(http://www.gartner.com/home)

LICENSED FOR DISTRIBUTION

Magic Quadrant for Enterprise Mobility Management Suites

08 June 2016 | ID:G00279887

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

Summary

Enterprise mobility management suites enable organizations to integrate and manage mobile devices in their IT infrastructures. End-user computing leaders must act amid rapid market changes to reach both short-term and long-term enterprise mobility objectives.

Market Definition/Description

Enterprise mobility management (EMM) suites are the "glue" that connects mobile devices to their enterprise infrastructure. Organizations use EMM tools to perform the following functions for their users:

Provisioning: EMM suites configure devices and applications for enterprise deployment and use, manage updates, and assist with device upgrade and retirement.

Auditing, tracking and reporting: EMM suites can track device inventories, settings and usage to verify compliance with enterprise policies and manage assets.

Enterprise data protection: EMM suites mitigate data loss, theft, employee termination or other incidents by adding controls for data encryption, data access rights, shared devices, application wrapping and containment, and device lockdown.

Support: EMM suites help IT departments troubleshoot mobile device problems through inventory, analytics and remote actions.

Five core EMM technical capabilities help IT organizations perform these services, some of which overlap. Organizations may use some or all of these features, depending on their requirements.

Mobile device management (MDM): MDM is a platform-dependent life cycle management technology that provides inventory, OS configuration management, device provisioning and deprovisioning, remote wipe, and remote viewing/control for

troubleshooting. MDM profiles, installed on the device, facilitate these functions. Several EMM players are moving upstream with products to manage workstation-class PCs and Macs.

Mobile application management (MAM): MAM applies management and policy control functionality to individual applications, which are then delivered via an app store and are managed locally on devices via the EMM console. MAM can also provide analytics capabilities to help administrators and application owners understand usage patterns. MAM functionality can include:

An enterprise app store, which can be used to deploy in-house-developed and commercially sourced applications for business purposes.

Support for the management and distribution of applications by using native OS APIs, such as Android for Work and iOS's Managed App Configuration, as well as the volume purchase of apps for Android, iOS and Windows.

Mobile identity (MI): EMM tools ensure that only trusted devices and users access enterprise applications by helping to manage identity and access management (IAM) functions, such as user and device certificates, app code signing, authentication and single sign-on (SSO). EMM tools are increasingly using contextual information (such as location and time) to evaluate access decisions.

Mobile content management (MCM): EMM tools use MCM to manage access rules for content distribution on mobile devices. The MCM function has three fundamental roles:

Policy enforcement: The EMM tool can enforce policies down to individual files, including device-independent encryption keys, authentication, file-sharing rules and copy/paste restriction. Examples include conditional access to attachments in email, files synced with a back-end repository or files synced with a cloud repository.

Content push: The EMM tool enforces rules for push-based file distribution, replacement and deletion.

Integration: Beyond basic file access policies, MCM tools are adding mobile compatibility for third-party rights management systems, as well as enterprise data loss protection (DLP) and enterprise digital rights management (EDRM) infrastructures.

Advanced MCM tools are also often full-featured enterprise file synchronization and sharing (EFSS) suites, offering additional functionality, such as collaboration and more advanced policy management, but are bundled as part of the EMM product suite.

Containment: EMM tools provide methods to encapsulate MDM, MAM, MI and/or MCM in quarantined environments designed to isolate business from personal usage, and to facilitate data and function isolation on shared multiuser devices. This capability is increasingly provided by mobile OS APIs. However, when built-in APIs are not available or are undesirable to use, containment within EMM tools is necessary to segment enterprise data. Containment can be a stand-alone, self-contained application, such as a personal information management (PIM) client. This capability can improve cross-platform compatibility by removing app dependence on specific APIs, and can add self-defending/hardening features that are particularly advantageous for apps running on unmanaged devices — that is, no MDM profile is installed. Containment technology can include:

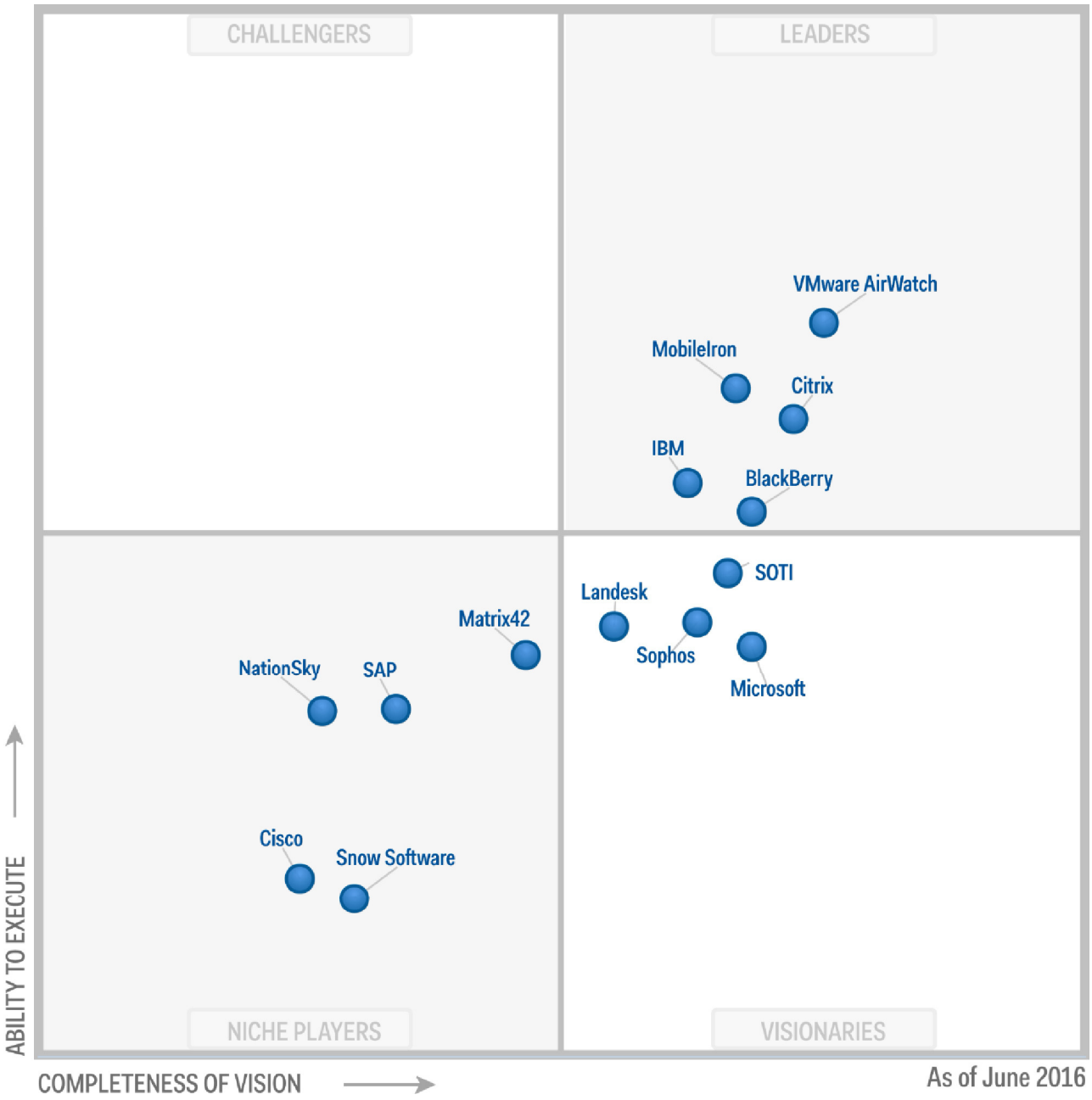
Preconfigured apps: EMM vendors provide proprietary mobile apps or integrate with particular third-party apps to provide enhanced levels of manageability and security for commonly requested functions, such as email calendaring and contact management, browsing, and file sharing.

Application extensions: These apply policies to applications through the use of a software development kit (SDK) or by wrapping individual apps with a security and management layer.

There are diverse vendor approaches to managing the mobile life cycle, with many focusing on identity and access, content security, and containment. To be classified as an EMM suite, Gartner requires inclusion of MDM, MAM and at least one of the following: MI, MCM or containment technologies. The most advanced suites will include all five technologies.

Magic Quadrant

Figure 1. Magic Quadrant for Enterprise Mobility Management Suites



Source: Gartner (June 2016)

Vendor Strengths and Cautions

BlackBerry

BlackBerry EMM is now sold in a package called "Good Secure EMM Suite," which consists of BES12 (at release 12.4), Good collaboration apps, Good Dynamics and WatchDox Enterprise. The acquisitions of Good Technology and WatchDox position BlackBerry to take a leading role in MCM and containment. Feedback to our research indicates that neither Good Secure EMM Suite nor BES12 regularly appeared in shortlists through open competition; however, they are gaining share inadvertently via the acquired Good

Technology customers. Feedback from BES12 users who manage non-BlackBerry device populations is positive, with indications of increasing investment. Good Secure EMM Suite is a good fit for organizations with stringent security requirements, those in regulated industries, or those with mobile app deployment plans that can benefit from the broad range of capabilities of the Good Dynamics platform.

STRENGTHS

Companies in highly regulated industries will find the strongest set of protections in the Good Secure EMM Suite. For those who continue to use BB10s and older models, BlackBerry has the strongest support in the industry for these legacy platforms.

With Good Work, BlackBerry provides the best secure PIM in the EMM marketplace.

BlackBerry support continues to receive positive feedback from customers; references have cited access to BlackBerry executives and company roadmaps as valuable.

CAUTIONS

Potential buyers may overlook BlackBerry's full product suite because the best-known and globally recognized BES brand name has been demoted to a subset. Current feedback indicates that companies still regard BES, Good and WatchDox as separate product lines and receive separate support, and may be confused by the end-of-life declarations as the product sets are reconfigured into the new suite.

For the multitenant cloud version of BES12, cloud service backup is stored in two locations that will conflict with national policies for some countries. The primary site is in Canada and the secondary site is in the Netherlands. For EU customers, Canada is first and foremost a problem because it is not an EU country. For U.S. customers, both sites could cause compliance violations and could expose customer data to writs and seizures outside U.S. jurisdictions.

The acquisitions of WatchDox and Good Technology have created complementary methods for containerization, synchronization and encrypted file management that will take time and effort for migration out of other products, as well as requiring new configurations for prior users of Good Technology and WatchDox. Buyers should expect functions and capabilities to continue to migrate to new product configurations during the next year.

Cisco

Cisco acquired Meraki in 2012, and picked up a basic device manager in the process. Cisco Meraki Systems Manager has expanded from a free to a paid and supported product that supports a wide range of platforms, ranging from iOS and Android devices to full Windows and Mac OS X systems. Systems Manager is included in this study because it

offers an unusually pervasive method to integrate user device management deeply into the network infrastructure. Systems Manager will appeal most strongly to companies that have chosen to conduct MDM as a network operations task.

STRENGTHS

Systems Manager provides a uniquely comprehensive single-pane management view of all networked devices in a Cisco network, including wireless access points, routers, firewalls, VPN gateways and user devices. It is designed to scale to many thousands of managed systems.

The management interface is simple and easy to understand. Setting up connections to external services, such as Active Directory (AD), and selecting policies for devices involves just a few clicks. The policies then automatically update for all equipment and devices in the Cisco/Meraki framework. This makes it easy to manage multiple remote locations with no IT staff.

Systems Manager is priced lower than any other paid EMM product on the market, with full support included. References indicate that support is fast, and product feature improvements are frequent. These factors have convinced early users to switch to the fully paid product.

CAUTIONS

The integrative benefits of Systems Manager are only applicable if an organization uses Cisco/Meraki as its primary network infrastructure.

There is no provision for MCM or MI at this time, and only a basic MAM. Systems Manager users indicate that they often pick other vendors to provide other parts of the EMM framework.

The breadth of policies in the management interface is limited. For example, individual rules must be written to block websites, rather than populating a list. Access controls are limited to a few actions, such as read only, full control or blocked, with no means to set up more complex conditions.

Citrix

Gartner continues to see reasonable growth in the Citrix XenMobile client base, which maintains its place as a frequent entry on client shortlists. Client-side innovation is evident in the Worx suite of containerized apps through updated features and new Worx offerings. Citrix offers one of the more full-featured EFSS clients in its ShareFile offering, along with a user-friendly DLP solution that offers customization of user-facing messages when sharing actions are blocked. Concerns with the product's appropriateness for large-scale (more than 20,000 devices) deployments are limited to SaaS, often when a shift to or a choice of on-premises deployment would have prevented these issues. This points to the

need for better presales guidance. A clean redesign of the console user experience (UX) provides a uniform view, despite the multiple products and consoles needed to interact with the full Citrix mobility management stack: NetScaler, ShareFile and Xen Mobile. XenMobile is good fit for organizations that have an existing Citrix infrastructure or that require a broad EMM feature set.

STRENGTHS

Citrix innovates in its client-side technology, specifically in the quality and breadth of its Worx app suite and its ShareFile client.

The vendor's offering is compelling for organizations that have investments in Citrix applications or desktop virtualization technology that they plan to extend to mobile devices.

User-side policy controls, such as the ability to tailor user messages generated by DLP policies or comprehensive settings migration on multiuser devices, have the potential to make Citrix managed devices more user-friendly.

CAUTIONS

Gartner has seen client issues with large SaaS-based deployments. Carefully evaluate the vendor's ability to meet scale and integration needs when choosing to consume XenMobile as a fully hosted SaaS deployment.

Although XenMobile is attractive for organizations deploying traditional Windows applications to mobile devices, and the vendor has improved its app discoverability through a unified app store and app configuration, making virtualized Windows apps and desktops touch-friendly remains an issue. Citrix offers a mobile SDK to address this, but it is not widely adopted.

The planned spinoff of the GoTo business unit in 2016 and a new CEO may have an impact on the XenMobile product.

IBM

IBM's MaaS360 is part of the IBM Security business unit. An increasing amount of IBM's investment in MaaS360 is used to provide synergies with IBM's security products (e.g., Trusteer for malware, Qradar for security intelligence) and IBM's IAM offerings. MaaS360 EMM manages the three popular mobile OSs: iOS, Android and Windows Phone, in addition to systems based on Windows 7/8/10 and Mac OS X. Often sold individually or as part of a larger bundle, customers consistently report MaaS360 to be an easy-to-use EMM tool. MaaS360 is a complete EMM suite offering all five functional areas. IBM offers broad support for third-party ISV mobile applications and is one of the founding members of the AppConfig standard. MaaS360 is a good fit for organizations interested in an easy-to-deploy EMM product and comprehensive mobile security.

STRENGTHS

MaaS360 app management and distribution capabilities have proven large-scale deployments.

IBM has a strong unified endpoint management (UEM) offering through long-standing MaaS360 client management capabilities and improved integration with IBM BigFix.

MaaS360's integration with QRadar enables administrators to create automated mobile device actions (for example, selective wipe), based on security events or newly discovered vulnerabilities.

CAUTIONS

Despite IBM's sales and marketing power, MaaS360 continues to show low visibility in large enterprise accounts. As such, most of MaaS360's clients are small and midsize organizations.

IBM does consistently provide frequent product updates and same-day support for new OSs releases, but at times lags behind competitors in new feature and functionality innovation.

The records of retired (unenrolled) devices are not automatically removed from the MaaS360 Admin view, which can result in unused devices consuming licenses. As a result, administrators must manually enable an automated action to remove retired devices.

Landesk

Landesk's primary vision is to provide a comprehensive UEM offering. The company is a strong player in the client management tool (CMT) market, and offers EMM (Landesk Mobility Suite) as an extension of CMTs. The UEM strategy involves an integrated console for administrators and a licensing strategy that bundles EMM, CMT, endpoint protection and the IT service desk. Landesk is good solution for organizations looking for a single solution to manage both desktops and mobile devices.

STRENGTHS

Landesk has one of the few truly integrated UEM offerings in the market, using the long-standing Landesk Management Suite console to manage PCs and mobile devices.

Secure PIM functionality provides administrators with enhanced email security capabilities (e.g., authentication into email and remote display attachments), while enabling users to employ the native email app on iOS, Android and Windows Phone.

Landesk's Xtraction reporting module (an add-on) provides presentable reports that are easy to create and customize.

CAUTIONS

Although Landesk has a mobility suite SaaS option, it is still an immature offering, and it has not yet been widely adopted by Landesk customers.

Landesk does not support Android for Work or Samsung Knox, providing only basic Android OS MDM API support.

Landesk iOS support is sufficient for basic mobility use cases; however, it lacks support for advanced iOS MDM capabilities that require tight control.

Matrix42

For many years, Matrix42 has provided a workspace management suite that combines CMT with IT service management (ITSM). Matrix42 positions the Silverback EMM suite as part of the holistic workspace management solution. The vendor has expanded its presence with new offices in the Netherlands, the U.K. and Australia. The company has traditionally been strong in supporting Windows platforms, and continues that support with Windows 10, iOS 9 and Android 6. Matrix42 is one of the few EMM vendors that has bundled its EMM suite with CMT and ITSM to provide an integrated solution through a single user license. Matrix42 also offers MyWorkspace as an IAM solution that integrates with EMM to provide adaptive access. Organizations primarily located in Europe and Australia that want an easy-to-use EMM for PCs and mobile devices should consider Matrix42.

STRENGTHS

Matrix42 provides a UEM bundle through user-based licensing for an unlimited number of devices per user for managing PCs and mobile devices through a single management console.

Customers report excellent support from the vendor during the implementation and postimplementation phases.

Matrix42 has a robust set of APIs to automate common IT operations tasks, such as provisioning and deprovisioning users, and it continues to enhance APIs on an ongoing basis.

CAUTIONS

Customers report uncertainty about the product's management capabilities as they migrate to Office 365. Matrix42 is addressing this with an upcoming Microsoft partnership.

Silverback does not currently support Apple Device Enrollment Program (DEP) on OS X, or geofencing and remote viewing/control of a mobile device.

Matrix42 does not provide its own app SDK or app-wrapping solution, and takes a

platform-centric approach to securing apps.

Microsoft

Microsoft's EMM product is the Enterprise Mobility Suite (EMS), which includes Microsoft Intune, Azure Active Directory Premium, Advanced Threat Analytics and Azure Rights Management. Intune provides the core EMM capabilities of MDM and MAM, and is only available as a cloud-based solution. Intune can be deployed in a stand-alone or hybrid mode, which integrates Intune with Configuration Manager (ConfigMgr) to support the management of user devices, Windows servers, Linux servers and Mac OS X from a unified console. Since November 2015, Intune has offered the ability to manage Outlook, the other Office 365 mobile apps and third-party ISV products that support Microsoft's standard without the need to manage the user's device.

Gartner frequently sees Intune used in what Microsoft calls "MAM-only mode," together with more mature EMM vendors that require clients to purchase full licenses for both products. Intune is increasingly deployed in organizations with Microsoft Enterprise Agreements (EAs), as EMS is frequently included. Intune is recommended for organizations of all sizes that have basic management requirements and are using Office 365 or Azure AD.

STRENGTHS

EMS's Office 365 suite policy management gives it strong appeal as a total mobile productivity solution.

Organizations purchasing or renewing Microsoft EAs will find EMS to be a cost-effective mobility solution with capabilities that extend beyond just the support of standard mobility.

Intune has strong integration with ConfigMgr.

CAUTIONS

Microsoft has made significant strides with Intune in the past year; however, its relative lack of maturity compared with leading products was apparent in several areas, such as the basic dashboard and self-service portal and its lack of Android for Work support.

Gartner frequently hears of product stability issues, especially with Android and Windows devices. Microsoft has stated that this has improved, but this has not been verified by Gartner, as the changes were made recently.

Clients report that the administrative interface requires three separate consoles and is difficult to use. Microsoft has promised to unify these consoles by year-end 2016.

MobileIron

MobileIron is a publicly traded company that continues to be one of the few stand-alone EMM vendors. It faces mounting challenges from its competitors, which frequently offer EMM as part of a bundle in a broader license agreement. The company has changed most of its executive leadership — there is a new director of engineering, director of sales, CFO and CEO. The company demonstrated significant growth in number of customers, its patent portfolio and the sophistication of its EMM deployments. MobileIron was the first EMM provider to introduce a Visual Privacy component to its app suite. MobileIron offers broad support for third-party ISV mobile applications and is one of the founding members of the AppConfig standard. MobileIron continues to receive high marks for its ability to stay current on the latest features across the three major mobile platforms and for its progress in securing U.S. federal certifications. Organizations that want a feature-rich, scalable and stable EMM product that integrates with a diverse ecosystem should consider MobileIron.

STRENGTHS

MobileIron's EMM console has incorporated several notable improvements in the past year, including the ability to create custom reports through preconfigured templates for policies, devices and users. It has also expanded its integration with third-party security information and event management (SIEM) solutions, such as Splunk and ArcSight. The console is mobile-enabled and is accessible on tablets as well.

MobileIron gets positive feedback from customers for its stability, solution readiness, scalability and extensive AppConnect ecosystem.

MobileIron continues to be one of the first to support the latest technologies across Android, iOS and Windows platforms. Its customers use latest features, including managed app conversion in iOS 9 and Windows 10 management.

CAUTIONS

MobileIron customers without a named technical support escalation contact report difficulty accessing appropriate support personnel for quick issue resolution. MobileIron has stated that it is currently expanding their support resources to address this.

MobileIron Apps@Work's look and feel is dated, and end users want a more feature-rich catalog.

A new executive management team creates short-term uncertainty. The company struggles with being the only pure-play, independent EMM provider, as it does not have offerings in adjacent markets.

NationSky

Headquartered in Beijing, NationSky was founded in 2005 and has offices across China. In December 2015, NQ Mobile completed the divestment of the NationSky business, which it had owned until August 2015. NationSky offers an EMM solution through its NQSky EMM product. NationSky is a founding member of the Global Enterprise Mobility Alliance (GEMA), a joint venture of 15 regional mobility service providers. NationSky has entered into reseller agreements that enable it to expand its channel sales network outside of China. However, it has little mind share beyond mainland China, where it stands out as the exclusive SaaS partner of China Mobile (the country's largest mobile carrier), as well as other carriers, including China Unicom and China Telecom.

NQSky EMM has feature parity with other general-purpose EMM providers, but none of the features truly differentiate the product. NQSky EMM also has a cloud offering, NQSky Cloud, which is hosted by Alibaba; however, this constitutes only a fraction of its installed base, because most clients purchase through a carrier. NQSky EMM is a good fit for organizations in China that are looking for a scalable, general-purpose EMM with local language customer support.

STRENGTHS

NQSky EMM is strong on Android with an antivirus app. It has the ability to set DLP policies that can restrict cut-copy-paste at either the application level or the container level, and offers network access policies that allow only specific Wi-Fi separate service set identifiers (SSIDs).

Customers speak highly of NationSky's dedicated and quick support to resolve issues.

The EMM console and dashboard support user, app and device administration, as well as the setting up of policies and settings (such as compliance settings). In addition, the console demonstrates the health of the runtime application server instances, such as CPU usage. The dashboard is customizable via a simple shortcut, and the screens support export to various formats.

CAUTIONS

NQSky EMM is not recommended outside China, due to its lack of built-in language packs for other languages. It relies on the browser plug-in (Microsoft Translator) for runtime translation into English. This is expected to be fixed in NQSky EMM version 4.1, due for release in July 2016.

The lack of advanced iOS functionality, such as Managed Open In, Apple Device Enrollment Program (DEP) and Apple Volume Purchase Program (VPP), prevents large-scale autoconfiguration of devices on activation, as well as app deployment and management at scale for paid apps.

Customers looking for Windows 10 support should not opt for NQSky EMM, because it

lacks the ability to manage both Windows 10 devices and Mac OS X laptops.

SAP

SAP's EMM offering is available as an on-premises solution known as Afaria and as a cloud-based solution known as SAP Mobile Secure. In evaluating the SAP EMM products over the past two years, Gartner has seen signals that EMM is not resourced as a strategic asset for the vendor. Minimal innovation in core EMM functions is underscored by a lack of baseline feature additions, and a lag between the announcement of major mobile platform features and support from SAP, which brings these features to market well behind competitors. Feedback from users points to the key benefit of the product being its low cost, although these organizations have noted that the solution's performance and capabilities are commensurate with the low investment required. SAP Mobile Secure is a good fit for organizations that want a SaaS-based service and have an existing SAP infrastructure.

STRENGTHS

Built-in support for SAP's mobile application development platform (MADP), cloud-based app development environment (SAP Web IDE) and SAP Fiori make SAP Mobile Secure a potentially attractive choice for organizations whose mobile strategy depends on SAP-developed or SAP-dependent mobile apps.

A low investment threshold for SAP customers makes SAP's EMM an attractive alternative to its competitors, although its performance and feature set rank lower than those of competing EMM offerings.

As part of the company's SAP Hana Cloud Platform platform-as-a-service offering, SAP Mobile Secure provides broad integration capabilities to customers who are extending, integrating and building mobile apps.

CAUTIONS

Based on the slow pace of updates and a relative lack of innovation, SAP EMM users may find it difficult to remain current in support of mobile platform and management capabilities.

Variations in UX design among multiple consoles may prove confusing for administrators working across the SAP EMM console and related offerings, such as SAP's Lumira server.

SAP's EMM role within SAP is focused on the company's mobile app ecosystem. The vendor's focus has (rightly) shifted to enabling mobile application development, rather than device management.

Snow Software

Headquartered in Stockholm, Sweden, Snow Software is, at its core, a software asset management (SAM) solution provider. Snow provides an EMM solution through its Snow Device Manager. This follows the company's acquisition of The Institution, and its EMM product, Revival, in February 2015. This positions Snow as one of the few vendors to uniquely offer a SAM platform that integrates mobile device inventory in EMM, with mobile app licensing through Snow License Manager, although this integration is still a work in progress. Snow Device Manager and Snow License Manager have to be licensed separately; however, a bundled solution is available. Snow Device Manager is a good fit for European-based organizations looking for a basic EMM solution, with a focus on cost optimization in the workplace by tracking application installations and usage across servers, desktops and common mobile platforms.

STRENGTHS

Snow's EMM solution is strong in areas such as the Apple VPP and application tracking that augment the SAM platform's overall license management capabilities.

The administration console in Snow Device Manager provides role-based access for differentiating between access privileges to the service administrator and superuser roles. Snow Device Manager's dashboard also has a handy visual indicator to determine whether a device has an MDM agent or MDM profile installed.

The self-service portal is combined with the app storefront to provide a single portal for reporting lost devices and requesting apps, as well as for requesting new services, IT support, and maintenance requests for computers and mobile devices. For new services and app requests, there's a built-in approval and check-out workflow.

CAUTIONS

Snow Device Manager has limited MCM capabilities, with its content app supporting only network file shares provisioned via AD groups. It does not have connectors to Box, Microsoft SharePoint and other Content Management Interoperability Services (CMIS) repositories. The container for documents is available only on iOS and Android.

Android for Work support is a work in progress and is not feature-complete. At publication time, Windows 10 EMM support lacked integration with Windows Store for Business; it is due to be available from June 2016.

Snow Device Manager's administration console for service administrators is a Windows desktop application with a legacy look and feel. The dynamic assignment of apps to device groups does not offer a scalable solution when the number of devices runs into the tens of thousands, because it's primarily based on applying filters to a dashboard grid.

Sophos

Sophos Mobile Control (SMC) version 6.1 is available either as a stand-alone, on-premises solution or in Sophos Cloud. It can integrate with a broadening portfolio that includes traditional endpoint protection (EPP), unified threat management (UTM), firewalls, secure web gateways (SWGs), VPN and Android antivirus protection. Sophos sells its EMM solution mainly to small businesses (78% have fewer than 500 managed devices); however, it can scale to 50,000 devices. Sophos can now fully manage Windows 10 tablets, notebooks and desktops. It provides full implementation of the container system, and iOS DEP support has been added to the latest release. It does not currently support Android for Work. Sophos is a good fit for organizations looking to consolidate EPP and EMM, and for push-type tasks that involve a self-managed secure container.

STRENGTHS

Sophos' references continue to cite ease of setup and administration, and quality of support (QoS) as positive factors.

Sophos' MCM encrypts files leaving a PC or mobile device to prevent data leakage. This integrates with third-party file storage providers and enables companies to securely use low-cost, third-party storage. Files can be accessed in the Sophos Secure Workspace container, or via a browser using HTML5 packages.

Sophos Secure Email client (which was licensed from Virtual Solution AG) is the first PIM client to be certified for the German government's BSI security standard and is one of the best PIM clients available. It offers an easy-to-use interface and runs as part of the Sophos Container together with secure documents and a corporate browser.

CAUTIONS

Buyers that don't need the broader Sophos product portfolio could dismiss SMC by making the wrong assumption that it is antivirus solution, rather than an EMM.

Sophos does not typically target large EMM customers. As such, the product's management interface has a focus on the small or midsize business (SMB) market, which may not be suitable for larger deployments.

SMC is mainly an on-premises solution, and is not yet fully integrated into Sophos Cloud, which accounts for only 8% of EMM user licenses.

SOTI

SOTI has extensive history and expertise in dedicated-purpose device management. Although its flagship product, MobiControl (now in version 13), has evolved over the years into a capable product for general-purpose use across iOS, Android and Windows, SOTI has continued to differentiate itself through its deep expertise as the leading platform for Android management and for ruggedized devices. SOTI pioneered efforts to unify fragmented Android management APIs with its Android+ technology, which is still

supported on a number of devices. It implements full Knox 2.0 and support for major original design manufacturer (ODM) APIs, including Sony API support, along with same-day support for Android for Work.

MobiControl supports kiosk mode on Android, and version 13 exposes a set of RESTful web service APIs for the integration of EMM functions into business workflows. SOTI is used across industries, but is deployed extensively in task-driven and dedicated-purpose device environments, such as transportation, retail, hospitality, healthcare, field service and manufacturing. SOTI is a good fit for environments that require broad EMM capabilities — especially those requiring process automation and workflows, and task worker mobility — and in situations in which there is extensive investment in Android.

STRENGTHS

SOTI's extensive experience with and comprehensive support for Android continue to make it one of the strongest EMM solutions for this platform.

SOTI's remote support capabilities for Android are still among the best in the industry.

References frequently cite the responsiveness of and collaboration with the product team on development of product as a satisfying characteristic.

CAUTIONS

As one of the only stand-alone EMM vendors, SOTI faces increasing competition from larger vendors looking to expand into SOTI's traditional markets of the ruggedized and IoT spaces.

SOTI's app analytics lag behind some of the leaders in this space.

Although SOTI has strong support for Android (and legacy Windows Mobile), it still has a relatively small percentage of iOS devices under management.

VMware AirWatch

During the past two years, VMware AirWatch has transitioned from an independent entity to becoming part of VMware's end-user computing business unit. As a result, AirWatch has become increasingly integrated with VMware technologies, most notably VMware's IAM and software-defined networking (SDN) products. VMware AirWatch's offering has comprehensive EMM functionality and, as a result, appears most frequently in Gartner clients' EMM vendor shortlists. AirWatch offers broad support for third-party independent software vendor (ISV) mobile applications and is one of the founding members of the AppConfig standard. Gartner has heard of periodic code quality issues with the AirWatch product, which are likely to be the result of attempts to provide a broad set of capabilities quickly.

Due to quality issues with the Inbox email application, VMware AirWatch acquired Boxer in October 2015. Other bundled applications, such as Content Locker, offer basic functionality to clients that choose to use more advanced third-party solutions instead. VMware AirWatch is a good fit for organizations that require a comprehensive EMM feature set on a broad range of platforms.

STRENGTHS

VMware AirWatch has proven large-scale deployments across most vertical markets.

Its administrative console is one of the easiest to use, with embedded training videos, links and a wizardlike approach to help new administrators become productive quickly.

VMware AirWatch continues to push innovation with zero-day support of new OSs and expansion into the management of Internet of Things (IoT) devices and unified workspaces.

CAUTIONS

Gartner continues to receive complaints about support for VMware AirWatch from clients who do not have a direct Technical Account Manager (TAM). Clients who have purchased the TAM option report satisfactory service.

The EMM version of Boxer is not currently available for Android or Windows, which forces clients to use either third-party PIM clients or the Inbox product. Due to the newness of Boxer on iOS, Gartner has not received any client confirmation that Boxer fixes the stability and usability problems of Inbox.

The planned acquisition of VMware's parent company, EMC, by Dell causes potential concern that the VMware AirWatch product will no longer receive the attention it has under a stand-alone VMware.

Vendors Added and Dropped

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

Added

Cisco

Matrix42

NationSky

Snow Software

Dropped

Globo: Globo is no longer in business (see "What Globo's Downfall Means for Its Customer and Buyers for MADP and EMM").

Good Technology: Good was acquired by BlackBerry in September 2015, and it is now included as part of the BlackBerry Enterprise Server.

Inclusion and Exclusion Criteria

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

The vendor must have at least $8 million in 2015 EMM revenue.

There must be five references from organizations using the EMM product in production, with at least one that has multiple OSs under management and one with 10,000 or more installed seats.

The vendor must offer EMM support for at least iOS, Android and Windows Phone.

The vendor must provide an EMM suite that contains MDM, MAM, and at least one of the following: mobile identity, MCM or containment technologies.

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

Advanced MAM that manages PIMs, browsers and other applications

Support for Mac OS X and Windows

Mobile identity and access through capabilities such as certificate management, enabling SSO on mobile devices and executing "contextual authentication" through dynamic conditions, such as time, location, user and device posture

Mobile analytics to understand usage trends and support troubleshooting

File-level protections to protect data consumed or created in a mobile context

Many vendors were considered for the Magic Quadrant, but did not qualify, because they did not meet the business metrics or the technical capabilities required for inclusion. The following are a few vendors that have increased their investments in EMM, but lacked the product completeness or established track record to qualify for inclusion:

Apperian is a leader in stand-alone MAM solutions that also offers full EMM functionality through a licensed MDM solution; however, it did not meet sales thresholds for market size inclusion. Although it has only basic MDM functionality, Apperian's MAM and containment functionality are strong. As such, Apperian should be considered by clients looking to deploy applications without the need to manage the entire device.

Centrify has offered a free EMM for several years, with an option to buy into a fully supported product. During 2014, Centrify was endorsed by Samsung as a Knox EMM provider. During the review period for this research, Centrify was unable to meet sales thresholds for market size inclusion. Centrify is separately pursuing secure server connections as alternatives to per-app virtual private networks (VPNs).

Virtual Solutions offers SecurePIM, which is a stand-alone PIM client that also integrates with a licensed EMM solution. SecurePIM was unable to meet sales thresholds for market size and platform support for inclusion. The PIM client is highly rated for ease of use, its unique support for enabling secure email and its extensive security certifications. SecurePIM should be considered for any organization that needs high-security data containment on mobile devices.

Evaluation Criteria

Ability to Execute

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

Product/Service: What features are provided, and does the vendor have customers using these features successfully in production environments?

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

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

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

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

Customer Experience: We assessed the vendor's reputation in the market based on customer feedback regarding customers' experiences working with the vendor, whether they were glad they chose the vendor's product and whether they planned to continue working with the vendor.

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

Table 1. Ability to Execute Evaluation Criteria

Evaluation Criteria	Weighting
Product or Service	High
Overall Viability	High
Sales Execution/Pricing	High
Market Responsiveness/Record	Medium
Marketing Execution	Medium
Customer Experience	High
Operations	Not Rated

Source: Gartner (June 2016)

Completeness of Vision

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

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

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

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

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

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

Vertical/Industry Strategy: This criterion looks at how the EMM vendor meets industry-specific challenges, and how it is using these opportunities to expand into the IoT.

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

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

Table 2. Completeness of Vision Evaluation Criteria

Evaluation Criteria	**Weighting**
Market Understanding	High
Marketing Strategy	Medium

Evaluation Criteria	Weighting
Sales Strategy	High
Offering (Product) Strategy	High
Business Model	Medium
Vertical/Industry Strategy	Not Rated
Innovation	High
Geographic Strategy	Medium

Source: Gartner (June 2016)

Quadrant Descriptions

Leaders

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

Challengers

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

Visionaries

Visionaries have unique capabilities in certain aspects of EMM. They meet the requirements of customers that place a high priority in certain critical EMM areas. They may not have the product completeness, support capability, business performance, mind share or track record compared with leading vendors.

Niche Players

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

Context

Organizations use EMM tools to integrate mobility into their business workflow. There are many factors that determine the appropriate vendor and product for your organization. The vendor must demonstrate the ability to keep up with the fast pace of mobile device change. Organizations must also factor in the EMM vendor's ability to support the enterprise's critical mobile applications and integrate with its IT infrastructure — for example, public-key infrastructure (PKI), VPN, wireless networking and IAM platforms.

EMM product requirements change as mobile platforms change. Keep abreast of these changes; engage Gartner analysts regularly to understand the changing mobile device landscape and the implications for mobility management. Best practices are to create your requirements first, consider all the possible mobile scenarios you may have in your organization (such as bring your own device (BYOD) initiatives and use cases specific to your organization), and then create a shortlist of vendors. Do not choose vendors simply on the basis of their position in the Magic Quadrant.

Market Overview

Gartner estimates that the average enterprise has deployed between eight and 15 mobile applications to its employees. Where mobile strategy previously consisted wholly of basic, horizontal productivity tools — such as email, contacts and calendar — role-specific and mission-critical apps and data are increasingly the bulk of what is being pushed to users' mobile devices. As this trend matures, the need for application-level controls and reporting, along with the ability to deliver and consume a growing number of content types, is at the heart of many mobile strategies. The needs of clients vary greatly across sectors,

with most clients using MDM and MAM functionality. However, advanced features, such as MI, MCM and containment, are used by a smaller percentage, with few clients using all five components of EMM.

EMM Is the "Glue"

EMM is the starting point, if you are planning to opt into managing anything on a mobile platform. Because it is the presumptive foothold agent, EMM is the logical choice to broker policies for other services and tools on the platform. EMM provides a common, cross-platform baseline to set, contain, validate, enforce and update device policies for gateways, proxies, VPNs, network access controls (NACs) and certificates, application certificates, content and rights management systems, IAM, version controls, backups, system updates, and device initialization, as well as wipe and countless other practice areas that enter the mobile space from adjacent markets.

As a single point of policy and accountability, EMM provides the opportunity to avoid agent bloat, which is so often seen on PCs, where an endless parade of add-on utilities steals local resources, duplicating and complicating the task of policy coordination for system administrators. PCs have the resources to cope with this situation; however, users of small mobile devices and particularly BYOD cannot succeed with so much unnecessary complexity.

MDM

MDM is the key enabler to the glue of EMM. MDM has changed from being a stand-alone product category doing basic policy management, such as passcode enforcement and device wipe, to a key required feature within EMM suites. MDM controls have evolved across all OSs and have expanded into traditional desktop management with Windows 10 and OSX. Each OS offers similar basic controls; however, advanced controls — such as OS version control for Windows 10 devices, automatic device staging for iOS with Device Enrollment Protocol (DEP), and the ability to apply different policies to work and personal environments with Android for Work and Samsung's Knox — vary greatly.

Gartner continues to see MDM as a key requirement for enterprise-owned devices. However, we are seeing increased push-back due to privacy and legal concerns, which are often based on a user's misunderstandings of MDM's capabilities.

MAM

MAM facilitates the deployment and operational life cycle management of mobile apps. This includes administrative push, the user-initiated deployment and updating of custom and public (app store) apps, and the management of associated app licenses. User-initiated deployment is facilitated via an enterprise app store, which is typically presented as a web-based portal or a mobile app. License management should support the major

enterprise or volume-licensing mechanisms, such as Apple's VPP. MAM also includes the ability to identify or tag apps as "managed" enterprise apps (versus personal apps in BYOD and corporate-owned, privately enabled [COPE] use cases), apply management and security policies to these apps, and selectively wipe them from the device, along with any associated data.

Policies commonly applied to enterprise apps include security policies and DLP policies, such as:

- Require initiation of per-app VPN connections on app launches
- Encrypt enterprise app data at rest (or at the file level, in some cases), sometimes with stronger encryption than that used by the underlying OS
- Restrict "open in" and similar app data exchange to only managed (enterprise) apps
- Restrict cut/copy/paste
- Require conditional launch or access — for example, device in approved state, no jailbreak or rooting detected

Differentiating features of MAM manifest in several areas. Enterprise app stores, for example, range from rudimentary to highly functional, some approaching the usability and features of major commercial app stores, such as Apple's App Store or Google Play. At the low end, these products may be little more than rudimentary web portals or simple apps that present all available apps to all users, provide no feedback or app-rating mechanisms, and are poor tools to help users discover apps.

Moreover, differentiation can manifest in OS support or the support of different MAM-enablement mechanisms. App policies can be applied by leveraging one of three common mechanisms:

- Native OS MAM APIs
- Proprietary SDKs compiled into apps during development
- App wrappers (code injection into the binary, postdevelopment)

An EMM vendor may support all three mechanisms across all major mobile OSs, while another supports only a subset. As an example, a vendor may include support for Apple's built-in MAM APIs, but no support for Google's Android for Work built in MAM APIs.

Containment

Although the term is used in several ways in the industry, "containment" here is shorthand for an extended set of capabilities that facilitate separation of business and personal data, including PIM clients, preconfigured public or ISV-provided mobile apps, and application extensions, such as SDKs or app wrappers:

PIMs — PIMs are mobile apps that provide business email, calendaring and contact management, typically providing security and manageability features that native email clients may lack. Although used by fewer organizations than in previous years, PIM is still often a requirement in regulated or high-security verticals, such as finance, healthcare and the public sector.

Preconfigured applications — EMM vendors provide proprietary mobile apps or integrate with particular third-party apps to provide enhanced levels of manageability. These most commonly include productivity and collaboration applications, as well as secure browsers provided by the EMM provider or a third party.

Application extensions — These proprietary tools provide the ability to make mobile apps manageable via EMM. SDKs provide libraries that can be compiled with mobile apps by organizations or ISVs to enable a specific EMM vendor's policies to be applied to them. Wrappers typically use a form of code injection into the executable binaries of mobile apps to enable a specific EMM vendor's policies to be applied. SDKs and/or wrappers are required for "MAM only" use cases, where managed apps must be delivered to devices that aren't (or can't be) enrolled in EMM (unless the ISV has used the specific EMM vendor's SDK). Some vendors support both SDK and app-wrapping approaches. Others may support only one or the other.

Finally, a given EMM vendor might support what they call "MAM only" use cases, in which app policies can be applied to apps on devices that aren't enrolled in EMM, whereas another may not. Gartner defines this as containment to avoid confusion with basic MAM terminology. Such containment use cases must leverage controls built into the application, SDKs or wrappers, because the native OS APIs can't be accessed without the "trusted relationship" of an EMM enrollment (see "Market Guide for Mobile Application Management").

MI and Access

Users no longer have a single device. They now frequently have a smartphone, a tablet and a laptop. More often than not, they want to use devices as part of a BYOD program. As a result, it has become important to determine not only who is connected to the network, but also whether they are connected with a corporate-authorized device. This is why Gartner recognizes MI as a key pillar in EMM. MI is typically done using digital certificates, but can also be accomplished with other technologies, including biometric and token-based authentication.

Gartner has seen the initial convergence of EMM with IAM tools. This has resulted in several EMM vendors enabling IAM functionality, such as SSO and acting as identity providers. Gartner has also seen the converse, with several identification as a service (IDaaS) vendors now offering basic EMM functionality.

The next wave of mobile identity is context-based, with authentication identifying not only the user and device, but also where and how a user connects to the network (that is, in the office, at home, on a public Wi-Fi or out of the country), and based on these contextual values, granting the user different levels of access. Over the next three years, Gartner expects context-based mobile identity to become standard functionality within EMM products.

EMM Executes File-Level Protection at the Edge

Protecting enterprise data on mobile devices has traditionally been based on a multipronged approach of encryption of data at rest, in use and in motion, as well as device- and app-level policies, such as screen lock timeouts, PIN enforcement and "open in" restrictions. However, these oblique protection approaches are incomplete, because once data leaves managed devices and networks, such protection schemes are rendered moot. Users can and often do get around such controls by emailing enterprise data to outside parties or personal email accounts, or copying data to their PCs, where open-in restrictions are absent. In response, there is a growing need to protect data intrinsically, and/or implement a rights-management-based approach to mobile data protection.

File-level encryption products encrypt the individual files themselves (rather than simply encrypting stored data and network tunnels) and facilitate managed file access through PKI, such that data can be protected wherever it is stored or accessed. No one without the encryption keys can access files protected in this manner.

Rights management products extend IAM frameworks to provide control over file operations for frequently used file types, in addition to file access. These products enable an organization to restrict who has permissions to read, edit or delete a file, or forward a file via email. Such products typically also facilitate file-level encryption as part of their mobile data protection schemes. Effective data classification is thus critical in making a rights management approach work in a given environment.

Some EMM vendors are building file-level protection and/or rights management capabilities as adjuncts to their core products, whereas others are enabling file-level protection by synergistically and tightly integrating their EMM systems with general-purpose identity and access management products. As with device-, app- or content-level policies, EMM should provide a single point of administration for encryption and access/rights policies where these capabilities are present.

UEM

Organizations have historically used different management tools for PCs and mobile devices. IT organizations are increasingly consolidating their PC and mobile device support groups and treating their devices as "endpoints." Meanwhile, the PC and mobile architectures continue to fuse together, blurring the boundaries between the EMM and CMT capabilities. This trend continues with Windows 10, which added to the MDM APIs introduced with Windows 8.1. It presents organizations with the potential to manage PCs with either EMM tools or agent-based CMTs. Large organizations will adopt both approaches, based on user segmentation. As Win32 applications decline in number, organizations will manage PCs, smartphones and tablets with the same toolset. This is easier said than done, as Win32 applications still provide many critical functions for most organizations today. It will take several years for most organizations to get to this point. Once organizations have retired their Win32 applications, the descriptor "unified" will not be necessary; at that point, the term will be "endpoint management."

UEM is not limited to PCs, tablets and smartphones. Smart devices, broadly grouped as part of the IoT, will increasingly become included in UEM. Devices such as Apple TVs, printers and smartwatches are identifiable examples of IoT devices managed by EMM tools. However, not all IoT objects will fall under the realm of EMM tools. Some devices may be managed directly by manufacturers. Other types of devices will have proprietary management tools. And many devices will not need to be managed at all. However, it is clear that the diversity and number of devices will continue to grow, and IT organizations must be ready.

Evaluation Criteria Definitions

Ability to Execute

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

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

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

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

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

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

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

Completeness of Vision

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

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

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

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

Business Model: The soundness and logic of the 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.

(http://gtnr.it/1KsfgQX)

© 2016 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. or its affiliates. This publication may not be reproduced or distributed in any form without Gartner's prior written permission. If you are authorized to access this publication, your use of it is subject to the Usage Guidelines for Gartner Services (/technology/about/policies/usage_guidelines.jsp) posted on gartner.com. The information contained in this publication has been obtained from sources believed to be reliable. Gartner disclaims all warranties as to the accuracy, completeness or adequacy of such information and shall have no liability for errors, omissions or inadequacies in such information. This publication consists of the opinions of Gartner's research organization and should not be construed as statements of fact. The opinions expressed herein are subject to change without notice. Gartner provides information technology research and advisory services to a wide range of technology consumers, manufacturers and sellers, and may have client relationships with, and derive revenues from, companies discussed herein. Although Gartner research may include a discussion of related legal issues, Gartner does not provide legal advice or services and its research should not be construed or used as such. Gartner is a public company, and its shareholders may include firms and funds that have financial interests in entities covered in Gartner research. Gartner's Board of Directors may include senior managers of these firms or funds. Gartner research is produced independently by its research organization without input or influence from these firms, funds or their managers. For further information on the independence and integrity of Gartner research, see "Guiding Principles on Independence and Objectivity. (/technology/about/ombudsman/omb_guide2.jsp)"

About (http://www.gartner.com/technology/about.jsp)

Careers (http://www.gartner.com/technology/careers/)

Newsroom (http://www.gartner.com/newsroom/)

Policies (http://www.gartner.com/technology/about/policies/guidelines_ov.jsp)

Privacy (http://www.gartner.com/privacy)

Site Index (http://www.gartner.com/technology/site-index.jsp)

IT Glossary (http://www.gartner.com/it-glossary/)

Contact Gartner (http://www.gartner.com/technology/contact/contact_gartner.jsp)