EMA Radar™ for Mobile Device Management (MDM)

Q1 2016 – Report Summary and VMware/AirWatch Profile

By Steve Brasen
ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) Radar Report
January 2016
# Table of Contents

Executive Summary .................................................................................................................. 1
The Scope of MDM .................................................................................................................. 1
Assessing the MDM Market .................................................................................................... 2
  Characteristics of a Preferred Solution ................................................................................. 2
    Architecture and Integration .............................................................................................. 2
    Functionality ...................................................................................................................... 3
    Deployment and Administration ......................................................................................... 4
    Cost Advantage ................................................................................................................ 5
    Vendor Strength ............................................................................................................... 5
Evaluation Criteria .................................................................................................................. 6
  Feature Eligibility ............................................................................................................... 6
  Financial Evaluation ......................................................................................................... 6
On the EMA RADAR™ ......................................................................................................... 7
  MDM Market Overview ................................................................................................... 7
  VMware – MDM Value Leader .......................................................................................... 7
  EMA Radar Profile: VMware/AirWatch ............................................................................ 8
Executive Summary

Productivity with an increasingly mobile workforce is dependent on the reliability and performance of portable devices—including smartphones and tablets—to access and run business applications while still meeting business requirement for security and compliance. Mobile device management (MDM) provides the endpoint-focused processes and solutions for accelerating user productivity and device reliability. This Enterprise Management Associates® (EMA™) RADAR report identifies the sixteen leading MDM platforms and empirically compares and grades them against a broad range of measurements to determine overall product strengths and cost efficiencies.

The Scope of MDM

Mobile employees are only as productive as the devices on which they rely. Although enterprise mobile management (EMM) processes have evolved with the goal of abstracting business resources (including data, applications, and services) from the mobile devices (i.e., smartphones and tablets) hosting them, any argument that management of the physical devices is completely unnecessary is eminently naive. At some point, something has to run locally on the devices to enable access to the business resources, and if that device or that point of connection should fail, it can profoundly impact the performance of the user. MDM includes the critical processes necessary to ensure user devices are able to optimally and securely access and run business resources without compromising enterprise requirements.

MDM practices can be logically segmented into five distinct areas.

- **Asset Management** – Processes for identifying, recording, and tracking devices, applications, and configurations through their entire enterprise lifecycle.
- **Device Provisioning** – Processes for deploying operating system, patches, updates, applications and other resources necessary to maintain business productivity and compliance.
- **Endpoint Configuration** – Processes for establishing system, network, and application settings essential for the access and the optimal utilization of business resources.
- **Problem Remediation** – Processes for enabling IT operations to remotely diagnose and resolve any issues that impede or diminish user access to business IT services.
- **Endpoint Security and Compliance** – Processes for ensuring the accessibility to business data and other resources on mobile endpoints does not compromise enterprise requirements.

It is important to note that MDM practices are entirely device-oriented. For instance, while the administration of an enterprise software catalog or the security hardening of enterprise data access points may be important characteristics of a broader EMM approach, they are not device management activities, and are therefore outside the scope of MDM. Some bring your own device (BYOD) features—such as containerization and virtualization—do directly impact the device and are therefore technically a part of MDM; however, EMA has chosen to evaluate these capabilities in a separate report (the EMA BYOD Management RADAR report). A prime assumption in the MDM Radar evaluation is that all managed endpoints are dedicated to performing business tasks.
Assessing the MDM Market

To assist organizations in the identification of solutions that deliver value in enterprise MDM, EMA has evaluated the leading platforms available on the market today. EMA defines “value” as the ratio derived from the strength of a product set against its cost efficiency. Put simply, the more you pay for a solution, the greater the advantages you should receive in terms of breadth of functionality and supportability. EMA's review process began with the determination of critical MDM features and capabilities. This list was used to establish evaluation KPIs that were ranked and weighted to correspond with the requirements EMA determined to be prioritized by organizations that have adopted or plan to adopt a MDM platform. The prioritization determinations are based on discussions with IT operations managers, survey-based research responses, and mobile users as well as EMA's own experience and knowledge of enterprise requirements and best practices.

From these KPIs, a minimum level of functional requirements was established to identify which management platforms qualify for recognition as MDM solutions. Minimum requirements included providing automation to support all five principle MDM elements (asset management, device provisioning, endpoint configuration, device remediation, and endpoint security). EMA identified and reviewed more than fifty vendors offering MDM solutions. Sixteen of these vendors were selected as offering the most comprehensive MDM support as defined by the pre-established KPIs, and each was invited to participate in the in-depth evaluation process.

A detailed questionnaire on the capabilities, cost, and supportability of their respective product sets was submitted to each of the selected MDM solution providers. More than 150 points of comparison were considered and all responses were carefully vetted for accuracy. EMA also conducted interviews with vendor customers to confirm product capabilities and indicate customer satisfaction with the product sets. Scoring of the vendor solutions was mathematically calculated by correlating available features, architectures, pricing, and capabilities with the predetermined KPIs. Some individual feature scores were adjusted based on firsthand customer experiences with the product sets. Final scoring of each product set was used in the product comparison charts and in the determination of award winners.

Characteristics of a Preferred Solution

The EMA RADAR report evaluation process standardizes the review of product sets in specific management disciplines by comparing vendor and product characteristics in five distinct categories: architecture and integration, functionality, deployment and administration, cost advantage, and vendor strength. Identified below are the elements EMA believes are indicative of an ideal MDM solution in each of the primary evaluation categories.

Architecture and Integration

The ideal MDM solution is architected to support all mobile resources from a single centralized management console. If multiple management servers are necessary to support especially large or geographically distributed environments, all devices should still be managed from a single master server and accessed from a single interface. Broad heterogeneous support for mobile platforms should be included with the product set to ensure a wide range of end users can be supported with the singular solution. Essential mobile platforms to be supported include iOS and Android; however, support for Windows devices is also well regarded in deference to the increased adoption rates of Windows mobile devices and the potential advantages of Windows 10 cross-platform support in enterprise environments.
Additionally, support for BlackBerry and other legacy mobile platforms also contribute to breadth of platform support. Scalability of the product set should be achieved by enabling expansion that is based on increasing enterprise requirements (i.e., growing number of support endpoints, expanded MDM process needs, etc.). EMA favors a modular approach to achieving scalability as it allows organizations to adopt and expand the platform according to their size and level of MDM maturity. However, to be effective, all modules must be fully integrated.

All management elements within a MDM solution should be fully integrated with each other, and direct integration with third-party management products should be established to extend the platform capabilities. Direct integration implies the solutions share common code, employ common data collection processes, utilize a common management interface, and/or store data in a common repository without the need for additional customization. Some examples of direct integrations with MDM platforms would be federated access to configuration management databases (CMDBs), integration with virtualization management platforms (e.g., VMware vCenter), integration with other endpoint management platforms (such as PC management solutions), and the ability to directly access and update records on a service desk (e.g., BMC Remedy). Additionally, robust APIs should be provided to allow the easy establishment of custom integrations.

Functionality

MDM encompasses a broad range of capabilities essential for ensuring reliable and responsible interactions with business IT services. Some product sets include unique features that perform very specialized tasks, so each organization should carefully identify and prioritize which capabilities are most applicable to its business requirements before initiating a product comparison. However, for the purposes of this evaluation, EMA has identified several specific areas of support that MDM platforms should include in order to be considered comprehensive. As previously noted, the primary focus of functional support capabilities in this report has been on device-centric features, including the following.

**Asset Management**
All mobile devices used to access business resources should be detected and recorded in a centralized data repository. Devices should be identified as either business-owned or user-owned and detailed configuration and status information should be automatically collected and tracked, including device brand and model, operating system version, system and network settings, installed applications, software licenses, and performance statistics.

**Provisioning**
A consolidated and controlled method must be enabled for secure delivery and access to business IT resources, including applications, business data, email, databases, messaging, and web services. IT administrators should have the ability to remotely install (i.e., “push”) applications, and end users should be empowered to provision IT resources themselves via an enterprise app store or a self-service user portal. Enterprises should also ensure all operating systems and applications are utilizing the latest versions and patch levels for optimal performance and security.

**Endpoint Configuration**
IT administrators should be able to remotely configure device systems, networks, and email accounts with little or no end-user interaction. Similarly, application configuration and security settings should be managed by administrators from a centralized console.
Problem Remediation
System, network, and application issues, including failure events, errors, and incidents of performance degradation, should be automatically identified and reported to IT operations in real time. Full details of the incident should be recorded and made accessible from the centralized console. Applicable details should include error messages, relevant log files, performance statistics, and active processes. IT administrators should have the ability to remotely log into and control supported mobile devices to perform remediation activities. In the event a device is damaged beyond repair, all device data should be recoverable from backups.

Endpoint Security and Compliance
Any business data or applications must be secured on the mobile device to prevent inappropriate access, duplication, or distribution. Features supporting this include application wrapping, cut and paste restrictions, lockdown of external devices (i.e., USB drives), or the use of business-dedicated secure applications. Password management and enforcement should also be included to ensure any restricted services are not compromised. In the event a device is lost or stolen, features such as location tracking should be employed to help recover systems or, failing that, capabilities should be available to remotely lock or wipe business data and resources. Since mobile devices are also susceptible to malicious software such as viruses, Trojan horses, and spyware, malware scanners and remediation should also be a part of any MDM solution. Of course, none of these preventative measures are effective if the end user circumvents enterprise security restrictions on their device, so comprehensive rooting and jailbreaking detection is essential, and access to business resources should be immediately and automatically disabled upon detection of any compromised devices. To ensure all enterprise and regulatory commitments are achieved, compliance auditing should also be performed on all devices and any deficiencies immediately reported to IT operations.

Deployment and Administration
The ease of which a solution can be deployed is directly related to the complexity of the infrastructure supporting it. The more hardware and software elements there are that need to be installed, the more challenging the deployment will likely be. An ideal solution will employ automation for enabling a turnkey deployment process, rapidly installing software components (such as databases, reporting engines, and console interfaces) and automatically detecting the mobile endpoints that will be supported. If agents need to be deployed on managed devices, they should be automatically pushed from the console server or made available for download by the end user from a publicly available source (such as a website or app store).

Administration is simplified with an intuitive and customizable console interface that consolidates all MDM processes, dashboards, and reports. A mobile application that accesses the console is advantageous for IT administrators that need to provide remote or out-of-hours support. The processes for collecting asset and status data from mobile endpoints should be automated, requiring little or no administrator interaction, and trigger-based automation should be available that remediates problems when certain predetermined conditions occur. Role-based profiles that are integrated with listing services (such as Active Directory) also simplifies administration by allowing users to be organized into logical groups (e.g., by job function, department, or device type) and collectively supported with a common set of permissions and restrictions. Also, the more self-service capabilities there are built into the solution, the fewer tasks there are that will need to be performed by administrative staff.
Vendors must also display a commitment to supporting the MDM platform and the user community. Maintenance contracts should be offered that deliver responsive and continuously available live support as well as timely product updates. Vendors should offer professional services that are staffed with support professionals that are knowledgeable about their solution set and MDM processes to assist customers with training, problem solving, environment optimization, and the initial product deployment. Vendors should also engage the user community by hosting online forums and regular conferences or meetings to educate organizations on the effective use of their platforms and on MDM best practices.

**Cost Advantage**

Pricing models for a MDM platform should be simple to understand and easy to calculate. Of the platforms EMA evaluated, all offer license pricing based on either the number of supported devices or the number of supported users (though some offer both). Since EMA research indicates 40% of business professionals employ more than one mobile device, many organizations will be advantaged with the adoption of user-based licenses, even though they are generally offered at a slightly higher rate than device-based licenses. Licenses are also offered for either a one-time perpetual fee or a recurring (monthly or annual) subscription fee. Maintenance contracts, which provide access to platform updates and the vendor's help desk, are typically offered to perpetual license customers for an annual fee (usually calculated as a percentage of the total license cost), but offered for free as part of subscription licensing. In general, the breaking point between perpetual and subscription licensing is between two to three years—in other words, after that amount of time, accumulated subscription costs exceed a one-time purchase cost, including maintenance costs. In deference to the reality that most organizations retain management solutions for many years or even decades, EMA's evaluation models reviewed total costs of ownership over three and seven year periods. As a consequence, the evaluation results did favor perpetual license solutions.

Vendors may offer on-premises solutions, cloud-hosted solutions, or both. While cloud-hosted solutions are most commonly offered for subscription pricing, on-premises solutions may be offered for either subscription or perpetual licenses. Also, while cloud-hosted solutions require no upfront costs or predeployment efforts (other than service registration), on-premises solutions require the purchase and installation of a physical server or appliance, its operating system, and often an SQL database. EMA recommends enterprises perform price comparisons that take into consideration all cost elements (license, maintenance, and infrastructure costs) and recognize their organization's unique requirements. Purchasing a low-cost solution may impede an organization from achieving long-term MDM goals and purchasing a more comprehensive solution may not be cost-effective if the advanced features are never used. It is important to right-size a solution based on projected future requirements as well as existing goals.

**Vendor Strength**

Consumers should always be aware of a vendor's stability and its commitment to a platform prior to adoption of the solution in order to be sure of its long-term viability. A vendor that is financially strong with high revenue and vast equity is more likely to continue support for a management platform. Solution providers that invest heavily in research and development will also be assured of maintaining continual value in the platforms architecture and feature set. Strategic and channel partnerships also increase
vendor relevance in the market space and customer loyalty extends visible credibility. Additionally, a vendor’s vision and strategy for development, innovation, and foresight of future requirements indicates whether a management solution will maintain optimal value in a dynamic marketplace.

**Evaluation Criteria**

**Feature Eligibility**

In order for a product set to be credited with a feature or capability in EMA’s evaluation, it was required to meet three strict criteria.

- The features needed to be generally available with the solution set at the time of the evaluation. Any features that were in beta testing or were scheduled to be included in later releases of the management suite were not eligible for consideration.

- All features needed to be self-contained within the included package sets. Any features not natively included in the evaluated package sets but available separately from the same vendor or third-party vendors for an additional cost did not qualify.

- All reported features needed to be clearly documented in publically available resources (such as user manuals or technical papers) for verification.

**Financial Evaluation**

To enable product license cost comparisons that are as fair as can possibly be attained through analytical process, EMA developed six sample support models and applied vendor pricing to each. Pricing included license or subscription costs for all products, add-ons, and modules necessary to achieve the functionality credited in the all other sections of this evaluation. Additionally, expenditures were added to account for any additional hardware and/or software infrastructure costs necessary for the platform to operate, and maintenance costs for the platform were calculated for the time period specified in each model. The results for each of the six models were empirically rated on a pricing scale (i.e., rated from 1-10 with a two decimal point level of accuracy). EMA primary research has indicated that 40% of mobile device users own/utilize more than one device to perform business tasks, so that statistical adjustment has been applied to each pricing model, where applicable. Ratings for all six models were then averaged to provide the final scoring reported in this evaluation. The six models used in EMA’s evaluation are shown here.

- **Short-Term Small Business Model** – supporting 100 users (140 devices) over 3 years
- **Long-Term Small Business Model** – supporting 100 users (140 devices) over 7 years
- **Short-Term Medium Business Model** – supporting 1,000 users (1,400 devices) over 3 years
- **Long-Term Medium Business Model** – supporting 1,000 users (1,400 devices) over 7 years
- **Short-Term Large Business Model** – supporting 10,000 users (14,000 devices) over 3 years
- **Long-Term Large Business Model** – supporting 10,000 users (14,000 devices) over 7 years

Organization that offer multiple product licensing and/or deployment models were evaluated and scored across all potential scenarios and the best scores achieved were included in the final review.
On the EMA RADAR™

**MDM Market Overview**

Value in any solution can be clearly defined by comparing the strength of the platform with its cost effectiveness. The EMA MDM Bubble Chart below provides graphical representations of evaluated industry leader positioning in relation to both critical axes. The “Product Strength” axis combines evaluation scores for **Functionality** with **Architecture & Integration**. “Cost Efficiency” is calculated by adding the scores achieved for **Cost Advantage** and **Deployment & Administration**. The size of each bubble indicates the Vendor Strength as quantified in their individual profiles.

<table>
<thead>
<tr>
<th>Vendor</th>
<th>Solution Impact</th>
<th>Deployment &amp; Administration</th>
<th>Cost Advantage</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMware/AirWatch</td>
<td>Exceptional</td>
<td>Exceptional</td>
<td>Exceptional</td>
</tr>
<tr>
<td>HEAT Software</td>
<td>Exceptional</td>
<td>Average</td>
<td>Basic</td>
</tr>
<tr>
<td>MobileIron</td>
<td>Average</td>
<td>Average</td>
<td>Basic</td>
</tr>
<tr>
<td>CA</td>
<td>Average</td>
<td>Average</td>
<td>Basic</td>
</tr>
<tr>
<td>IBM</td>
<td>Average</td>
<td>Average</td>
<td>Basic</td>
</tr>
<tr>
<td>SOTI</td>
<td>Average</td>
<td>Average</td>
<td>Basic</td>
</tr>
<tr>
<td>Citrix</td>
<td>Basic</td>
<td>Average</td>
<td>Basic</td>
</tr>
<tr>
<td>Zoho/ManageEngine</td>
<td>Basic</td>
<td>Average</td>
<td>Basic</td>
</tr>
<tr>
<td>Sophos</td>
<td>Basic</td>
<td>Average</td>
<td>Basic</td>
</tr>
<tr>
<td>JAMF</td>
<td>Basic</td>
<td>Average</td>
<td>Basic</td>
</tr>
<tr>
<td>Kaséya</td>
<td>Basic</td>
<td>Average</td>
<td>Basic</td>
</tr>
<tr>
<td>LANDesk</td>
<td>Average</td>
<td>Average</td>
<td>Basic</td>
</tr>
<tr>
<td>Citrix</td>
<td>Basic</td>
<td>Average</td>
<td>Basic</td>
</tr>
<tr>
<td>MobileIron</td>
<td>Exceptional</td>
<td>Exceptional</td>
<td>Exceptional</td>
</tr>
<tr>
<td>HEAT Software</td>
<td>Exceptional</td>
<td>Exceptional</td>
<td>Exceptional</td>
</tr>
<tr>
<td>VMware/AirWatch</td>
<td>Exceptional</td>
<td>Exceptional</td>
<td>Exceptional</td>
</tr>
<tr>
<td>MobileIron</td>
<td>Average</td>
<td>Average</td>
<td>Basic</td>
</tr>
<tr>
<td>CA</td>
<td>Average</td>
<td>Average</td>
<td>Basic</td>
</tr>
<tr>
<td>IBM</td>
<td>Average</td>
<td>Average</td>
<td>Basic</td>
</tr>
<tr>
<td>SOTI</td>
<td>Average</td>
<td>Average</td>
<td>Basic</td>
</tr>
<tr>
<td>Citrix</td>
<td>Basic</td>
<td>Average</td>
<td>Basic</td>
</tr>
<tr>
<td>Zoho/ManageEngine</td>
<td>Basic</td>
<td>Average</td>
<td>Basic</td>
</tr>
<tr>
<td>Sophos</td>
<td>Basic</td>
<td>Average</td>
<td>Basic</td>
</tr>
<tr>
<td>JAMF</td>
<td>Basic</td>
<td>Average</td>
<td>Basic</td>
</tr>
<tr>
<td>Kaséya</td>
<td>Basic</td>
<td>Average</td>
<td>Basic</td>
</tr>
<tr>
<td>LANDesk</td>
<td>Average</td>
<td>Average</td>
<td>Basic</td>
</tr>
<tr>
<td>Citrix</td>
<td>Basic</td>
<td>Average</td>
<td>Basic</td>
</tr>
<tr>
<td>MobileIron</td>
<td>Exceptional</td>
<td>Exceptional</td>
<td>Exceptional</td>
</tr>
<tr>
<td>HEAT Software</td>
<td>Exceptional</td>
<td>Exceptional</td>
<td>Exceptional</td>
</tr>
<tr>
<td>VMware/AirWatch</td>
<td>Exceptional</td>
<td>Exceptional</td>
<td>Exceptional</td>
</tr>
<tr>
<td>MobileIron</td>
<td>Average</td>
<td>Average</td>
<td>Basic</td>
</tr>
<tr>
<td>CA</td>
<td>Average</td>
<td>Average</td>
<td>Basic</td>
</tr>
<tr>
<td>IBM</td>
<td>Average</td>
<td>Average</td>
<td>Basic</td>
</tr>
<tr>
<td>SOTI</td>
<td>Average</td>
<td>Average</td>
<td>Basic</td>
</tr>
<tr>
<td>Citrix</td>
<td>Basic</td>
<td>Average</td>
<td>Basic</td>
</tr>
<tr>
<td>Zoho/ManageEngine</td>
<td>Basic</td>
<td>Average</td>
<td>Basic</td>
</tr>
<tr>
<td>Sophos</td>
<td>Basic</td>
<td>Average</td>
<td>Basic</td>
</tr>
<tr>
<td>JAMF</td>
<td>Basic</td>
<td>Average</td>
<td>Basic</td>
</tr>
<tr>
<td>Kaséya</td>
<td>Basic</td>
<td>Average</td>
<td>Basic</td>
</tr>
<tr>
<td>LANDesk</td>
<td>Average</td>
<td>Average</td>
<td>Basic</td>
</tr>
<tr>
<td>Citrix</td>
<td>Basic</td>
<td>Average</td>
<td>Basic</td>
</tr>
</tbody>
</table>

**VMware – MDM Value Leader**

Following its acquisition of AirWatch in 2013, VMware has been systematically integrating the platform with its extensive VMware Horizon and VMware App Volumes end user computing solutions. AirWatch is designed to help organizations easily deploy, configure, secure, manage, and support smartphones, tablets, and other devices across a variety of operating environments. The AirWatch platform includes solutions for mobile device, email, application, content, and browser management. EMA analysis indicated AirWatch provides the broadest overall MDM feature set among all the evaluated solutions included in this report.
Introduction
Initially founded in 2003, AirWatch has been recognized as a leading provider of management solutions for wireless and smart devices at every phase of the modern mobile revolution. The vendor’s flagship enterprise mobile management platform is designed to help organizations easily deploy, configure, secure, manage, and support smartphones, tablets, and other devices across a variety of operating environments. The AirWatch platform includes solutions for mobile device, email, application, content, and browser management. In 2014, AirWatch was acquired by cloud and virtualization solution provider VMware and its platform has since been systematically integrated with many of VMware’s end-user computing solutions, including VMware Horizon and VMware App Volumes. Based in Atlanta, AirWatch is employed by customers in more than 150 countries and its solutions are available in 17 languages.

Architecture and Integration
AirWatch is offered as an on-premises, cloud-hosted software-as-a-service (SaaS), or hybrid solution. All three approaches employ a common console interface and a centralized reporting engine. A single instance of the on-premise solution can support more than 100,000 devices while the SaaS solution supports an unlimited number of endpoints. All platform features support iOS and Android devices, and most features can also be employed to support Windows devices. AirWatch also provides some support for BlackBerry, Chrome, Mac OS X, QNX, and Extended Android (i.e., Samsung SAFE, Samsung KNOX, and Intel DPT) devices.
The AirWatch Cloud Connector (ACC) enables organizations to integrate AirWatch with their back-end enterprise components, including email relay (SMTP), directory services (LDAP and AD), email management Exchange, O365, BlackBerry Enterprise Server (BES), and Lotus Domino Web Service. Additionally, the AirWatch Mobile Access Gateway (MAG) provides a secure method for individual applications to access corporate resources, such as SharePoint, websites, web apps, and internal applications. Direct integrations have been established with third-party management platforms, including Microsoft System Center Configuration Manager (SCCM), ServiceNow, Splunk, RSA Envision, ArcSight, IBM Tivoli, and Q1 Labs. Also, direct integration with the Apple Volume Purchase Program (VPP) simplifies management of application licenses on iOS devices, and additional integrations are possible through availability of more than 500 SOAP and REST-based APIs.

Functionality
AirWatch performs real-time discovery of any bare-metal or installed devices connected to the local network and records endpoint information in a centralized asset database. The ownership of the device is designated as owned by either the employee or the business. Inventory management features support application usage and version tracking, license management and enforcement, and software metering. From the administrative console, administrators can deploy or remove device access, applications, updates, email, and containers. A centralized software catalog enables user self-service access to public apps, proprietary apps, web apps, email, secure web browsing, data sharing sites, and remote access portals. The software catalog may be accessible through an enterprise app store, a hosted web service, and/or through integration with a public app store. Device, network, application, email, and printer configurations may be remotely configured from the management console. Remote device control is provided for Android, Windows Mobile, Windows CE and Mac devices.

Device security features offered by AirWatch include full or selective lock and wipe, application white and blacklisting, cut and paste restrictions, compliance assurance reporting and alarming, and rooting and jailbreaking detection. Data is secured on user devices with at-rest, in-motion, and in-use encryption, and content registration is employed for identifying confidential or sensitive information. Enterprise resources are isolated on mobile endpoints with the use of workspace containers, individual application containers, and or app wrapping. From the management console, administrators can centrally perform management tasks on enterprise resources inside user containers, including application authorization, password authentication, enable single sign-on, ensure secure document sharing, restrict cut and paste actions, and white or blacklist applications. The solution also natively provides secure email, web browsing, and remote access tools.

Deployment and Administration
The on-premise edition of AirWatch requires the installation of an administrative console server, device services, and a SQL database for storing asset and environmental data. The SaaS solution may be completely hosted in the cloud to enable rapid deployment while eliminating up-front infrastructure and maintenance costs. The SaaS approach may also optionally employ locally installed ACC and MAG components for improved integration with back-office services. Devices are auto detected or can be imported from a listing service, such as Active Directory, and client agents may be installed remotely by administrators or by end users through public app stores. A wide variety of user self-service capabilities are supported by the solution to empower end users and minimize administrator support.
tasks. AirWatch can also automatically respond to trigger events by initiating management tasks, such as to deploy patches, reconfigure applications, blacklist applications, disable user access, lock or wipe devices, send notifications to report noncompliant devices, or request a device check-in.

Maintenance contracts with AirWatch provide access to remote live service desk support accessible via phone or email, 24x7x365. AirWatch also offers professional service for on-site support to assist with installation, training, and problem remediation. Administrators are also supported with an integrated knowledgebase portal and access to supported online community forums. Diagnostic information, including error messages on the server and supported devices, is automatically collected and may be reported directly to AirWatch to assist with problem remediation and platform improvement. Updates for the platform are released roughly every two to three months.

Cost Advantage
AirWatch by VMware provides transparent pricing with bundles listed directly on its website (www.air-watch.com/pricing). The cloud-hosted solution is offered for annual subscription licenses while the on-premise solution is offered for one-time, perpetual licenses. In both cases, licenses may be purchased per device or per user. The latter may provide significant cost savings if users employ more than one device. While maintenance is included in cloud-hosted, subscription licenses, an annual maintenance fee (calculated as a fixed percentage of the initial purchase price) is required for ongoing support and updates.

Four tiered editions of AirWatch are offered, with pricing increasing proportional to the amount of included functionality. For the purposes of EMA’s assessment, the AirWatch Blue Management Suite was selected as this provided the broadest feature set applicable to the MDM Radar Report evaluation KPIs. However, it should be noted that more cost-effective editions are available if a lower level of functionality is required. Deployment and professional services are also offered for an additional cost. Discounts are also available for bulk license purchase and extended period pricing agreements (i.e., three year agreements versus one year agreements).

Vendor Strength
Broadly recognized as a leader in enterprise mobility management, AirWatch is focused on delivering solutions that empower companies to be innovative with the employment of mobile technologies rather than struggle with the complexities of managing mobility. To achieve this, the vendor maintains a common development platform, a multitenant and highly scalable architecture, and a broad development ecosystem that crosses OEMs, application developers and third-party solution providers. AirWatch’s parent company, VMware, is a leader in cloud and virtualization technology and was recently recognized by Forbes as one of the world’s most innovative companies.

AirWatch has a broad, global channel. AirWatch maintains development and channel relationships with more than 450 partners. EMA interviews with AirWatch customers revealed they believe the vendor is committed to providing mobility solutions and ensuring end users receive “the best experience possible.”
Strengths and Limitations

AirWatch MDM strengths are:

• **Breadth of Functionality** – EMA analysis indicated AirWatch provides the broadest MDM feature set among all the evaluated solutions.

• **Updates** – Application updates can be pushed and removed remotely by administrators or provisioned directly by end users, providing much broader support than most competing solutions.

• **Self-service Capabilities** – AirWatch empowers end users with the most comprehensive set of self-service capabilities of any solution in EMA’s evaluation. Self-service features include application provisioning, email configuration, container installation, data storage access, service request initiation, device location, remote lock and wipe, messaging, set roaming, clearing passcodes, and personal content management.

• **Identity Management** – AirWatch provides comprehensive, centralized support for identity management, including password authentication, password synchronization, self-service password resets, privileged password management, and single sign-on features.

AirWatch MDM limitations are:

• **Native Malware Protection** – AirWatch does not include any antivirus or antimalware scanning, reporting, or remediation tools out of the box. However, the platform does integrate with third-party solutions including F-Secure, Appthority, Veracode, Blue Coat, Zscaler, Lacoon, Webroot, and Symplified.

• **Virtualization Support** – Desktop and application VMs cannot be provisioned, deployed, or removed directly from the management console or through the software catalog. However, the solution does offer mobile hypervisor and workspace virtualization support, and it is integrated with the broader VMware Horizon portfolio which offers strong desktop and application VM solutions.

• **Communication Filtering** – No filters are provided to block or limit inappropriate communications via short message service (SMS) or multimedia messaging service (MMS).

About Enterprise Management Associates, Inc.

Founded in 1996, Enterprise Management Associates (EMA) is a leading industry analyst firm that provides deep insight across the full spectrum of IT and data management technologies. EMA analysts leverage a unique combination of practical experience, insight into industry best practices, and in-depth knowledge of current and planned vendor solutions to help EMA’s clients achieve their goals. Learn more about EMA research, analysis, and consulting services for enterprise line of business users, IT professionals and IT vendors at www.enterprisemanagement.com or blogs.enterprisemanagement.com. You can also follow EMA on Twitter, Facebook or LinkedIn.

This report in whole or in part may not be duplicated, reproduced, stored in a retrieval system or retransmitted without prior written permission of Enterprise Management Associates, Inc. All opinions and estimates herein constitute our judgement as of this date and are subject to change without notice. Product names mentioned herein may be trademarks and/or registered trademarks of their respective companies. “EMA” and “Enterprise Management Associates” are trademarks of Enterprise Management Associates, Inc. in the United States and other countries.

©2016 Enterprise Management Associates, Inc. All Rights Reserved. EMA™, ENTERPRISE MANAGEMENT ASSOCIATES®, and the mobius symbol are registered trademarks or common-law trademarks of Enterprise Management Associates, Inc.