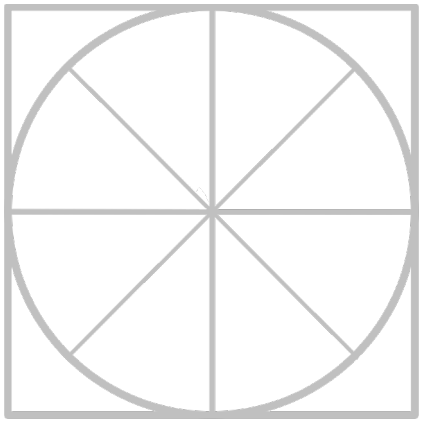
The Radicati Group, Inc.
Palo Alto, CA 94301
Phone: (650) 322-8059
www.radicati.com

THE RADICATI GROUP, INC.

Enterprise Mobility Management - Market Quadrant 2016



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

April 2016

Radicati Market Quadrant[SM] is copyrighted April 2016 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[SM] 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[SM] 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.

TABLE OF CONTENTS

RADICATI MARKET QUADRANTS EXPLAINED 2
MARKET SEGMENTATION – ENTERPRISE MOBILITY MANAGEMENT 4
EVALUATION CRITERIA 6
MARKET QUADRANT – ENTERPRISE MOBILITY MANAGEMENT 9
KEY MARKET QUADRANT HIGHLIGHTS 10
ENTERPRISE MOBILITY MANAGEMENT - VENDOR ANALYSIS 10
TOP PLAYERS 10
TRAIL BLAZERS 29
SPECIALISTS 32
MATURE PLAYERS 38

==========

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. ***Top Players*** – These are the current market leaders with products that offer, both breadth and depth of functionality, as well as posses a solid vision for the future. Top Players shape the market with their technology and strategic vision. Vendors don't 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 to innovate.

2. ***Trail Blazers*** – These vendors offer advanced, best of breed technology, in some areas of their solutions, but don't necessarily have all the features and functionality that would position them as Top Players. Trail Blazers, however, have the potential for "disrupting" the market with new technology or new delivery models. In time, these vendors are most likely to grow into Top Players.

3. ***Specialists*** – This group is made up of two types of companies:

    a. Emerging players that are new to the industry and still have to develop some aspects of their solutions. These companies are still developing their strategy and technology.

    b. Established vendors that offer a niche product.

4. ***Mature Players*** – These vendors are large, established vendors that may offer strong features and functionality, but have slowed down innovation and are no longer considered "movers and shakers" in this market 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, they may choose to slow development on existing products.

Copyright © April 2016, The Radicati Group, Inc. Reproduction Prohibited

b. In other cases, a vendor may simply have become complacent and be out-developed by hungrier, more innovative Trail Blazers or Top Players.

c. Companies in this stage will either find new life, reviving their R&D efforts and move 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 solutions adding features and functionality, it will move vertically along the "y" functionality axis.

The horizontal "x" strategic vision axis reflects a vendor's understanding of the market and their strategic direction plans. It is common for vendors to move in the quadrant, as their products evolve and market needs change.

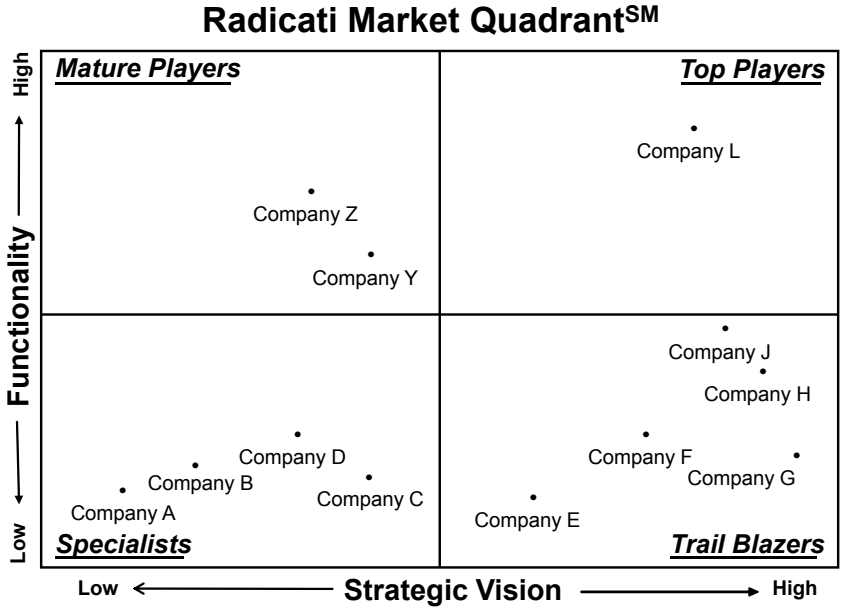


Figure 1: Sample Radicati Market Quadrant

Copyright © April 2016, The Radicati Group, Inc. Reproduction Prohibited

MARKET SEGMENTATION – ENTERPRISE MOBILITY MANAGEMENT

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: *BlackBerry, Citrix, IBM, Kaspersky Lab, Microsoft, MobileIron, SAP, Sophos, SOTI, Symantec, Trend Micro*, *VMware AirWatch,* 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:

  - *Mobile Device Management (MDM)* – device level management features such as: remote configuration; remote wipe; selective wipe; remote locking, and more.

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

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

  - *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

Copyright © April 2016, The Radicati Group, Inc. Reproduction Prohibited

Enterprise Mobility Management market in the context of BYOD office employee use.

- Worldwide revenues for the EMM market will total over $1.7 billion by year-end 2016. This figure is expected to grow to over $4.5 billion by year-end 2020. An average annual growth rate of 27% over the next four years. Figure 1, shows the worldwide revenue for the Enterprise Mobility Management market from 2016 to 2020.

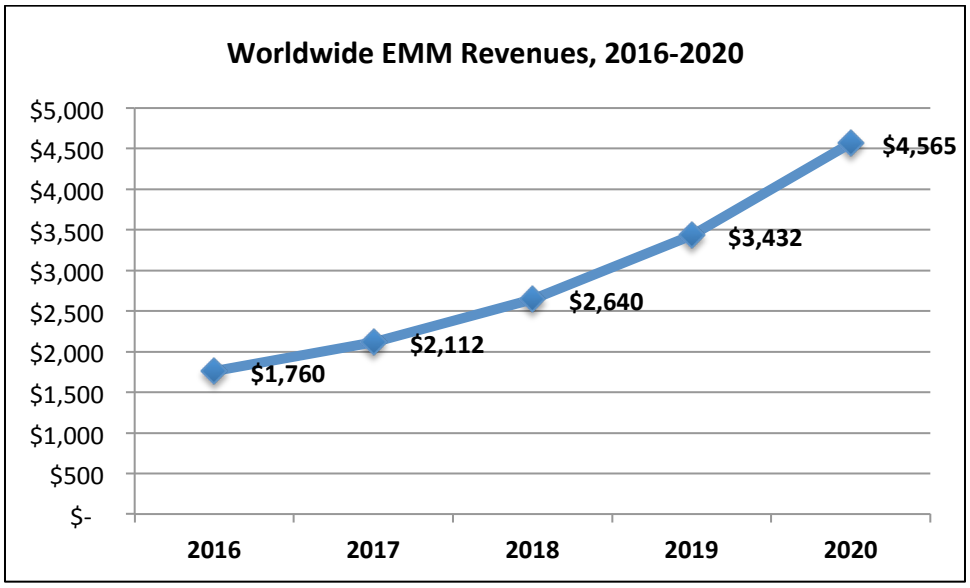


Figure 2: Worldwide Enterprise Mobility Management Revenue, 2016-2020

Copyright © April 2016, The Radicati Group, Inc. Reproduction Prohibited

EVALUATION CRITERIA

Vendors are positioned in the quadrant according to two criteria: *Functionality* and *Strategic Vision*.

Functionality is assessed based on the breadth and depth of features of each vendor's solution. All features and functionality do not necessarily have to be the vendor's own original technology, but they should be integrated and available for deployment when the solution is purchased.

Strategic Vision refers to the vendor's strategic direction, which comprises: a thorough understanding of customer needs, ability to deliver through attractive pricing and channel models, solid customer support, and strong on-going innovation.

To be considered a complete EMM solution, vendors should provide comprehensive feature sets in the areas of MDM, MAM, Mobile Security, and Mobile Content Management.

Vendors in the *EMM* space are evaluated according to the following key features and capabilities:

- **Mobile OS Support** – support for a variety of mobile OS's, including: Apple iOS, Google Android, Windows Phone, 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.

Copyright © April 2016, The Radicati Group, Inc. Reproduction Prohibited

- **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, and more.

- **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 and/or content-aware data loss prevention (DLP).

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

- **Administration** – easy, single pane of glass management across all users and network resources.

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

In addition, for all vendors we consider the following aspects:

- *Pricing* – what is the pricing model for their solution, is it easy to understand and allows customers to budget properly for the solution, as well as is it in line with the level of functionality being offered, and does it represent a "good value".

- *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.

- *Professional Services* – does the vendor provide the right level of professional services for planning, design and deployment, either through their own internal teams, or through partners.

Copyright © April 2016, The Radicati Group, Inc. Reproduction Prohibited

***Note**: On occasion, we may place a vendor in the Top Player or Trail Blazer category even if they are missing one or more features listed above, if we feel that some other aspect(s) of their solution is particularly unique and innovative.*

Copyright © April 2016, The Radicati Group, Inc. Reproduction Prohibited

MARKET QUADRANT – ENTERPRISE MOBILITY MANAGEMENT

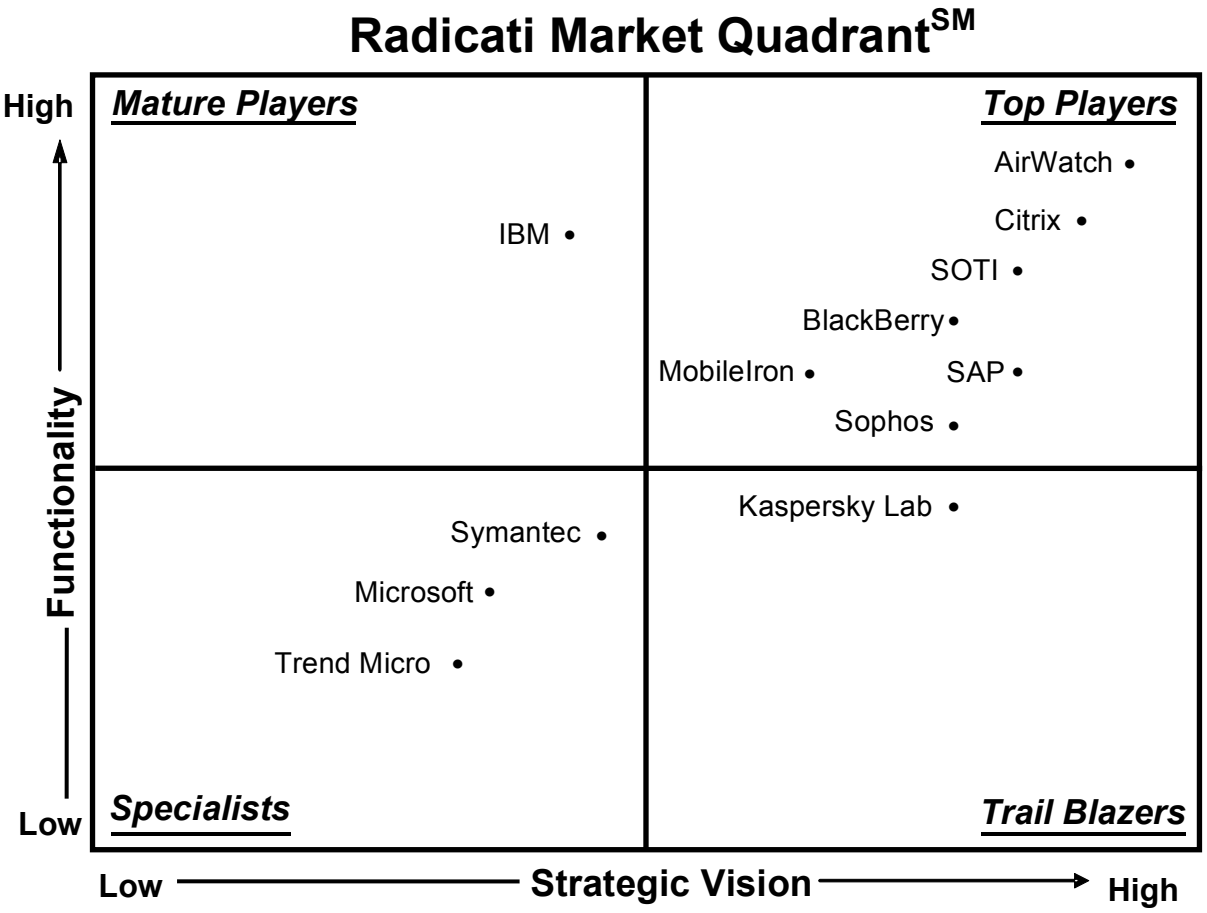


Figure 3: Enterprise Mobility Management Market Quadrant, 2016

· Radicati Market Quadrant℠ is copyrighted April 2016 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.

Copyright © April 2016, The Radicati Group, Inc. Reproduction Prohibited

KEY MARKET QUADRANT HIGHLIGHTS

- The **Top Players** in the Enterprise Mobility Management market are *VMware AirWatch, Citrix, SOTI, BlackBerry, SAP, MobileIron,* and *Sophos*.
- The **Trail Blazers** quadrant includes *Kaspersky Lab*.
- The **Specialists** quadrant includes *Symantec, Microsoft,* and *Trend Micro*.
- The **Mature Players** quadrant includes *IBM*.

ENTERPRISE MOBILITY MANAGEMENT - VENDOR ANALYSIS

TOP PLAYERS

VMWARE AIRWATCH

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

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 solutions are deployed by customers of all sizes; ranging from SMBs to large enterprises.

SOLUTIONS

AirWatch Enterprise Mobility Management includes mobile device, application, identity, content, browsing, and email management solutions for both corporate-owned and BYOD deployments. The AirWatch solution unifies endpoint management and security for smartphones,

Copyright © April 2016, The Radicati Group, Inc. Reproduction Prohibited

tablets, laptops, printers and IoT devices across operating systems, including Android, Apple iOS, BlackBerry, Chrome, Mac and Windows, through a single management console. The EMM solution provides device lifecycle management from enrollment, profile configuration, security policies and remote support. The AirWatch platform also provides application lifecycle management and various solutions for app containerization and development. Organizations can choose to deploy the AirWatch EMM solution as a multi-tenant SaaS, on-premises or hybrid with perpetual and subscription licensing models.

Optionally, organizations can deploy **AirWatch Content Locker**, a mobile content management solution that protects sensitive content in a corporate container and provides users with a central application to securely access and collaborate on the latest documents from their mobile devices. It provides mobile users with an aggregated view of corporate content repositories and user content in a single mobile app.

AirWatch Container provides apps based management for end users requiring access to corporate applications without device management. AirWatch Container enables a secure workspace with complete separation of corporate and personal data. This allows organizations to standardize enterprise security and data loss prevention strategies across mobile devices through a containerization approach.

VMware launched **VMware Workspace ONE**, a secure enterprise platform that delivers and manages device apps while integrating identity, applications and enterprise mobility. Key features include: consumer-grade self-service access; BYOD or corporate-owned device choice; secure productivity apps such as mail, calendar, docs and social; data security and endpoint compliance; as well as real-time app delivery and automation.

STRENGTHS

- AirWatch offers comprehensive support for a wide variety of operating systems, including Apple iOS, Android, BlackBerry, Windows, Chrome OS, and Mac OS X.

- 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 per user or device.

Copyright © April 2016, The Radicati Group, Inc. Reproduction Prohibited

- Non-compliant devices managed with AirWatch 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 30+ 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 VMware 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

- AirWatch offers highly sophisticated solutions, which go well beyond Enterprise Mobility Management to offer a full mobile computing environment, however this may be a bit overwhelming for customers that are looking simply for an add-on EMM solution for mobile security and management purposes.

- Different components of a full AirWatch solution set may not all be at the same level of maturity, customers should be careful to investigate the exact feature set and deployment model they will be using.

- AirWatch does not provide its own DLP technology, but supports the ICAP protocol, which allows easy integration with third party DLP solutions.

Copyright © April 2016, The Radicati Group, Inc. Reproduction Prohibited

- As one of the most affordable EMM platforms available today, AirWatch will experience increased pricing pressures as MDM and MAM solutions continue to be folded natively into mobile operating systems and devices.

CITRIX SYSTEMS, INC.

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

Founded in 1989 and headquartered in Santa Clara, California, Citrix offers an array of mobility, desktop and app virtualization, cloud networking, cloud platforms, collaboration and data sharing solutions.

SOLUTIONS

Citrix's XenMobile 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 2014, Citrix announced its Citrix Workspace Suite, which incorporates mobility, virtualization, networking, data, and some cloud services. In 2015, Citrix announced Citrix Workspace Cloud, which allows for the entire solution to be delivered from the cloud.

Citrix also offers a suite of mobile productivity apps, available as on-premises or as a SaaS offerings, which include:

- *WorxMail* – secure email client.
- *WorxWeb* – secure browser.
- *ShareFile* – secure file sync and sharing application, which allows mobile users to edit and annotate documents directly on the mobile device, with complete audit trails for information access.
- *WorxNotes* – a secure note taking application, with email and calendar integration for streamlined mobile workflows.
- *WorxTasks* – secure task management application integrated with email and calendar.

Copyright © April 2016, The Radicati Group, Inc. Reproduction Prohibited

- *WorxEdit* – offline editing capabilities on mobile devices.
- *ShareConnect* – secure remote access.
- *WorxForms* – due later in 2016, a secure app for creating, publishing, populating, and storing digitized version of commonly used forms with no coding required.

Citrix has a strong focus on end user and administrator user experience. For the end users, XenMobile provides a suite of Worx Apps that are tightly integrated out of the box for a seamless experience, and support single sign-on. The XenMobile administrative console offers a unified platform for IT administrators to enforce policies on mobile devices, applications and data.

Citrix XenMobile provides a secure and contained environment for enterprise apps and data without requiring MDM (device) enrollment.

STRENGTHS

- Citrix offers a comprehensive EMM platform that includes MDM, MAM, and mobile data and content management capabilities, and is available on-premises or in the cloud.

- XenMobile supports all of its advanced Mobile Application Management (MAM) security features, including local data storage encryption, without requiring MDM enrollment.

- 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 mobile productivity applications (i.e. WorxMail, WorxWeb, ShareFile, WorxNotes, WorxTasks, WorxEdit and WorxForms).

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

Copyright © April 2016, The Radicati Group, Inc. Reproduction Prohibited

- Granular app policies can be applied across native mobile apps, HTML5 and other Web apps, SaaS apps, and Windows Desktop apps. iOS and Android apps can be wrapped prior to being imported into XenMobile without the need for additional development work.

- Citrix offers comprehensive analytics through its partnership with Aternity. Citrix enables administrators to gather usage and performance analytics for Worx and third-party applications.

- Citrix XenMobile provides capabilities to enhance Microsoft Office 365, for instance users can get Office 365 apps delivered through a corporate app store.

WEAKNESSES

- Citrix's EMM solution is best when deployed in the context of Citrix's virtualized desktop and server environment.

- Citrix's ShareFile solution does not currently support DLP based on specific content type, but Citrix partners with a number of DLP vendors to achieve this functionality.

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

- Citrix EMM solutions tend to be slightly pricier than solutions from competing vendors.

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 of managing a multi

Copyright © April 2016, The Radicati Group, Inc. Reproduction Prohibited

OS, multi-vendor, and multi-purpose mobile environment. Founded in 1995, SOTI is headquartered in Ontario, Canada and has regional offices in the UK, Germany, UAE, Australia, and India.

SOLUTIONS

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. The key components of MobiControl include: mobile device management, mobile security management, mobile content management, mobile application management, mobile email management, telecom expense management, and secure web browsing.

Key integrated features include built-in remote helpdesk tools (including remote control and mobile helpdesk chat), rapid staging and provisioning, URL filtering (including whitelisting and blacklisting), anti-virus/anti-malware, remote diagnostics, and more.

The solution provides a single pane of glass for management of smartphones, tablets, laptops, printers, scanners, wearables, digital kiosks, ATM machines and other connected devices, hence unifying management and support of the growing spectrum of connected endpoints.

SOTI has announced extended support for connected peripherals, and continues to work with Google to deploy and redefine Android for Work.

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

Copyright © April 2016, The Radicati Group, Inc. Reproduction Prohibited

file directory remotely over the air, as well as conduct two-way chat between user and support administrator.

- SOTI includes Web filtering in its MobiControl solution, and its secure browser, also provides data loss prevention technologies.

- SOTI offers FIPS certified encryption for data on mobile devices, as well as enforces encryption on supported operating systems.

- SOTI's offering in the Windows Desktop space allows mobile Point of Service (POS) devices to deploy kiosk modes that restrict access to only approved applications, without needing to modify the Windows operating system.

WEAKNESSES

- While SOTI offers EMM for a variety of mobile platforms, they are best known for their strong emphasis on Google Android devices.

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

- Mobile app analytics and reporting could be improved.

- SOTI does not offer its own app containerization technology, rather it relies on the device native OS containerization solutions, as well as third-party technologies.

Copyright © April 2016, The Radicati Group, Inc. Reproduction Prohibited

BLACKBERRY

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

BlackBerry is a mobile communications vendor founded in 1984. BlackBerry offers mobile products and solutions aimed at organizations of all sizes, ranging from SMBs to very large enterprises. BlackBerry is headquartered in Waterloo, Ontario, Canada and operates offices in North America, Europe, Asia Pacific, and Latin America.

In 2015, BlackBerry acquired several other vendors with offerings in the EMM market, including: Good Technology, developer of mobile security and containerization technology; and WatchDox, provider of Enterprise File Sync and Share (EFSS) with integrated Digital Rights Management (DRM).

SOLUTIONS

BlackBerry offers five Enterprise Mobility Management (EMM) suites – **Good Secure Management Suite**, **Good Secure Enterprise Suite**, **Good Secure Collaboration Suite, Good Secure Mobility Suite,** and **Good Secure Content 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.

- *Good Secure Management Suite* - helps provide an enterprise app store, and offers secure access to the corporate intranet and documents behind the corporate firewall.

- *Good Secure Enterprise Suite* - governs application usage and includes all Good Management Suite features, as well as secure email, contacts, calendar, corporate intranet access, web browsing, and container to separate corporate and personal information.

- *Good Secure Collaboration Suite* - helps mobilize content, deploy business apps and deliver enhanced collaboration, it includes all Good Enterprise Suite features, as well as Mobile

Copyright © April 2016, The Radicati Group, Inc. Reproduction Prohibited

Content Management (MCM) for documents, business intelligence, customer records and more.

- *Good Secure Mobility Suite* - supports new custom developed apps and includes all Good Collaboration Suite features, as well as unlimited licenses to deploy custom-developed Good-secured apps, enterprise mobile back end as a service (MBaaS) capabilities, and more.

- *Good Secure Content Suite* – enables document security and includes all Good Mobility Suite features, as well as Secure Enterprise File Synchronization and Sharing (EFSS), embedded digital rights management (DRM) protection, controls on access, view, edit, copy, print or forward files, and more.

Key capabilities and products within these suites include:

BES12 - provides a cross-platform way to set policies solution across iOS, Android™, Windows, Windows Phone®, Samsung KNOX, Android for Work, Mac OS X and BlackBerry devices. It delivers a scalable architecture and streamlined user experience that consolidates EMM control in a single console. It offers an attribute-driven, endpoint-permissions model, which gives users and administrators control of devices, applications and data, by-person or by group.

Good Work - an all-in-one mobile collaboration app built on the Good Dynamics platform. Good Work provides a fully integrated, collaboration experience similar to desktop capabilities. It integrates email, calendar, contacts, presence from Microsoft Skype for Business and/or Jabber, directory information from Active Directory, and documents from multiple repositories into a single experience. It is available as a cloud, on-premise or hybrid deployment.

Good Dynamics Secure Mobility Platform - enables companies to support complete mobile app lifecycle management, from building and deploying containerized apps to the ongoing management and support of those apps, devices, and the associated infrastructure. It includes app containerization, a shared services framework and capabilities for application reliability.

Trusted Security Architecture - Good-secured apps (i.e., apps in the Good Enterprise and Collaboration Suites, the Good ISV App Ecosystem and customer-built Good-secured apps)

Copyright © April 2016, The Radicati Group, Inc. Reproduction Prohibited

automatically take advantage of Good's trusted security architecture, which includes FIPS-certified strong encryption, advanced data protection and Common Criteria EAL 4+ certification.

Good ISV App Ecosystem - Good Technology has an extensive customer and ISV ecosystem, which securely interact with each other through the Good Dynamics Shared Services Framework.

STRENGTHS

- BlackBerry provides a one-stop vendor approach to EMM that includes support for iOS, Android, Windows, Windows Phone, Mac OS X, BlackBerry devices, as well as support for Samsung KNOX and Android for Work.

- BlackBerry 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 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.

- BlackBerry solutions support all form factors (i.e. cloud, on-premise and hybrid).

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

- 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.

- 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.

Copyright © April 2016, The Radicati Group, Inc. Reproduction Prohibited

- 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

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

- BlackBerry does offer a single pane of glass for management. However, some integration issues still exist between the BlackBerry and Good technology stacks. BlackBerry is working to address this in the 2016 timeframe.

- Despite an attractive technology portfolio, BlackBerry continues to see an erosion of its BlackBerry OS base. BlackBerry is addressing by investing in cross-platform EMM, including a number of acquisitions that extend its technology portfolio, as well as offering Android-based devices.

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.

Copyright © April 2016, The Radicati Group, Inc. Reproduction Prohibited

SOLUTIONS

SAP Mobile Secure provides end-to-end management and security of mobile devices, applications, and content. It includes the following functionality:

- *Mobile Device and App Management* – SAP Mobile Secure offers mobile device and app management for the latest versions of Apple iOS, Google Android (including Android for Work and Samsung SAFE and Samsung KNOX), and all flavors of Windows devices. Administrators can separate personal and corporate data on devices, provision devices and deliver apps OTA, extend corporate security policies, remote lock and/or wipe devices, and more. MDM is available as an on-premises solution or as a cloud-based service. SAP Mobile Place, is a brand-able, localizable multichannel enterprise app store where a company's employees, partners and customers can optionally enroll in device management, provision mobile apps and set up related services, such as network access, email and identity, and more.

- *App Containment* – SAP Mobile Secure offers mobile application level security enabling administrators the ability to embed an SDK or to 'app wrap' granular security and data leakage policies around mobile web apps and native apps. SAP offers 14 application protection policies for iOS and Android platforms. SAP includes a secure browser for web applications enabling access to Microsoft SharePoint, corporate intranet sites, web apps, and portals. Additionally SAP provides integration with Mocana's Atlas Platform as well as single sign-on for wrapped apps. Mobile app protection can be deployed either on-premises or as a cloud service.

- *Mobile Content Management* – SAP Mobile Secure provides mobile content management and secure access to business documents. Users can access personal documents or corporate content stored within SAP's ERP systems and from any CMIS compliant Content Management System including Sharepoint, Documentum, OpenText, FileNet and others, from their Apple iOS, Google Android, Microsoft Windows and Apple Macintosh desktop and laptop clients, and HTML5 user interfaces. Mobile content management is available as an on-premises solution or as a cloud service.

Copyright © April 2016, The Radicati Group, Inc. Reproduction Prohibited

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.

- SAP's EMM solution provides a single console for mobility management of both MDM managed and non-MDM managed devices.

- 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 cloud IDP's (like OKTA, PING, and others), enterprise directory services and PKI systems, which eases provisioning, administration and policy management.

- SAP offers strong integration with other SAP systems such as SAP Web IDE, 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 partners with third parties such as Zimperium for anti-malware.

- SAP Mobile Secure does not support BlackBerry devices.

- SAP Mobile Secure is best when used in conjunction within the broader portfolio of SAP solutions, such as its SAP Cloud Identity Service.

- SAP Mobile Secure is a better fit for larger organizations than for SMBs.

Copyright © April 2016, The Radicati Group, Inc. Reproduction Prohibited

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 is publicly traded.

SOLUTIONS

The MobileIron EMM platform enables enterprises to secure and manage operating systems in mixed-use mobile device environments. It incorporates identity, context, and privacy enforcement to set the desired level of access to enterprise data and services. MobileIron secures data-at-rest on the mobile device, in mobile apps, and in cloud storage. MobileIron offers two key EMM solutions: **MobileIron Core** for on-premises deployments and **MobileIron Cloud** for cloud-based deployments. MobileIron's solutions are managed from a customizable console. For larger deployments, administration can be delegated based on region, device type, or other factors.

The MobileIron EMM platform consists of the following solutions:

- *MobileIron Core* – integrates with backend enterprise IT systems and enables IT to define security and management policies for mobile apps, content and devices. It offers support for Apple iOS, Mac OS X, Google Android, and Windows 10.

- *MobileIron Cloud* – is the cloud-based version of MobileIron Core. It offers support for Apple iOS, Google Android, and Windows 10 (Mac OS X is on the roadmap for 2016).

- *MobileIron Sentry* – is an in-line gateway that manages, encrypts, and secures traffic between the mobile device and back-end enterprise systems.

- *MobileIron Client* – called Mobile@Work, is an app that end users download to automatically configure their device enforce the configuration and security policies set by their IT department.

Copyright © April 2016, The Radicati Group, Inc. Reproduction Prohibited

MobileIron also offers a number of Client-side solutions that can be installed on mobile devices to enhance end user productivity. These include:

- *Apps@Work* – is MobileIron's enterprise app storefront, which lets users download IT approved in-house as well as third party apps. The app storefront experience can be customized by IT administrators, to define which applications are assigned to a given user.

- *Docs@Work* – provides the ability to access, annotate, share, and view documents across a variety of email, as well as on-premise and cloud content management systems, such as SharePoint, Dropbox, OneDrive Pro, Office 365 and Box. It also provides DLP for email attachments by decrypting documents delivered through Sentry.

- *Web@Work* – is a secure browser that lets users access web content within the corporate intranet without requiring the user to go through complex procedures such as starting a device-wide VPN session. It includes data loss prevention (DLP) capabilities.

- *Help@Work* – allows mobile end users to request IT help directly from their iOS devices. It enables IT to support mobile devices more easily and cost effectively.

- *DataView* – offers mobile data usage monitoring capabilities, enabling IT departments to set data limits and then notify end users, via real time alerts, so that they do not exceed their data plan limits, especially during roaming.

- *MobileIron Tunnel* – enables "iOS 7 or later" managed applications to access protected corporate data and content behind a firewall through a secure per-app VPN connection without requiring a device-wide traditional VPN solution. It also enables MobileIron's mobile management software to continuously monitor mobile device security before access is granted to protected enterprise resources.

- *MobileIron AppConnect* – containerizes apps to protect data-at-rest without affecting personal data. Once integrated, the applications become part of the secure container on the device managed by the MobileIron Client.

MobileIron has an extensive partner ecosystem, which includes applications developed by customers as well as third-parties using its AppConnect technology. It serves to further increase

Copyright © April 2016, The Radicati Group, Inc. Reproduction Prohibited

the number of applications integrated with the MobileIron enterprise mobility management platform.

STRENGTHS

- MobileIron offers flexible deployment options, including: cloud-based, on-premises, and virtual solutions.
- MobileIron solutions are simple to deploy and use by IT administrators, as well as by end users.
- MobileIron focuses on preserving the native user experience on mobile devices.
- 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 could improve the depth and granularity of its app analytics reporting.
- MobileIron is a best-of-breed vendor in the EMM space. However, as EMM overlaps increasingly with other security, compliance and mobility areas it may become difficult for MobileIron to compete with larger vendors with broader portfolios.

Copyright © April 2016, The Radicati Group, Inc. Reproduction Prohibited

SOPHOS

The Pentagon
Abingdon Science Park
Abingdon OX14 3YP
United Kingdom
www.sophos.com

Sophos provides IT security and data protection products for businesses on a worldwide basis. Sophos is headquartered in Oxford, UK, and is publicly traded on the London Stock Exchange.

SOLUTIONS

Sophos Mobile Control protects mobile devices with one solution with a standard offering and an advanced offering. Both are available as an on-premise implementation or as a cloud-based service.

- **Sophos Mobile Control (SMC) – Standard** provides security for Apple iOS, Google Android (including LG and Sony), and Windows Mobile devices. Sophos provides encryption enforcement, password enforcement, device wiping (corporate and full), and complete MDM capabilities. In addition, MAM capabilities include an enterprise app store to securely distribute internal and public apps to individual users or groups along with the ability to whitelist and blacklist apps. On the device side, Sophos MAM comes with an App Catalog and a mobile app SDK. Container solutions include support for Samsung Knox, Sophos Secure Email App for Android and iOS and Secure Documents Container with secure corporate browser.

- **Sophos Mobile Control – Advanced** is an extended offering for protection of corporate data on mobile devices. It includes all features of Sophos Mobile Control - Standard and adds the following:

    - **Sophos Secure Email** – a Personal Information Management (PIM) container solution for email, calendar and contacts. It helps IT provision email to employee mobile devices across iOS and multiple Android versions.

Copyright © April 2016, The Radicati Group, Inc. Reproduction Prohibited

- **Sophos Mobile Security –** an anti-virus and anti-malware solution, designed to protect users in Android devices from mobile malware. Companies or users can establish filters for malicious webpages or webpages with inappropriate content in a number of different categories.

- **Sophos Secure Workspace –** an app to provide secure and controlled access to a corporate documents container. Usage of public cloud services (e.g. Dropbox, Google Drive, Microsoft OneDrive, WebDav environments, and Box) is secured with compliance policy. In addition, Enterprise File Share and Sync services are supported including via Windows Server, Egnyte, or OwnCloud. Mobile data protection is tightly integrated with the Sophos Safeguard Encryption solution, so that users can access encrypted files on their mobile devices and remain compliant with encryption policy even when cloud storage services are used. Data remains secure via document encryption and Data Loss Protection (DLP) rules that control access, edit rights and facilitate sharing of files. Sophos Secure Workspace also supports collaboration through editing of text files and annotation of PDF files. A corporate browser within Sophos Secure Workspace (SSW) delivers safe and secure access to company websites and frequently used sites.

- **Sophos Mobile SDK –** helps companies add security to their applications for mobile access. An extensive list of controls is available including geo-location or time based policies, additional authentication, and denial of access if jailbreaking or rooting activity is detected.

STRENGTHS

- Sophos' offers a straightforward 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 intuitive, web-based user interface. This is essential to enable small to mid-market customers with limited IT resources.

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

Copyright © April 2016, The Radicati Group, Inc. Reproduction Prohibited

- Integration with Sophos Safeguard Encryption enables users to share encrypted files to their mobile devices and safely utilize cloud storage locations for collaboration. The Sophos Secure Workspace solution allows users to securely add, view and edit encrypted documents stored in the cloud.

- Sophos Mobile Control integrates with Sophos UTM, encryption and endpoint protection solutions for a comprehensive 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.

- Mobile app analytics could be improved.

TRAIL BLAZERS

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. The company has a global presence with offices in 30 different countries.

SOLUTIONS

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

Copyright © April 2016, The Radicati Group, Inc. Reproduction Prohibited

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 10 for Mobile consists of five components, as follows:

- *Exchange Active Sync* – the EAS connector supports all popular mobile platforms including Android, iOS, and Windows Phone. It supports rich controls such as password management, encryption enforcement, camera/Bluetooth use, application use controls, and more.

- *Apple MDM* – allows management of iPhones and iPads and supports all Apple MDM features, including device management and configuration controls, device and application usage information and more.

- *Samsung MDM* – supports Samsung KNOX devices allowing for deeper control and administration of select Samsung devices (e.g. Samsung Galaxy Tab).

- *Android for Work* – supports Android 5.0+ devices allowing creating and managing the encrypted profile with the Google Apps for Work productivity suite.

- *Security Agent* – supports all popular smartphones and tablets. It provides anti-malware and anti-phishing protection through the Kaspersky Security Network, anti-theft controls which include remote lock, full or select wipe, GPS tracking and SIM control, applications control and encryption through containerization, web/safe browsing detection, jailbreak/rooting detection.

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. Kaspersky Endpoint Security Cloud is due to release later in 2016 and will provide cloud-based management of mobile devices, along with endpoints.

STRENGTHS

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

Copyright © April 2016, The Radicati Group, Inc. Reproduction Prohibited

- 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 in-house developed anti-malware and anti-phishing protection, and containerization (app wrapping) to separate personal and corporate data.

- Kaspersky Anti-theft functionality provides the possibility to control mobile device compliance to the corporate policies alongside with the ability to alarm, locate, lock or wipe the single device.

WEAKNESSES

- Kaspersky's EMM solutions are currently delivered only as on-premises software. Cloud-based services, however, are on the near term roadmap in 2016.

- 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.

- Kaspersky Lab's EMM solutions focus on security and remote management functionality, and don't currently provide mobile app analytics.

- Kaspersky Lab's EMM does not include DLP functionality.

Copyright © April 2016, The Radicati Group, Inc. Reproduction Prohibited

SPECIALISTS

SYMANTEC

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

Symantec, founded in 1982, provides a broad range of security solutions for consumers and businesses. The company's product portfolio includes solutions for endpoint, email, web, mobile and more.

SOLUTIONS

In the Enterprise Mobility Management space, Symantec offers **Symantec Mobility: Suite**, an integrated, modular, suite of components which include: MDM, MAM, Workforce Apps, and Threat Protection. Mobility:Suite supports iOS, Android, and Windows Phone, and Windows 10. It 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. Specific features include: configuring passwords, remote lock and wipe, policies for individuals, devices, or groups from the directory system, and more.

- *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. Workforce Apps applies a layer of enterprise-grade security to each productivity app, including encryption, data loss prevention policies and secure proxies for safe transit of data from the corporate network to the apps, helping to reduce the risk of data leakage.

- *Symantec Mobility: Application Management* - 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.

Copyright © April 2016, The Radicati Group, Inc. Reproduction Prohibited

- *Symantec Mobility: Threat Protection* - 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. It provides proactive protection that lets users scan apps before downloading them from Google Play. It includes protection against malware, grayware and risk apps, apps that leak data and content, drain battery or consume excessive data, and anti-phishing web protection.

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. Enterprises can easily add modules, as their mobility needs evolve.

- Symantec prices Mobility Suite on a per-user basis regardless of the number of devices. This contains costs for enterprises where users utilize multiple mobile devices.

- 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 Mobility: Suite is meant to be deployed in the context of Symantec's Endpoint Protection suite, rather than on its own.

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

Copyright © April 2016, The Radicati Group, Inc. Reproduction Prohibited

- App analytics and reporting could be improved. While Symantec Mobility: Workforce Apps offers app wrapping and containerization it does not allow for very granular policy settings.

MICROSOFT
One Microsoft Way
Redmond, WA 98052-6399
www.microsoft.com

Microsoft delivers products and services to businesses and consumers through an extensive product portfolio that includes solutions for office productivity, messaging, collaboration, and more.

SOLUTION

The **Microsoft Enterprise Mobility Suite (EMS)**, first released in early 2015, is comprised of the following three key components:

Microsoft Intune – which offers MDM and MAM functionality across iOS, Android and Windows Phone devices. It supports selective wiping of apps and data, app wrapping and containerization. It can integrate with System Center 2012 Configuration Manager for administration in a hybrid scenario.

Azure Rights Management Services (RMS) – which delivers document and data security. It also offers integration with native applications through an SDK.

*Azure Active Directory Prem*ium – for identity rights management. It includes self-service password reset capabilities, group management, group provisioning and access management policy enforcement, synchronization of user identity with on-premise directories, and Multi-Factor Authentication (MFA).

Microsoft EMS is intended to be deployed in the cloud or as a hybrid solution. It is available through the Microsoft Enterprise Volume Purchasing plan.

Copyright © April 2016, The Radicati Group, Inc. Reproduction Prohibited

STRENGTHS

- Microsoft EMS is a good solution for organizations fully vested in Microsoft collaboration solutions and cloud strategic direction. It allows organizations to deploy a BYOD strategy across all their users, which integrates seamlessly with investments in identity and rights management.

- Microsoft EMS is affordably priced to appeal to organizations of all sizes, particularly if they are already vested in Microsoft access rights management.

- Microsoft EMS was designed from the ground up to fit well into a hybrid Microsoft environment where a full transition to cloud computing is underway but still proceeding in phases.

WEAKNESSES

- In terms of EMM capabilities, Microsoft Intune is not as advanced and granular as many competing EMM solutions that have been on the market for a number of years now. We expect Microsoft will quickly close the gap but in the meantime EMS should be viewed primarily as a starter-level solution for Microsoft-centric organizations.

- Microsoft EMS does not offer significant app analytics reporting.

- Microsoft EMS's app wrapping and containerization are still fairly basic when compared to the competition.

Copyright © April 2016, The Radicati Group, Inc. Reproduction Prohibited

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. Solutions are available as software, appliances, and hosted solutions.

SOLUTIONS

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.

Mobile Security includes the following functionality:

- *Mobile Security* – protection for mobile devices, apps and data. Support for a broad range of mobile platforms, including iOS, Android, BlackBerry, and Windows Phone.

- *Mobile Device Management (MDM)* – allows administrators to remotely enroll, provision, de-provision, and track devices. Supports the setting and monitoring of cross-device and group policies.

- *Mobile Device Security* – blocks malware and malicious websites, monitors and blocks calls, MMS and SMS sent to and from devices.

Copyright © April 2016, The Radicati Group, Inc. Reproduction Prohibited

- *Mobile Application Management* – provides application black listing and white listing, allows administrators to manage and block apps based on categories, identifies and blocks risky Android apps leveraging the Trend Micro Mobile Application Reputation Service. Pushes apps to end-user devices through a corporate app store, provides inventory management and reporting of apps used across devices and groups.

- *Data Protection* – provides remote lock, wipe, selective wipe and device location capabilities. Enforces encryption, blocks the use of jail broken or unencrypted devices. It also allows administrators to lock down device features such as cameras, Bluetooth, SD card readers, and more.

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.

Copyright © April 2016, The Radicati Group, Inc. Reproduction Prohibited

MATURE PLAYERS

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 the mobility space, the vendor's enterprise mobility management solution is built on technology from its Fiberlink acquisition in 2013.

SOLUTIONS

IBM MaaS360 (formerly *IBM MobileFirst Protect*) is available in all forms of deployment: on-premises, hybrid, and cloud. IBM MaaS360 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.

Delivered as a cloud service, IBM MaaS360 provides streamlined provisioning and configuration, which allows customers to be set up in minutes. Updates and new functionality are provided automatically so customers are always on the latest version.

IBM MaaS360 offers an App Security SDK that can integrate security features, such as authentication and copy/paste restrictions into custom-built enterprise apps on mobile devices. IBM MaaS360 also partners with public apps vendors as part of IBM's Workplace Partner Program.

STRENGTHS

- IBM MaaS360 provides multiple ways to separate corporate and personal data on mobile devices. This includes containerization, with granular level policy management and data protection controls.

Copyright © April 2016, The Radicati Group, Inc. Reproduction Prohibited

- The IBM MaaS360 Cloud Extender integrates with Microsoft Exchange ActiveSync, Microsoft Office 365, and IBM Notes.

- IBM MaaS360 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.

- IBM MaaS360 has a secure document sharing application to provide mobile users access to enterprise content. Document access and distribution include the integration of Microsoft SharePoint, NFS, Box, Google Drive, and other third party solutions. Customers also have the option to leverage IBM MaaS360 Doc Cloud, to securely host and distribute files.

- IBM MaaS360 can also protect Microsoft Windows and Apple Mac OS X systems, which helps simplify protection deployment across mobile devices and workstations.

- IBM MaaS360 can be deployed as part of IBM's MobileFirst solution that brings together mobile security, app development, identity management, and professional services, for a complete BYOD mobile enterprise enablement strategy.

WEAKNESSES

- IBM MaaS360 tends to be most effective and offers deeper functionality when integrated with a number of other IBM solutions, such as IBM Trusteer.

- While IBM MaaS360 can be deployed on its own, IBM tends to push its deployment as part of a broader MobileFirst solution set, which has a heavy professional services component that may turn off smaller customers looking just for EMM.

- Mobile app analytics and reporting could be improved.

- IBM MaaS360 does not include DLP functionality.

Copyright © April 2016, The Radicati Group, Inc. Reproduction Prohibited

THE RADICATI GROUP, INC.
http://www.radicati.com

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.

Copyright © April 2016, The Radicati Group, Inc. Reproduction Prohibited

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:

Title	Released	Price*
US Email Statistics Report, 2016-2020	Mar. 2016	$3,000.00
Email Statistics Report, 2016-2020	Mar. 2016	$3,000.00
Instant Messaging Market, 2016-2020	Feb. 2016	$3,000.00
Instant Messaging Growth Forecast, 2016-2020	Feb. 2016	$3,000.00
Social Networking Growth Forecast, 2016-2020	Feb. 2016	$3,000.00
Mobile Growth Forecast, 2016-2020	Jan. 2016	$3,000.00
Endpoint Security Market, 2015-2020	Dec. 2015	$3,000.00
eDiscovery Market, 2015-2020	Dec. 2015	$3,000.00
Microsoft SharePoint Market Analysis, 2015-2019	Aug. 2015	$3,000.00
Email Market, 2015-2019	Jul. 2015	$3,000.00
Cloud Business Email Market, 2015-2019	Jul. 2015	$3,000.00
Corporate Web Security Market, 2015-2019	Jul. 2015	$3,000.00
Office 365, Exchange Server and Outlook Market Analysis, 2015-2019	Jun. 2015	$3,000.00

*** Discounted by $500 if purchased by credit card.**

Upcoming Publications:

Title	To Be Released	Price*
Advanced Threat Protection Market, 2016-2020	April 2016	$3,000.00
Information Archiving Market, 2016-2020	April 2016	$3,000.00
Enterprise Mobility Management Market, 2016-2020	April 2016	$3,000.00

*** Discounted by $500 if purchased by credit card.**

All Radicati Group reports are available online at http://www.radicati.com**.**

Copyright © April 2016, The Radicati Group, Inc. Reproduction Prohibited