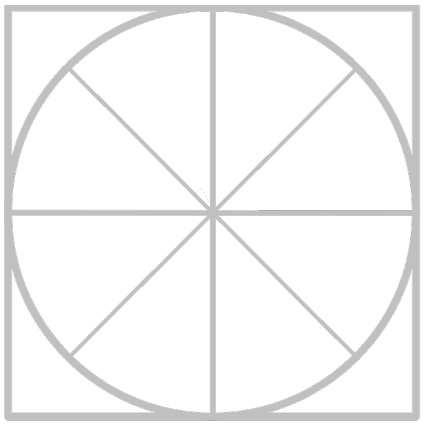
The Radicati Group, Inc.
www.radicati.com

THE RADICATI GROUP, INC.

Enterprise Mobility Management - Market Quadrant 2017



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

March 2017

TABLE OF CONTENTS

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 possess 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.

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.

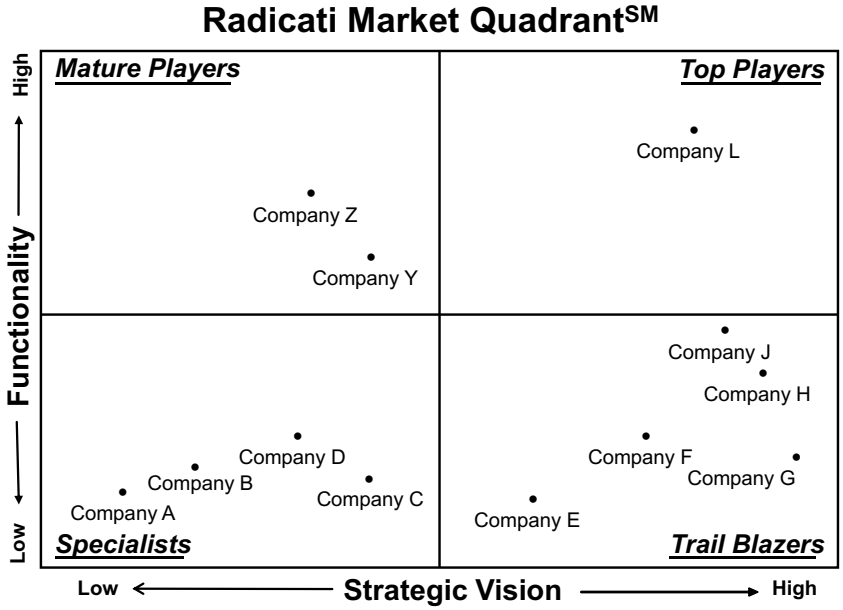


Figure 1: Sample Radicati Market Quadrant

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 Systems, IBM, Kaspersky Lab, Microsoft, MobileIron, SAP, Sophos, SOTI,* and *VMware AirWatch*.

- 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

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

- Worldwide revenues for the EMM market will total over $1.8 billion by year-end 2017. This figure is expected to grow to over $3.8 billion by year-end 2021. An average annual growth rate of 18% over the next four years. Figure 1, shows the worldwide revenue for the Enterprise Mobility Management market from 2017 to 2021.

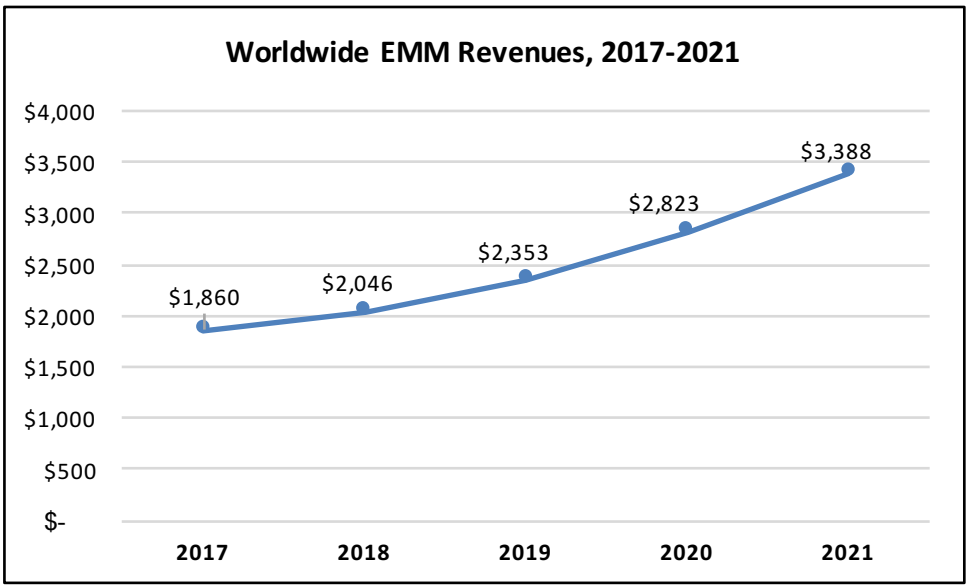


Figure 2: Worldwide Enterprise Mobility Management Revenue, 2017-2021

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.

- **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.

***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.*

MARKET QUADRANT – ENTERPRISE MOBILITY MANAGEMENT

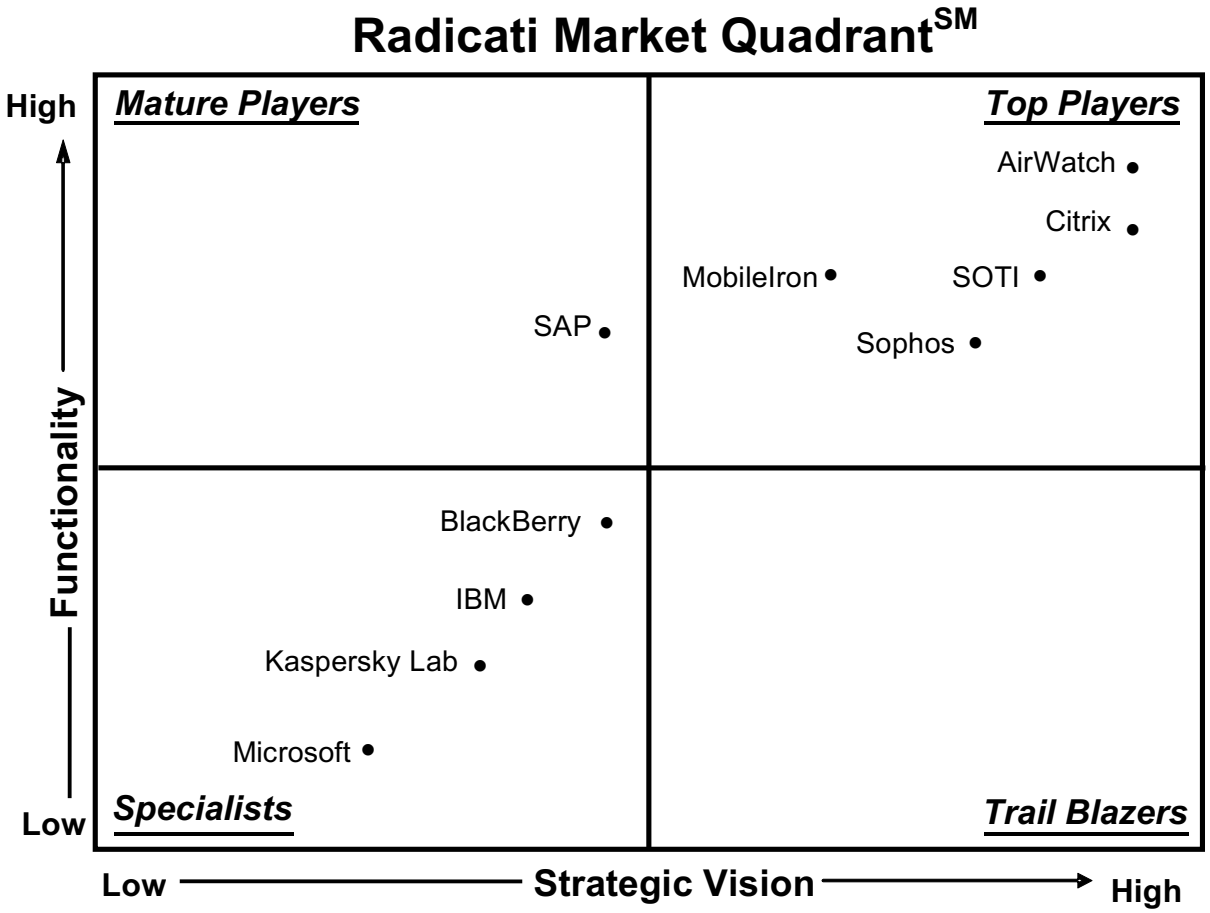


Figure 3: Enterprise Mobility Management Market Quadrant, 2017*

* Radicati Market Quadrant℠ is copyrighted March 2017 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 HIGHLIGHTS

- The **Top Players** in the Enterprise Mobility Management market are *VMware AirWatch, Citrix Systems, SOTI, MobileIron,* and *Sophos.*

- The **Specialists** quadrant includes *BlackBerry, IBM, Kaspersky Lab* and *Microsoft*.

- The **Mature Players** quadrant includes *SAP*.

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 unified workspaces, 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, tablets, laptops, printers, wearables and IoT devices across operating systems, including Android, Apple iOS, BlackBerry, Chrome, macOS, QNX, Tizen 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.

VMware launched **VMware Workspace ONE**, a secure enterprise platform that delivers and manages devices and apps while integrating identity, applications and enterprise mobility. Key features include: consumer-grade self-service access to any app; 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. Workspace ONE also provides apps-based management for end users requiring access to corporate apps without device management through a containerization approach, separating corporate and personal data.

STRENGTHS

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

- 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.

- 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 macOS and Windows 10 laptops alongside smartphones and tablets.

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

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.

- Customers of SaaS installations indicated that the response times for the management console could be improved. Also, some reporting features could be streamlined to offer easier customization.

- AirWatch will experience growing competition and pricing pressures, as more MDM and MAM solutions continue to be folded natively into mobile operating systems and devices.

- The recent acquisition of VMware's parent company, EMC, by Dell, raises some concerns about the continued level of R&D investment in AirWatch solutions going forward.

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. When delivered as a cloud service, the corresponding services are called **XenMobile Standard Service**, **Advanced Service**, and **Premium Service**. In 2014, Citrix announced its Citrix Workspace Suite, which incorporates mobility, virtualization, networking, data, and some cloud services. In 2015, Citrix announced Citrix Cloud, which allows for the entire solution to be delivered from the cloud.

Citrix also offers a suite of mobile productivity apps, available with both on-premises and SaaS XenMobile deployments, which include:

- *Secure Mail* – secure email client.
- *Secure Web* – 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.
- *Secure Notes* – a secure note taking application, with email and calendar integration for streamlined mobile workflows.
- *Secure Tasks* – secure task management application integrated with email and calendar.
- *QuickEdit* – offline editing capabilities on mobile devices.
- *ShareConnect* – secure remote access.
- *ScanDirect* – a mobile app that allows convenient document and photo capture directly from the mobile device.

- *Secure Forms* – a secure app for creating, publishing, populating, and storing digitized versions 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 XenMobile Apps that are tightly integrated out of the box for a seamless experience, with support for single sign-on. The XenMobile administrative console offers a unified endpoint management platform for IT administrators to enforce policies on mobile devices, desktops, applications and data using a single pane of glass.

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 advanced Mobile Application Management (MAM) security features, including local data storage encryption, without requiring MDM enrollment.

- Citrix XenMobile is tightly integrated with other Citrix products, such as XenDesktop and XenApp for virtualized delivery of Windows desktops and apps to mobile devices, as well as mobile collaboration apps like GoToMeeting, GoToAssist, ShareFile, Podio, and Talkboard.

- XenMobile when deployed as an integrated Citrix Workspace solution provides IT admins with the flexibility to provision end users with single-sign-on onto native mobile, web as well virtual apps and desktops thus saving the deployment effort and cost while maintaining a seamless end user experience

- Citrix offers a strong product portfolio of mobile productivity applications (i.e. Secure Mail, Secure Web, ShareFile, Secure Notes, Secure Tasks, QuickEdit, ShareConnect, ScanDirect, and Secure Forms).

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

- 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 XenMobile and third-party apps.

- Citrix XenMobile provides capabilities to enhance Microsoft Office 365. For instance, users can get Office 365 apps delivered through a corporate app store. Also, Office 365 apps can recognize documents opened from XenMobile apps and prevent them from being stored in unapproved locations.

WEAKNESSES

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

- While Citrix XenMobile can be deployed as a standalone solution, its full power is best achieved as part of a unified workspace strategy, that may include XenApp, XenDesktop, XenServer and ShareFile. Customers needing MDM only may wish to look at other solutions.

- Customers report some uneven functionality, with regards to setting authentication and access control policies across the various components of the XenMobile suite.

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

SOTI

5770 Hurontario St.
Suite 1100, Mississauga,
Ontario L5R 3G5, Canada
www.soti.net

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 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-premises, 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, content management (including URL filtering), 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, which helps unify management and support of a growing spectrum of connected endpoints.

STRENGTHS

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

- SOTI has a well-established presence in the business-critical mobility market, with its roots in managing traditionally rugged devices. This gives the vendor a clear advantage as these customers transition to Apple iOS, Google Android, and Windows 10 devices.

- SOTI's capabilities expand beyond EMM to include integrated mobile support management.

- SOTI's SDK for Apple iOS devices allows organizations to wrap iOS apps for additional MAM functionality. Administrators can view and access the wrapped application's file directory remotely over the air, as well as conduct two-way chat between user and support administrator.

- SOTI includes content containerization capabilities via its SOTI hub content management app, and via its SOTI surf secure browser app which provides web filtering, and split tunneling capabilities to access corporate intranet sites without the need for a VPN.

- 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's focus on business-critical mobility reduces its mindshare with general EMM deployments.

- While SOTI does provide app-level containerization of content, it leverages native OS containerization solutions, as well as third-party technologies, to containerize email and enterprise apps.

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 is available for on-premises deployments and 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, macOS, Google Android, and Windows 10.

- *MobileIron Cloud* – is the cloud-based version of MobileIron Core. It offers support for Apple iOS, Google Android, macOS, and Windows 10.

- *MobileIron Monitor* – is a dashboard solution for its on-premises based MobileIron Core customers which allows administrators to effectively monitor the health of all deployed MobileIron EMM components.

- *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.

- *MobileIron Access* – is a cloud security solution that allows administrators to set granular access control policies based on application, IP address, identity, device posture and other elements. It also assists administrators into gaining more complete insight into user activities.

- *MobileIron Bridge* – serves to unify mobile and desktop operations for mobile devices and Windows 10 workstations through a single management console.

MobileIron also offers several 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* – allows 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. This serves to increase 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 areas of security, compliance and mobility it may become increasingly difficult for MobileIron to compete with larger vendors that offer broader solution portfolios.

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 protects mobile devices with one solution with a standard offering and an advanced offering. Both are available as a solution in Sophos Central, which provides unified, cloud-based administration interface for all Sophos products, or as a solution for on-premises installation.

- **Sophos Mobile – Standard** provides security for Apple iOS, Google Android (including Samsung, LG and Sony), and Windows Mobile & Desktop 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 distribute internal and public apps securely to individual users or groups along with the ability to whitelist and blacklist apps. Native container solutions include support for Android for Work, Samsung Knox, and iOS. Sophos also recently added was the ability to manage IoT devices running Android Things or Windows 10 IoT.

- **Sophos Mobile – Advanced** is an extended offering that adds MCM, Sophos Mobile Security, and Sophos Mobile SDK to all the features of Sophos Mobile Standard. Sophos Mobile Advanced includes:

    - **Sophos Mobile Security –** anti-virus and anti-malware, designed to protect users on Android devices from mobile malware or potentially unwanted/harmful applications that could compromise the performance of the device. In addition, companies or users can establish filters for malicious webpages or webpages with inappropriate content in a number of different categories.

    - **Sophos Secure Email** – one of two applications that make up the Sophos mobile container solution. SSE is a Personal Information Management (PIM) application for email, calendar and contacts that helps IT provision email to employee mobile devices across iOS and different Android versions.

    - **Sophos Secure Workspace –** provides secure and controlled access to a corporate document container and to corporate websites. Facilitates secure usage of public cloud services (e.g. Dropbox, Google Drive, Microsoft OneDrive, and various WebDAV-based services) secured by compliance policies. In addition, Enterprise File Share and Sync services are supported including Windows Server, Box, Egnyte, or OwnCloud. Mobile data protection is tightly integrated with the Sophos Safeguard Encryption solution, which lets users 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 enable secure file sharing and collaboration. Sophos Secure Workspace also offers editing of text and Office format files (Word, Excel, PowerPoint), as well as lets users annotate PDF files. A corporate browser within Sophos Secure Workspace 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 a license fee based on number of users, regardless of how many devices each employee uses.

- Sophos Mobile 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.

- Integration with Sophos Safeguard Encryption enables users to access encrypted files on 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 integrates with Sophos UTM, encryption and endpoint protection solutions for a comprehensive security strategy.

WEAKNESSES

- Support for macOS devices is not yet available, but is on the roadmap for future releases.

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

- Mobile app analytics granularity and reporting could be improved.

SPECIALISTS

BLACKBERRY

2240 University Avenue, East
Waterloo, Ontario
Canada N2L 3W8
www.blackberry.com

BlackBerry is a mobile communications vendor founded in 1984. BlackBerry offers security and software 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.

SOLUTIONS

BlackBerry, originally best known for its smartphone business, has undergone a significant change of direction choosing to concentrate primarily on its Enterprise Mobility Management portfolio. To this effect, BlackBerry has worked to integrate its acquisitions of Good Technology and WatchDox, into a single Enterprise Mobility Management (EMM) platform called **BlackBerry Secure**.

BlackBerry Secure enables secure communication, information sharing, document synchronization, and user collaboration, through a wide range of mobile devices and apps. Key capabilities and products within these suites include:

Multi-Layered Security – BlackBerry Secure offers a multi-layered approach to mobile security. Organizations can apply security controls and policy at the device, app and content level. Each of these capabilities is best-in-class in their respective approaches and can be layered with one another or used in isolation for maximum flexibility across use cases. This delivers a scalable architecture and streamlined user experience. All EMM control are delivered via a single unified console.

Unified Endpoint Management – BlackBerry Secure manages device policies including not just a rich set of Mobile Device Management (MDM) controls but enhanced secure

communication. It provides a cross-platform way to set policies solution across iOS, Android™, Windows, Windows Phone®, Samsung KNOX, Android for Work, macOS and BlackBerry devices. It offers an attribute-driven, endpoint-permissions model, which gives users and administrators control of devices, applications and data, by-person or by group.

App Level Controls and Secure Container – BlackBerry Dynamics, a part of BlackBerry Secure, 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. BlackBerry Dynamics was the first mobile app container and remains the most mature. It is also the only container to have obtained Common Criteria EAL-4+ certification. Beyond containerization it also includes a shared services framework and capabilities for application reliability.

Collaboration Apps – BlackBerry offers a broad portfolio of collaboration apps purpose-built for business. The flagship app is BlackBerry Work which provides a fully integrated, collaboration experience, similarly 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-premises or hybrid deployment. BlackBerry also delivers a series of standalone apps for mobilizing enterprise IM, notes, tasks, document access, secure intranet access and browsing and more.

ISV App Ecosystem - BlackBerry has an extensive customer and ISV ecosystem, which securely interact with each other through the BlackBerry Dynamics Shared Services Framework. These apps are available on common mobile operating systems, including iOS and Android.

Content-Level DRM and EFSS – BlackBerry Workspaces provide secure file-level protections including DRM controls for common documents. It also includes an integrated Enterprise File Sync and Share (EFSS) solution built for mobile, desktop and web. With BlackBerry Workspaces, organizations can be confident that key proprietary information will not leave the enterprise.

BlackBerry delivers all capabilities via the BlackBerry Enterprise Mobility Suite, which is available in five editions, to allow organizations to choose the set of capabilities that best meet their needs.

STRENGTHS

- BlackBerry provides EMM support for iOS, Android, Windows, Windows Phone, macOS, BlackBerry devices, as well as support for Samsung KNOX and Android for Work.

- BlackBerry delivers multi-layered security including device policies, app controls and containerization, and file-level DRM in a single unified solution. This provides both a high degree of security as well as maximum flexibility.

- 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., BlackBerry Work, BlackBerry Access, BlackBerry, Connect, ISV apps, customer built apps, etc.) 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-premises and hybrid).

- BlackBerry-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 BlackBerry Dynamics 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.

- 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 BlackBerry offers highly sophisticated solutions, these may be somewhat overwhelming for organizations just beginning to deploy mobile security. BlackBerry is addressing this by offering flexible licensing where organizations can choose only the capabilities that they need.

- BlackBerry offers extensive analytics for its own portfolio of apps, however, BlackBerry is still working to extend these capabilities to non-BlackBerry third party apps.

- BlackBerry offers a rich and interesting portfolio of EMM solutions for a wide range of platforms, however, features and functionality are still not the same across all platforms and integration issues remain with regards to solution components derived from its Good Technology and WatchDox acquisitions.

- BlackBerry is going through a major business transformation from mobile phone manufacturer to software and services delivery, it still remains to be seen how successful this transition will be.

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 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, secure chat, browser, editors, a full unified endpoint management (UEM) solution 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 OS version. MaaS360's cognitive capabilities based on IBM Watson technology deliver insights, and recommendations as needed to meet evolving threats and vulnerabilities.

App security is provided in several ways: through native app wrapping capabilities within the IBM MaaS360 product; through an App Security SDK, which can integrate security features, such as authentication and copy/paste restrictions into custom-built enterprise apps on mobile devices; as well as through integration with AppConfig, an ISV framework for secure mobile app delivery.

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.

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

- IBM MaaS360 provides a secure web browser web gateway, which provides organizations access to internal Intranet sites and web application servers without the need for users 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 macOS 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 mobile enterprise enablement strategy.

WEAKNESSES

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

- 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.

- Mobile app analytics and reporting could be improved. IBM is working to address this.

- While IBM MaaS360 provides containerization capabilities, it does not include DLP functionality.

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 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), Total Security for Business for enterprises, or Kaspersky Endpoint Security Cloud for SMB customers. Kaspersky Security 10 for Mobile consists of five components, as follows:

- *Exchange ActiveSync* – 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 usage, application 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 creation and management the encrypted working profile with the Google Apps for Work productivity suite.

- *Security Agents* – support all popular smartphones and tablets. They provide anti-malware and anti-phishing protection through the cloud-based service Kaspersky Security Network

(KSN), anti-theft for remote lock, GPS tracking, mugshot, full or select device wipe, and SIM control, applications control and encryption through containerization for Android; web/safe browsing detection for Android, iOS and Windows Phone. Jailbreak/rooting detection is provided to check the device compliance for corporate policies.

Kaspersky Security for Mobile is centrally managed from administration solutions: **Kaspersky Security Center** supports on-premises centralized management of mobile devices as well as other IT endpoints and servers across the corporate network, plus Web Console and Self-Service Portal; **Kaspersky Endpoint Security Cloud** provides cloud-based centralized management of mobile devices, along with endpoints.

STRENGTHS

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

- 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.

- Kaspersky's EMM solutions are available as on-premises or cloud-based solutions.

WEAKNESSES

- 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 app containerization is somewhat more limited in scope and functionality than competing solutions.

- Kaspersky Lab's EMM solutions do not provide mobile app analytics.

- Kaspersky Lab's EMM device level analytics and remote device management could be improved to offer greater granularity.

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 + Security (EMS)**, formerly Microsoft Enterprise Mobility Suite, is comprised of the following 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 Information Protection – a new service that builds on Microsoft Azure Rights Management (Azure RMS) and Microsoft's acquisition of Secure Islands, which offers data classification and labeling technology.

Azure Active Directory Premium – includes *Azure Active Directory Identity Protection* for identity rights management, which offers self-service password reset capabilities, group

management, group provisioning and access management policy enforcement, synchronization of user identity with on-premises directories, and Multi-Factor Authentication (MFA).

Microsoft Advanced Threat Analytics – available for on-premises deployments, serves to identify known advanced persistent threats and security issues.

Cloud App Security – offers advanced threat protection for cloud deployments.

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.

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 competing EMM solutions. 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.

MATURE PLAYERS

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.

SOLUTIONS

SAP offers mobile capabilities as part of the company's PaaS solution, SAP Cloud Platform. The **SAP Cloud Platform mobile service for app and device management** provides end-to-end management and security of mobile devices, applications, and content. It includes the following functionality:

- *Mobile Device and App Management* – SAP offers mobile device and app management for the latest versions of Apple iOS, Google Android (including Android for Work and Samsung SAFE), and Windows Phone 8 and 10 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 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 offers mobile application level security through 3rd party tools. The SAP Cloud Platform mobile integration framework includes 3rd party vendor solutions that enable administrators to embed an SDK or to 'app wrap' security and data leakage policies around hybrid and native apps.

- *Mobile Content Management* – SAP Cloud Platform 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 a cloud service.

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 cloud services within the SAP Cloud Platform.

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

- SAP 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 (e.g. 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 Fiori, 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.

- While SAP continues to support existing on-premises SAP Afaria customers, its focus for new customers is to offer the EMM solution as a service within SAP Cloud Platform. While this is optimal for customers that are fully cloud-vested, it will not meet the needs of customers that prefer an on-premises solution.

- SAP's EMM solution is best when used in conjunction within the broader portfolio of SAP solutions.

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.

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:

Title	Released	Price*
Social Networking Statistics Report, 2017-2021	Feb. 2017	$3,000.00
Instant Messaging Market, 2017-2021	Feb. 2017	$3,000.00
Email Statistics Report, 2017-2021	Feb. 2017	$3,000.00
Endpoint Security Market, 2016-2020	Dec. 2016	$3,000.00
Secure Email Gateway Market, 2016-2020	Dec. 2016	$3,000.00
Microsoft SharePoint Market Analysis, 2016-2020	Jul. 2016	$3,000.00
Office 365, Exchange Server and Outlook Market Analysis, 2016-2020	Jul. 2016	$3,000.00
Email Market, 2016-2020	Jun. 2016	$3,000.00
Cloud Business Email Market, 2016-2020	Jun. 2016	$3,000.00
Corporate Web Security Market, 2016-2020	May 2016	$3,000.00
Advanced Threat Protection Market, 2016-2020	Mar. 2016	$3,000.00
Enterprise Mobility Management Market, 2016-2020	Mar. 2016	$3,000.00
Information Archiving Market, 2016-2020	Mar. 2016	$3,000.00
US Email Statistics Report, 2016-2020	Mar. 2016	$3,000.00
Mobile Growth Forecast, 2016-2020	Jan. 2016	$3,000.00

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

Upcoming Publications:

Title	To Be Released	Price*
Enterprise Mobility Management Market, 2017-2021	Apr. 2017	$3,000.00
Advanced Threat Protection Market, 2017-2021	Apr. 2017	$3,000.00

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

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