Gartner.

Magic Quadrant for Mobile Device Management Software

17 May 2012 ID:G00230508

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

VIEW SUMMARY

Although MDM features have commoditized with little differentiation, the platforms are expanding deeper into enterprise mobile software and document management support. Enterprises should look not just at a vendor's MDM technology but also at how well it can support enterprise mobile needs.

Market Definition/Description

This document was revised on 21 June 2012. The document you are viewing is the corrected version. For more information, see the Corrections **page on gartner.com.**

Enterprise mobile device management (MDM) software is primarily a policy and configuration management tool for mobile handheld devices, such as smartphones and tablets based on smartphone OSs. 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. This is especially important as bring your own device (BYOD) initiatives become the focus of many enterprises. It can support corporate-owned as well as personal devices, and helps support a more complex and heterogeneous environment. The primary delivery model is on-premises, but it can also be offered as software as a service (SaaS) or through the cloud. Although some MDM vendors also support PCs, this Magic Quadrant focuses only on mobile capabilities.

Return to Top

Magic Quadrant

Figure 1. Magic Quadrant for Mobile Device Management Software

Source: Gartner (May 2012)

Return to Top

Vendor Strengths and Cautions

AirWatch

A number of vendors assessed for this Magic Quadrant were not included because they did not meet our criteria. Many of them, however, offer some type of MDM software or services. Examples include:

3LM
Absolute Software
AetherPal
Alcatel-Lucent
Alepo
Apperian
Avoceen
Blackbox Mobile
BMC Software
CA Technologies
Capricode
Cloud Systems
CommSolv
CommonTime
Cortado
Equinox Software
Finepoint Software
Gill Technologies
Google
Halosys
HP
InnoPath
iPass
JAMF Software
Juniper Networks
LRW Technologies
Mformation Technologies
MobiDM
Mobi Wireless
MobileFrame
Mobiquant
Microsoft
NitroDesk
Notify Technology
Novell
Perlego Systems
Sirrix
Virtela
Wavelink
Wyse Technology
Zelog

There are a few companies that are not in this year's Magic Quadrant. They did not meet our inclusion criteria; however, they could have a profound role in MDM during the next year, because many are considering entering this space. These include:

Research In Motion — RIM is just getting to commercial availability of its MDM platform, Mobile Fusion. Although it doesn't meet this year's criteria because of market launch timing, it does have an installed base of 10,000 enterprises that it can target. RIM won't bring any new capabilities to managing iOS and Android this year that others can't do, but could be a force if it decides to invest more in this area.
Microsoft — The company is increasing its capability of SCMDM and Windows Intune with

Based in Atlanta, Georgia, AirWatch has seen significant growth of its customer base during the past year in North America, Western Europe, Australia and New Zealand. It primarily delivers MDM through its cloud service, although it can also support on-premises needs. AirWatch has done a good job scaling its business during the past year and has grown its head count by more than 250%, with a significant portion of its staff in Europe (establishing one of the stronger positions locally). It is one of the more innovative companies, adding features before most of its competitors. Those features include content management, Secure Multipurpose Internet Messaging Extensions (S/MIME), Kerberos integrations, and an extensive Web and application development framework. Its cloud services support some of the biggest deployments of MDM, some with greater than 40,000 lines managed. AirWatch also provides a wireless LAN (WLAN) management console solution designed to provide a single point of management, monitoring and support for all wireless network infrastructures. AirWatch is recommended for midsize and large companies, especially those that have broad MDM needs.

Strengths

It has a strong security focus, with enterprise integration services that encrypt the traffic between an enterprise's servers and its cloud system.

AirWatch offers Web-based as well as agent-based enrollment.

It has a strong capability to profile, with detailed and easy-to-use policy settings.

Its strong administrative interface is easy to use and manage.

AirWatch is easy to scale and can support large numbers of users across multiple areas.

Cautions

AirWatch does not yet support the ability to customize views and dashboards.

It needs to increase its support of alternative channels in the enterprise market, especially with communications service providers.

Its international client support and responsiveness have been reported as occasionally limited. AirWatch needs to raise its level of local support outside the U.S., directly or through partners, as it grows its global sales volume.

Return to Top

Amtel

Amtel is a small telecom expense vendor from Santa Clara, California. Although its focus primarily has been on telecom expense management (TEM), it released a self-developed MDM tool in 2011, which has had significant uptake across its customer base. Amtel offers basic MDM capabilities at very low rates, which has been a key to its success. Amtel is recommended for small and midsize companies that are looking for basic MDM services.

Strengths

It provides a clear and easy-to-use MDM tool.

Amtel can incorporate single-company TEM and MDM functionality.

Cautions

Amtel has a small sales and marketing group to support MDM.

It has little visibility in MDM, and is slower to incorporate features than competitors.

Amtel has little market presence outside of the U.S.

Return to Top

BoxTone

BoxTone is based in Columbia, Maryland. It initially was focused on real-time mobile monitoring for BlackBerry deployments. During the past three years, it has expanded its coverage into broad mobile device and mobile application management, with support for iOS and Android devices. BoxTone includes an integration framework that connects with many popular system management and monitoring platforms (for example, Microsoft, HP, CA Technologies, IBM and BMC Software) and integrates with many key mobile technology and enterprise infrastructure vendors (such as Appthority, Accellion, Mocana and Aruba Networks) for customer flexibility. BoxTone mobile service management extends MDM to include service desk management, incident management, problem management and application performance management.

Strengths

BoxTone has had a long-term focus on enterprise mobility, with a deep understanding of IT security, management, processes and service-level requirements.

Its product vision is centered on IT process automation, to enable cost-effective quality of service, security and manageability, and to eliminate unnecessary human interventions. Through integration with enterprise infrastructure, such as Active Directory and real-time monitoring — combined with real-time monitoring, mobile analytics and autoenforcement — BoxTone can proactively detect and remediate policy and compliance violations.

It has strong security support through a multilayer defense approach that encompasses users, devices, applications, files and content, and connections that include Federal Information Processing Standard (FIPS) and other certifications. For secure mobile app management, BoxTone provides containerization, data loss prevention (DLP) and encryption on devices. It also provides unique IPsec tunnel encryption for over-the-air communication of

---

its 2012 versions, but is not expected to have a general availability product until year-end 2012. It will likely focus on supporting Windows Phone 7 and Windows 8 products primarily, but looking to extend to iOS and Android.

Google — The company has some online MDM functions today, with limited capabilities for Apple and Android, cloud only. It hasn't said or indicated what it wants to do with the 3LM acquisition it got through Motorola. However, most companies are hoping it will use it to include an enterprise version of Android to OEMs.

BMC — Will need time to integrate its recent acquisition of Numara, a small MDM provider. It also partners with AirWatch and others.

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

individual applications through a technology partner, Mocana.

The company emphasizes a comprehensive, modular mobility management approach spanning multiple IT roles — user self-service, service desk, IT operations, data center operations, security, compliance, applications, finance and IT management. Its management of mobility servers — in particular, BlackBerry enterprise server (BES) — allows an IT administrator to manage all devices, including BlackBerry, through a single console, Good for Enterprise, which allows management of hybrid deployments and Microsoft Exchange ActiveSync.

Cautions

BoxTone has a very U.S.-centric presence in the market, and a relatively small presence in Europe and Asia/Pacific. It has been leveraging partners and management service providers for international reach. Direct international expansion may remain challenging for the company, because competitors are moving fast internationally.

While feedback on BoxTone's level of support is always positive, some customers in regions other than the U.S. reported a lack of local support and consequent delays in responding to requests.

Its application containerization through Mocana technology is not used for existing native applications on the device (for example, the Apple email client), although BoxTone offers a wrapped version of NitroDesk's TouchDown email application for Android, as well as support for Good Technology.

Despite the significant installed base, BoxTone's visibility in the market is less than that of leading vendors in the MDM space.

Return to Top

Fiberlink

Fiberlink is a private company based in Blue Bell, Pennsylvania, that was founded in 1991. It is a unique player in the MDM market, providing a pure cloud-based MDM offering — MaaS360 — through SaaS and managed services. MaaS360 support is offered for a variety of devices, including Android, iOS, BlackBerry and Windows Phone 7 models. Originally focused on remote-access service management (offering a connection agent to negotiate worldwide Internet access for traveling users), since 2007, it has increasingly prioritized on MDM activities. Fiberlink is recommended for companies of all sizes and geographies.

Strengths

Fiberlink has proven long-term viability, with most revenue originating in North America and Europe, and growing activities in the Middle East and Asia/Pacific. The company is profitable, growing in revenue and staffing.

Its global presence is developing through a network of channel partners, including resellers, distributors, managed service providers and carriers (such as Verizon Wireless and O2). The MaaSters partner program enables third parties to market, sell, implement and support MaaS360. In 2011, 40% of Fiberlink's total revenue was generated through partners.

It has expertise and a track record in complementary markets, such as mobility and telecom services delivered through scalable cloud-based network operations centers (NOCs). Fiberlink's MaaS360 management client agent and user self-service portal are well-known in the remote-access and VPN markets. Also, MaaS360 supports complete life cycle management for PCs and Macs (laptops and desktops) with Visibility and Control Services.

A range of new functions extend MaaS360 capabilities on mobile application management (MAM) and containerization of corporate data. For MAM, MaaS360 provides corporate application catalogs, mobile application policies, and a mobile cloud API and software development kit (SDK) to enhance its own application security and management (AppExtender). For containerization, it enables lockdown of corporate email (native email on iOS, through TouchDown on Android) and documents on personal devices (Doc Cloud and Doc Catalog).

Fiberlink clients recurrently indicated very positive feedback on smooth implementation, configuration and testing, as well as excellent customer support. It had great feedback on integration with cloud email services, such as Microsoft BPOS and Office 365.

Cautions

The MaaS360 pure cloud service offering restricts viability only to organizations that are comfortable with the cloud model. While MDM cloud services had growing demand during the past 12 months, and Gartner expects rising adoption in the future, many heavily regulated organizations cannot afford to keep corporate data on third-party clouds and are obliged to deploy on-premises for compliance.

Fiberlink's international activities outside the U.S. and Europe are still very limited. Its lack of local presence in those regions may affect its ability to support out-of-area customers in the short term. Fiberlink is actively extending its reach through its partnering channel network.

The current implementation of containerization in MaaS360 is limited to links of corporate email and documents, and does not include applications — either third-party or proprietary applications.

MaaS360's management approach is device-centric and not user-centric, and doesn't support simple management of devices and applications per user. This is increasingly limiting for IT organizations managing mobility for employees who own more than one device and have multiple applications on them.

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 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.

Good Technology

Good Technology is based in Sunnyvale, California. Good for Enterprise (GFE) is a mobility suite that supports mobile collaboration, with strong support for security and management. The main components of the suite are Good Mobile Messaging, for secure wireless email; Good Mobile Control, for MDM; Good Mobile Access, for secure access to corporate data; and Good Dynamics, for developing and deploying containerized applications. Management and security capabilities are available only as part of the entire mobility suite, and require the adoption of the Good Mobile Messaging client on devices, for secure access to corporate intranet sites, applications and data that are inside the firewall without requiring a VPN infrastructure. Good for Government adds support for Common Access Card integration and security features, such as S/MIME.

Good receives recurrent licensing payments from Research In Motion (RIM), Microsoft and other vendors that settled patent litigations with Visto. A patent litigation is currently ongoing with Excitor in the U.S. Good Technology is recommended for large companies that want strong security support for their mobile devices, and for those customers concerned about the legal liabilities of intermixed business and consumer information.

Strengths

Good Technology has a long history and successful track record in enterprise mobility. It has a deep understanding of security and compliance issues and requirements.

It has a large installed base in regulated sectors, such as financial services, government, defense, public sector, healthcare and professional services.

Good Technology has the strongest implementation of containerization currently available in the market, to protect and isolate corporate data and applications from personal data and applications. Containerization is available for multiple OS platforms (iOS, Android and Windows Phone). With data leakage prevention and encryption, it protects Good's proprietary applications (email, calendar, contacts and browser), as well as applications developed with its SDKs and APIs (or third-party apps wrapped for containerization).

It has strong security capabilities, including FIPS 140-2 crypto libraries, end-to-end 192-bit encryption, multiple-factor authentication and multiple certifications.

It has strategic partnerships with mobile operators, including Vodafone, T-Mobile, Sprint, AT&T, Verizon and Telstra. These help Good in providing support, better data contracts and service levels to international customers.

Cautions

The cost of the Good solution is relatively high per user seat, compared with other vendors, because Good includes its MDM solution as part of its Good for Enterprise. That solution secures mobile collaboration (email, calendar and contacts), providing secure access to corporate intranet applications and data, and enables secure file management.

Good does not offer management or integration for BlackBerry devices and BES.

There are no cloud offerings, nor does Good yet integrate with major cloud-based email service providers.

Good Technology's MDM capabilities cannot be used independently of its messaging application. No lightweight MDM offering is available for organizations that would like to privilege the user experience with native apps on the device (such as the native email client), and care less about locking down the corporate footprint on the device.

Some Good users complain about their usage experiences with native applications on the mobile device — for example, the lack of real-time email push and notifications in the Good Messaging client for iOS; or the Safari browser not allowed within the container to access the corporate intranet.

IBM

IBM, headquartered in Armonk, New York, is the latest big vendor to launch an MDM offering. Based on its purchase and launch of BigFix for PCs, its MDM has only recently become available in the market. IBM's MDM capability is very complementary to that of PCs, and it is one of the few vendors in this Magic Quadrant that can support PCs and mobile devices. IBM also has additional products that could integrate well into an MDM platform, such as TEM capabilities through its Emptoris acquisition, and mobile application development with Worklight. To date, IBM hasn't offered any integrated product with MDM. Gartner recommends IBM for midsize and large businesses, especially those that are already BigFix customers.

Strengths

It is a good complement to PC management.

It does not rely on enterprise application software or IBM Traveler.

It is clear and easy to navigate.

The solution can provide a full enterprise mobile solution, including TEM, MDM and mobile application development.

Cautions

IBM is not a mobile-focused vendor, and some of the features and formats in its MDM tool

show its PC-focused experience, looking more computing-centric versus communications-centric.

It does not provide any network service management.

IBM can support only native device encryption.

Its user interface design is basic, with minimal reporting functions.

LANDesk

LANDesk, based out of Salt Lake City, Utah, is one of the few providers that support PCs and mobile devices. Known for its PC management, LANDesk grew, largely through organic product development. The modules within LANDesk Management Suite (LDMS) share a common look and feel. Starting in November 2010, it released a Microsoft Exchange-based MDM solution to all LANDesk customers as part of LANDesk Management Suite. A year later, LANDesk released an MDM product, LANDesk Mobility Manager, which operates from the LDMS console. LANDesk should be considered by large companies that want an integrated PC and MDM suite.

Strengths

LANDesk supports PCs and mobile devices.

It is a strong player in the PC management market, and it also understands enterprise needs.

Cautions

LANDesk has some past experience in mobility, but only in Windows and Palm, and is new to supporting iOS and Android platforms.

It is virtually unknown for mobile support today, and does not extend much beyond its installed base of LDMS users.

It has one of the more nonintuitive and complex interfaces for navigation and use.

There is no separation of the core management product from that of mobility.

It has minimal Android support, and weak application and software management.

McAfee

Based in Santa Clara, California, McAfee is a long-standing player in endpoint security. McAfee holds leadership positions in related Magic Quadrants (see "Magic Quadrant for Mobile Data Protection" and "Magic Quadrant for Endpoint Protection Platforms"). McAfee's MDM product, Enterprise Mobility Management (EMM), provides broad support for new and legacy mobile platforms, including Android, iPhone and iPad, Nokia S60, Windows Mobile 6.x and Windows Phone 7. McAfee's strengths in adjacent markets get noticed by buyers who are leveraging platforms and seeking to avoid point solutions, and McAfee has followed a familiar competitive pattern of discounts for combined purchases.

Strengths

EMM is built from technologies acquired from Trust Digital, which already had a strong reputation for mobile phone security when it was acquired in 2010.

EMM licenses no critical-path technologies from other companies that could be challenged by an outside acquisition.

Its long-term strategic work with Intel may provide unique opportunities for McAfee security technologies to play a critical role for new smartphone and tablet platforms.

Cautions

Gartner client feedback characterized EMM as a vestigial consideration, rather than a shortlist priority. Purchases were made on the basis of attractive pricing and bundling, rather than on competitive features.

AT&T has resold EMM as on-premises software for more than a year, but this approach also had little effect on competitive visibility. AT&T also sells other MDM vendor products, rather than exclusively promoting McAfee.

MobileIron

MobileIron is a private company based in Mountain View, California. Funded by leading venture capitalists, such as Sequoia Capital, MobileIron entered the market in August 2009. Since then, it has experienced swift growth in visibility, sales and market share — growing more than 400% in revenue in 2011. MobileIron's business is entirely focused on enterprise mobility management, with its on-premises product, Virtual Smartphone Platform (VSP), and cloud service offering, Connected Cloud.

Strengths

MobileIron has great visibility and adoption in the MDM market in multiple regions. MobileIron owns high levels of mind share in the MDM market, and appears frequently on shortlists.

It has a very articulated and rich mix of partnership relations with distribution channels and OEMs (such as AT&T, Vodafone Global Enterprise, SingTel, Deutsche Telekom and Virtela), strategic technology partners (for example, Apple, Google, Microsoft, RIM, Cisco, HP and IBM), and business application partners — Accellion, Box, GroupLogic and MeLLmo (Roambi).

MobileIron has a growing presence in multiple regions outside North America, thanks to its channel network. This includes some of Europe and Asia/Pacific (Australia, New Zealand and China).

The company emphasizes comprehensive life cycle management, including usage monitoring, cost control, and application deployment and version control. It offers strong support for corporate and personal devices.

The product has strong reporting and dashboard capabilities. Among the many features, it supports text messaging archiving for devices connected to corporate email with archiving systems.

Cautions

MobileIron does not support containerization for corporate data and applications. It is not possible to isolate the corporate footprint from personal applications and data. Although it offers a broad range of capabilities to enforce controls on mobile devices connected to corporate systems, most policies must be applied to the entire device (as opposed to the corporate portion only). With BYOD, this may limit an owner's freedom to download and execute applications, such as Dropbox, for personal use.

Its application management capabilities are limited. MobileIron products do not provide mechanisms to enforce security and manageability on enterprise-developed or third-party applications through integration with its MDM platform (for example, wrapping).

It does not have its own encryption capabilities, and must work with what's on-device or through partners, which could cause higher costs. Buyers need to understand the limits of embedded protections on each platform, because these will be the limits to what MobileIron can manage.

MobileIron needs to continue to increase its support for larger installations. Some customers have been concerned by some limitation in platform scalability for large or mass-scale deployments of greater than 20,000 devices.

MobileIron had relied on inconsistent local support through partners, but has recently moved to provide direct Tier 1 support in the U.S. and EMEA.

Return to Top

MYMobile Security

Based in London, England, MYMobile Security is a midsize mobile security vendor primarily in the antivirus business. It has just recently created an MDM offering for enterprises. MYMobile Security is recommended for small companies, especially in EMEA, that are looking more for client-side protection.

Strengths

It is a security-focused company, with a large installed base of users.

MYMobile Security focuses on client-side protection.

Cautions

It has no real experience with midsize and large enterprises.

MYMobile Security has no visibility outside of Western Europe, and no North American office and support.

It has more consumer than enterprise experience.

Return to Top

OpenPeak

Based in Boca Raton, Florida, OpenPeak is a newer vendor in the MDM space. It provides a way to secure (through its Sanction product), deliver (through OpenShop), and manage (through Sector) any content and any application to almost any device. It also provides end-to-end application management with OpenShop. It wraps any application — third-party found on an app store, or enterprise-developed — in its secure, encrypted wrapper. All application and firmware packages are signed and encrypted. It is then downloaded to a proprietary container, what it calls the Sector Virtual Workspace, on the device where it can be managed and IT rules about the movement of the application or content are applied. OpenPeak is recommended for midsize and large companies, especially those located in North America, with a focus on BYOD, plus secure application and content management.

Strengths

It has strong MDM console features and navigation.

Its easy-to-use user interface is clean and modern-looking.

OpenPeak's complete MDM solution includes application and content management.

Cautions

It is a relatively small vendor, so it will have to work hard to prove its capability for scale and

customers.

OpenPeak has low visibility in MDM today. It needs to invest in its marketing and sales capabilities.

SAP

SAP, a public company based in Waldorf, Germany, is a leader in business software, with offices all over the world. Through the acquisition of Sybase, it is now in the mobility space, with a number of offerings — including MDM. That product was formerly listed in the MDM Magic Quadrant as Sybase's Afaria, but is now branded as SAP. Afaria is the longest-established MDM platform, reaching back to PCs in the late 1980s. Afaria for laptops was created in 1997, and subsequently released in 2000 as the first nonindustrial MDM platform for Palm and Windows devices. The current version of Afaria (7.0) is delivered as an on-premises software product, through SaaS or as a managed service through partners.

SAP has relied mostly on its direct sales channel for the past year to deliver its product to market. This has excluded most other channels, although it still has some arrangements with telecom providers, such as Verizon. This has also reduced its visibility in the MDM market space. However, recent changes to its senior management team, and its renewed focus on mobility and expanding its indirect channel, will make SAP a big contender in this space during the coming year. Its plans to integrate its mobile application development platform, and recent announcement on its partnership with Amazon on a cloud offering, will make it very competitive in the market. Gartner recommends using SAP in midsize and large companies that also have needs for mobile application development.

Strengths

SAP's highly scalable solution can support very large installations through highly available instances and content synchronization across distributed servers in different physical locations. For example, it delivers 140,000 user deployments on four servers.

The mobile application management capability in Afaria 7.0 includes an enterprise application portal on the device to enable business application distribution, security enforcement through application certificates and application management. SAP's Afaria, which also appears in two other Gartner Magic Quadrants (see "Magic Quadrant for Mobile Device Management Software" and "Magic Quadrant for Mobile Application Development Platforms"), is better positioned to provision applications built on SAP's mobile application platform. However, its application store is not multiplatform across PCs and mobile devices.

Its advanced support for help desk support, and application and service management, includes new reporting, analytics and device usage features.

Afaria's Android support includes an application portal for enterprise application management and extended APIs — for the Advanced Enterprise Security (AES) module for Samsung (more than 150 APIs), Motorola and LG.

Cautions

SAP has lacked leadership in MDM innovation in recent years. The company only creates features once demand has developed in the market. For example, Afaria does not yet support Windows Phone 7 or mobile file-sharing capabilities. Some competitors have these capabilities already available in commercial offerings. SAP has only recently launched a much needed updated user interface. However, with new management changes in its Mobility unit, SAP is significantly investing in improving its innovation and execution this coming year.

Customer feedback indicates that Afaria can be expensive, for seat licenses (twice that of competitors) and maintenance. The company is looking at all aspects of pricing, on-premises and cloud.

Feedback to Gartner indicates that buyers find the installation of Afaria to be complex. Although the new interface is better, companies planning a new or first purchase must plan for a learning curve. The company's cloud deployment plans could help in this area.

SilverbackMDM

Based out of Sydney, Australia, Silverback is new in the MDM market. Its product has been out for one year. It comes from a background of enterprise security though, so is not new to securing enterprise needs. Silverback has had very little presence outside Asia/Pacific, although it has recent hires in North America to build its market presence. It was one of the first to market with an integrated file-sharing capability. The product does not require Simple Certificate Enrollment Protocol (SCEP) for enrollment of iOS devices, and was early in its support for network access control (NAC) for increased security postures. Silverback is recommended for midsize companies, especially in Asia/Pacific.

Strengths

Silverback has a strong background in security and enterprise services.

It has a clean user interface and tool design that is easy to use and full-featured.

It is one of the few vendors with a perpetual licensing model, rather than annual licensing.

Silverback offers multiple types of enrollment, including PIN-based.

Cautions

It has no agent support on Android.

SilverbackMDM's weak reporting (beyond agent dashboards) forces clients to use third-party business intelligence systems.

Smith Micro Software

Based in Aliso Viejo, California, Smith Micro is new to the MDM business, but not to the wireless world. Smith Micro's main business is writing communications and user software for carrier remote-access services and products, including wireless modems and aircards. Much of its communications experience comes from working with carriers on their wireless services. Smith Micro is recommended for midsize companies looking for basic MDM services.

Strengths

Smith Micro is a longtime wireless and mobile software developer.

It has revenue outside of MDM.

Cautions

It does not have a dedicated channel to market.

Smith Micro has not shown commitment to MDM. It has a short track record in this space.

Sophos

Sophos met the inclusion criteria for the 2011 Magic Quadrant by exceeding sales and license thresholds, along with the release of multiple platform support. Sophos is headquartered jointly in Boston, Massachusetts and Abingdon, U.K. Sophos generates 65% of its revenue outside of North America, earning favor in rest-of-world markets.

Strengths

Sophos Mobile Control (SMC) will be integrated with Sophos Enterprise Management, providing benefits for companies invested broadly in the company's products. SMC is developed in-house and, therefore, is not subject to cross-license or acquisition risks in the crowded MDM marketplace.

Sophos offers products in several related markets, which contributes to competitive visibility, including leader ranking for mobile data endpoint protection and unified threat management.

Sophos sells an innovative add-on tool, Sophos Mobile Encryption, which can be set to transparently encrypt data that leaves a mobile device, including writing to a cloud service through a third-party application like DropBox, or writing to a Secure Digital (SD) card. This method may appeal in some DLP scenarios.

Sophos offers an optional cloud-based mobile app reputation database that can be used by companies to push modified device profiles if unwanted apps are detected by the on-device agent.

Cautions

Despite global visibility and a long track record in many security markets, SMC has had little visibility as a mobile security and MDM solution.

Its MDM revenue during the study period was on the low end of the market range. Sophos' acquisition of Dialogs occurred after the end of the study period, and will bring new investment, channels and clients into the picture for next year's market evaluation.

Based on a Sophos design decision resulting from customer feedback, SMC currently doesn't differentiate between personal and company devices. Policy declarations are separated across platforms, and there is no option to declare a master setting dialogue framework and then to note which policies are supported or not among different platforms or model devices in the list.

Soti

Soti is a private company based in Mississauga, Ontario, Canada. Soti has a long and successful track record in supporting ruggedized handhelds based on a variety of Microsoft mobile OSs — with the product MobiControl. During the past two years, MobiControl has broadened to include MDM of ruggedized and nonruggedized Android, Apple and Microsoft devices. MobiControl is available on-premises, as a managed service and in the cloud (SaaS). Soti has had less visibility in the larger, more horizontal deployments than competitors, and has slower adoption in its iOS management growth than some others. Soti is suitable for those companies targeting primarily Android-based deployments, especially with an industrial, application-specific use.

Strengths

Soti has a strong global presence through a large partner program. OEM relationships include Apple, Casio, HTC, Motorola, LG, RIM, Panasonic, Intermec, Honeywell, Psion, Lenovo, Samsung and ZTE. With Samsung, Soti has exclusive agreements around Remote Control

APIs that were co-developed by Soti for Samsung Android products. Soti also provides "remote view" for iOS devices.

Soti provides device-layer MDM integration for Android, which improves consistency and depth-of-management functions across devices from different manufacturers with different builds and versions of the Android OS.

Its scalability of the platform on large-volume deployments has been proven by a number of very large deployments (in the postal sector) with volumes greater than 130,000 units.

It offers a good administrative user interface and multiple methods of use. The dashboard has an effective and customizable graphic display and reporting views. MobiControl integrates with AirWave LAN infrastructure management solutions.

Cautions

Soti's focus has been on the Android market, which has emerging but lower interest among nonindustrial enterprise companies, compared with Apple iPhones and iPads.

Soti is very successful in vertical industries in relation to ruggedized device deployments, but is less known for its MDM offering to manage smartphones and media tablets, especially in the newer BYOD market, based on competitive visibility checks across multiple sources.

Potential buyers should inquire about support options, particularly 24/7 service levels, outside of Soti's directly supported geographies.

Symantec

Symantec Mobile Management (SMM) has provided MDM for two years, based originally on a license of Odyssey Software. Symantec, headquartered in Mountain View, California, acquired Odyssey Software after the end of the evaluation period and will fully integrate its console and mobile DLP solution into the Symantec security solution, SMM. SMM provides Symantec's first competitive entry in the MDM market. It has also recently acquired Nukona, a mobile application security and management company, and it will also support deeper mobile application management. However, its integrated product is not yet available. Symantec is recommended for those companies that want a broad MDM platform integrated into their overall enterprise security suites.

Strengths

Symantec will offer one of the broadest mobile security, device management and application management systems through its recent acquisitions of Odyssey and Nukona.

Integration with other Symantec product frameworks is a strategic advantage for long-term Symantec customers.

Symantec has a consistent and strong track record for overall viability, and for competitive sales and support of a wide range of security services. Its global reseller network is strong and well-trained.

Digital signatures may be set up for a variety of use cases, including task-specific policies. Symantec can leverage its strong position in certificate authority (CA) and public-key infrastructure (PKI) to attract security-conscious buyers.

Symantec Web Gateway, a secure Web gateway, can provide a valuable Internet security filter for mobile devices when managed under SMM.

Cautions

Historically, Symantec has not quickly integrated its acquired technology, but made progress with recent acquisitions like Vontu and VeriSign. Symantec needs to integrate Nukona capabilities and execute in the field.

The company's considerable sales resources need to leverage Symantec's leadership in adjacent markets to more clearly articulate a holistic story if it is to compete with smaller companies touting their point solutions.

Symantec intends to include its mobile NAC capabilities within its Mobile Security product; however, the current product doesn't have built-in automated compliance actions out of the box.

Tangoe

Based in Orange, Connecticut, Tangoe is the largest TEM provider, and continues to work to tie the TEM service market to the enterprise managed mobility service market. Tangoe's focus is on complete communications life cycle solutions and managed mobility services, providing integrated TEM, MDM, Tangoe's rTEM, machine to machine, sourcing, and device recycling. As such, Tangoe is typically not as leading edge with functionality as its MDM-only focused competitors, typically six to nine months following first occurrence in the market, as was the case with content management. Its interface is not as attractive as those of competitors, although the company is planning an update in this year that will address user interface and TEM-MDM integration issues.

Although it offers very competitive market pricing, usually the low-cost provider, it has not focused on the stand-alone MDM market as much as it has on the TEM market. Gartner thinks Tangoe is best-suited for its new and existing TEM customers looking for bundled MDM capabilities and a managed service solution versus a stand-alone MDM software tool.

Strengths

This is one of the few integrated TEM and MDM platforms.

Tangoe offers a managed service, as well as on-premises hosted solutions. There are no cloud offerings yet.

It is one of the larger companies in the MDM space. It is very communications-focused.

Tangoe offers a low-cost MDM platform.

It has one of the stronger network system management features, via its acquisition of Anomalous Networks.

Cautions

Tangoe focuses on a broader communications management solution and, as such, allocates less of its overall product investment on MDM-only features, as compared with competitors in the Leaders quadrant. As a result, Tangoe lags its competitors on some MDM features by as much as six to nine months.

Tangoe's MDM solution is due for a significant user interface and TEM integration update, which are planned for 2012.

Tangoe typically does not focus solely on the MDM stand-alone market. It needs to improve its MDM direct and indirect channel capabilities beyond IBM and Dell.

Trend Micro

Based in Cupertino, California, Trend Micro is one of the bigger players in the security market, with a focus on consumer and enterprise systems. The majority of its sales come from Asia/Pacific. Its MDM functionality began in 2009, with Windows Mobile, and iOS and Android were added during the past year. Trend Micro is recommended for midsize and large companies, especially those with Trend Micro as their security vendor, and those based in Asia/Pacific.

Strengths

Its user interface is very simple and is easily used by legacy customers.

It integrates well with the existing Trend Micro OfficeScan security platform.

Cautions

Trend Micro has little visibility in the MDM market, and has primarily focused on extending its offer to its installed base of customers.

It has weak application management, no support from Apple's volume purchasing program, and no wipe based on rules, manual only.

It is known as much for consumer support as it is for enterprise support.

Zenprise

Zenprise, based in Redwood City, California, was founded in 2003. It is a small company focused solely on MDM. It has a full feature set for life cycle management, including cost control through usage monitoring. It has significant venture capital funding, and expanded its customer service and operations capabilities during the past year. Zenprise has done a good job in increasing visibility among midsize and large companies during the past year, and continues to innovate and lead in vision for the MDM market, creating early support for mobile applications and collaboration capabilities (like browsers and SharePoint) and mobile DLP. Supported devices include iOS, Android, BlackBerry, Symbian S60, Windows Mobile 6.x and Windows Phone 7. Gartner recommends Zenprise for midsize and large companies in any geography.

Strengths

Zenprise's revenue growth more than doubled during the past year, confirming its viability as a point solution provider and putting it at the bottom of the range of high performance in this market.

Zenprise Mobile DLP provides innovative secure container solutions to operate locally on mobile devices, as well as to be accessed in the cloud.

Its application-blacklisting technique works across Apple iOS and Google Android devices.

Zenprise offers its own secure Web gateway and can also integrate with Blue Coat Systems and Palo Alto Networks.

Zenprise provides extensive support for NAC and specializes in client scenarios, where mobile devices need to be placed on internal LANs. Capabilities include integration with third-party NAC solutions, such as Cisco ISE, various Wi-Fi infrastructure vendors, and security information and event management (SIEM) integration.

Cautions

Gartner still hears about occasional support response issues; however, improvements have been seen in 1Q12 as the company reported an increase in support staff and a substantial decrease in the time it takes to close trouble tickets.

There has been some channel conflict between Zenprise and its partners.

Zenprise is still growing its international capabilities.

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

These vendors were included, because they met the criteria we cite later in this Magic Quadrant:

        Amtel
        IBM
        LANDesk
        MYMobile Security
        OpenPeak
        SilverbackMDM
        Sophos
        Trend Micro

Dropped

These vendors were dropped for various reasons, because they did not meet this year's MDM inclusion criteria:

        Capricode — It did not meet the revenue and other requirements.

        Excitor — It did not meet the revenue requirements.

        FancyFon Software — It did not meet the revenue requirements.

        Fixmo — It did not meet the revenue requirements.

        Ibelem — It did not meet the revenue requirements.

        Mobile Active Defense — It did not meet the revenue requirements.

        Motorola Solutions — It did not meet the criteria for multi-OS support and sales levels.

        The Institution — It did not meet the revenue requirements.

These vendors were dropped because they were acquired by another listed provider:

        Odyssey — It was acquired by Symantec in March 2012.

        Ubitexx — It was acquired by RIM. RIM's new multiplatform MDM system, Mobile Fusion, was just recently made generally available. It will be evaluated for potential inclusion in next year's Magic Quadrant.

        Fromdistance — It was acquired by Numara, which was then acquired by BMC Software.

Inclusion and Exclusion Criteria

Gartner is aware of more than 100 vendors, on a global basis, that claim some level of MDM functionality, and come from many areas of mobile support, including security, messaging, notebook management, wireless hardware manufacturing and mobile applications. 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 Magic Quadrant cover not just the technology, but also business metrics in this growing market.

Inclusion Criteria

After due consideration, we selected 20 vendors to be included for ranking in this Magic Quadrant. Meeting these criteria was necessary for inclusion:

        Support for enterprise-class (noncarrier), 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)

        Security management, with at least these features:
            Enhanced abilities to download, monitor, and revoke certificates for email, apps, Wi-Fi, VPN and so on

            Enforced password

- Device wipe
- Remote lock
- Audit trail/logging, including the ability to verify device configuration from a central console
- Jailbreak/rooted detection
- At least three mobile OS platforms supported

Policy and compliance management

Software management, with at least these capabilities supported:
- Application downloader — the ability to push or pull applications on a mobile device
- Application verification — the ability to verify origin of the mobile application
- Application update support
- Application patch support
- Application store support — the ability to list and manage enterprise and third-party applications

Hardware management, with at least these capabilities supported:
- External memory blocking — block any use of flash memory cards or other external memory
- Configuration change history — audit trail on any changes made on the hardware

Having sold at least 75,000 licenses

Five referenceable accounts

No more than 70% of revenue in one main geographic region or market

At least $1.5 million in MDM-specific revenue

General availability by mid-1Q12

Exclusion Criteria

MDM companies not included (see Note 1 and Note 2) in this Magic Quadrant might have been excluded for one or more of these conditions:

- The company did not have a competitive product in the market for a sufficient amount of time during calendar-year 2011, and the first quarter of 2012, to establish a visible, competitive position and track record.
- The company did not meet the listed inclusion criteria.
- The company delivered its software through a third party, or as a service only, and does not have an enterprise software platform.

The large number of vendors claiming a presence in this market makes it impossible to include every company. Vendors were individually reviewed, discussed and selected by a team of Gartner analysts.

Return to Top

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 (see Table 1). 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 were also looking for a diversity of channel support, operations capability and the ability to support a global organization.

Table 1. Ability to Execute Evaluation Criteria

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

Source: Gartner (May 2012)

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 opportunity for the provider, which is especially important in a diverse mobile world, with no platform standardization and a quickly moving market and technology. MDM providers should have a significant vision (see Table 2) of the evolving market, including software delivery methods, innovative and differentiated features, and geographic expansion, as well as distribution and technology partnerships.

Table 2. Completeness of Vision
Evaluation Criteria

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

Source: Gartner (May 2012)

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 one of the leading MDM providers in sales, they are, at a minimum, the most critical competitive threat 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 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.

Return to Top

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 that may not show up as often, nor win as many 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.

Return to Top

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.

Return to Top

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.

Return to Top

Context

Although some of the vendors and products have been around for a long time, MDM is a nascent market, and the vendors' offerings have little consistency and are evolving rapidly. "MDM" is a misnomer, because products support more than just "managing" a device. MDM products are broadening out in areas of security, application and enterprise document management. Many come from mobile backgrounds like messaging and security to support MDM, and worldwide, there are more than 100 companies in this space. Of these, 75 were deemed potential candidates for this Magic Quadrant.

Return to Top

Market Overview

"Mobile Device Management" Defined

MDM is not new on the market, but the demands of new platforms keep MDM valuable to enterprises. Although many companies are trying to solve a similar problem, it takes multiple types of mobile software to address a full solution. A full MDM solution has four main components:

Software management — This is the ability to manage and support mobile applications, content and operating systems. The components are:
   - Configuration
   - Updates
   - Patches/fixes
   - Backup/restore
   - Provisioning
   - Authorized software monitoring
   - Transcode
   - Hosting
   - Managed mobile enterprise application platforms (MEAPs)
   - Development
   - Background synchronization.

Network service management — This is the ability to gain information off of the device that captures location, usage, and cellular and WLAN network information. The components are:
   - Invoice/dispute
   - Procure and provision
   - Reporting
   - Help desk/support
   - Usage
   - Service and contract

Hardware management — Beyond basic asset management, this includes provisioning and support. The components are:
   - Procurement
   - Provisioning
   - Asset/inventory
   - Activation
   - Deactivation
   - Shipping
   - Imaging
   - Performance
   - Battery life
   - Memory

Security management — This is the enforcement of standard device security, authentication and encryption. The components are:
   - Remote wipe
   - Remote lock
   - Secure configuration
   - Policy enforcement password-enabled

Encryption
Authentication
Firewall
Antivirus
Mobile VPN

Although many MDM vendors may have different definitions, these are the general areas we assess in MDM.

MDM Market Growth

The market and interest in MDM continue to grow. Driven by the move from well-managed and secured BlackBerrys, to consumer-focused devices based on iOS, MDM is the fastest-growing enterprise mobile software ever (in terms of number of suppliers, revenue growth and interest from Gartner clients). In terms of priority, our EXP CIO Survey, released in January 2012, rates mobility second, up from third last year. This is primarily because of the new smartphones and tablets that enterprises need to manage. Many vendors are seeing fast growth — bringing on 30 to 40 new deals each week, compared with a quarter of that 12 months ago. This is driving MDM licensing revenue up from $200 million in 2010, to more than $350 million in 2011, with the majority of sales in North America and Western Europe. MDM licensing revenue alone is expected to top $500 million globally in 2012. This rapid growth has interested new companies to enter this space, as demonstrated by this Magic Quadrant. However, not all companies are faring well, and many of the regional MDM vendors have not grown at the same rate, with the dominant players based in North America selling to multinational companies needing global support.

MDM Market Drivers

Interest in MDM continues, based on these main reasons:

During the past year, many companies have moved to iOS as their main mobile device platform, with others to follow during the next 12 to 18 months. An April 2012 Gartner survey showed that 58% of enterprises have or will make iOS their primary platform during the next 12 months, compared with 20% staying with BlackBerry and 9% on Android. Most companies started out supporting these devices, using the policies found in Exchange ActiveSync, but after a while, needed a fuller platform to support devices (see Note 3). As enterprises continue to offer multiplatform support, and new platforms continue to emerge (like Windows 8), MDM needs will continue to grow.

The introduction of new form factors, like tablets in the enterprise, is also driving the growth of MDM. Although most enterprises are not replacing a PC or phone with a tablet, nor are they paying for them, users are purchasing and using their own tablets to access enterprise data. The larger format of a tablet makes reading enterprise content easier and more convenient. It also presents the need for more security and policy to manage the greater amounts of data found on these employee-owned devices.

Although more features and policies are being supported on MDM platforms than ever before, much of this is driven by what the mobile OS providers allow. With each release of a new OS, Apple increases the number of policies that can be instituted on its devices. However, Apple has strict guidelines about its device support. In the end, every vendor manages Apple devices the same way. There is no differentiation there among vendors. Google is similar, but still offers a weaker management support. In the latest version of Android, 4.0, it opened only 16 MDM APIs for OEMs and MDM providers to manage, compared with more than 500 on the latest version of BlackBerry. Some OEMs have gone in and built their own MDM APIs, but this is time-consuming and expensive to do for each device and version of Android.

This has severely limited Android adoption in the enterprise, and even today, very few enterprises provide support. MDM is primarily sold as on-premises software, and around 85% of MDM licenses are premises-based. However, as more cloud/SaaS offerings emerge, and as enterprises need to scale to more than 30,000 supported devices, cloud-based systems will continue to grow. This will also help drive down the MDM ASPs, from approximately $60 per user, per year on average in 2012, to less than $40 per user, per year in 2015.

The Future of MDM

Those companies that have recently developed MDM differentiate their products from other management consoles by security vendors, or PC management and remote support vendors, by their focus on mobility and the ease of use and design of their interface. This is becoming more important in the light of BYOD programs at many companies. In 2011, MDM was focused on supporting basic security on consumer mobile devices and enforcing enterprise policies. Although this still exists, the drivers to support third-party and enterprise-developed business applications and content are continuing the growth of, and interest in, MDM in 2012 and beyond. Supporting the larger form factor, tablets, which makes it easier to create and consume content, is a priority.

Many users have already moved to synchronize their data with Internet-based cloud file synchronization systems like Dropbox or Box. The basic offerings were not explicitly meant for enterprise data. As a result, they represent security risks. A number of vendors have emerged in the MAM sector, because they focus on the application part of the solution. Those stand-alone MAM solutions cost the same or more than a full-function MDM, even with their lighter management capabilities. Much of this functionality is already present or is being built and acquired by the leading MDM vendors. Symantec's acquisition of Nukona is one indication. This year, most of the top MDM providers will have some type of enterprise document management

system that supports secure storage and transfer of enterprise content.

Another big area of growth has been in the enterprise application store. Again, most MDM vendors support the ability to store and transfer enterprise applications, as well as link to popular application stores from Apple and Google. Extended security is another area that MDM developers are exploring. Since MDM has the ability to manage by profile or user segment, it makes sense to integrate with DLP systems that manage and secure enterprise content. MDM profiles will enable easier setup of permissions and policies in DLP, and allow for more-flexible management of enterprise content.

Today, the more mobile-oriented providers are having the best success in managing mobile devices. According to our recent survey data, most organizations are managing their devices in their messaging and network operations groups, with about 25% of companies managing their mobile devices in their endpoint computing groups. Gartner expects that number to continue to grow. As more vendors provide tools that support mobile platforms as well as PCs, we are seeing an increase in management outside of these areas, and we believe this trend will continue.

More data is being put on mobile devices today, and enterprises are fast developing their own applications to support their mobile users. As mobile devices continue to displace traditional PCs, enterprises will look to their existing MDM systems to support more devices, enterprise applications and data. MDM vendors are moving beyond security to support enterprise and third-party applications, data, and content — mobile document management systems. During the next two years, we will continue to see MDM platforms broaden out and become enterprise mobile management system (EMMS) platforms, going beyond just devices. This broadening out of MDM EMMS will offer full solutions as more enterprises rely on mobile devices for more usage throughout the workday, displacing traditional PCs, especially for mobile users.

Return to Top

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