EMA Radar™ for Mobile Device Management (MDM)

Q1 2016 – Report Summary and Zoho/ManageEngine 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  
  Zoho/ManageEngine – MDM Strong Value ........................................................................... 7  
  EMA Radar Profile: Zoho/ManageEngine ............................................................................ 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 even 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 publically 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.

---

**Zoho/ManageEngine – MDM Strong Value**

ManageEngine Mobile Device Management Plus extends management support of the vendor’s flagship endpoint management platform, Desktop Central, to smartphones and tablets and provides functionality for application management, security management, and “bring your own device (BYOD) management. Self-service functionality—including the ability of users to provision applications, track devices, or lock devices—is a particular strength of the platform noted by existing users.
Introduction
Established in 2003 as a company division of Zoho Corporation, ManageEngine is a provider of enterprise IT management software, supporting networks, servers, desktops, applications, mobile devices, security, Active Directory, and help desk solutions. ManageEngine Desktop Central is the vendor’s core endpoint management platform with native support for desktop management, including patching provisioning, asset management, and remote administration. ManageEngine Mobile Device Management Plus is offered as a standalone solution or as an add-on package to Desktop Central, extending management support to tablet and smartphone devices. The platform provides features for application management, security management, and “bring your own device” (BYOD) management.

Architecture and Integration
ManageEngine Desktop Central and Mobile Device Management Plus may be adopted an on-premises software-based solution. A single on-premises management server can support up to 20,000 endpoints. As a fully integrated platform, the combined solution can natively manage both PC and mobile devices. Supported mobile platforms include iOS, Android, and Windows Phone. The solution also integrates directly with ManageEngine ServiceDesk Plus to directly facilitate help desk support and to store job objects as CIs in the natively included configuration management database (CMDB).
Functionality
With ManageEngine Mobile Device Management Plus, mobile devices connected to the local network are discovered and device details—including system information, installed applications, device ownership, and license information—are collected and stored in a centralized asset database. Enterprise applications email and patches may be deployed directly from the centralized management console or by end users via an enterprise app store, a public apps store, or a self-service user portal. Systems, networks, applications, and email can be remotely configured directly from the management console. Security features include device lock and wipe, password management, application blacklisting and whitelisting, compliance assurance reporting and alarming, and rooting and jailbreaking detection.

Deployment and Administration
ManageEngine Mobile Device Management Plus must be hosted on a Windows server with a built-in Postgres database for local record storage. Mobile device clients require the installation of a software agent that is downloaded during the user enrollment process. For iOS devices, enrollment may be initiated through Apple Configurator or Apple Device Enrollment Program (DEP). Bulk enrollments may be accomplished by importing a CSV file. Administrators access ManageEngine Mobile Device Management Plus via a web-accessible, centralized console interface. Role-based access allows the interface to be customized to limit access to only the features necessary for accessing users to perform authorized job tasks. On detection of a policy breach, the solution can automatically perform tasks—including application reconfigurations, application blacklisting, and device wipe—without administrator interaction. Code fixes and updates to the solution are release roughly every two to three months.

For organization that adopt a service contract, ManageEngine provides live service desk support, including 24x7 (except holidays) phone and email support. ManageEngine also hosts an online social network where IT professional can share management tips and find solutions to specific IT challenges. The vendor also offers professional services that can assist with installation, problem resolutions, and training.

Cost Advantage
ManageEngine provides transparent pricing for its endpoint management solutions (available online at [https://store.manageengine.com/desktop-central/index.html](https://store.manageengine.com/desktop-central/index.html)). ManageEngine Mobile Device Management Plus is offered as an add-on to any core Desktop Central management platform (sold separately) and is licensed for either a one-time perpetual fee or for an annual subscription fee per supported device. Licenses are purchased in groups with discounts applied proportional to the number of licenses purchased. Maintenance and support contracts are included with subscription licenses, but they must be purchased for an additional annual fee to support devices with perpetual licenses.

Vendor Strength
ManageEngine is a privately held subsidiary of Zoho Corporation and is headquartered in Pleasanton, CA. Zoho’s other divisions are focused on providing business productivity applications in the cloud, and its long term strategy is to integrate these solution—including CRM, email, and project management—to the MDM container. The vendor believes mobile containerization and enterprise mobility management are the future of end-user computing, as this will enable enterprises to clearly separate personal and corporate data and manage them with ease. As a privately held company, Zoho does not publicly disclose its revenue or development financing.
Strengths and Limitations

ManageEngine MDM strengths are:

• **Licensing** – License costs for ManageEngine Mobile Device Management Plus are among the lowest of all the solutions included in EMA’s evaluation. Licensing costs are transparent, easy to understand, and flexible to support a broad range of business requirements.

• **Unified Endpoint Management** – Management of both PC and mobile endpoints are accessed from a common management interface and record data in a consolidated asset database.

• **Self-Service Features** – Users have the ability to provision application resources through on-demand access to in-house and app store software. Additionally, the ability of end users to remotely track and/or lock their devices was specifically identified by customers as favored features.

ManageEngine MDM limitations are:

• **Third-Party Integrations** – There are currently no direct integrations with third-party systems or service management solutions.

• **Native Malware Protection** – Antivirus, anti-spyware, or other antimalware scanning, reporting, or remediation tools are not included out-of-the-box with the solution.

• **Secure Web Access** – Web applications cannot be secured, wrapped, and/or provisioned through the platform, and no secure web browser is provided.

• **Remote Control** – Mobile devices cannot be remotely accessed and controlled through terminal emulation directly from the management console.

• **Crash Reporting** – Crash events and application errors are not recorded in real time and historically tracked.

• **Backup and Recovery** – No mobile device backup and recovery capabilities are included natively with the solution.

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 EMAs 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.