data — Gartner's position is that any enterprise data needs to be protected and managed. MDM is a start, by enforcing enterprise policy around encryption and authentication. We also believe containers should be used to manage email and other mobile content, like file sharing, or enterprise apps, like sales force automation (SFA). These are also delivered by MDM vendors.

Absolute Software

Absolute Software is a publicly traded company based in Vancouver, British Columbia, Canada. The vendor provides endpoint management and security tools to track, secure and manage PCs, Macs and mobile devices. Absolute was one of the early client management vendors to enter the MDM space, and has done a good job of driving MDM adoption within its installed base. Recently, Absolute has strengthened its partnership with Samsung, which will include Absolute's persistence' technology in the firmware of select devices later in 2013, and also included Absolute as one of the MDM providers to support its recently announced Knox platform. Absolute Manage is sold at a low price point, and the majority of its MDM revenue comes from education (K-12 and higher education) customers. Absolute Software is positioned in the Niche Players quadrant and should be assessed for adoption, especially in the education market or by companies that want a single tool for PCs and mobile devices.

Strengths

- The vendor provides a strong management capability across mobile devices and traditional PCs, with particular strengths on Mac OS X.
- Absolute Software has a very good reputation for customer service and support.
- Absolute Manage gets good feedback from references for ease of use and deployment.

Cautions

- The software lacks some enterprise-class features built into competitive products, such as built-in certificate authority, although an alternate model is provided that leverages existing infrastructure, such as Active Directory and Network Device Enrollment Service, to issue user certificates automatically embedded in configuration profiles for Exchange authentication.
- Absolute Manage needs stronger mobile application management (MAM) capabilities, such as mobile app wrapping, email containerization for Apple iOS, an app-level VPN and application analytics.

AirWatch

AirWatch is a privately held company based in Atlanta, Georgia. It continued its international expansion, adding new offices and data centers in North America, Europe, India and Australia. The vendor developed a strong presence in sectors such as airlines, pharmaceutical, energy and retail. AirWatch had a very successful execution during the past 12 months, more than doubling its total customer number in 2012. More than 70% of customers deployed cloud-based software as a service (SaaS), but AirWatch also offers a complete on-premises-based solution. AirWatch's enterprise MDM offering has broad MDM functional breadth and maturity, including enhanced mobile security, application security and management, mobile content management (through Secure Content Locker) and mobile email management, as well as enterprise back-end infrastructure integration. AirWatch is positioned in the Leaders quadrant and is recommended for all size companies, especially those with broad MDM needs.

Strengths

- AirWatch supports containerization of corporate email, browsing, content and applications, mostly through integrating third-party technologies such as NitroDesk's TouchDown, Enterproid Divide and Samsung Knox. In addition to dual personas, multiuser mode is also supported, to manage multiple users on the same device.
- Secure Content Locker offers secure file synchronization and sharing capabilities for mobile devices with policy enforcement on document manipulation and application access — both on-premises and in the cloud.
- Cross-platform needs — More than ever, companies will begin to support multiple OSs. Although today Apple dominates smartphone sales in the enterprise, users will want to bring a variety of other devices to work that MDM providers can manage in an integrated fashion. Once your company has such a diverse environment, MDM becomes a necessity.
- Delivery — Companies need to decide on whether they want MDM on-premises or in a SaaS/cloud model. SMBs prefer the SaaS model because it reduces the cost and total cost of ownership, based on having hardware to support fewer users. Large companies that are comfortable with the cloud model, usually in nonregulated markets, also are moving toward SaaS. In a global, highly distributed environment, they also like the appeal of the reduction in hardware and server management that cloud brings, versus on-premises servers. MDM managed services are also emerging, but are currently limited in scope and adoption..

NOTE 3
DECIDING TO MOVE FROM EAS TO A MORE COMPREHENSIVE MDM PLATFORM

Most companies started out using EAS to manage their devices, but found it lacking in the following areas, which pushed them to purchase a more complete MDM suite:

- Volume of devices. It is difficult to manage a larger volume of devices on EAS. Once companies got to more than 500 devices, they typically looked for a more complete MDM suite.
- Mix of platforms. Companies that had two or more mobile OS platforms to manage found it difficult to do so on EAS.
- Granular support/policy. More complete MDM systems offer a deeper management capability, with more-detailed policies. For example, EAS allows passwords to be enforced (depending on the mobile OS), but more-comprehensive MDM systems allow more flexibility in the password type, length and complexity.
- Reporting. EAS is very weak on device reporting. Companies that wanted better reporting moved to more complete MDM systems.
- Ability to block certain device platforms. Companies may want to restrict the types of mobile OSs they will support.
- Need to identify rooted/jailbroken devices. There is concern over rooted or jailbroken devices because companies cannot control their data if devices are compromised.
- Advanced capabilities to manage mobile apps. Application provisioning and updating are important to companies today.

- AirWatch has aggressive pricing and great flexibility in software and service licensing in individual contracts that meet most industry- or company-specific requirements.
- The vendor offers a layered approach in its cloud model, including via traditional implementation in its own data center in Atlanta, through infrastructure as a service (e.g., with AT&T, Telstra and Verizon Terremark) and through Amazon Web Services (AWS) in selected countries.

Cautions

- Despite the strong focus on customer support and great account management (often with the direct involvement of the CEO), occasionally reference feedback has been suboptimal, with negative experiences specifically regarding implementation and postsales technical support for on-premises installations and upgrades.
- Enhanced features for corporate containerization are not equally supported across iOS, Android, and Windows Phone platforms and OS variants. This fragmentation may result in increased complexity where device diversity is a priority.
- AirWatch has grown rapidly (with over 1,000 employees by the end of 2012), but there has not been matching growth in the executive leadership team. This may affect the ability of the vendor to grow to the next level.
- Despite its achievements, AirWatch still needs to grow its visibility in the market. For example, it still doesn't have a complete social community experience for customers and developers.

BlackBerry

One of the new entrants in this Magic Quadrant this year, BlackBerry is a global public company with headquarters in Waterloo, Ontario. It ended its fiscal year in February 2013 with $11.1 billion in sales, including $4.2 billion in software and services. BlackBerry's focus has been on developing the new BlackBerry 10 (BB10) devices to compete with existing smartphone platforms. The vendor launched its first cross-platform MDM server, called Mobile Fusion, after the last Magic Quadrant research was developed, so it did not qualify. Its latest MDM product was released in January 2013 as part of the BlackBerry Enterprise Service 10 (BES 10) announcements to support the new devices. BES 10 has limited experience supporting non-BlackBerry devices, but still leads the way for mobility management based on its own platform. Although there hasn't been much adoption of cross-platform MDM from BlackBerry, there has been significant interest among its core base. Its success in MDM will rely on uptake of the new BB10 devices and the updating of older versions of BES to BES 10. BlackBerry is not considered much of an innovator in cross-platform MDM; although it does manage Android, it does not yet support advanced Android APIs from Samsung Safe-certified devices, but does have the strongest offering to manage and support BlackBerry devices. Although some vendors offer limited BlackBerry device support, these devices have a closed system that doesn't allow deep support outside the devices' own servers. BlackBerry has also created a unique and secure way to route MDM traffic through its infrastructure, eliminating the need to use a separate VPN. BlackBerry is positioned in the Niche Players quadrant and should only be considered for BlackBerry management or for cross-platform if iOS is needed and BES 10 has been purchased.

Strengths

- BlackBerry has designed an easy upgrade path to support BB10 devices by which current BES 5 customers can get a free upgrade, with over 12,000 installs of BES 10 by May 2013.
- BlackBerry supports basic iOS and Android device policies equal to other MDM vendors and provides industry leadership functionality for its own devices.
- The containerization of BlackBerry devices, called BlackBerry Balance, is the best example of the separation of corporate data from personal data while retaining a strong user experience.

EVALUATION CRITERIA DEFINITIONS

Ability to Execute

Product/Service:
Core goods and services offered by the vendor that compete in/serve 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 (Business Unit, Financial, Strategy, Organization):
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 and Track 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,

Cautions

- BlackBerry has been more focused on policy management and the management and enablement of cross-platform enterprise mobility than on mobile content management. It still requires a third-party partner to provide extended Android support.
- Combined with BlackBerry device support, cross-platform MDM can get very expensive and it does not have a cloud offering or partner.
- BlackBerry uses third-party solutions to secure and containerize iOS and Android.

BoxTone

BoxTone is a privately held company based in Columbia, Maryland and Mountain View, California — with eight years of experience in the MDM market. The vendor established its presence in the U.S. market — specifically in regulated markets such as financial, government and healthcare — and, during the past year, it has been focusing on international expansion in other regions, particularly Asia and Europe, through partnerships with international carriers and service providers. Traction in the market grew in terms of customers, revenue and partnerships, despite aggressive competition from market leaders. The vendor's distinguishing element is its focus on mobile service quality, and service-level and workflow management. BoxTone 7 brings a "single pane of glass" platform-based approach to support the full life cycle of mobility management from a system management/ITIL perspective. BoxTone is positioned in the Visionaries quadrant and is recommended for enterprises and managed service providers (MSPs) with hybrid mobility server and container environments (e.g., BlackBerry, Good Technology, Exchange ActiveSync [EAS], etc.) with service-level and workflow management requirements.

Strengths

- BoxTone assumed control of Motorola 3LM to enforce strong security on Android devices, and built a range of technology provider partnerships, including with Good Technology, Mocana and Samsung. Its offerings evolved in multiple areas, including containerization, analytics for application management and enhanced mobile service management.
- BoxTone is expanding its presence in regions other than the U.S. through new offices in London and Tokyo, and a range of embedded partnerships with carriers in Japan, such as NTT Docomo and KDDI. In addition, enterprise IT vendors and MSPs (such as IBM, HP, Dell, CSC, Xerox and Mahindra Satyam) embed or resell BoxTone software.
- BoxTone enjoys excellent customer feedback in multiple areas, including presales and postsales support, assistance during implementation, direct technical support, ease of use, and breadth of services.

Cautions

- Despite improvements, BoxTone still suffers from a limited presence outside the U.S., in terms of local support and sales, especially compared with the capillary presence established by some MDM competitors in the past 12 months.
- BoxTone does not offer native file synchronization and sharing capabilities as part of its mobility management product; rather, it partners with a number of specialized third-party players, such as Accellion, Box and Good Technology. It also relies on third-party technology and partnerships for some MDM capabilities that are becoming core, like containerization and enterprise file synchronization and sharing (EFSS).
- While offering cloud-based services (through Xerox, HP and CSC partnerships), BoxTone's track record and installed base on SaaS/cloud is still pretty limited.

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 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 vendor's underlying business proposition.

Vertical/Industry Strategy:
The vendor's strategy to direct resources, skills and offerings to meet the specific needs of individual market segments, including vertical markets.

Innovation:
Direct, related, complementary and synergistic layouts of resources, expertise or capital for investment, consolidation, defensive or pre-emptive purposes.

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

Citrix

Citrix is a public global company with U.S. headquarters in Santa Clara, California, and it had 2012 revenue of $2.59 billion. Its primary focus is cloud computing and the vendor has only recently turned its direction to mobile, with the launch of CloudGateway 2 in 2012 and the acquisition of one of the MDM market leaders, Zenprise, which closed in January 2013. Citrix's primary MDM product is called XenMobile MDM, which includes application containerization (Citrix MDX) and data containerization (ShareFile). Although the MDM revenue and MDM product of Citrix's is mostly based on Zenprise, it has quickly moved to rebrand and integrate the MDM products into its current on-premises mobility solution, in addition to offering MDM as a cloud offering. Zenprise saw significant growth in 2012, but often struggled in market presence and awareness, compared with competitors that had deeper channel partnerships and direct sales support. Gartner expects that investment and integration by Citrix will accelerate that growth and awareness in 2013. The vendor is positioned in the Leaders quadrant and should be assessed by companies of all sizes and industry segments.

Strengths

- Citrix has a strong, broad set of enterprise mobile offerings in all the major MDM areas.
- The vendor has a deep understanding of enterprise application and mobility needs, and a long history of supporting mobile endpoints and remote access through product innovation and acquisitions. It's one of the few companies that offers secure containers for smartphones, tablets, Macs and PCs.
- It has an integrated product solution across all major MDM areas.

Cautions

- It often presents a cloud-first product, although XenMobile MDM is offered both as cloud-hosted and on-premises.
- XenMobile can only be purchased in two forms: MDM only or the entire suite with MDM, MAM, sandboxed email and browser, unified app store, and single sign-on (SSO). Citrix does not sell all these products a la carte.
- Citrix does not have a strong consumerization play (meaning enterprise products not supported by IT and brought in by end users) nor is it known for having a small or midsize business (SMB) offering.

Fiberlink

Fiberlink is a privately held company based in Blue Bell, Pennsylvania, running an MDM business since 2007. Fiberlink has proven long-term viability, with an established presence mostly in North America and Europe, and a developing one in the Middle East and Asia/Pacific region. It does not specialize in specific sectors, but tends to serve organizations that are not constrained by tight regulations and can adopt the cloud model. In the past year, Fiberlink experienced massive business growth, with revenue up 320% and customers up 250%, driven by the cloud model, simplified pricing and ease of implementation. Fiberlink's MaaS360 is a pure MDM multitenant cloud services offering for organizations aiming to support corporate and personal devices. MaaS360 supports containerization, enterprise app stores and mobile content management, including SharePoint access and sharing document links in email. Fiberlink is positioned in the Leaders quadrant and is recommended for companies of all sizes and industries, but only those that support cloud only offerings as it does not have an on-premises solution.

Strengths

- Fiberlink has a large installed user base and a great track record, and is focused entirely on a cloud-based model.
- Fiberlink's performance with clients is rated highly, as proven by excellent reference client feedback. Clients greatly appreciate its presales and postsales support, smooth and uneventful implementations, and technical assistance during installations. Smooth integration of MaaS360 with third-party cloud email services is commonly reported.
- The vendor offers competitive pricing and personalization of contracts, offerings and pricing to meet specific requirements are recognized for this in the market.

Cautions

- The lack of an on-premises option restricts the viability of MaaS360 with only a pure cloud services offering to organizations that are comfortable with the cloud model.
- Despite improvements coming from its channel partners' activities, Fiberlink's activities outside the U.S. and Europe are still developing. Its limited local presence in the Asia/Pacific, Latin American and Middle East regions can affect its ability to support out-of-area customers in the short term.
- Current support for mobile content management (via MaaS360 Secure Document Sharing) supports the secure central distribution of documents for teams, secure email attachment storing and user-fetched SharePoint documents, but it lacks broader support for corporate file servers and network drive access, file sharing, and PC folder synchronization.

Good Technology

Good Technology is a privately held company based in Sunnyvale, California. It has been in the MDM business since 2000. The vendor has a long history and successful track record in enterprise mobility, specifically in regulated sectors, but 50% of its customers include customers outside these industries who are concerned with data protection and security. Good has grown its presence during the past 24 months in regions outside the U.S., increasing sales by 95% in EMEA and the Asia/Pacific region between 2010 and 2012, and now representing 25% of the overall business, (which is under the average of 25% of international sales for MDM companies). Specifically, Good experienced overall strong growth in 2012, some of it based on its acquisitions of Copiun and AppCentral that year. Good for Enterprise (GFE) is a mobility suite encompassing security, management, mobile application development and management, content management, and mobile collaboration. The vendor offers a unique form of corporate containerization across multiple mobile device OSs, with complete isolation of the corporate footprint from personal content. GFE provides full cross-platform MDM capabilities, as well as management of the corporate container. The vendor has entered into a strategic partnership with BoxTone to add service management of the whole device and to improve its application management and reporting functions. Good owns 56 issued U.S. patents and 117 issued non-U.S. patents and key intellectual property rights in multiple fields of enterprise mobility, including mobile synchronization, device and application management, and security, and is currently in litigation with competitors for patent infringement. The vendor is listed in the Leaders quadrant and is recommended for companies of all sizes, especially those with a focus on data protection and security, secure enterprise email, and secure integration with third-party and custom enterprise applications.

Strengths

- Good provides a strong platform to enable secure communications between its own apps, enterprise applications and many third-party independent software vendor (ISV) apps, creating efficient workflows.
- Good offers strong security capabilities, including FIPS 140-2 crypto libraries, end-to-end Advanced Encryption Standard (AES) encryption, multiple-factor authentication and multiple certificate management systems.
- The vendor has a broad spectrum of management capabilities, including application security and management functions, offered through Good Dynamics and AppCentral, and Good Share for file synchronization and sharing, integrated with email (as a result of the Copiun acquisition).
- Good maintains a large customer installed base in industries such as financial services, government, defense, public sector, healthcare, manufacturing and professional services.

Cautions

- Good's approach is often rated negatively by users because of the restrictions on the native applications' experience on the mobile device — for example, the lack of real-time email push and notifications in the Good Messaging client for iOS.
- Pricing of Good MDM is high in the market, compared with competing offerings.
- Its primary focus on the on-premises model limits Good's execution in a broad enterprise market where, increasingly, cloud services attract interest and investments. Good Share, available only on-premises, does not support extended organization scenarios with external nonemployee users.
- Good does not offer management or integration for BlackBerry devices and BES, except through its additional product offering with BoxTone.

IBM

IBM is a publicly traded company based in Armonk, New York. IBM Endpoint Manager for Mobile Devices provides MDM while using the same IBM Endpoint Manager infrastructure (formerly BigFix) used to manage PCs, Macs and servers. The IBM MDM offering is relatively new and was developed from the vendor's BigFix acquisition. It offers solid device management functionality for iOS, Android, Windows Mobile and Phone, BlackBerry, and Windows RT. IBM has grown its MDM customer base nicely, primarily by selling the product to existing client and server management customers. IBM is investing in MDM to expand its enterprise mobile offerings, a key component, including the integration of the vendor's mobile application development platform, IBM Worklight, and IBM Endpoint Manager for Mobile Devices. IBM plans to add more MAM capabilities where applications developed in IBM Worklight can include policies that are then implemented by IBM Endpoint Manager. IBM is positioned in the Visionaries quadrant and should be considered by large companies that are looking for support across client and mobile devices.

Strengths

- IBM Endpoint Manager can maintain compliance standards across a wide range of endpoints, including mobile devices, PCs, Macs and servers.
- It can be licensed by user or device, offering flexibility for organizations managing multiple devices per user.
- IBM Endpoint Manager's relay architecture enables a high degree of scalability with relatively few servers.
- IBM has started to integrate its mobile application development solution with MDM for stronger application provisioning.

Cautions

- The software currently lacks built-in MAM capabilities to containerize email and mobile content, and to provide advanced features such as an in-app VPN. However, IBM partners and provides integration with NitroDesk's TouchDown and Enterproid Divide.
- IBM extended the concepts of relevance language and fixlets from its traditional endpoint management offering to mobile devices. This gives its customers good flexibility in creating customized policies; however, customers state that IBM needs to provide more out-of-the-box content to ease administration.
- The software also doesn't have a dashboard view that is common in other products, where key alerts and actions are easily viewed.

Kaspersky Lab

Kaspersky Lab has its main headquarters in Moscow and is a private company focused mostly on consumer and SMB security products. It has reported unaudited revenue of $628 million at year-end 2012. The vendor's main MDM product is called Kaspersky Security for Mobile and was released in 2012, so is new on the MDM market. Kaspersky Lab's emphasis on MDM is part of its security roots, with its strengths in the integration onto its security platform, and its products for mobile antivirus and malware. Kaspersky is positioned in the Niche Players quadrant in this Magic Quadrant. It targets SMBs and should be assessed for basic MDM needs in that area.

Strengths

- The vendor has a strong emphasis on mobile device security, including mobile VPN, and antivirus and malware.
- The software offers simple configuration and an easy-to-use portal.
- Kaspersky Lab provides a unified MDM and security management to give detailed control over the deployment and management of mobile platforms as well as wide range of endpoints.

Cautions

- For Android, the vendor only supports basic policies today, and it does not work directly with original design manufacturers.
- The vendor does not extend much beyond the basic policies and security of mobility (for example, it does not provide an integrated enterprise file sharing capability).
- Kaspersky Lab's strategy is to only offer on-premises servers as part of its overall security suite, with no cloud offerings.

LANDesk

LANDesk is a privately held company based in South Jordan, Utah. It is an established player in the client management tool space through its flagship product, LANDesk Management Suite (LDMS). LANDesk provides Mobility Manager, which has been augmented through the vendor's 2012 acquisition of Wavelink. Wavelink was an MDM provider, particularly known for its support of ruggedized device platforms. LANDesk's strategy is to provide unified device management for all end-user endpoints; however, it still has work to do in modernizing and unifying its consoles for MDM and client management. The legacy LANDesk Win32 console provides integrated MDM and client management. The MDM product can also be administered using a more intuitive and portable Web-based console, but does not provide client management. LANDesk is positioned in the Niche Players quadrant and should be considered by companies with a large installed base of industrial devices.

Strengths

- LANDesk provides smart device, ruggedized device and mobile device management, and PC and Mac management, with particular strength in PC management.
- LANDesk provides a user-based licensing model that allows customers to license Mobility Manager, LDMS, and LANDesk Security Suite by user, rather than by device.
- The MDM product provides strong ruggedized device management capabilities, with the agent preloaded on many ruggedized handheld models.

Cautions

- Mobility Manager lacks app wrapping to manage mobile applications with a greater level of control than can be accomplished through standard device management.
- LANDesk does not have a secure file share capability, either through a proprietary product or a partner, with integration into Mobility Manager.
- Through the acquisition of Wavelink, large-scale deployments in upward of 200,000 ruggedized devices have been proven and mixed-use device implementations have been deployed by more than 5,000 users.

McAfee

McAfee, based in Santa Clara, California, is a long-term, global player in endpoint protection markets. Comprehensive security management is provided for a wide range of platforms, including all major workstation configurations and mobile device platforms. McAfee ePolicy Orchestrator (ePO) integration with McAfee Enterprise Mobility Management (EMM) will be a future competitive advantage; for example, buyers could take advantage of McAfee Risk Advisor (available for an extra charge) to provide a prioritized, risk-based or threat view of mobile device behaviors and profiles. Like other endpoint protection platform (EPP) vendors, McAfee will sell its products based on reputation in other security markets and as a value-add to workstation contracts, particularly for worldwide companies seeking solid management and reporting capabilities across a number of disparate security controls. As a long-term player in security, the vendor's mindset is on prevention of malware, data loss prevention (DLP), blacklisting, access controls and other classic security measures, but it hasn't been as focused on the MDM market. Buyers who seek leading-edge MAM and container solutions will need to supplement EMM with additional products, and should consider alternate MDMs with more extensive integration or ownership of MAM and containerization solutions. McAfee is positioned in the Niche Players quadrant and should be considered by its existing customer base and those looking for integrated EPP security products.

Strengths

- Gartner client inquiries strongly associate McAfee's mobile data protection and endpoint protection products for suite purchasing. As a result EMM gains instant credibility, but mainly as a component of the vendor's larger product framework.
- Granular policies make it easy to add, change and delete certificate authorizations, and to remind users of expiring credentials. Two certificates are used to track each mobile device, making copying and cloning difficult. App usage can be tagged by roles that control execution contexts without requiring a divided user interface (UI).
- Standard maintenance support is included at no charge.

Cautions

- Buyers are weathering changes in both mobile management and mobile device platforms that call for short investment periods for MDM — perhaps as little as 18 months. Integrating EMM with ePO increases stickiness, and could increase the switching costs of organizations considering downstream migrations. As mentioned earlier, leveraging ePO integration in a long term investment is among the strongest arguments in favor of considering EMM.
- EMM pricing did not follow competitive trends during the study period. McAfee confirmed its willingness to negotiate, but pricing examples reviewed by Gartner were based on per-device prices, whereas the trend is moving to month-by-month, per-user pricing, with no cancelation penalties.

MobileIron

MobileIron is a private company based in Mountain View, California, and has been focused on the MDM market for almost three years, since its first product launch. Its main MDM products are the mobile policy configuration engine VSP version 5.5 and Sentry. Its complete solution also includes products in the mobile software and content management space, called AppConnect and Docs@Work. The vendor has been in the Leaders quadrant in the Magic Quadrant for Mobile Device Management Software for the previous two years now. It has driven its success through many channel partners and delivers its solution mainly through its appliance globally. In 2012, it had another strong sales year and is one of the top five MDM vendors in terms of sales revenue and number of mobile devices supported. It has a very strong vision for enterprise mobility and has developed or acquired the technology to deliver. It has executed well in sales, support and customer service. In 2013, MobileIron is again listed as a Leader and should be considered for MDM for companies of all sizes and in all regions, especially those that want an appliance model.

Strengths

- The vendor has a proven strong vision of enterprise mobility and MDM, and has executed well in terms of product development, launches and support.
- MobileIron has a focus beyond simple policy management and configuration, and is usually first to market with an integrated solution focused on the mobile enterprise.
- MobileIron has proven management, scaling and financial viability in a competitive market.

Cautions

- MobileIron's strength is in delivering software via an on-premises appliance, and although it launched its SaaS version in 2011, it made significant progress in providing a stronger cloud solution in the past year.
- MobileIron received a number of complaints regarding customer service when it was delivered by partners, but has taken back Level 1 support and has seen increased customer satisfaction.

SAP

SAP is headquartered in Walldorf, Germany, and has U.S. headquarters in Newtown Square, Pennsylvania. It is a global provider of business software. It invested in the MDM market to support its customers and partners in the pursuit of mobilizing their employees by managing devices, applications and content. SAP acquired mobile management, application development and security technologies from Sybase and has expanded development of MDM under the Afaria name. SAP emphasizes scalability, integration, application development and usability as primary objectives, but also has critical security and management features in place. It recently increased certificate management and updated its directory integration capabilities. SAP also has a strong enterprise presence and cross-sells Afaria with a mobile application development platform through a global direct sales team. Since our last Magic Quadrant research, SAP also signed and executed a substantial OEM deal for Afaria with CA Technologies (the first of its kind with a leading system management player), and expanded its position in the telecom/value-added reseller (VAR) area by licensing Afaria to Ingram Micro, the world's largest technology distributor. SAP is positioned in the Leaders quadrant in the Magic Quadrant, and should be considered by companies that invest in new and existing SAP products and services, and those that can benefit from tighter linkages between application development tools and MDM platforms. It should also be evaluated in terms of the strength of Afaria, its container architecture and application development tools, and its third-party ISV program with over 100 partners.

Strengths

- Buyers already invested in SAP will find that Afaria strengthens the long-term viability of SAP's mobility road map. The vendor's 200,000-plus business customer base, global partner ecosystem and worldwide direct sales teams will fuel growth.
- SAP provides a comprehensive app-neutral mobile container strategy, although it has a limited number of app partners. Applications must be compiled with the Afaria software development kit (SDK), but SAP should be able to attract a growing ISV community, in addition to its large base of users leveraging its analytics SDK. SAP can attract partners on a more complementary basis than some of its competitors coming from adjacent markets, such as endpoint protection or life cycle management.
- SAP has the global scale to build mobile partnerships with companies in security, life cycle management and business apps, with considerably more leverage and less apparent competition than other MDM vendors.
- The Afaria tool has one of the longest and most mature track records of all MDM tools, and is well-regarded for its functionality, including integrated capabilities of SAP BusinessObjects into the Afaria management console, which can be enhanced with SAP Hana, giving it strong analytical and reporting functions that support the real-time analysis of mobile user trends.

Cautions

- Buyers that do not have or want long-term investments in SAP's larger framework might find that even a modest investment in Afaria might lead to trade-offs against opportunities for increasing functionality, although SAP has demonstrated faster innovation during this past year.
- SAP has some challenges selling Afaria stand-alone in competitive MDM deals. Gartner expects that SAP will move to offer an aggressively priced per-device commercial model for stand-alone MDM cloud services to eliminate barriers to entry — a move that will reduce margins and fuel further price competition around core MDM functionality.

Sophos

Sophos is a global company with U.S. headquarters in Boston and U.K. headquarters in Oxfordshire. It earns a fair balance of business in North America, Europe and, increasingly, in the Asia/Pacific region. Its MDM tool, Sophos Mobile Control (SMC), now in version 3.5, was added to the Sophos portfolio by a combination of in-house development and the acquisition of Dialogs. Sophos' share of the MDM market was sufficient to meet inclusion criteria and was nearly four times that of prior reports, but is still smaller in comparison to the established market leaders. Gartner has seen Sophos compared aggressively in competitive bids from other EPP vendors that have added MDM capabilities, but it also routinely competes against pure-play MDM vendors. The vendor applies a security mindset to mobile data privacy, with an emphasis on malware defense, filter-based DLP and secure Web gateways. Sophos has aggressively priced SMC to sell as a stand-alone solution. It was among the first of the MDM vendors to offer a cloud solution for under $2 per month that allows unlimited devices per user and has no contract cancellation penalties, and has seen rapid uptake in the past 12 months. Sophos is positioned in the Niche Players quadrant for 2013 and is very competitive for any company seeking core cross-platform policy management, especially for SMBs.

Strengths

- Buyers will take Sophos' long-term play in the endpoint protection markets, combined with a steady entry into MDM, as a vote of confidence when seeking integrated endpoint security frameworks.
- While all EPP vendors have implemented MDM, Sophos was one of only five from that market that could qualify for MDM ranking. Sophos comes in second among EPP vendors for both execution and vision and provided quantitative data to verify market presence.

- Sophos developed a complementary file sharing utility that transparently encrypts files leaving a PC or mobile device in order to prevent data leakage. This integrates with third-party file storage providers and allows companies to securely use low-cost third-party storage.

Cautions

- Companies that require trusted certificates should note that Sophos currently supports only the Microsoft Certificate Services.
- Sophos has not provided the same MAM capabilities as the leading vendors.

Soti

Soti is a private company based in Mississauga, Ontario, Canada, with local sales and support offices around the world, including the U.S., U.K., Australia, India and Columbia. The vendor has a long and successful track record in managing consumer Android, and iOS devices, as well as rugged mobile devices, with MobiControl. To improve the isolation between corporate and personal content, Soti's strategy is to primarily provide strong support for system-level containerization (e.g., with Samsung Knox) when possible; however, when that is not possible (e.g., with iOS), Soti's strategy supports an SDK solution. In addition, Soti has applications with data isolation for corporate email (e.g., NitroDesk) and corporate content libraries (e.g., SharePoint integration into MobiControl's Content Library) to isolate corporate and personal content. Soti is positioned in the Visionaries quadrant and should be considered for organizations that require strong device management capabilities, especially where there is a need to support a wide range of Android-based devices with its Android+ functionality (e.g., silent application deployment, remote control, lockdown [kiosk mode] and device feature controls).

Strengths

- MobiControl provides comprehensive policy controls for a wide variety of Android device manufacturers, and includes innovative functions like antivirus, silent application installation, geoaware policies, remote control and Web content filtering.
- MobiControl application deployment provides an autoconfigure option, which allows administrators to deploy mobile applications with relevant corporate settings (e.g., application development information) included.
- MobiControl provides remote control for a wide variety of Android devices and remote view for iOS applications via the MobiControl iOS SDK.

Cautions

- MobiControl does not have comprehensive integrated mobile app management capabilities, such as an app-level VPN and application analytics.
- Customers have stated that MobiControl must improve its reporting through a wider variety of out-of-the-box reports and by making it easier to create custom reports.

Symantec

Symantec is a global security company with worldwide headquarters in Mountain View, California. It is publicly traded and ended the 2012 fiscal year with $6.73 billion in revenue, driven by both enterprise and consumer products. Mobile solutions have been its emphasis for some time, going back to its acquisition of Altiris, which many companies use to support laptops. In 2012, it acquired two companies, Odyssey Software and Nukona, to expand its MDM offerings in policy and application management. In 4Q12, Symantec launched an integrated product suite for MDM called Symantec Mobile Management Suite. It carries all the necessary components of a strong enterprise mobile offering, including the ability to wrap apps. Even with a strong product offering, the vendor has executed weakly in terms of very low mind share and market presence in MDM, and is rarely listed in shortlists or proposals that Gartner sees, compared with competitors. It has recently reorganized its business units and has a new general manager, and should be able to increase its marketing of and channel partnerships for MDM for greater visibility in 2013. Symantec is listed in the Visionaries quadrant for 2013 and should be considered by companies of all sizes and in all regions, especially those that already use Symantec for enterprise security.

Strengths

- Symantec has a broad integrated MDM offering that supports each of the critical components of MDM.
- With its consumer products, the vendor is well-positioned to secure and support BYOD initiatives, and has focused business groups for both personal and corporate products.
- Symantec has integrated strong security features for mobile DLP and identity and access management (IAM).
- It is focused on providing a large app catalog via the Symantec Sealed Program, although today the offering is limited, with few applications.

Cautions

- Symantec's broad offerings often overlap and there is sometimes confusion over what is available and which offerings are enterprise-focused versus consumer-focused.
- Symantec has not proven execution in the MDM market the way it has for laptops and PCs.
- With its broad offering, Symantec is well above the median price for similar basic MDM solutions, although broader offerings are competitive.

Tangoe

Tangoe is headquartered in Orange, Connecticut, and began trading on Nasdaq in July 2011. It is a communications-life-cycle-management-technology-enabled service provider with revenue of $154.5 million as of December 2012. Its MDM solution has been available for four years as a result of an acquisition. Through 2011, Tangoe primarily bundled its MDM solution with its telecom expense management suite and experienced modest growth. As of 2012, Tangoe increased its R&D, sales and marketing investments in MDM, and is experiencing accelerating growth with stand-alone MDM buyers and buyers purchasing its managed mobility services, including MDM. The result of Tangoe's increasing investment is apparent through its improved user interface and platform support, despite being deficient in some of the leading-edge features that more advanced buyers desire. The vendor is positioned in the Niche Players quadrant and should be considered by companies seeking MDM, MDM managed services and/or a broader managed mobility service.

Strengths

- The vendor's business is exclusively focused on enterprise mobile solutions, with a strong emphasis on managed mobility services.
- Tangoe operates globally and can support global MDM implementations.

Cautions

- MDM is a piece of Tangoe's larger managed mobility services; therefore, it receives a smaller proportional R&D and resource investment.
- Tangoe employs an open-architecture strategy, which results in some non-native capabilities, such as containerization and content management.

Trend Micro

Trend Micro is a global company with U.S. headquarters in Dallas. It has built its MDM capabilities from internal technologies and sells them as add-ons to the OfficeScan suite. Revenue is strong, in contrast with virtually no client inquiries regarding the vendor's MDM, even from Gartner clients in the Asia/Pacific region. Trend Micro is maintaining healthy sales and a strong presence in its main Asia/Pacific markets, and shows sufficient presence in other geographies to merit evaluation in this Magic Quadrant. Uptake is steady; however, for other strong MDM players, revenue is increasing markedly. Trend Micro is positioned in the Niche Players quadrant, and should be considered if you have a long-term product and contract commitment to integrate MDM with the next generation of OfficeScan and are approaching MDM with traditional security expectations. Trend Micro focuses on device policies, secure Web gateway, malware defense and app controls based on whitelisting and blacklisting. Consider alternatives if your road map emphasizes containerization and secure mobile application development. Trend Micro should also be considered for its SMB focus and for global organizations, especially those with an emphasis in the Asia/Pacific region.

Strengths

- Graphical priorities in the administrative UI lead to powerful at-a-glance management decision support. Pop-up advice helps administrators prioritize tasks, such as chasing down noncompliance devices and evaluating software updates.
- Reporting and analysis can be performed on a per-user basis, from an organization unit point of view. This helps companies monitor resources, find problems and set compliance goals based on job roles. Devices and apps can have their profiles, hardware functions and whitelists modified in real time when a user changes location or geography.
- Trend Micro's enterprise app store provides a common view and status reporting across device platforms, meaning that iOS and Android application utilization can be easily compared. Apps can be specified as required or optional within managed device profiles.

Cautions

- The vendor doesn't offer containerization solutions, but does offer alternatives using DLP sync and share.
- Trend Micro is pursuing data privacy as a DLP problem, which requires voluntary opt-in to use SafeSync for file sharing. The product currently lacks certain basic detection filters, such as an email system "shim" to catch restricted or sensitive information.
- The vendor does not provide integration with trusted third-party certificate authorities (CAs), and does not provide its own built-in trusted CA.

Vendors Added or 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 appearing 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. This may be a reflection of a change in the market and, therefore, changed evaluation criteria, or a change of focus by a vendor.

Added

There were many new entrants supporting the critical components of MDM in 2012. The following vendors met this year's criteria and were added to the Magic Quadrant:

- Absolute Software — A longtime PC management vendor, it also launched mobile support in 2013 and has seen rapid adoption in its installed base. It is one of the few MDM vendors supporting both mobile device and PC management.
- BlackBerry — Its initial MDM product, Mobile Fusion, was released in 2Q12 and didn't qualify for inclusion in last year's Magic Quadrant. Although the vendor has integrated its MDM capabilities into the new BES 10, it continues to support cross-platform management and, with BlackBerry sales and support, has qualified for inclusion in 2013.
- Kaspersky Lab — Known for its security and antivirus products, Kaspersky Lab launched its MDM product in 2012 and, based on its installed base of customers, it qualifies in 2013.

Dropped

The following vendors were dropped from the Magic Quadrant for various reasons, most business-related rather than technical:

- Amtel — While showing solid growth and technical innovation, its enterprise MDM business metrics did not qualify for inclusion this year.
- MYMobileSecurity — Its focus is too much on security versus MDM, and its enterprise MDM business metrics did not qualify for inclusion this year.
- OpenPeak — This vendor has put together very solid partnerships and sales in MDM, but its go-to-market strategy, based on partners and white-label solutions, did not qualify for inclusion this year.
- SilverbackMDM — Although showing solid growth and technical innovation, its enterprise MDM business metrics did not qualify for inclusion this year.
- Smith Micro Software — It has put together very solid partnerships and sales in MDM, but its go-to-market strategy, primarily based on telecom partners and white-label solutions does not qualify for inclusion this year.
- The following vendor was dropped because it was acquired by another listed provider:
- Zenprise — It was officially acquired by Citrix in January 2013, and is listed in this Magic Quadrant under the new brand name.

Inclusion and Exclusion Criteria

Gartner is aware of more than 100 vendors, on a global basis, that have at least one of the four critical MDM components of hardware, software, security and network service management. Like last year, many come from diverse areas of mobile technologies, including security, messaging, PC management, wireless hardware manufacturing, software development, cloud computing, and mobile applications and development. In most markets, even growth markets, there continues to be a large number of competing vendors with similar products and feature sets. Our criteria for inclusion in the MDM software Magic Quadrant covers not just the technology, but also the business metrics in this growing market.

Inclusion Criteria

After due consideration, 18 vendors were selected to be included for ranking in this Magic Quadrant. Meeting the following criteria was necessary for inclusion:

Technical Requirements:

- Support for enterprise-class (noncarrier), branded, multiplatform support MDM (software or SaaS), with an emphasis on mobility
- Specific MDM product focus and feature set, or a primary focus on MDM in another product set (messaging or security), made up of the four critical MDM components
- Support for three different mobile OS platforms (not versions)

Business Requirements

- At least 500,000 devices licensed
- Five referenceable accounts
- No more than 65% of revenue in one main geographic region or market
- At least $8 million in MDM-specific revenue
- 200 MDM customers
- One customer with 20,000 seats or more

- General availability by 1Q13

To qualify, vendors had to meet all the technical requirements, and at least four of the business requirements.

Exclusion Criteria

MDM vendors not included (see Note 1) in this Magic Quadrant might have been excluded for one or more of these conditions:

- The vendor did not have a competitive product in the market for a sufficient amount of time during calendar year 2012 and the first quarter of 2013 to establish a visible, competitive position and track record.
- The vendor did not meet the listed inclusion criteria as previously described.
- The vendor delivered its software through a third party or as a service only, and did not have an enterprise software platform.
- The large number of vendors claiming a presence in this market makes it impossible to include all of them. Vendors were individually reviewed, discussed and selected by a team of Gartner analysts.

Evaluation Criteria

Ability to Execute

Gartner analysts evaluate technology providers on the quality and efficacy of the processes, systems, methods or procedures that enable IT provider performance to be competitive, efficient and effective, and to positively affect revenue, retention and reputation. For MDM, this involved providing on-premises-based or SaaS/cloud delivery capability, with the required number of features to manage the software, security and hardware of a midsize or large (more than 1,000 devices) organization. We also look for diversity in channel support and operations capability, and the ability to support a global organization.

Source: Gartner (May 2013)

Evaluation Criteria	Weighting
Product/Service	High
Overall Viability (Business Unit, Financial, Strategy, Organization)	High
Sales Execution/Pricing	Standard
Market Responsiveness and Track Record	Standard
Marketing Execution	Standard
Customer Experience	High
Operations	Standard

Table 1. Ability to Execute Evaluation Criteria

Completeness of Vision

Gartner analysts evaluate technology providers on their ability to convincingly articulate logical statements about current and future market direction, innovation, customer needs, and competitive forces, as well as how they map to the Gartner position. Ultimately, technology providers are rated on their understanding of how market forces can be exploited to create opportunities for the provider, which is especially important in a diverse mobile world, with no platform standardization, a quickly moving market and rapidly changing technology. MDM providers should have a significant vision of the evolving market, including software delivery methods, innovative and differentiated features, and geographic sales diversity.

Source: Gartner (May 2013)

Evaluation Criteria	Weighting
Market Understanding	High
Marketing Strategy	Standard
Sales Strategy	Standard
Offering (Product) Strategy	High
Business Model	Standard
Vertical/Industry Strategy	No Rating
Innovation	High
Geographic Strategy	Standard

Table 2. Completeness of Vision Evaluation Criteria

Quadrant Descriptions

Leaders

Leaders demonstrate balanced progress, effort and clout in all execution and vision categories and are the first to envision, develop and launch new MDM features, partnerships and strategies. If they are not among the leading MDM providers in sales, they are, at a minimum, the most critical competitive threats to their peers in open competition. A leading vendor is not a default choice for all buyers, and clients are warned not to assume that they should buy only from the Leaders quadrant. To stay on the right side of the chart, Leaders (and Visionaries) must offer features that remove significant roadblocks to the complex challenges that enterprises face when attempting to treat mobile consumer devices as business tools. One example of a competitively disruptive activity might include delivering a sandbox method to prevent data leakage between personal and business applications. Another is the ability to support enterprise and third-party applications, provide a deeper security capability, and actively partner for technology capabilities.

Challengers

Challengers have attractive products that address the typical baseline needs for MDM, with competitive visibility that is strong enough to demand attention in RFPs, but may not show up as often, nor win as many clients as Leaders. Challengers may win contracts by competing on a limited selection of functions or a limited selection of prospective buyers by industry, geography or other limiting factors, even if, on speculation, their products have broad functions. They may be perceived as a threat by other vendors, but that threat will be primarily focused on a limited class of buyers, rather than the MDM market as a whole. Challengers are efficient and expedient choices for defined access problems.

Visionaries

Visionaries are able to demonstrate long-term strategies for MDM that point to the product and service approaches that will be most competitive in the future. Visionaries might affect the course of MDM, but they lack the execution influence to outmaneuver Challengers and Leaders. Also, Visionaries may not have the funding nor the capability to scale their businesses and provide robust operations and customer support. Marketing and mind share are also weak areas for Visionaries. Buyers may pick Visionaries for best-of-breed features, and for broader infrastructure investments than Niche Players. Smaller vendors may take risks on potentially disruptive technologies, while larger vendors may be in the process of building out their next-generation portfolios. Buyers of Visionaries' products may base their selections on specific technology features and by participating in the vendor's road map.

Niche Players

Niche Players meet the typical needs of buyers, and fare well when given a chance to compete in a product evaluation, but are usually smaller, and many buyers may be unaware of their services. Larger companies in the Niche Players quadrant may not have fully articulated a vision or strategy, and may have fallen behind the competition as the market moves forward. They may not be as invested in the MDM market as other companies, and are focused on more of their core market offerings. Niche Players generally lack the clout to change the course of the market or have not yet made the investment to do so. They may offer an uncommon delivery mechanism for products and services. They may rely on a self-limiting business model, and/or have limited influence outside of a particular industry or geography. Niche Players may target clients that, for various reasons, prefer not to buy from larger network players. In many Gartner market studies, buyers report that Niche Players tend to provide more personal attention to their needs.

Context

The rapidness of technology development in mobile and the speed of new releases of mobile OSs and devices make it difficult to assess MDM software. Often, companies will have multiple major updates to MDM software every year, and multiple minor updates every quarter. MDM policy software is often restricted as to what APIs the mobile OS vendors support. Android is different because device OEMs develop their own specific APIs, which also adds a large degree of variability to the platform. Maturity of MDM is based on the maturity of the specific mobile platform it supports. MDM also covers a broad array of technologies, not just policy enforcement, including application management, enterprise app stores, data security, enterprise file sharing and synchronization. Among the more than 100 companies in this space, only 18 met the technical and business requirements for inclusion in this Magic Quadrant.

Market Overview

Mobile Device Management Defined

Although the product capabilities of MDM continue to increase, each new product can be found to fall under one of the following main critical components:

1. Software management — This is the ability to manage and support mobile applications, data and OSs.
2. Network service management — This is the ability to gain information off of the device that captures location, usage, and cellular and wireless LAN (WLAN) network information, using GPS technology. Network access control (NAC) features are also found here.
3. Hardware management — Beyond basic asset management, this includes device provisioning and support.
4. Security management — This is the enforcement and support of standard device and data security, authentication, and encryption. Application containerization, VPN and encryption software are also part of this capability.

These components, and some examples of policies, are listed below. Although many MDM vendors may have different definitions, these are the general areas that Gartner assesses in MDM:

Software Management:

- Configuration
- Updates
- Patches/fixes
- Backup/restore
- Provisioning
- Authorized software monitoring
- Transcode
- Hosting

Network Service Management:

- Invoice/dispute
- Procure and provision
- Help desk/support
- Usage
- Service and contract

Hardware Management

- Procurement
- Provisioning
- Asset/inventory
- Activation
- Deactivation
- Imaging
- Performance
- Battery life
- Memory
- Shipping

Security Management

- Remote wipe
- Remote lock
- Secure configuration
- Policy enforcement password-enabled
- Authentication
- Firewall
- Antivirus
- Mobile VPN
- Encryption

Companies are always asking when is the right time to assess and adopt MDM. Note 2 and Note 3 cover the decision criteria that companies should use when assessing the adoption of MDM and the use of EAS for MDM.

MDM Market Data

MDM has seen rapid growth during the past two years as companies have adopted more consumer-designed smartphones and are looking to enforce policies across multiple mobile OS platforms. In 2012, Gartner saw license revenue run to $784 million worldwide, and it is expected to rise to over $1.6 billion in 2014. Of that, 83% of lines were managed in on-premises servers, with cloud accounting for 17%, up from 5% in 2011. Although penetration has hit about 30% in North America, it is still growing and is much lower in other regions. The additional growth in smartphones, tablets and BYOD is driving adoption of MDM and will continue to do so for the next few years at a similar rate. The expansion into additional security products, such as DLP, containerization and VPN, as well as mobile content management areas, such as EFSS and MAM-like app stores, will continue this growth.

Increased competition, the movement toward cloud services and the impact of larger MDM companies will continue to put pricing pressure on this segment. In 2012, Gartner saw per-seat pricing decrease by up to 30% on average from the beginning to the end of the year. Increased product expansion into mobile software and content management can delay this in 2013, but continued competition on a global basis will push pricing in a downward trend. Potential mergers and acquisitions could delay some of the pricing pressure.

As in previous years, North America has seen the biggest number of MDM sales in 2012, with 65% of revenue gained in North America. Western Europe was second, at 17%, with the rest of the regions in single digits. Financial services led the way with 25% of sales, followed by manufacturing and healthcare and government. MDM is also being adopted by companies of all sizes, with over 70% of sales at 500 seats or lower. Gartner expects continued adoption and growth in all segments through 2014.

MDM Market Driver

The growth of consumer-based devices in the market continues, with 63% of companies in North America planning for iOS to become the primary platform in the next 12 months.[1] Android, the most popular smartphone platform (see "Forecast: Mobile Phones, Worldwide, 2011-2017, 1Q13 Update"), at 50% market share for both the consumer and business markets at year-end 2012, has under 20% in enterprise-only market share today, which varies based on region. However, Gartner believes that, by 2016, over 40% of enterprise-supported mobile devices will be Androids, so cross-platform MDM will be in even greater demand. The drive for many companies to support individual users' mobile devices (both smartphones and tablets), as well as to secure corporate data and support mobile users, are the primary drivers for MDM adoption.

MDM is typically introduced as a method to implement and support mobile data security on smartphones and tablets. Most adopting companies are already supporting basic mobile device policies through EAS (see Note 2) before they adopt a more thorough MDM solution. This is because they are looking for more detailed mobile data security capabilities and are looking to support more-complex mobile computing and communications processes. For 2013 and beyond, the main trends will be:

Security Trends

- Application-based VPN — Using a VPN for every app transaction can drain battery life and also increases data traffic for nonbusiness needs. There is a movement to enforce application-based VPN on business apps to guarantee security.
- Data containerization — Companies are assessing the opportunity to separate business data from personal data, either by application or by putting it into separate workspaces, as a way to increase data integrity and management, while affording additional privacy to personal data. This is especially important for BYOD programs.
- NAC — The use of NAC and identity management with MDM is to enforce segmented policies, and can use the network to allow, deny or grant limited access to devices, based on their compliance with these policies.

Mobile Enablement Trends

- EFSS — These offerings enable productivity and collaboration for mobile workers who use multiple devices by allowing file sharing for internal and external use. Consumer-grade products are dominant today, but enterprises are evaluating solutions that will afford them increased data security and management.
- App catalog — Companies are looking for solutions that will provide access to secure and manageable third-party apps commonly found in application markets, but want to be able to add enterprise policies and controls. MDM providers are partnering with ISVs and third-party app developers to configure enterprise-grade apps and provide them in an extensive app catalog. An app store is used independent of the apps available in a catalog.
- Application provisioning and support — As part of a total mobile software management solution, enterprises need the ability to provision and support third-party, ISV and enterprise mobile applications. Many want an easier way to support apps across different types of users, with multiple policy possibilities. MDM is well-positioned to provide this as part of advanced mobile app management capabilities.
- Application virtualization — Also in the app area, companies are assessing the use of mobile workspace aggregation, where the app would run in the cloud versus on the endpoint. While this is compelling because it would reduce the need for app customization based on the mobile platform, it would require an optimization of the app to run in the network as well as require increased network access. Offline requirements are also important when mobile users are disconnected, but still need access to data.
- There are many vendors to choose from and the MDM software Magic Quadrant is the guide to use to help create a shortlist of MDM vendors to assess. Not all MDM vendors could be included in the deeper assessment if they did not meet the inclusion criteria. These vendors are listed in Note 3; they were not included in the Magic Quadrant, but have some type of MDM offering.

The Future of MDM and Enterprise Mobility Management

As companies support mobile users, devices and content, the challenge of putting together an enterprise mobile solution continues. Because of the lack of standardization in mobility and the fact that users have different mobility profiles and application requirements, there is no one size fits all when it comes to providing this mobile solution. Today, enterprises often have to sew together a number of point solutions to enable a mobile solution. Often, those point solutions come from a nonmobile legacy and are not optimized for mobility, leading to a poor user experience and an expensive option that is underutilized.

As MDM adoption grows, it is expanding out of a pure policy management function to incorporate an enterprise mobile management and enablement solution. Many companies see the MDM platform as the main tool to both implement and manage a mobile solution. Since the EMM concept was introduced by Gartner last year, MDM has evolved to become a broad system management offering, what we call enterprise mobility management. This entails many of the services for optimizing and enabling mobile applications and data on the device, as well as for ensuring the security of that data. Many products are still evolving in this area, but it will be the primary focus of many MDM providers during the next few years.

Additional research contribution and review: Song Chuang, Bryan Taylor, Ken Dulaney, Leif-Olof Wallin