Enterprise Mobility Management - Market Quadrant 2015

An Analysis of the Market for Enterprise Mobility Management Revealing Top Players, Trail Blazers, Specialists and Mature Players.

April 2015
TABLE OF CONTENTS

RADICATI MARKET QUADRANTS EXPLAINED .......................................................... 3
MARKET SEGMENTATION ..................................................................................... 5
EVALUATION CRITERIA ......................................................................................... 7
MARKET QUADRANT – ENTERPRISE MOBILITY MANAGEMENT VENDORS .......... 9
KEY MARKET QUADRANT TRENDS ..................................................................... 10
ENTERPRISE MOBILITY MANAGEMENT - VENDOR ANALYSIS .......................... 11
TOP PLAYERS ....................................................................................................... 11
TRAIL BLAZERS .................................................................................................... 18
SPECIALISTS ....................................................................................................... 27

Please note that this report comes with a 1-5 user license. If you wish to distribute the
report to more than 5 individuals, you will need to purchase an internal site license for an
additional fee. Please contact us at admin@radicati.com if you wish to purchase a site license.

Companies are never permitted to post reports on their external web sites or distribute by
other means outside of their organization without explicit written prior consent from The
Radicati Group, Inc. If you post this report on your external website or release it to
anyone outside of your company without permission, you and your company will be
liable for damages. Please contact us with any questions about our policies.
Radicati Market Quadrants Explained

Radicati Market Quadrants are designed to illustrate how individual vendors fit within specific technology markets at any given point in time. All Radicati Market Quadrants are composed of four sections, as shown in the example quadrant (Figure 1).

1. **Specialists** – This group is made up of two types of companies:
   
   a. Emerging players that are still very new to the industry and have not yet built up much of an installed base. These companies are still developing their strategy and technology.
   
   b. Established vendors that offer a niche product.

2. **Trail Blazers** – These vendors offer cutting edge technology, but have not yet built up a large customer base. With effective marketing and better awareness, these companies hold the power to dethrone the current market leaders. “Trail blazers” often shape the future of technology with their innovations and new product designs.

3. **Top Players** – These are the current leaders of the market, with products that have built up large customer bases. Vendors do not become “top players” overnight. Most of the companies in this quadrant were first specialists or trail blazers (some were both). As companies reach this stage, they must fight complacency and continue product innovation, or else they will be replaced by the next generation of “trail blazers.”

4. **Mature Player** – These vendors have large, mature installed bases of customers, but no longer set the pace for the rest of the industry. These vendors are no longer considered “movers and shakers” as they once were.

   a. In some cases, this is by design. If a vendor has made a strategic decision to move in a new direction, it may slow development on one product line and start another.
b. In other cases, a vendor may simply become complacent as a top vendor and be out-developed by hungrier “trail blazers” and other top players.

c. Companies in this stage either, find new life and revive their R&D, moving back into the “top players” segment, or else they slowly fade away as legacy technology.

Figure 1, below, shows a sample Radicati Market Quadrant. As a vendor continues to develop its product, it will move horizontally along the “x” axis. As market share changes, vendors move vertically along the “y” axis. It is common for vendors to move between quadrants over the life of a product, as their products improve and market requirements evolve.

**Figure 1: Sample Radicati Market Quadrant**

- **Functionality** – is rated from 1 to 10, with 10 being the highest, and 1 – the lowest.

- **Market Share** – is assigned according to the company’s ranking in our latest annual reports, based on its user Installed Base (e.g. the company with the largest installed base market share is number 1, the one with the second largest installed base market share is number 2, etc.).
MARKET SEGMENTATION

This study looks at the Enterprise Mobility Management market as comprising one segment:

- **Enterprise Mobility Management** solutions – provide businesses with the ability to secure and manage the mobile devices used by their employees. EMM solutions are aimed at smartphone and tablet devices and should support multiple mobile operating systems. Leading vendors in this market include: AirWatch, BlackBerry, Citrix, IBM, Good Technology, Kaspersky Lab, McAfee, MobileIron, SAP, Sophos, SOTI, Symantec, Trend Micro, and others.

- EMM solutions are available as on-premises software, cloud-based services, or hybrid solutions.

- Enterprise Mobility Management comprises four main areas of functionality, which include:
  
  o **Mobile Device Management (MDM)** – device level management features such as: remote configuration; remote wipe; selective wipe; remote locking, and more.

  o **Mobile Security** – includes features such as encryption of the device storage, SD cards, emails and folders; two-factor authentication, and more.

  o **Mobile Application Management (MAM)** – includes features such as containerization; app wrapping, app usage analytics, and more.

  o **Mobile Content Management** – includes features such as secure email, calendar, contacts, document management software integration, and more.

- Many vendors offer solution components aimed at addressing some aspect of enterprise mobility management and there are many pure-play mobility vendors that focus on a single component of EMM. For the purpose of this report, vendors offering solutions that focus only on a single component of EMM are not included.
• Also, for the purposes of this report, rugged devices, such as those used by fleet operations, are not included in this segmentation. This report is meant to only offer a view of the Enterprise Mobility Management market in the context of BYOD office employee use.

• Worldwide revenues for the EMM market will total $1,495 million by year-end 2015. This figure is expected to grow to over $4.4 billion by year-end 2019. This represents an average annual growth rate of over 30% in the next four years. Figure 1, shows the worldwide revenue for the Enterprise Mobility Management market from 2015 to 2019.

![Worldwide EMM Revenues, 2015 - 2019](image)

**Figure 2: Worldwide Enterprise Mobility Management Revenue, 2015-2019**
EVALUATION CRITERIA

Enterprise Mobility Management vendors are positioned in the quadrant, according to two criteria: Market Share and Functionality.

Market Share – is based on the installed base published in our “Enterprise Mobility Management Market, 2015-2019” report. Installed base is defined as “number of devices under management”. The Enterprise Mobility Management vendor with the largest installed base has a market share of 1, the one with the second largest installed base has a market share of 2, etc. Vendors with higher market shares are positioned in the Top Player or Mature quadrants. Enterprise Mobility Management vendors with smaller installed bases are positioned either in the Trail Blazer, or Specialist quadrants.

Functionality – we assess each Enterprise Mobility Management vendor’s solution based on a number of key differentiators in capabilities.

To be considered a complete EMM platform, vendors should provide comprehensive feature sets in the areas of MDM, MAM, Mobile Security, and Mobile Content Management. The following list summarizes the functionality and features that vendors should provide to be considered a complete EMM platform.

Mobile OS Support — support for a variety of mobile OS’s, including: Apple iOS, Google Android, Windows Phone/Mobile, Symbian, and BlackBerry.

Deployment Scenarios - flexible deployment options, including: on-premises, cloud-based, and hybrid models.

Remote Device Configuration — the ability to configure devices remotely, as well as perform remote device wipe, selective wipe, remote lock, password resets, and more.

Remote Device Management — the ability to remotely disable the device’s Wi-Fi, camera, Bluetooth connection, and more.

Device Level Analytics — the richness of usage statistics about device use.
**Encryption** — encryption-level protection of device storage, SD card, emails, folders, and more.

**App Containerization** — the availability of app SDK, app wrapping, block copy/paste between apps or emails, remote app updating.

**Mobile App Analytics** — the richness of data about app behavior, download stats, and more.

**Authentication** — including single sign-on, two-factor app/data authentication.

**Data Loss Prevention** — support for outbound data loss prevention (DLP).

**Jailbreak/Rooting Detection** — the ability to identify, report, and block device jailbreak or rooting.

**Licensing costs**— available licensing models, e.g. perpetual, recurring, etc. Ease of understanding and estimating costs.

**Partner Ecosystem** – the overall partner ecosystem including carriers, app stores, global partner reach, etc.

**Global Support** - 24x7 help desk support. Also, vendors should provide helpdesk automation, which includes a self-service portal that users can access to perform basic MDM functions, such as device wiping, password resetting, and more.

**Note:** On occasion, we may put a player on the right side of the quadrant by giving them a higher than typical Functionality Score, even if they are missing one or two of the features mentioned above, if we feel that the other aspects of their solution are particularly unique and innovative.
MARKET QUADRANT – ENTERPRISE MOBILITY MANAGEMENT VENDORS

Enterprise Mobility Management Market Quadrant,

<table>
<thead>
<tr>
<th>Mature Players</th>
<th>Top Players</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>AirWatch •</td>
</tr>
<tr>
<td></td>
<td>MobileIron •</td>
</tr>
<tr>
<td></td>
<td>BlackBerry</td>
</tr>
<tr>
<td></td>
<td>Citrix •</td>
</tr>
<tr>
<td></td>
<td>Good •</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Specialists</th>
<th>Trail Blazers</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAP</td>
<td>SOTI •</td>
</tr>
<tr>
<td>McAfee</td>
<td>Sophos</td>
</tr>
<tr>
<td>Trend Micro</td>
<td>IBM</td>
</tr>
<tr>
<td>Symantec</td>
<td>Kaspersky Lab</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Figure 3: Enterprise Mobility Management Market Quadrant, 2015

Note: Market share is based on installed base, defined as “number of devices under management”.

Radicati Market Quadrant℠ is copyrighted April 2015 by The Radicati Group, Inc. Reproduction in whole or in part is prohibited without expressed written permission of the Radicati Group. Vendors and products depicted in Radicati Market Quadrants℠ should not be considered an endorsement, but rather a measure of The Radicati Group’s opinion, based on product reviews, primary research studies, vendor interviews, historical data, and other metrics. The Radicati Group intends its Market Quadrants to be one of many information sources that readers use to form opinions and make decisions. Radicati Market Quadrants℠ are time sensitive, designed to depict the landscape of a particular market at a given point in time. The Radicati Group disclaims all warranties as to the accuracy or completeness of such information. The Radicati Group shall have no liability for errors, omissions, or inadequacies in the information contained herein or for interpretations thereof.
KEY MARKET QUADRANT TRENDS

• The Top Players in the Enterprise Mobility Management market are AirWatch, MobileIron, BlackBerry, Citrix, and Good Technologies.

  o AirWatch offers feature-rich solutions covering all aspects EMM for a wide range of mobile devices and operating systems.

  o MobileIron is an innovation leader in the EMM space with a robust offering for all mobile devices and operating systems.

  o BlackBerry was one of the first vendors to provide robust, leading edge security features with its BES management solution. BlackBerry has successfully diversified outside its own devices to fully support the BYOD trend.

  o Citrix offers powerful EMM solutions aimed at the needs of customers of all sizes.

  o Good Technology is one of the early innovators and thought leaders in EMM and mobile security.

• The Trail Blazers quadrant includes SAP, IBM, Sophos, Kaspersky Lab, and SOTI.

  o SAP is a leading global enterprise software vendors, and views mobility and mobility management as a key element of its enterprise product portfolio.

  o IBM offers a feature-rich EMM solution, which is now a critical component of the IBM MobileFirst portfolio.

  o Sophos’s EMM solution offers mobile security across a broad range of mobile operating systems, and is available as an on-premises product, a cloud-based service, or a hybrid solution.
 enterprise mobility management – market quadrant 2015

- Kaspersky Lab offers strong EMM solutions that show a deep understanding of the EMM requirements of corporate customers.

- SOTI offers a comprehensive EMM platform that includes modules for MDM, MAM, mobile security management, mobile content management, and mobile email management.

• The Specialists quadrant includes McAfee, Symantec and Trend Micro.

  - McAfee is a clear leader in the enterprise endpoint security market and offers an EMM solution which is a strong complement to its endpoint security.

  - Symantec’s EMM platform offers strong support for the management of mobile apps and is a good add-on for customers of its endpoint security solutions.

  - Trend Micro mobile security covers a wide range of mobile platforms, and integrates fully with Trend Micro’s management console for easy management and provisioning.

• There are currently no Mature Players in this market.

enterprise mobility management – vendor analysis

top players

AirWatch by VMware

1155 Perimeter Center West, Suite 100
Atlanta, GA 30338
www.air-watch.com

AirWatch by VMware (AirWatch), acquired by VMware in February 2014, focuses on mobile security and enablement solutions, but has also expanded to include mobile identity management, social collaboration, telecom management, intelligent networking,
and app mobilization and infrastructure. **AirWatch Enterprise Mobility Management** includes mobile device, application, content, laptop, browser, and email management along with solutions for BYOD, containerization, secure chat and video management. It provides security for most mobile operating systems, including Apple iOS, Android, BlackBerry, Windows Phone, Windows Mobile, Symbian, Apple TV, Mac OS X and Windows PC/RT. The EMM solution can enforce encryption, passwords, Web usage, remote view, remote control, automated helpdesk, and more. Organizations can choose to deploy AirWatch as a multi-tenant cloud, on-premises or hybrid solution with perpetual and subscription licenses available.

**FUNCTIONALITY: 9**
**MARKET SHARE: 1**

**KEY STRENGTHS:**

- AirWatch by VMware offers comprehensive support for a wide variety of operating systems, including iOS, Android, BlackBerry, Windows Mobile, Windows Phone, Symbian, Apple TV, Mac OS X and Windows PC/RT.

- A variety of deployment models enable businesses to choose the most appropriate option whether it be cloud, on-premises or hybrid. Additionally, businesses choose a subscription-based or perpetual license pricing structure.

- Non-compliant devices managed with AirWatch by VMware are not dependent on a network connection to perform a remote wipe.

- AirWatch offers strong integration with enterprise systems and resources, such as an Active Directory synchronization tool and an SDK for integrating AirWatch security and management features into custom enterprise apps.

- AirWatch provides robust support for email access and management, such as Microsoft Office 365 integration, Microsoft Exchange Server integration, and more.

- AirWatch offers a secure content viewing and collaboration application that integrates with Microsoft SharePoint, network file shares, WebDav, Office 365, OneDrive,
Google Drive, Amazon S3 and 25+ CMIS integrations.

- AirWatch offers a robust unified laptop management solution, so users can manage Mac OS X and Windows laptops alongside smartphones and tablets.

- Secure Web browsing is available with the AirWatch Browser application that can authenticate users, apply blacklists/whitelists, and more. The browser is available for Apple iOS, Google Android and Windows Phone.

**Weaknesses:**

- As one of the most affordable EMM platforms available today, AirWatch may experience increased pricing pressures as the price point for MDM and MAM solutions continues to fall.

**MobileIron**

415 East Middlefield Rd  
Mountain View, CA 94043  
www.mobileiron.com

MobileIron, founded in 2007, focuses on securing and managing mobile apps, content, and devices. MobileIron offers two key EMM solutions: MobileIron Core for on-premises deployments and MobileIron Cloud for cloud-based deployments. MobileIron Cloud offers support for Apple iOS and Google Android and Windows Phone. MobileIron Core offers support for the same platforms, but it adds support for Windows 8.1, Windows Phone, and Mac OS X, plus legacy support for BlackBerry, Symbian, and Windows Mobile. MobileIron’s solutions are managed from a customizable console. For larger deployments, administration can be delegated based on region, device type, or other factors.

**Functionality:** 9  
**Market Share:** 2
**KEY STRENGTHS:**

- MobileIron offers flexible deployment options, including: cloud-based, on-premises, and virtual solutions.

- MobileIron focuses on preserving the native user experience on mobile devices.

- MobileIron’s EMM solution offers protection for Apple Mac OS X devices, making deployment simpler for enterprises that also need to lockdown these workstations.

- MobileIron contains DLP features for mobile devices, such as preventing distribution of certain documents, copy and pasting controls, and more.

- MobileIron seamlessly integrates with multiple email platforms, such as Microsoft Exchange, Microsoft Office 365, and others.

**WEAKNESSES:**

- MobileIron does not offer anti-malware software natively within their EMM platform. Malware detection functionality is only available through third-party integrations.

- MobileIron is a best-of-breed vendor in the EMM space. However, as EMM overlaps with other security, compliance and mobility areas it may become difficult for MobileIron to compete with larger vendors with broader portfolios.

**BLACKBERRY LIMITED**

295 Phillip Street  
Waterloo, Ontario  
Canada N2L 3W8  
www.blackberry.com

BlackBerry Limited, formerly known as Research in Motion (RIM), offers mobile products and solutions aimed at organizations of all sizes, ranging from SMBs to very
large enterprises. BlackBerry delivers EMM functionality via BES12, a cross-platform EMM solution designed to manage enterprise mobility across iOS, Android™, Windows Phone®, Samsung KNOX and BlackBerry devices. BES12, launched in November 2014, introduces a new, scalable architecture and streamlined user experience that consolidates EMM control in a single console. A new attribute-driven, endpoint-permissions model also gives users and administrators control of devices, applications and data, by-person or by group.

**FUNCTIONALITY:** 7  
**MARKET SHARE:** 3

**KEY STRENGTHS:**

- BES12 provides a one-stop vendor approach to EMM that includes support for iOS, Android, Windows Phone and BlackBerry devices.

- BES12 offers management and security for a range of device ownership models on all supported devices, from high-secure corporate lockdown (COBO), to Corporate Owned Personal Enabled (COPE), to BYOD from a single console.

- BlackBerry provides containerization for BlackBerry 10 devices via BlackBerry Balance, which ensures personal data/apps are kept separate from work related apps/data. With BES12 and Secure Work Space, BlackBerry provides application wrapping and containerization technology for iOS and Android devices, which secures data at rest on devices and in transit using BlackBerry’s secure global network infrastructure.

- BlackBerry provides a comprehensive security solution, which includes management servers, the BlackBerry infrastructure, a mobile OS and smartphone devices. This is attractive for organizations looking for complete end-to-end security across all aspects of the mobile experience.

- BlackBerry’s EMM solutions can leverage Microsoft Active Directory to retrieve user profiles and synchronize user groups for streamlined user onboarding, policy creation and application management.
**Weaknesses:**

- While BES12 offers strong EMM and security features across a broad range of devices, the on-premises solution makes sense primarily for organizations that have existing investment in the deployment of BES and BlackBerry smartphones, but also want to allow BYOD while still ensuring effective management across other popular mobile platforms.

- BES12 is primarily focused on providing security and EMM functionality for smartphone devices, while some of its competitors in the EMM space can also extend coverage to laptop devices.

- Despite offering some excellent security technology, BlackBerry continues to see an erosion of its corporate smartphone device installed base due to the BYOD trend.

**Citrix Systems, Inc.**

4988 Great America Parkway  
Santa Clara, CA 95054  
www.citrix.com

Citrix offers an array of mobility, desktop and app virtualization, cloud networking, cloud platforms, collaboration and data sharing solutions. Citrix’s [XenMobile](https://www.citrix.com) solutions include: *XenMobile MDM Edition* and *XenMobile Advanced Edition*. Citrix also offers *XenMobile Enterprise Edition* that combines XenMobile MDM Edition and XenMobile Advanced Edition features. In May 2014, Citrix announced its Citrix Workspace Suite, which incorporates mobility, virtualization, networking and cloud services. Citrix also offers a suite of mobile productivity apps, which include: WorxMail (secure email client), WorxWeb (secure browser), ShareFile (secure file sync and sharing application), WorxNotes (secure note taking application with email and calendar integration for streamlined mobile workflows), WorxEdit (offline editing capabilities on mobile devices), and WorxDesktop (secure remote access). Full versions are available as on-premises or as a SaaS offering.
FUNCTIONALITY: 8
MARKET SHARE: 4

KEY STRENGTHS:

• Citrix offers a comprehensive EMM platform that includes MDM, MAM, and mobile data and content management capabilities. XenMobile offers great deployment and administrative flexibility for enterprise IT.

• Citrix solutions for mobility go beyond XenMobile, integrating with other Citrix products such as XenDesktop and XenApp for virtualized delivery of Windows desktops and apps to mobile devices, as well as Citrix’s portfolio of mobile collaboration apps like GoToMeeting, GoToAssist, ShareFile, Podio, and Talkboard. XenMobile also integrates with other collaboration tools outside of the Citrix portfolio.

• A strong product portfolio of supplementary mobile productivity applications which include solutions for secure email (WorxMail), mobile web browser (WorxWeb), secure document sharing (ShareFile), secure note taking (WorxNotes), mobile and offline editing (WorxEdit), and secure remote access (WorxDesktop).

• One-click live IT support and chat sessions can be initiated directly from a user’s device.

• Granular app policies can be applied across HTML5 and native mobile apps. iOS and Android apps can be wrapped prior to being imported into XenMobile without additional development.

• Citrix’s unified corporate app store provides a single point of access for the delivery of mobile apps, Windows apps, and web/SaaS apps to any device, including: smartphones, tablets, PCs, or MACs.

• Citrix offers comprehensive analytics through its partnership with Aternity. Citrix enables administrators to gather usage and performance analytics for Worx and third-party applications to deliver the best mobile user experience.
Weaknesses:

- Citrix’s EMM solution does not currently support DLP based on specific content type.

- Citrix’s EMM solutions lack anti-malware functionality.

Good Technology

430 N. Mary Ave, Suite 200
Sunnyvale, CA 94085
www.good.com

Good Technology provides secure mobility solutions that secure access to applications and data. Good Technology offers four Enterprise Mobility Management (EMM) suites - Good Management Suite, Good Enterprise Suite, Good Collaboration Suite and Good Mobility Suite. The Good EMM suites enable secure communication, information sharing, document synchronization, and user collaboration through a wide range of mobile devices and apps. All suites are available as cloud, on-premise or hybrid deployment options. In 2014, Good Technology introduced Good Work, an all-in-one mobile collaboration app built on the Good Dynamics platform. It is available as a cloud, on-premise or hybrid deployment.

Functionality: 9
Market Share: 4

Key Strengths:

- Good delivers comprehensive security and meets Common Criteria EAL 4+ certification for iOS and Android. Good-secured apps (e.g., Good Work, Good Access, ISV apps, customer built apps) provide powerful DLP features, including granular control over open-in, data sharing and cut/copy/paste between apps or to the cloud.
• Good Technology solutions support all leading mobile platforms and in all form factors (i.e. cloud, on-premise and hybrid).

• Good Technology’s customizable enterprise app store allows for the distribution of apps to any mobile device, regardless of whether it’s MDM-managed or not. This allows enterprises to easily extend mobile apps to external business partners, contractors and customers.

• Good-secured apps can transparently access behind-the-firewall resources without a VPN, providing a significant benefit to enterprise organizations.

• The Good Dynamics shared services framework enables developers to easily build and deploy mobile apps by publishing their own shared services for reuse and leveraging shared services exposed by ISV partner applications.

• Good’s Mobile Service Management (MSM) provides end-to-end visibility across mobile environments through real-time monitoring.

• The Good Platform has been extended with a wearables framework and container to enable notifications and interactions from wearables such as those running Google’s Android Wear.

• The Good Platform offers split-billing capabilities so that all data and related data expense used by Good apps is allocated to the company and does not show on the employee’s phone bill, whereby eliminating complex expensing, and legal/HR issues.

Weaknesses:

• Good Technology provides sophisticated solutions, which may be somewhat overwhelming for organizations just beginning to deploy mobile security. Good is addressing this by offering Good Management Suite and Good Enterprise Suite (cloud-based or on premise) as entry-level solutions.

• Despite an attractive technology portfolio, Good Technology has not yet been profitable.
SAP

Dietmar-Hopp-Allee 16
69190 Walldorf
Germany
www.sap.com

SAP SE is a German global software developer of enterprise software. SAP is best known for its enterprise resource planning (ERP) solutions, but has expanded in many other software areas, such as data warehousing, business object software, mobile products and in-memory computing. SAP Mobile Secure provides end-to-end management and security of mobile devices, applications, and content. It includes features for Mobile Device and App Management, App Wrapping, and Mobile Content Management.

**FUNCTIONALITY:** 6  
**MARKET SHARE:** 5

**KEY STRENGTHS:**

- SAP offers a robust set of mobile device, application, and content management solutions. Available individually or bundled as a platform. SAP delivers its solutions as on-premises software or as cloud services.

- A convenient feature for users is the mobile-optimized secure Web browser, useful for secure access to mobile web-based apps.

- SAP’s MDM offering provides detailed business intelligence information through the SAP Lumira software. Businesses can report and track activity usage among employees’ mobile devices.

- SAP offers strong integration with enterprise directory services and PKI systems, which eases provisioning, administration and policy management.

- SAP offers strong integration with other SAP systems such as SAP Mobile Platform, SAP Cloud Identity Service and SAP Business Apps. Customers benefit from
configuration and discovery services to help customize, configure and package apps for easy distribution.

**Weaknesses:**

- SAP does not currently provide anti-malware protection.
- SAP Mobile Secure is best used in conjunction with other SAP solutions, such as SAP Cloud Identity Service.

**IBM Corporation**

1 New Orchard Rd.
Armonk, NY 10504
www.ibm.com

IBM is a global technology company that specializes in computers, IT consulting, messaging and collaboration software, and more. In 2013, IBM acquired Fiberlink and renamed the Fiberlink’s MaaS360 platform, as **MobileFirst Protect**, is now a critical component of the **IBM MobileFirst** portfolio. IBM MobileFirst Protect is available in all forms of deployment: on-premises, hybrid, and cloud. It includes mobile device management (MDM), mobile application management (MAM), mobile content management (MCM), mobile expense management (MEM), mobile threat management (MTM), mobile identity management (MIM), secure email, browser, editors, and access to network resources with the use of a web gateway.

**Functionality: 8**

**Market Share: 6**

**Key Strengths:**

- MobileFirst Protect provides multiple ways to separate corporate and personal data on mobile devices. This includes a containerization solution, which includes granular level policy management and data protection controls.
• The MobileFirst Protect Cloud Extender integrates with Microsoft Exchange ActiveSync and does not sit “in-line” with email infrastructure. This means that MobileFirst Protect cannot cause a mail outage or delay. It can also integrate with Microsoft Office 365 and IBM Notes.

• MobileFirst Protect provides a secure web browser web gateway in order to provide organizations access to internal Intranet sites and web application servers without the need for the user to initiate a VPN connection.

• MobileFirst Protect has a secure document sharing application to provide mobile users access to enterprise content. Document access and distribution include the integration of SharePoint, NFS, Box, Google Drive, and other third party solutions. Customers also have the option to leverage their cloud content delivery system, MobileFirst Protect Doc Cloud, to securely host and distribute files.

• MobileFirst Protect can also protect Microsoft Windows and Apple Mac OS X systems, which simplifies deployments for administrators that need to protect mobile devices and workstations.

• MobileFirst Protect has added malware detection and remediation with the integration of IBM Trusteer for both corporate owned and BYOD users.

**Weaknesses:**

• MobileFirst Protect subscription based pricing structure will be more costly in the long run when compared to perpetual license based solutions.

• MobileFirst Protect is most effective and offers deeper functionality when integrated with a number of other IBM solutions, such as IBM Trusteer.

• MobileFirst Protect is losing some mindshare since the IBM acquisition as it is now part of IBM’s larger mobility portfolio.
SOPHOS

3 Van de Graaff Drive
Burlington, MA 01803
www.sophos.com

Sophos offers a range of security solutions that include encryption, endpoint, web, email, mobile and network security. Sophos protects mobile devices with two solutions: **Sophos Mobile Control (SMC) – Standard** which provides security for Apple iOS, Google Android, Windows Phone 8 devices, and **Sophos Mobile Control – Advanced** an extended offering for protection of corporate data on mobile devices. Advanced includes all features of Sophos Mobile Control - Standard and adds: **Sophos Mobile Security** an anti-virus and anti-malware solution, designed to protect users in Android devices from mobile malware, **Sophos Secure Workspace** an app to provide access to corporate documents, and **Sophos Mobile SDK** which adds security and control to company apps via geo-location or time based policies, additional authentication and jailbreak/rooting detection.

**FUNCTIONALITY: 7**

**MARKET SHARE: 6**

**KEY STRENGTHS:**

- Sophos’ offers an easy to understand one user/one license pricing structure. Organizations are charged one fee regardless of how many devices an employee uses.

- Sophos Mobile Control gives administrators an easy to understand, web-based user interface. This is key for small to mid-market customers and with limited administrative support

- Sophos offers strong malware and web protection functionality within their EMM solution.

- The Sophos Secure Workspace solution gives users a tool for securely adding, viewing and editing encrypted documents stored in the cloud. It currently supports Dropbox, Microsoft OneDrive, Google Drive, Egnyte, Mediacenter and WebDAV (e.g. OwnCloud, Windows Server).
• Sophos Mobile Control can integrate with Sophos UTM and endpoint protection solutions for a comprehensive endpoint security strategy.

**Weaknesses:**

• Sophos Secure Workspace is only available for Apple iOS and Google Android devices.

• Sophos offers an SDK for app data protection, but does not support the wrapping of apps.

• Sophos has limited extended MDM support for Google Android devices from certain manufacturers, such as Motorola and HTC.

• Integration with Microsoft Office 365 is not currently offered.

• Mobile app analytics could be improved.

**Kaspersky Lab**

39A Leningradsky Highway
Moscow 125212
Russia
www.kaspersky.com

Kaspersky Lab, a privately held company founded in 1997, offers security solutions targeted at the consumer and enterprise market. **Kaspersky Security for Mobile** is a mobile security and management solution aimed at the needs of corporate customers, across all sizes from SMBs to very large customers. The latest version **Kaspersky Security 10 for Mobile** is available as a standalone solution, or bundled with Kaspersky’s business security suites: Endpoint Security for Business (Select/Advanced), or Total Security for Business. Kaspersky Security for Mobile is centrally managed from a single administration console, **Kaspersky Security Center**, which supports centralized
management of mobile devices as well as other IT resources across the corporate network.

**FUNCTIONALITY:** 7  
**MARKET SHARE:** 8

**KEY STRENGTHS:**

- Kaspersky has established a large installed base of enterprise customers, which is a key differentiator that enables Kaspersky to sell their mobile solutions to their existing customer base.

- Kaspersky’s EMM solutions provide support for a broad range of mobile devices, including: iOS, Android and Windows Phone.

- Kaspersky’s roots in the enterprise security market enable them to offer native mobile security functionality without the need to deploy a third-party security solution that other pure-play MDM vendors require.

- Kaspersky offers secure Web browsing as a part of their MDM solution, which enables filtering of Web content based on categories, such as gambling or entertainment, as well as anti-phishing protection.

- Kaspersky includes its own anti-malware protection, anti-phishing, anti-theft, encryption, and containerization (app wrapping) to separate personal and corporate data.

**WEAKNESSES:**

- Kaspersky’s EMM solutions are currently delivered as on-premises software. Cloud-based services, however, are on the roadmap.

- Feature sets across all supported mobile platforms are not identical. Businesses with BYOD environments and several different mobile operating systems within their corporate setting may find some difficulties in managing these devices.
SOTI
5700 Hurontario St.
Suite 1100, Mississauga,
Ontario L5R 3G5
Canada
www.soti.com

SOTI provides enterprise mobility solutions for managing, securing, supporting and tracking mobile devices, desktop computing devices, and connected peripherals. SOTI unifies mobility management from a single management console, removing the complexity from managing a multi OS, multi-vendor, and multi-purpose mobile environment. SOTI’s EMM offering, MobiControl, supports Apple iOS, Google Android, Microsoft Windows Mobile devices, as well as computers running Apple and Microsoft Desktop and Server operating systems. MobiControl can be deployed in the cloud, on-premise, or as a managed solution. Key components of MobiControl include: mobile device management, mobile security management, mobile content management, mobile application management, and mobile email management. The solution provides a single pane of glass for management of smartphones, tablets, laptops, printers, scanners, wearables, and other connected devices, hence unifying management and support of the growing spectrum of connected endpoints.

**FUNCTIONALITY:** 9  
**MARKET SHARE:** 9

**KEY STRENGTHS:**

- MobiControl is available in different deployment options, including: cloud-based, on-premises, and managed solutions.

- SOTI has a well-established presence in the rugged device market which gives the vendor an advantage as these rugged device customers transition to Apple iOS, Google Android, and Windows Phone devices.

- SOTI’s SKD for Apple iOS devices enables organizations to wrap iOS apps for additional MAM functionality. Administrators are able to view and access the
wrapped application’s file directory remotely over the air.

- SOTI includes Web filtering in its MobiControl solution that can create white/black lists for websites, browsing rules by category, and more.

- SOTI offers robust FIPS certified encryption for data on mobile devices.

**Weaknesses:**

- While SOTI offers EMM for a variety of mobile platforms, their strong emphasis on Google Android devices gives the false impression to customers that the vendor does not have strong support for iOS or other popular platforms.

- SOTI needs to raise its market visibility outside of the rugged device market to gain more mindshare with enterprise EMM deployments.

**Specialists**

**McAfee**

2821 Mission College Boulevard  
Santa Clara, CA 95054  
www.mcafee.com

McAfee, a wholly owned subsidiary of Intel Corporation, delivers a wide variety of security products for endpoints, email, Web, data, data centers, and databases. **McAfee Enterprise Mobility Management (McAfee EMM)** is the vendor’s mobile security solution. It can be deployed separate from other McAfee security solutions. However, McAfee EMM also integrates with McAfee ePolicy Orchestrator (McAfee ePO) management software. This allows single-pane of glass management of mobile users and devices along with traditional endpoints. McAfee EMM is also available bundled with McAfee’s Complete Endpoint Protection suite. McAfee EMM provides protection for Apple iOS, Android, and Windows Phone. It provides slightly different sets of features for the different mobile platforms under management.
**FUNCTIONALITY:** 5  
**MARKET SHARE:** 6

**KEY STRENGTHS:**

- McAfee EMM benefits from McAfee’s strength in malware detection.
- McAfee EMM fits seamlessly with McAfee ePolicy Orchestrator for a single-pane of glass management experience.
- McAfee EMM is available as a standalone solution or bundled with McAfee’s enterprise endpoint security solution for a comprehensive endpoint security strategy.

**WEAKNESSES:**

- McAfee EMM provides somewhat different features for different mobile platforms, for instance containerization is only available for Android devices.
- Many of the benefits of McAfee EMM are visible only when it is deployed in the context of other McAfee security solutions, such as ePolicy Orchestrator and McAfee’s endpoint solutions.

**SYMANTEC**

350 Ellis St  
Mountain View, CA 94043  
www.symantec.com

Symantec provides a broad range of security solutions, which include Enterprise Mobility Management (EMM), archiving, eDiscovery, messaging security, and more. In Oct 2014, Symantec launched a new integrated, modular product called **Symantec Mobility: Suite**. Symantec Mobility: Suite is an integrated, modular Enterprise Mobility Management (EMM) solution that is made up of the following modules: **Symantec Mobility: Device Management** - offers advanced management features for Apple iOS, Google Android,
and Microsoft Windows Phone devices; *Symantec Mobility: Workforce Apps* allows IT to give employees apps that include Work Mail, Work Web and Work File, a secure file editor and content management app for accessing corporate files; *Symantec Mobility: Application Management* which enables IT administrators to deploy, secure, and manage mobile apps beyond essential productivity apps on corporate-owned, and employee-liable devices. Businesses can also wrap any in-house, third-party, or web app by creating and enforcing policies on a per-app basis; *Symantec Mobility: Threat Protection* which leverages technology and intelligence from Norton Mobile Insight, a dynamic machine-learning system that constantly downloads and analyzes new or updated Android apps across 200+ Android app stores, including Google Play.

*Functionality: 4*

*Market Share: 7*

*Key Strengths:*

- Symantec Mobility: Suite is an integrated, flexible solution. Through a single Web-based console, enterprises can manage devices, apps, content, secure data and apply threat protection. Companies can license either the entire Suite or only the modules they need. Since it’s an integrated solution, enterprises can easily add modules, as their mobility needs change.

- Symantec offers its Mobility Suite on a per-user basis regardless of the number of devices. Enterprises with users that utilize multiple mobile devices will benefit from this pricing structure.

- The Symantec Mobility: Suite lets organizations containerize apps to keep corporate data separate from personal data. Organizations can enforce policies on a per-app basis and apps can be updated without re-wrapping.

- Symantec’s mobile products have robust encryption capabilities and can offer FIPS-certified encryption through integration with its encryption solution.

- Symantec offers a secure content delivery system via Symantec Mobility: Workforce Apps that can give employees access to applications, documents, links, and more.
**Weaknesses:**

- Symantec only provides basic MDM for Windows Phone and Windows Mobile devices through their Mobility Suite solution.

- Device level analytics is somewhat basic and could be improved.

**Trend Micro**

Shinjuku MAYNDS Tower, 1-1,
Yoyogi 2-Chome, Shibuya-ku
Tokyo, 151-0053, Japan
www.trendmicro.com

Founded in 1988, Trend Micro provides multi-layered network and endpoint security solutions, which include email, Web, and endpoint security. **Trend Micro’s Mobile Security** provides visibility and control of mobile devices, apps, and data through a single built-in console. It combines Mobile Device Management (MDM), Mobile Application Management (MAM), Application Reputation Services, and Device Antivirus (for Android) into a single solution. Trend Micro Mobile Security integrates with the Trend Micro Control Manager console, allowing customers to centralize policy and management across Trend Micro OfficeScan endpoint security as well as other Trend Micro solutions, for a single-pane-of-glass management approach.

**Functionality:** 3
**Market Share:** 7

**Key Strengths:**

- Trend Micro supports all leading mobile device platforms.

- Trend Micro Mobile Security integrates with the vendor’s Trend Micro Control Manager console to provide a single pane-of-glass management experience across mobile and endpoint devices.
• Trend Micro Mobile Security is available standalone or bundled with Trend Micro’s enterprise security suites.

• Trend Micro Mobile Security benefits from Trend Micro’s Mobile Application Reputation Service to ensure app safety.

WEAKNESSES:

• Trend Micro Mobile Security is really intended to be used in the context of Trend Micro’s full suite of endpoint security solutions.

• Trend Micro Mobile Security does not support containerization or app wrapping to allow users to keep personal and business data separate.

• Analytics and reporting is minimal compared to other EMM solutions.
The Radicati Group, Inc. is a leading Market Research Firm specializing in emerging IT technologies. The company provides detailed market size, installed base and forecast information on a worldwide basis, as well as detailed country breakouts, in all areas of:

- Email
- Security
- Instant Messaging
- Unified Communications
- Identity Management
- Web Technologies

The company assists vendors to define their strategic product and business direction. It also assists corporate organizations in selecting the right products and technologies to support their business needs.

Our market research and industry analysis takes a global perspective, providing clients with valuable information necessary to compete on a global basis. We are an international firm with clients throughout the US, Europe and the Pacific Rim.

The Radicati Group, Inc. was founded in 1993, and is headquartered in Palo Alto, CA, with offices in London, UK.

Consulting Services:

The Radicati Group, Inc. provides the following Consulting Services:

- Management Consulting
- Whitepapers
- Strategic Business Planning
- Product Selection Advice
- TCO/ROI Analysis
- Multi-Client Studies

To learn more about our reports and services, please visit our website at www.radicati.com.
MARKET RESEARCH PUBLICATIONS

The Radicati Group, Inc. develops in-depth market analysis studies covering market size, installed base, industry trends and competition. Current and upcoming publications include:

Currently Released:

<table>
<thead>
<tr>
<th>Title</th>
<th>Released</th>
<th>Price*</th>
</tr>
</thead>
<tbody>
<tr>
<td>Social Networks Statistics Report, 2015-2019</td>
<td>Mar. 2015</td>
<td>$3,000.00</td>
</tr>
<tr>
<td>Email Statistics Report, 2015-2019</td>
<td>Mar. 2015</td>
<td>$3,000.00</td>
</tr>
<tr>
<td>Instant Messaging Market, 2015-2019</td>
<td>Mar. 2015</td>
<td>$3,000.00</td>
</tr>
<tr>
<td>Mobile Statistics Report, 2015-2019</td>
<td>Feb. 2015</td>
<td>$3,000.00</td>
</tr>
<tr>
<td>Cloud Business Email Market, 2014-2018</td>
<td>Oct. 2014</td>
<td>$3,000.00</td>
</tr>
<tr>
<td>Email Market, 2014-2018</td>
<td>Oct. 2014</td>
<td>$3,000.00</td>
</tr>
<tr>
<td>Messaging Platforms Market, 2014-2018</td>
<td>Sept. 2014</td>
<td>$3,000.00</td>
</tr>
<tr>
<td>Corporate Web Security Market, 2014-2018</td>
<td>Sept. 2014</td>
<td>$3,000.00</td>
</tr>
<tr>
<td>Enterprise Mobility Management Market, 2014-2018</td>
<td>June 2014</td>
<td>$3,000.00</td>
</tr>
<tr>
<td>Office 365, Exchange Server and Outlook Market Analysis, 2014-2018</td>
<td>Apr. 2014</td>
<td>$3,000.00</td>
</tr>
</tbody>
</table>

* Discounted by $500 if purchased by credit card.

Upcoming Publications:

<table>
<thead>
<tr>
<th>Title</th>
<th>To Be Released</th>
<th>Price*</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information Archiving Market, 2015-2019</td>
<td>May 2015</td>
<td>$3,000.00</td>
</tr>
<tr>
<td>APT Prevention Market, 2015-2019</td>
<td>May 2015</td>
<td>$3,000.00</td>
</tr>
<tr>
<td>Enterprise Mobility Management Market, 2015-2019</td>
<td>May 2015</td>
<td>$3,000.00</td>
</tr>
</tbody>
</table>

* Discounted by $500 if purchased by credit card.

All Radicati Group reports are available online at [http://www.radicati.com](http://www.radicati.com).