2014
MOBILE DATA MANAGEMENT BUYER'S GUIDE

THE INSIDER'S GUIDE TO EVALUATING MOBILE DATA MANAGEMENT SOFTWARE PRODUCTS

By Howard Haile

www.dcig.com

DCIG 2014 MOBILE DATA MANAGEMENT BUYER'S GUIDE

THE INSIDER'S GUIDE TO EVALUATING MOBILE DATA MANAGEMENT SOFTWARE PRODUCTS

Table of Contents

DCIG 2014 MOBILE DATA MANAGEMENT BUYER'S GUIDE

THE INSIDER'S GUIDE TO EVALUATING MOBILE DATA MANAGEMENT SOFTWARE PRODUCTS

Introduction

Since the preliminary *Midrange Array Buyer's Guide* in 2010, DCIG has been diligent in its efforts to continue to provide accurate and applicable Buyer's Guides for organizations such as yours. One of the newest Guides added to our portfolio is the *DCIG 2014 Mobile Data Management (MDM) Buyer's Guide.*

DCIG has seen many trends. Such movements in the market usher in change for connected industries. One of those tidal waves of transformation is the Bring Your Own Device (BYOD) movement. *Many businesses have recently taken to the BYOD trend to grant their workers mobile access to company networks.*[1] As mobile devices enter the workforce, organizations are forced to adapt or be left in the dust.

Mobile Data Management Works For You

All organizations hope for higher output and the BYOD trend seems to be providing just that. Statistics note that *almost one in five small businesses in the U.S., Canada and Australia have seen at least a 30 percent gain in productivity as a result of their BYOD implementations.*[2] However, whereas larger enterprises are able to offer solutions to mobile data management on-premise, scalability can sometimes prevent SMBs from being able to implement the necessary data supervision themselves. In that regard, small to mid-sized business (SMB) may chose other options.

Due to this and other more perplexing questions a new technological need has emerged. MDM providers have risen and are aptly prepared to provide an off-site, yet hands on and personal solution for organizations which desire to enforce a governing policy on personal devices being brought to work; primarily to SMBs. In recognition of the growing need in the area of mobile data management DCIG has issued its first *DCIG 2014 Mobile Data Management Buyer's Guide.* This Guide focuses on MDM features that are necessary to effectively manage an enterprise's mobile environment while easily complying with corporate policies and standards. Examples of MDM providers covered in this Buyer's Guide include: Sophos, Symantec, MobileIron and Tangoe.

The *DCIG 2014 Mobile Data Management Buyer's Guide* will give businesses an understanding of:

- The MDM provider's flexibility to areas such as architecture diversity
- How providers approach security and compliance features
- The provider's ability in regards to administrative features and support issues
- How the MDM vendor is able to meet the needs and demands of a robust MDM implementation

1. Centerbeam Industry News. "Mobile Device Management has Room for Growth Along with BYOD." 5 July 2013. http://www.centerbeam.com/news/IT-Strategy/Mobile-device-management-has-room-for-growth-along-BYOD-CBOID120831543-GRPOID50590016/View.aspx.
2. Citrix Systems, Inc. "Global Research Shows Mobilizing Your Small Business Creates Competitive Edge." 6 June 2013. http://www.citrix.com/news/announcements/jun-2013/global-research-shows-mobilizing-your-small-business-creates-competitive-edge.html.

Introduction continued

First of its Kind

Like all prior DCIG Buyer's Guide, this DCIG 2014 Mobile Data Management Buyer's Guide continues to help any company looking to quickly understand what features MDM providers provide without having to do a lot of in-depth research which is very hard to do by traditional means. This guide will give system and network administrators, senior IT leaders, and security and compliance officers a "one-stop shop" to see where a MDM vendor stands on different and important features.

This first-ever comprehensive report weights, scores and ranks 26 mobile data management companies. Management, Operating Environment, User Experience, Security and Compliance, and Security are the main areas evaluated and are given a classification of "Basic", "Good", "Excellent", "Recommended", and "Best-in-Class". The report offers all the information an organization should need to make a highly informed decision on what mobile device management vendor is the right fit for their organization.

Note that this Buyer's Guide is not intended to be a substitute for bringing individual MDM solutions in-house and testing them with specific applications. That function should still be done, if possible, since every MDM solution will perform differently under different real-world application workloads.

We believe you will find this Buyer's Guide meets this intended purpose in your environment.

Executive Summary

Recent statistics surrounding Mobile Data Management (MDM) along with the bring your own device (BYOD) movement are astounding. Consider these facts:

- ***Sixty-one percent*** of small to mid-sized businesses (SMBs) have adopted a BYOD policy or initiative for employee-owned smartphones, tablets, or computers[1]
- In 2011, worldwide mobile enterprise management software revenue totaled $444.6 million. This number is expected to grow at a compound annual growth rate (CAGR) of 31.8% over the forecast period, resulting in total Mobile Enterprise Management (MEM) software revenue of ***$1.8 billion by 2016***[2]
- In 2010-2011 companies such as MobileIron, AirWatch, Good Technology, Fiberlink, and Zenprise each realized ***triple-digit growth***[3]

An Age of Solutions

One could say, *"It all began with the Blackberry®."* The advent of this multi-functioning mobile device gave corporate America a whole new set of possibilities in the workplace. Employers and employees alike realized the potential for growth and recognizable positive production with the use of devices that went wherever they did. Few considered any security risks or dealt with corporate policy compliance issues due to the ability to control the entire device issued by the company.

However, the market continued to develop. Competitive counterparts entered the scene. Apple's iPhone and iPad emerged, then the Android platform, all of which forced organizations to maneuver past a corporate-liable policy and accept a BYOD strategy.

Though the concept of allowing private mobile devices at work may not be entirely new, how organizations have decided to deal with the onslaught of usage is. Instead of managing the entire personal device, organizations simply want to control the trail of sensitive information.

In exchange for corporate issued devices, organizations began to look into geo-fencing as a means to control data. Other state-of-the-art solutions were needed to alleviate the risk of data leakage and augment security around the information going to and from the devices on the company network. Therefore, management of devices needed to be flexible. Solutions needed to be open to work with either on-premise infrastructure, the cloud, or a hybrid approach delivery model.

1. Citrix Systems, Inc. "Global Research Shows Mobilizing Your Small Business Creates Competitive Edge." 6 June 2013. http://www.citrix.com/news/announcements/jun-2013/global-research-shows-mobilizing-your-small-business-creates-competitive-edge.html.
2. Crook, Stacey K., Stephen D. Drake, Benjamin Hoffman. "IDC Market Analysis: Worldwide Mobile Enterprise Management Software 2012-2016 Forecast and Analysis and 2011 Vendor Shares." September 2012. http://idcdocserv.com/236835e.
3. Ibid.

Executive Summary continued

The Cloud

Research has found that the *mobility of the BYOD could be a way to maintain company efficiency during the usually slower summer months.*[4] Despite this fact, even with the use of BYODs on the upswing, *twenty-six percent of businesses have yet to set up comprehensive MDM strategies alongside their BYOD plans.*[5]

Hence, a solution for data management evolved along with DCIG's interest in this growing area of the market. Our research shows that the ideal business for an MDM solution is the small to midsize business (SMB). For such organizations, the use of the cloud or a hybrid model for data storage is most cost-effective. As cloud adoption continues to gain acceptance so does the concern with administrative and security features available for differing mobile operating systems.

DCIG understands these needs and has risen to the unique challenge of providing you and your organization with a comprehensive list of MDM providers and their competing features. Our goal is to assist you in this all-important buying decision while removing much of the mystery around how MDM providers are configured and the stress in selecting which ones are suitable for which purposes.

A high score for a MDM vendor means that it had the most complete feature set around the key areas of focus for this Buyer's Guide: Management, Operating Environment, User Experience, Security and Compliance, and Support.

Easy, Comprehensive and Objective

This *DCIG 2014 Mobile Data Management Buyer's Guide* accomplishes the following:

- Provides an objective, third party evaluation of mobile data management providers that scores their features from an end user's viewpoint
- Includes recommendations on how to best use this Buyer's Guide
- Scores and ranks the features on each mobile data management vendor based upon the criteria that matter most to end users so they can quickly know which MDM solution is the most appropriate for them to use and under what conditions
- Provides 26 data sheets from 26 different MDM providers so end users can do quick comparisons of the features that are supported and not supported.
- Provides insight into which features on a MDM solution will result in improved performance
- Provides insight into what features MDM providers offer to optimize their BYOD integration
- Gives any organization the ability to request competitive bids from different providers of MDM solutions that are one-to-one comparisons

4. Centerbeam Industry News. "Mobile Device Management has Room for Growth Along with BYOD." 5 July 2013. http://www.centerbeam.com/news/IT-Strategy/Mobile-device-management-has-room-for-growth-along-BYOD-CBOID120831543-GRPOID50590016/View.aspx.

5. Ibid.

How to Use the 2014 Mobile Data Management Buyer's Guide

This *DCIG 2014 Mobile Data Management Buyer's Guide* is intended to aid in the efforts of an organization's search for a suitable solution to managing their secure data on mobile devices. Whether the data is stored in the cloud or in a hybrid setting, it is important to note that this Buyer's Guide is intended to help users in their purchase of a MDM solution *NOT* to tell users exactly which MDM solution to purchase. Think of this Buyer's Guide rather as an assistant who compiled a list of competitive MDM solutions and comparable features suited to your organization's specific needs.

The "Best-in-Class", "Recommended", "Excellent", "Good" and "Basic" rankings included in this Buyer's Guide are a measure of how much functionality and capability each solution has relative to the overall landscape—not whether the solution is the most appropriate fit for any particular organization.

Rather, this Buyer's Guide does give organizations some sense of how each mobile data management solution compares to other solutions of its classification as well as offer additional insight into what service and feature offerings are available.

Organizations should, therefore, use this Buyer's Guide as a handbook to understand:

- Who provides mobile data management solutions
- What mobile data management solutions are available
- What features, functions and services are available through each MDM solution

This Buyer's Guide also provides comments & thoughts on each MDM solution that has been weighted, scored and ranked; observations & recommendations on those rankings; numerous data sheets on each MDM solution; a glossary of terms; and provider contact information should you wish to reach out to them.

It is recommended that you and your management team use this *DCIG 2014 Mobile Data Management Buyer's Guide* as a guide to understand:

1. ***Accelerate the process of assessing available MDM solutions.*** Organizations such as yours can bypass the need to compile your own list of mobile data management companies along with the features, functions and services each company offers.
2. ***Augment your ability to evaluate MDM solutions.*** DCIG has already ranked each MDM solution/company as "Best-in-Class," "Recommended," "Excellent," "Good" and "Basic" on each solution's respective data sheet. This immediately provides organizations such as yours with a third party resource to help substantiate your own findings and recommendations.
3. ***This Buyer's Guide normalizes complex mobile data management terminology.*** Every computing industry has a proclivity to adopt acronyms and jargon that is specific to it. The mobile data management industry is no different as it also tends to use unfamiliar terms and sometimes even refers to the same technology in different ways which complicates any technology evaluation. The Appendix of this Buyer's Guide explains the jargon specific to mobile data management solutions in order to enhance the quality and productivity of the discussions around the technology.
4. ***Provides a concise summary of each MDM solution for ease of reporting and sharing.*** Each organization has professionals in various departments within their infrastructure. Even technology-based organizations inevitably have to report back to the business side and when that occurs—nothing rings truer than numbers. So to help in this endeavor, each product is scored and ranked so conversations regarding mobile data management can more quickly shift to a focus on which technology to buy and how the purchase of this solution will help the bottom line.

Disclosures

Over the last few years the general trend in the US has been for both large and boutique analyst firms to receive some or all of their revenue from mobile data management (MDM) providers.

DCIG is no different in this respect as it also receives payment for the different services it performs for MDM providers. The services that DCIG provides include blogging, case studies, product reviews, executive white papers, full length white papers and Special Reports.

So in the interest of being fully transparent, a number of the MDM providers included in this *DCIG 2014 Mobile Data Management Buyer's Guide* are or have been DCIG clients.

This is not to imply that they were given preferential treatment in the Buyer's Guide. All it meant was that DCIG had more knowledge of their MDM solution(s) and that DCIG would consider their solution for inclusion in this Buyer's Guide.

In that vein, there are a number of important facts to keep in mind when considering the information contained in this *DCIG 2014 Mobile Data Management Buyer's Guide* and its merit.

- No MDM provider paid DCIG any fee to develop this Buyer's Guide
- DCIG did not guarantee any MDM provider that its solution would be included in this Buyer's Guide
- DCIG did not imply or guarantee that a specific MDM solution would receive a good score on this Buyer's Guide ahead of time
- All research was based upon publicly available information, information provided by the MDM provider and the expertise of those evaluating the information
- Because of the number of features analyzed, how these features were weighed and then how these MDM providers were scored and then ranked, there was no way for DCIG to predict at the outset how individual MDM solutions would end up scoring or ranking.

DCIG wants to emphasize that no MDM provider was privy to how DCIG did the scoring and ranking of the MDM solutions. In every case the MDM providers only found out the scores and rankings of its solution after the analysis was complete.

Mobile Data Management Inclusion and Exclusion Criteria

Inclusion of products in the *DCIG 2014 Mobile Data Management Buyer's Guide* was based primarily upon the following criteria:

- ***The solution's primary purpose had to be for managing mobile devices.*** The main intent of these products is to provide enterprises the ability to manage mobile devices based on corporate defined policies and standards.
- ***Its primary intent is to provide enterprises the ability to maintain security and manage features over corporate or personal devices.*** Management of devices may be delivered by an on-premise infrastructure, delivered via the cloud, or a hybrid approach delivery model.
- ***While a number of solutions may offer the same feature options depending on the delivery model, it was not a prerequisite for the feature sets to be identical.***
- ***Must provide functionality as original software, i.e. not licensed from original equipment manufacturer (OEM).*** There are service providers and consultants that offer MDM through a combination of licensed best-in-class MDM software and associated services. DCIG excluded these providers and consultants and their respective MDM offerings from this Buyer's Guide.
- ***Must support functionality asked about through software, i.e. not thru services.*** Based upon the evolution of the MDM software market, it is not unusual for MDM providers to provide support for a specific feature through services as opposed to software. DCIG does give these providers ranking points for supporting those features.
- ***Must provide sufficient information for DCIG to draw a meaningful conclusion.*** DCIG made a good faith effort to identify, reach out and obtain information from as many MDM providers as possible by providing access to an online survey for them to complete. However in a few cases MDM software had to be excluded due to lack of response and/or cooperation from certain MDM providers and/or lack of reliable publically available information.
- ***Must be generally available prior to June 15th, 2013.*** A cut-off date had to be put in place or this Buyer's Guide would never be published. Some allowances were made for feature or product enhancements that were made in Late June 2013 that did not positively or negatively affect the rankings for any one vendor in developing this Buyer's Guide.

The Seven Step Process Used to Score and Rank Mobile Data Management Providers

To score and rank each mobile data management provider, DCIG went through a seven (7) step process to come to the most objective conclusion possible.

1. DCIG listed out of all of the features available on all of the mobile data management solutions. Prior to selecting the features that were included in the final evaluation in the Buyer's Guide, DCIG went through and quantified what features each mobile data management provider possessed. DCIG then 'normalized' the list of features available on mobile data management technology such that a common name for each feature was established.
2. DCIG established which features would be included in the Buyer's Guide. One of the goals of this Buyer's Guide was to try to only include features on each mobile data management solution that could be objectively and authoritatively analyzed. For example, "At-Rest Encryption" was evaluated as a feature along with "In-Transit Encryption." Organizations can use both at-rest and in-transit encryption to ensure maximum data protection from unauthorized access. The use of both at-rest and in-transit encryptions together insures the entire data path remains secure—all of which makes each of these strong features for DCIG to evaluate.
3. Each feature had a weighting associated with it. The weightings were used to reflect whether or not a feature was supported and potentially how well it was implemented. For example, "Support Staff Availability" is more of a "24x7x365" answer than a "Yes" or "No" type response, whereas "Methods of Support" could include a number of different protocols. As such, each feature was weighted and scored differently.
4. A questionnaire that asked about each of the features scored in this Buyer's Guide was sent to each provider. In addition to using the information that was publicly available on each provider's website, each provider included in this Buyer's Guide had the opportunity to respond to a questionnaire sent by DCIG. This was done to both verify that the information DCIG found on the provider's website was correct as well as remove any ambiguities that existed regarding how some of the features were implemented.
5. All of the features were scored based upon the information that was gathered. The weighting and scoring was done by DCIG and by a select group of end-users who assisted DCIG in selecting the features to be evaluated in this Buyer's Guide.
6. The features for mobile data management providers broke down into four larger categories: Management, Operating Environment, User Experience, Security and Compliance, and Support.
   - Device Management. *Focuses on the administrative features related to management of devices*
   - Operational Environment. *Focuses on device deployment options and device management operating features*
   - Security & Compliance. *Focuses on management of security controls and management of features of compliance concern*
   - Support. *Focuses on available vendor support options*
7. The mobile data management providers were ranked using standard scoring techniques. The goal of all DCIG Buyer's Guides is to establish clear lines of differentiation between the products included in them. To accomplish this objective, after each product is weighted and scored, the mean or average score and standard deviation for all of the products were determined. These were then used as the basis for developing a ranking for each mobile data management solution:

- Those mobile data management providers that were .5 or greater standard deviations below the mean were given the rank of "Basic"
- Those mobile data management providers that were .5± standard deviations above or below the mean were ranked as "Good"
- Those mobile data management providers that were .5 standard deviations above the mean were ranked as "Excellent"
- Those mobile data management providers that were greater than 1.5 standard deviations above the mean were ranked as "Recommended"
- The top ranked mobile data management provider was given the classification of "Best-in-Class"

Using this scoring and ranking method, DCIG feels confident that all of the providers included in this report can be reasonably classified as a "Mobile Data Management" solution as all providers came within two (2) standard deviations of the mean.[1]

1. +/- 5%.

DCIG Comments and Thoughts on Mobile Data Management…

Cloud

Companies both large and small are seeing an ever increasing migration from corporate issued to personally owned devices. Due to this impetus, companies have become more open and willing to move to cloud provided MDM services. As a result of this increasing adoption of cloud-based MDM, DCIG has included cloud-based device management in the *2014 DCIG Mobile Data Management Buyer's Guide*.

The benefits of cloud-based mobile data management are many, including rapid deployment and low infrastructure investment. But cloud also has its limitations. The key restriction is the device management feature sets. These are often more robust with on-premise installations, but scaling the number of devices needing to be managed from a cloud installation perspective can be challenging. Larger enterprises, with a significant number of managed devices along with a more mature IT environment, may be less inclined to move into a hosted MDM model. Thus, on-premise and hybrid infrastructures for deployment are better options for these enterprises.

At-rest and In-transit encryption

Many companies face compliance mandates such as HIPAA[1], HITECH[2], SOX[3]. Other companies need to protect day-to-day business information. These issues have become difficult due to the dynamic environment of policies in the professional-realm. This has led to personally identifiable information being increasingly reliant on encryption. Data encryption is often the only "safe harbor" from sanctions in the face of a data breach. At-rest and in-transit encryption play significant roles in MDM from data stored resident on devices as well as data being transmitted wirelessly.

At-rest applies to encryption once the data has arrived at the target device. At-rest is fundamentally different than in-transit encryption. In-transit encryption takes place through a software algorithm as the sending device encrypts the data while it is being transferred to the receiving target.

Organizations can use both at-rest and in-transit encryption to ensure maximum data protection is employed. If both encryption methods are used together, the data is encrypted from beginning to end, thus protecting the entire data process path from unauthorized access.

Automation

Mobile data management automation is an area of emphasis for many organizations. The employment of automation promises to facilitate efficient management of an organization's MDM solution, and thus enable a more agile response from IT to changes its business requirements. Ultimately, automation means more staff time can be spent addressing business specifications rather than managing routine tasks around MDM.

For example, support for automated device provisioning, security policy restriction, policy deployment, and enforcement can:

- simplify management
- reduce complexity
- reclaim IT staff time
- reduce inefficiency

Security Policy Enforcement

Device policy enforcement is a primary tenant to MDM. Organizations invest in MDM for many reasons, two of which are: 1) to reduce business risks and 2) to maintain the ability to create policies to match the organization's risk appetite. Both are benefits to device policy enforcements and serve as keys to the successful integration of a MDM solution for any organization.

Though policies can often be difficult to work with, they help ensure compliance with the organization's security requirements to reduce the possibility of a breach in corporate data. However, when a device is jailbroken and rooted, the built-in security features on the most popular mobile device platforms are bypassed and the device can then be exploited for unauthorized access to hardware and software. DCIG focused on the MDM provider's ability to safeguard data through robust policy management. Without the ability to safeguard data in a flexible way to meet the organization's goals, MDM would not be effective in providing the data protection needed.

2. Health Insurance Portability and Accountability Act.
3. Health Information Technology for Economic and Clinical Health Act.
4. Sarbanes-Oxley Act.

Observations and Recommendations for Each Mobile Data Management Provider Ranking

General Observations

All twenty-six (26) mobile data management (MDM) providers that were weighted, scored and ranked in the *DCIG 2014 MDM Buyer's Guide* held the following characteristics:

- All MDM providers provision different device platforms
- All MDM providers provide basic MDM functionality
- Out of 26 MDM providers, twelve (12) offer cloud-based delivery models
- Hybrid delivery model, a mixture of cloud and on-premise delivery models, is the least offered feature
- Product support offerings vary widely between product providers

"Best-in-Class" and "Recommended" Rankings

Observations:

The mobile data management provider(s) that earned "Best-in-Class" and "Recommended" rankings in the *DCIG 2014 MDM Buyer's Guide* generally shared the following characteristics:

- Provides infrastructure flexibility between on-premise or cloud-based delivery models (hybrid delivery model)
- Offers scalable high availability configurations
- Supports device encryption as well as secure communications
- Detects security requirements around jailbroken or rooted devices
- Manages anti-virus on devices
- Offers a corporate application store (App Store)
- Provides strong product support

Recommendations:

MobileIron, Amtel, and Symantec competed for the top spot in the "Best-in-Class" category. All offer features required by a MDM solution, but MobileIron leads. MobileIron's feature leadership is due to its rich security feature set, delivery model flexibility, and strong product support. Amtel and Symantec came in second and third, respectively, with a ranking of "Recommended".

MobileIron provides a high level of device scalability with a single cluster configuration supporting up to 100,000 devices. MobileIron offers other capabilities many organizations will find useful including:

- PKI[1] Certificate support
- Support for Windows 8
- SIEM[2] and DLP[3] integration
- Support for the Apple VPP and Samsung SAFE program
- Two-Factor authentication support
- Customizable dashboards

"Excellent" Ranking

Observations:

The mobile data management provider(s) that earned the ranking of "Excellent" in the *DCIG 2014 MDM Buyer's Guide* generally shared the following characteristics:

- Support hardware and software provisioning
- Integration with Microsoft(r) Active Directory and LDAP
- Provides support for Corporate App Store, Android 4.x, and IOS 6.x
- Support for device encryption: data at rest and data in transit

Recommendations:

Out of the four (4) mobile data management providers that achieved a ranking of "Excellent", Fixmo and Excitor grabbed the top two positions. When scoring

1. Public Key Infrastructure.
2. Security Information and Event Management.
3. Data Loss Prevention.

the providers in this category, a noticeable decrease in Management, as well as Security and Compliance feature sets were seen when compared to those rated "Best-in-Class" or "Recommended". Yet, product support remained strong, though it may have varied among the "Excellent" providers.

IT departments should be careful to consider: 1) high-availability and 2) device scalability. These two factors are essential when an organization is selecting a mobile data management provider.

"Good" Ranking

Observations:

The mobile data management provider(s) that earned the ranking of "Good" in the *DCIG 2014 MDM Buyer's Guide* generally shared the following characteristics:

- Supports the on-premise deployment option
- Provisions different device platforms

Recommendations:

Seven (7) mobile data management providers shared the ranking of "Good". The top three providers that captured the highest scores in this category were: Fiberlink, Sybase (SAP) Afaria, and Motorola. All seven providers that earned the "Good" ranking varied widely in their feature support options. For instance, Security and Compliance support differed significantly from those ranked "Best-in-Class" and "Recommended". Alongside the disparity in Security and Compliance, a decrease of MDM product support options was noted as well.

In spite of setbacks in support, cloud deployment options are offered and employed by three MDM providers in the "Good" category.

"Basic" Ranking

Observations:

The mobile data management provider(s) that earned the ranking of "Basic" in the *DCIG 2014 MDM Buyer's Guide* generally shared the following characteristics:

- Supports provisioning of different platforms
- Only three (3) MDM providers in the basic category support a cloud-based deployment

Recommendations:

In the category of "Basic", twelve (12) mobile data management providers were weighted, scored and ranked. Three (3) beat out their competitors by scoring better than the rest: Silverback, OpenPeak and SOTI. All the providers in this category were found to be limited in three specific areas when compared to the "Good" category: 1) deployment options, 2) security features and 3) support options. The limitations noted among the "Basic" MDM providers may be found particularly in the area of support for common security features, such as encryption.

Despite the fact that product support options are limited, even at the "Basic" level organizations can find needed administrative and support options depending on the different offerings by each vendor.

MOBILE DATA MANAGEMENT SCORES AND RANKINGS

The scores and rankings for the mobile data management products contain the following information:

- Charts that list the Overall scores and rankings for all of the products
- The mean and the standard deviation that was used to establish how each software product was ranked
- A summary of the primary findings

OVERALL SCORES AND RANKINGS

	MOBILE DATA MANAGEMENT SOFTWARE	SCORE	RANKING
1.	MobileIron® Advanced Mobile Management	116.00	BEST-IN-CLASS
2.	Amtel Mobile Lifecycle Management	115.50	Recommended
3.	Symantec™ Mobile Management Suite	104.00	Recommended
4.	Fixmo® EMP	92.50	Excellent
5.	Excitor DME Mobile Device Manager	92.25	Excellent
6.	Tangoe Mobile Device Management	80.75	Excellent
7.	Sophos Mobile Control	69.50	Excellent
8.	Fiberlink MaaS360 Mobile Device Management	52.25	Good
9.	SAP (Sybase) Afaria	46.25	Good
10.	Motorola Mobile Services Platform v4	41.25	Good
11.	Airwatch Mobile Device Management	35.50	Good
12.	BoxTone Mobile Device Management	35.50	Good
13.	The Institution Revival Mobile Management Suite	32.75	Good
14.	Mobile Active Defense Mobile Enterprise Compliance and Security Server	28.50	Good
15.	Silverback Mobile Device Management	27.00	Basic
16.	OpenPeak Advanced Device and Application Management (ADAM)	26.50	Basic
17.	SOTI MobiControl	24.00	Basic
18.	Citrix® XenMobile (Zenprise)	24.00	Basic
19.	FancyFon Software FAMOC	22.00	Basic
20.	RIM Blackberry® Enterprise Service 10	20.50	Basic
21.	McAfee® Enterprise Mobility Management	20.00	Basic
22.	Trend Micro™ Mobile Security	19.75	Basic
23.	Smith Micro Software Enterprise Device Management	15.75	Basic
24.	Good™ Technology Good Mobile Manager	13.50	Basic
25.	IBM® MobileFirst Management	9.50	Basic
26.	Capricode SyncShield®	7.50	Basic

Total Number of Products **26**

Rankings

Highest Score	**116.00**	Recommended	**96.17 – 116.00**
Lowest Score	**7.50**	Excellent	**62.12 – 96.16**
Average (Mean)	**45.10**	Good	**28.07 – 62.11**
Standard Deviation	**34.05**	Basic	**7.50 – 28.06**

MOBILE DATA MANAGEMENT BUYER'S GUIDE PRODUCTS

Airwatch Mobile Device Management

DCIG Scores and Rankings

OVERALL SCORE	Management	Operating Environment	User Experience	Security and Compliance	Support
35.50	12.75	7.75	5.00	10.00	0.00
GOOD	GOOD	GOOD	BASIC	BASIC	BASIC

MANAGEMENT

Provision Platforms	Supported
Policy Restriction	Unsupported
Hardware Inventory	Supported
Device Ownership	Unsupported
Customizeable Dashboard	Supported
Bulk Device Management	Unsupported
Policy Alerts	Supported
Administrator Deployment	Unsupported
Device Change	Supported
Deploy Multiple Groups	Unsupported
Combined Group	Unsupported
Automatic Provision	Supported
SSAE-16	Unsupported
Database Instance (Total #)	1
Solution Options (Total #)	1
Device Change (Total #)	2
Notifications (Total #)	4
Dedicated Database	Unsupported
Backup and Recovery	Unsupported
Software Inventory	Unsupported
Apple VPP	Supported
Corporate v. Personal	Unsupported
Single Console	Supported
Change Propagations	Supported

OPERATING ENVIRONMENT

Deployment Options (Total #)	2
Solution Integration (Total #)	3
Cloud and On-Premise Same	Unsupported
Full MDM Functionality	Unsupported
Third Party Solution	Supported
DMZ Replication	Supported
High Availability	Supported
Secure Communications	Supported
Remote Troubleshooting	Unsupported
Corporate App Store	Unsupported
MDM Server	Unsupported
Location Services	Unsupported
Single Cluster Configuration	0
Windows 8	Unsupported
Windows 8 Plan	Supported

SUPPORT

Annual Downtime	Unsupported
Support Staff Availability	Unsupported
Methods of Support	Unsupported
Phone Support Hours	Unsupported
Not Under Contract Support	Unsupported
Not Under Contract Availability	Unsupported
Support Forum	Unsupported

SECURITY AND COMPLIANCE

Cloud Based	Supported
PKI Certificate	Supported
SIEM Integration (Total #)	0
DLP Integration (Total #)	0
Geo-Fencing	Supported
Detect Security Requirements	Unsupported
Jailbroken	Supported
Selective Wiping	Unsupported
Strong Password	Supported
Two-Factor Authentication	Supported
Device Encryption	Unsupported
Choose Enforcement	Unsupported
Blacklisted Applications	Unsupported
Rooted Device Detection	Unsupported
Manage Anti-Virus	Unsupported
Auto-Deletion	Unsupported
VPN Support	Unsupported
DLP Integration	Unsupported
Integrate AD/LDAP	Supported
Whitelisting Applications	Unsupported
Encryption Data-at-Rest	Unsupported
Server in DMZ	Supported
Data in DMZ	Supported
Granular Level	Supported
SAFE Program	Unsupported
Differing Mobile Policies	Unsupported

Supported Unsupported

Amtel Mobile Lifecycle Management

DCIG Scores and Rankings

OVERALL SCORE	Management	Operating Environment	User Experience	Security and Compliance	Support
115.50	32.00	16.25	16.00	43.75	7.50
RECOMMENDED	RECOMMENDED	EXCELLENT	BEST-IN-CLASS	RECOMMENDED	BEST-IN-CLASS

MANAGEMENT

Provision Platforms	✔
Policy Restriction	✔
Hardware Inventory	✔
Device Ownership	✔
Customizeable Dashboard	✔
Bulk Device Management	✔
Policy Alerts	✔
Administrator Deployment	✖
Device Change	✔
Deploy Multiple Groups	✔
Combined Group	✖
Automatic Provision	✔
SSAE-16	✔
Database Instance (Total #)	1
Solution Options (Total #)	3
Device Change (Total #)	3
Notifications (Total #)	4
Dedicated Database	✖
Backup and Recovery	✖
Software Inventory	✔
Apple VPP	✔
Corporate v. Personal	✔
Single Console	✔
Change Propogations	✖

OPERATING ENVIRONMENT

Deployment Options (Total #)	2
Solution Integration (Total #)	3
Cloud and On-Premise Same	✖
Full MDM Functionality	✔
Third Party Solution	✖
DMZ Replication	✖
High Availability	✔
Secure Communications	✔
Remote Troubleshooting	✔
Corporate App Store	✔
MDM Server	✔
Location Services	✖
Single Cluster Configuration	8,000
Windows 8	✖
Windows 8 Plan	✔

SUPPORT

Annual Downtime	✖
Support Staff Availability	24×7×365
Methods of Support	Email/Phone/Remote Monitoring/Web Chat
Phone Support Hours	24×7×365
Not Under Contract Support	8AM EST to 8PM PST
Not Under Contract Availability	Business Day Local
Support Forum	✔

SECURITY AND COMPLIANCE

Cloud Based	✖
PKI Certificate	✔
SIEM Integration (Total #)	✔
DLP Integration (Total #)	2
Geo-Fencing	✔
Detect Security Requirements	✔
Jailbroken	✔
Selective Wiping	✔
Strong Password	✔
Two-Factor Authentication	✔
Device Encryption	✔
Choose Enforcement	✔
Blacklisted Applications	✔
Rooted Device Detection	✔
Manage Anti-Virus	✔
Auto-Deletion	✔
VPN Support	✔
DLP Integration	✔
Integrate AD/LDAP	✔
Whitelisting Applications	✔
Encryption Data-at-Rest	✔
Server in DMZ	✖
Data in DMZ	✖
Granular Level	✔
SAFE Program	✔
Differing Mobile Policies	✔

✔ Supported ✖ Unsupported

Boxtone Mobile Device Management

DCIG Scores and Rankings

OVERALL SCORE	Management	Operating Environment	User Experience	Security and Compliance	Support
35.50	8.00	2.50	9.00	16.00	0.00
GOOD	GOOD	BASIC	GOOD	GOOD	BASIC

MANAGEMENT

Provision Platforms	Supported
Policy Restriction	Supported
Hardware Inventory	Supported
Device Ownership	Supported
Customizeable Dashboard	Unsupported
Bulk Device Management	Supported
Policy Alerts	Supported
Administrator Deployment	Supported
Device Change	Supported
Deploy Multiple Groups	Supported
Combined Group	Supported
Automatic Provision	Supported
SSAE-16	Unsupported
Database Instance (Total #)	1
Solution Options (Total #)	0
Device Change (Total #)	0
Notifications (Total #)	Supported
Dedicated Database	Supported
Backup and Recovery	Unsupported
Software Inventory	Supported
Apple VPP	Supported
Corporate v. Personal	Supported
Single Console	Supported
Change Propagations	Unsupported

OPERATING ENVIRONMENT

Deployment Options (Total #)	2
Solution Integration (Total #)	3
Cloud and On-Premise Same	Unsupported
Full MDM Functionality	Unsupported
Third Party Solution	Supported
DMZ Replication	Supported
High Availability	Supported
Secure Communications	Supported
Remote Troubleshooting	Supported
Corporate App Store	Supported
MDM Server	Supported
Location Services	Supported
Single Cluster Configuration	0
Windows 8	Unsupported
Windows 8 Plan	Supported

SUPPORT

Annual Downtime	Unsupported
Support Staff Availability	Unsupported
Methods of Support	Unsupported
Phone Support Hours	Unsupported
Not Under Contract Support	Unsupported
Not Under Contract Availability	Unsupported
Support Forum	Unsupported

SECURITY AND COMPLIANCE

Cloud Based	Unsupported
PKI Certificate	Supported
SIEM Integration (Total #)	0
DLP Integration (Total #)	0
Geo-Fencing	Unsupported
Detect Security Requirements	Supported
Jailbroken	Supported
Selective Wiping	Supported
Strong Password	Supported
Two-Factor Authentication	Supported
Device Encryption	Supported
Choose Enforcement	Supported
Blacklisted Applications	Supported
Rooted Device Detection	Supported
Manage Anti-Virus	Unsupported
Auto-Deletion	Supported
VPN Support	Supported
DLP Integration	Unsupported
Integrate AD/LDAP	Supported
Whitelisting Applications	Supported
Encryption Data-at-Rest	Supported
Server in DMZ	Supported
Data in DMZ	Unsupported
Granular Level	Supported
SAFE Program	Supported
Differing Mobile Policies	Supported

Supported Unsupported

Capricode SyncShield

DCIG Scores and Rankings

OVERALL SCORE	Management	Operating Environment	User Experience	Security and Compliance	Support
7.50	3.00	2.50	2.00	0.00	0.00
BASIC	BASIC	BASIC	BASIC	BASIC	BASICC

MANAGEMENT

Provision Platforms	Supported
Policy Restriction	Unsupported
Hardware Inventory	Unsupported
Device Ownership	Unsupported
Customizeable Dashboard	Unsupported
Bulk Device Management	Unsupported
Policy Alerts	Unsupported
Administrator Deployment	Unsupported
Device Change	Unsupported
Deploy Multiple Groups	Unsupported
Combined Group	Unsupported
Automatic Provision	Unsupported
SSAE-16	Unsupported
Database Instance (Total #)	0
Solution Options (Total #)	0
Device Change (Total #)	0
Notifications (Total #)	Unsupported
Dedicated Database	Unsupported
Backup and Recovery	Unsupported
Software Inventory	Unsupported
Apple VPP	Unsupported
Corporate v. Personal	Unsupported
Single Console	Unsupported
Change Propagations	Unsupported

OPERATING ENVIRONMENT

Deployment Options (Total #)	2
Solution Integration (Total #)	0
Cloud and On-Premise Same	Unsupported
Full MDM Functionality	Unsupported
Third Party Solution	Unsupported
DMZ Replication	Unsupported
High Availability	Unsupported
Secure Communications	Unsupported
Remote Troubleshooting	Unsupported
Corporate App Store	Unsupported
MDM Server	Unsupported
Location Services	Unsupported
Single Cluster Configuration	0
Windows 8	Unsupported
Windows 8 Plan	Unsupported

SUPPORT

Annual Downtime	Unsupported
Support Staff Availability	Unsupported
Methods of Support	Unsupported
Phone Support Hours	Unsupported
Not Under Contract Support	Unsupported
Not Under Contract Availability	Unsupported
Support Forum	Unsupported

SECURITY AND COMPLIANCE

Cloud Based	Unsupported
PKI Certificate	Unsupported
SIEM Integration (Total #)	0
DLP Integration (Total #)	0
Geo-Fencing	Unsupported
Detect Security Requirements	Unsupported
Jailbroken	Unsupported
Selective Wiping	Unsupported
Strong Password	Unsupported
Two-Factor Authentication	Unsupported
Device Encryption	Unsupported
Choose Enforcement	Unsupported
Blacklisted Applications	Unsupported
Rooted Device Detection	Unsupported
Manage Anti-Virus	Unsupported
Auto-Deletion	Unsupported
VPN Support	Unsupported
DLP Integration	Unsupported
Integrate AD/LDAP	Supported
Whitelisting Applications	Unsupported
Encryption Data-at-Rest	Unsupported
Server in DMZ	Supported
Data in DMZ	Supported
Granular Level	Supported
SAFE Program	Unsupported
Differing Mobile Policies	Unsupported

Supported Unsupported

Citrix XenMobile (Zenprise)

DCIG Scores and Rankings

OVERALL SCORE	Management	Operating Environment	User Experience	Security and Compliance	Support
24.00	7.00	4.00	6.00	7.00	0.00
BASIC	BASIC	GOOD	GOOD	BASIC	BASIC

MANAGEMENT

Provision Platforms	✓
Policy Restriction	✗
Hardware Inventory	✗
Device Ownership	✗
Customizeable Dashboard	✗
Bulk Device Management	✗
Policy Alerts	✓
Administrator Deployment	✗
Device Change	✗
Deploy Multiple Groups	✗
Combined Group	✗
Automatic Provision	✗
SSAE-16	✗
Database Instance (Total #)	0
Solution Options (Total #)	0
Device Change (Total #)	0
Notifications (Total #)	0
Dedicated Database	✗
Backup and Recovery	✗
Software Inventory	✗
Apple VPP	✓
Corporate v. Personal	✗
Single Console	✗
Change Propagations	✗

OPERATING ENVIRONMENT

Deployment Options (Total #)	1
Solution Integration (Total #)	1
Cloud and On-Premise Same	✗
Full MDM Functionality	✗
Third Party Solution	✗
DMZ Replication	✗
High Availability	✓
Secure Communications	✗
Remote Troubleshooting	✗
Corporate App Store	✓
MDM Server	✗
Location Services	✗
Single Cluster Configuration	0
Windows 8	✗
Windows 8 Plan	✓

SUPPORT

Annual Downtime	✗
Support Staff Availability	✗
Methods of Support	✗
Phone Support Hours	✗
Not Under Contract Support	✗
Not Under Contract Availability	✗
Support Forum	✓

SECURITY AND COMPLIANCE

Cloud Based	✗
PKI Certificate	✗
SIEM Integration (Total #)	0
DLP Integration (Total #)	0
Geo-Fencing	✓
Detect Security Requirements	✗
Jailbroken	✗
Selective Wiping	✓
Strong Password	✓
Two-Factor Authentication	✓
Device Encryption	✗
Choose Enforcement	✗
Blacklisted Applications	✗
Rooted Device Detection	✗
Manage Anti-Virus	✓
Auto-Deletion	✗
VPN Support	✗
DLP Integration	✗
Integrate AD/LDAP	✗
Whitelisting Applications	✗
Encryption Data-at-Rest	✗
Server in DMZ	✗
Data in DMZ	✗
Granular Level	✗
SAFE Program	✗
Differing Mobile Policies	✗

✓ Supported ✗ Unsupported

Excitor DME Mobile Device Manager

DCIG Scores and Rankings

OVERALL SCORE	Management	Operating Environment	User Experience	Security and Compliance	Support
92.25	29.00	1575	11.00	32.50	4.00
EXCELLENT	RECOMMENDED	EXCELLENT	EXCELLENT	EXCELLENT	EXCELLENT

MANAGEMENT

Provision Platforms	Supported
Policy Restriction	Supported
Hardware Inventory	Supported
Device Ownership	Supported
Customizeable Dashboard	Unsupported
Bulk Device Management	Supported
Policy Alerts	Supported
Administrator Deployment	Unsupported
Device Change	Supported
Deploy Multiple Groups	Supported
Combined Group	Unsupported
Automatic Provision	Supported
SSAE-16	Unsupported
Database Instance (Total #)	1
Solution Options (Total #)	3
Device Change (Total #)	3
Notifications (Total #)	0
Dedicated Database	Supported
Backup and Recovery	Unsupported
Software Inventory	Supported
Apple VPP	Unsupported
Corporate v. Personal	Supported
Single Console	Supported
Change Propagations	Unsupported

OPERATING ENVIRONMENT

Deployment Options (Total #)	1
Solution Integration (Total #)	1
Cloud and On-Premise Same	Unsupported
Full MDM Functionality	Unsupported
Third Party Solution	Unsupported
DMZ Replication	Unsupported
High Availability	Supported
Secure Communications	Unsupported
Remote Troubleshooting	Unsupported
Corporate App Store	Supported
MDM Server	Unsupported
Location Services	Unsupported
Single Cluster Configuration	0
Windows 8	Unsupported
Windows 8 Plan	Supported

SUPPORT

Annual Downtime	Unsupported
Support Staff Availability	24×7×365 8AM EST to 8PM PST
Methods of Support	Email/Phone/Remote Login/Web Chat
Phone Support Hours	24×7×365
Not Under Contract Support	Unsupported
Not Under Contract Availability	Unsupported
Support Forum	Unsupported

SECURITY AND COMPLIANCE

Cloud Based	Supported
PKI Certificate	Unsupported
SIEM Integration (Total #)	0
DLP Integration (Total #)	0
Geo-Fencing	Unsupported
Detect Security Requirements	Supported
Jailbroken	Supported
Selective Wiping	Supported
Strong Password	Supported
Two-Factor Authentication	Supported
Device Encryption	Supported
Choose Enforcement	Supported
Blacklisted Applications	Unsupported
Rooted Device Detection	Supported
Manage Anti-Virus	Unsupported
Auto-Deletion	Unsupported
VPN Support	Supported
DLP Integration	Unsupported
Integrate AD/LDAP	Supported
Whitelisting Applications	Supported
Encryption Data-at-Rest	Supported
Server in DMZ	Supported
Data in DMZ	Unsupported
Granular Level	Supported
SAFE Program	Unsupported
Differing Mobile Policies	Unsupported

Supported Unsupported

FancyFon Software FAMOC

DCIG Scores and Rankings

OVERALL SCORE	Management	Operating Environment	User Experience	Security and Compliance	Support
22.00	5.50	1.50	4.00	11.00	0.00
BASIC	BASIC	BASIC	BASIC	GOOD	BASIC

MANAGEMENT

Provision Platforms	Supported
Policy Restriction	Unsupported
Hardware Inventory	Supported
Device Ownership	Unsupported
Customizeable Dashboard	Unsupported
Bulk Device Management	Unsupported
Policy Alerts	Unsupported
Administrator Deployment	Unsupported
Device Change	Unsupported
Deploy Multiple Groups	Unsupported
Combined Group	Unsupported
Automatic Provision	Unsupported
SSAE-16	Unsupported
Database Instance (Total #)	0
Solution Options (Total #)	1
Device Change (Total #)	0
Notifications (Total #)	0
Dedicated Database	Unsupported
Backup and Recovery	Supported
Software Inventory	Unsupported
Apple VPP	Unsupported
Corporate v. Personal	Unsupported
Single Console	Unsupported
Change Propagations	Unsupported

OPERATING ENVIRONMENT

Deployment Options (Total #)	1
Solution Integration (Total #)	0
Cloud and On-Premise Same	Unsupported
Full MDM Functionality	Unsupported
Third Party Solution	Supported
DMZ Replication	Unsupported
High Availability	Unsupported
Secure Communications	Unsupported
Remote Troubleshooting	Unsupported
Corporate App Store	Unsupported
MDM Server	Unsupported
Location Services	Unsupported
Single Cluster Configuration	0
Windows 8	Unsupported
Windows 8 Plan	Supported

SUPPORT

Annual Downtime	Unsupported
Support Staff Availability	Unsupported
Methods of Support	Unsupported
Phone Support Hours	Unsupported
Not Under Contract Support	Unsupported
Not Under Contract Availability	Unsupported
Support Forum	Unsupported

SECURITY AND COMPLIANCE

Cloud Based	Unsupported
PKI Certificate	Unsupported
SIEM Integration (Total #)	1
DLP Integration (Total #)	1
Geo-Fencing	Unsupported
Detect Security Requirements	Unsupported
Jailbroken	Supported
Selective Wiping	Supported
Strong Password	Supported
Two-Factor Authentication	Unsupported
Device Encryption	Supported
Choose Enforcement	Unsupported
Blacklisted Applications	Unsupported
Rooted Device Detection	Unsupported
Manage Anti-Virus	Supported
Auto-Deletion	Unsupported
VPN Support	Supported
DLP Integration	Unsupported
Integrate AD/LDAP	Unsupported
Whitelisting Applications	Unsupported
Encryption Data-at-Rest	Supported
Server in DMZ	Unsupported
Data in DMZ	Unsupported
Granular Level	Unsupported
SAFE Program	Unsupported
Differing Mobile Policies	Unsupported

Supported Unsupported

Fiberlink MaaS360
Mobile Device Management

DCIG Scores and Rankings

OVERALL SCORE	Management	Operating Environment	User Experience	Security and Compliance	Support
52.25	13.00	8.25	10.00	21.00	0.00
GOOD	GOOD	GOOD	EXCELLENT	GOOD	BASIC

MANAGEMENT

Provision Platforms	✓
Policy Restriction	✓
Hardware Inventory	✓
Device Ownership	✓
Customizeable Dashboard	✓
Bulk Device Management	✓
Policy Alerts	✓
Administrator Deployment	✓
Device Change	✓
Deploy Multiple Groups	✓
Combined Group	✓
Automatic Provision	✓
SSAE-16	✓
Database Instance (Total #)	0
Solution Options (Total #)	0
Device Change (Total #)	0
Notifications (Total #)	0
Dedicated Database	✗
Backup and Recovery	✓
Software Inventory	✓
Apple VPP	✓
Corporate v. Personal	✓
Single Console	✓
Change Propagations	✓

OPERATING ENVIRONMENT

Deployment Options (Total #)	1
Solution Integration (Total #)	1
Cloud and On-Premise Same	✗
Full MDM Functionality	✓
Third Party Solution	✓
DMZ Replication	✗
High Availability	✓
Secure Communications	✓
Remote Troubleshooting	✓
Corporate App Store	✓
MDM Server	✓
Location Services	✗
Single Cluster Configuration	0
Windows 8	✗
Windows 8 Plan	✗

SUPPORT

Annual Downtime	✗
Support Staff Availability	24×7×365
Methods of Support	Email, Phone, Web chat
Phone Support Hours	✗
Not Under Contract Support	✓
Not Under Contract Availability	✓
Support Forum	✓

SECURITY AND COMPLIANCE

Cloud Based	✗
PKI Certificate	✗
SIEM Integration (Total #)	0
DLP Integration (Total #)	0
Geo-Fencing	✗
Detect Security Requirements	✗
Jailbroken	✗
Selective Wiping	✓
Strong Password	✓
Two-Factor Authentication	✗
Device Encryption	✓
Choose Enforcement	✓
Blacklisted Applications	✗
Rooted Device Detection	✗
Manage Anti-Virus	✗
Auto-Deletion	✗
VPN Support	✓
DLP Integration	✗
Integrate AD/LDAP	✗
Whitelisting Applications	✓
Encryption Data-at-Rest	✗
Server in DMZ	✗
Data in DMZ	✗
Granular Level	✗
SAFE Program	✓
Differing Mobile Policies	✗

✓ Supported ✗ Unsupported

Fixmo EMP

DCIG Scores and Rankings

OVERALL SCORE	Management	Operating Environment	User Experience	Security and Compliance	Support
92.50	25.25	15.25	12.00	37.00	3.00
EXCELLENT	EXCELLENT	EXCELLENT	EXCELLENT	RECOMMENDED	EXCELLENT

MANAGEMENT

Provision Platforms	✓
Policy Restriction	✓
Hardware Inventory	✓
Device Ownership	✓
Customizeable Dashboard	✗
Bulk Device Management	✓
Policy Alerts	✓
Administrator Deployment	✓
Device Change	✓
Deploy Multiple Groups	✓
Combined Group	✓
Automatic Provision	✓
SSAE-16	✗
Database Instance (Total #)	1
Solution Options (Total #)	1
Device Change (Total #)	3
Notifications (Total #)	1
Dedicated Database	✗
Backup and Recovery	✗
Software Inventory	✓
Apple VPP	✓
Corporate v. Personal	✓
Single Console	✓
Change Propagations	✗

OPERATING ENVIRONMENT

Deployment Options (Total #)	2
Solution Integration (Total #)	3
Cloud and On-Premise Same	✓
Full MDM Functionality	✓
Third Party Solution	✗
DMZ Replication	✗
High Availability	✓
Secure Communications	✓
Remote Troubleshooting	✗
Corporate App Store	✓
MDM Server	✓
Location Services	✓
Single Cluster Configuration	0
Windows 8	✗
Windows 8 Plan	✗

SUPPORT

Annual Downtime	✗
Support Staff Availability	24x7x365
Methods of Support	Dispatch Technician Onsite/eMail/Phone/ Remote login problem solving
Phone Support Hours	Business Day (local time)
Not Under Contract Support	Business Day Local
Not Under Contract Availability	Business Day Local
Support Forum	✓

SECURITY AND COMPLIANCE

Cloud Based	✗
PKI Certificate	✓
SIEM Integration (Total #)	0
DLP Integration (Total #)	0
Geo-Fencing	✗
Detect Security Requirements	✓
Jailbroken	✓
Selective Wiping	✓
Strong Password	✓
Two-Factor Authentication	✓
Device Encryption	✓
Choose Enforcement	✓
Blacklisted Applications	✓
Rooted Device Detection	✓
Manage Anti-Virus	✗
Auto-Deletion	✓
VPN Support	✓
DLP Integration	✗
Integrate AD/LDAP	✓
Whitelisting Applications	✓
Encryption Data-at-Rest	✓
Server in DMZ	✓
Data in DMZ	✗
Granular Level	✓
SAFE Program	✓
Differing Mobile Policies	✗

✓ Supported ✗ Unsupported

2014 DCIG Mobile Data Management Buyer's Guide

Good Technology Good Mobile Manager

DCIG Scores and Rankings

OVERALL SCORE	Management	Operating Environment	User Experience	Security and Compliance	Support
13.50	1.00	0.50	5.00	7.00	0.00
BASIC	BASIC	BASIC	BASIC	BASIC	BASIC

MANAGEMENT

Provision Platforms	✓
Policy Restriction	✗
Hardware Inventory	✗
Device Ownership	✗
Customizeable Dashboard	✗
Bulk Device Management	✗
Policy Alerts	✗
Administrator Deployment	✗
Device Change	✗
Deploy Multiple Groups	✗
Combined Group	✗
Automatic Provision	✗
SSAE-16	✗
Database Instance (Total #)	0
Solution Options (Total #)	0
Device Change (Total #)	0
Notifications (Total #)	0
Dedicated Database	✗
Backup and Recovery	✗
Software Inventory	✗
Apple VPP	✗
Corporate v. Personal	✗
Single Console	✗
Change Propagations	✗

OPERATING ENVIRONMENT

Deployment Options (Total #)	1
Solution Integration (Total #)	0
Cloud and On-Premise Same	✗
Full MDM Functionality	✗
Third Party Solution	✓
DMZ Replication	✗
High Availability	✗
Secure Communications	✗
Remote Troubleshooting	✗
Corporate App Store	✗
MDM Server	✗
Location Services	✗
Single Cluster Configuration	0
Windows 8	✗
Windows 8 Plan	✓

SUPPORT

Annual Downtime	✗
Support Staff Availability	✗
Methods of Support	✗
Phone Support Hours	✗
Not Under Contract Support	✗
Not Under Contract Availability	✗
Support Forum	✗

SECURITY AND COMPLIANCE

Cloud Based	✗
PKI Certificate	✗
SIEM Integration (Total #)	0
DLP Integration (Total #)	0
Geo-Fencing	✗
Detect Security Requirements	✗
Jailbroken	✓
Selective Wiping	✓
Strong Password	✓
Two-Factor Authentication	✗
Device Encryption	✗
Choose Enforcement	✗
Blacklisted Applications	✗
Rooted Device Detection	✗
Manage Anti-Virus	✗
Auto-Deletion	✗
VPN Support	✓
DLP Integration	✗
Integrate AD/LDAP	✗
Whitelisting Applications	✗
Encryption Data-at-Rest	✓
Server in DMZ	✗
Data in DMZ	✗
Granular Level	✗
SAFE Program	✗
Differing Mobile Policies	✗

✓ Supported ✗ Unsupported

IBM MobileFirst Management

DCIG Scores and Rankings

OVERALL SCORE	Management	Operating Environment	User Experience	Security and Compliance	Support
9.50	3.00	0.50	5.00	1.00	0.00
BASIC	BASIC	BASIC	BASIC	BASIC	BASIC

MANAGEMENT

Provision Platforms	✔
Policy Restriction	✖
Hardware Inventory	✖
Device Ownership	✖
Customizeable Dashboard	✖
Bulk Device Management	✖
Policy Alerts	✖
Administrator Deployment	✖
Device Change	✖
Deploy Multiple Groups	✖
Combined Group	✖
Automatic Provision	✖
SSAE-16	✖
Database Instance (Total #)	0
Solution Options (Total #)	0
Device Change (Total #)	0
Notifications (Total #)	0
Dedicated Database	✖
Backup and Recovery	✖
Software Inventory	✖
Apple VPP	✖
Corporate v. Personal	✖
Single Console	✖
Change Propagations	✖

OPERATING ENVIRONMENT

Deployment Options (Total #)	1
Solution Integration (Total #)	0
Cloud and On-Premise Same	✖
Full MDM Functionality	✖
Third Party Solution	✖
DMZ Replication	✖
High Availability	✖
Secure Communications	✖
Remote Troubleshooting	✖
Corporate App Store	✖
MDM Server	✖
Location Services	✖
Single Cluster Configuration	0
Windows 8	✖
Windows 8 Plan	✖

SUPPORT

Annual Downtime	✖
Support Staff Availability	✖
Methods of Support	✖
Phone Support Hours	✖
Not Under Contract Support	✖
Not Under Contract Availability	✖
Support Forum	✖

SECURITY AND COMPLIANCE

Cloud Based	✖
PKI Certificate	✖
SIEM Integration (Total #)	0
DLP Integration (Total #)	0
Geo-Fencing	✖
Detect Security Requirements	✖
Jailbroken	✖
Selective Wiping	✖
Strong Password	✖
Two-Factor Authentication	✖
Device Encryption	✖
Choose Enforcement	✖
Blacklisted Applications	✖
Rooted Device Detection	✖
Manage Anti-Virus	✖
Auto-Deletion	✖
VPN Support	✖
DLP Integration	✖
Integrate AD/LDAP	✖
Whitelisting Applications	✖
Encryption Data-at-Rest	✔
Server in DMZ	✖
Data in DMZ	✖
Granular Level	✖
SAFE Program	✖
Differing Mobile Policies	✖

✔ Supported ✖ Unsupported

The Institution
REVIVAL Mobile Management

2014 DCIG BUYER'S GUIDE MOBILE DATA MANAGEMENT

DCIG Scores and Rankings

OVERALL SCORE	Management	Operating Environment	User Experience	Security and Compliance	Support
32.75	6.00	4.75	7.00	15.00	0.00
GOOD	BASIC	GOOD	GOOD	GOOD	BASIC

MANAGEMENT

Provision Platforms	Supported
Policy Restriction	Unsupported
Hardware Inventory	Supported
Device Ownership	Unsupported
Customizeable Dashboard	Unsupported
Bulk Device Management	Unsupported
Policy Alerts	Unsupported
Administrator Deployment	Unsupported
Device Change	Unsupported
Deploy Multiple Groups	Unsupported
Combined Group	Unsupported
Automatic Provision	Unsupported
SSAE-16	Unsupported
Database Instance (Total #)	0
Solution Options (Total #)	0
Device Change (Total #)	0
Notifications (Total #)	0
Dedicated Database	Unsupported
Backup and Recovery	Unsupported
Software Inventory	Supported
Apple VPP	Unsupported
Corporate v. Personal	Unsupported
Single Console	Unsupported
Change Propagations	Unsupported

OPERATING ENVIRONMENT

Deployment Options (Total #)	2
Solution Integration (Total #)	2
Cloud and On-Premise Same	Unsupported
Full MDM Functionality	Unsupported
Third Party Solution	Unsupported
DMZ Replication	Unsupported
High Availability	Supported
Secure Communications	Unsupported
Remote Troubleshooting	Unsupported
Corporate App Store	Unsupported
MDM Server	Supported
Location Services	Unsupported
Single Cluster Configuration	0
Windows 8	Unsupported
Windows 8 Plan	Unsupported

SUPPORT

Annual Downtime	Unsupported
Support Staff Availability	Unsupported
Methods of Support	Unsupported
Phone Support Hours	Unsupported
Not Under Contract Support	Unsupported
Not Under Contract Availability	Unsupported
Support Forum	Unsupported

SECURITY AND COMPLIANCE

Cloud Based	Supported
PKI Certificate	Supported
SIEM Integration (Total #)	0
DLP Integration (Total #)	0
Geo-Fencing	Unsupported
Detect Security Requirements	Supported
Jailbroken	Unsupported
Selective Wiping	Supported
Strong Password	Supported
Two-Factor Authentication	Unsupported
Device Encryption	Supported
Choose Enforcement	Unsupported
Blacklisted Applications	Unsupported
Rooted Device Detection	Unsupported
Manage Anti-Virus	Unsupported
Auto-Deletion	Unsupported
VPN Support	Unsupported
DLP Integration	Unsupported
Integrate AD/LDAP	Unsupported
Whitelisting Applications	Unsupported
Encryption Data-at-Rest	Unsupported
Server in DMZ	Unsupported
Data in DMZ	Unsupported
Granular Level	Unsupported
SAFE Program	Unsupported
Differing Mobile Policies	Unsupported

Supported Unsupported

McAfee Enterprise Mobility Management

DCIG Scores and Rankings

OVERALL SCORE	Management	Operating Environment	User Experience	Security and Compliance	Support
20.00	2.00	4.00	3.00	11.00	0.00
BASIC	BASIC	GOOD	BASIC	GOOD	BASIC

MANAGEMENT

Provision Platforms	Supported
Policy Restriction	Supported
Hardware Inventory	Supported
Device Ownership	Supported
Customizeable Dashboard	Supported
Bulk Device Management	Supported
Policy Alerts	Supported
Administrator Deployment	Supported
Device Change	Supported
Deploy Multiple Groups	Supported
Combined Group	Supported
Automatic Provision	Supported
SSAE-16	Unsupported
Database Instance (Total #)	1
Solution Options (Total #)	0
Device Change (Total #)	0
Notifications (Total #)	0
Dedicated Database	Unsupported
Backup and Recovery	Unsupported
Software Inventory	Supported
Apple VPP	Unsupported
Corporate v. Personal	Supported
Single Console	Supported
Change Propagations	Supported

OPERATING ENVIRONMENT

Deployment Options (Total #)	1
Solution Integration (Total #)	1
Cloud and On-Premise Same	Unsupported
Full MDM Functionality	Supported
Third Party Solution	Supported
DMZ Replication	Unsupported
High Availability	Supported
Secure Communications	Unsupported
Remote Troubleshooting	Unsupported
Corporate App Store	Supported
MDM Server	Supported
Location Services	Unsupported
Single Cluster Configuration	0
Windows 8	Unsupported
Windows 8 Plan	Supported

SUPPORT

Annual Downtime	Unsupported
Support Staff Availability	Unsupported
Methods of Support	Dispatch on-site, Phone, Email, Web chat, Remote monitoring
Phone Support Hours	24×7×365
Not Under Contract Support	Unsupported
Not Under Contract Availability	Unsupported
Support Forum	Supported

SECURITY AND COMPLIANCE

Cloud Based	Unsupported
PKI Certificate	Supported
SIEM Integration (Total #)	1
DLP Integration (Total #)	1
Geo-Fencing	Unsupported
Detect Security Requirements	Supported
Jailbroken	Supported
Selective Wiping	Supported
Strong Password	Supported
Two-Factor Authentication	Supported
Device Encryption	Supported
Choose Enforcement	Supported
Blacklisted Applications	Supported
Rooted Device Detection	Supported
Manage Anti-Virus	Supported
Auto-Deletion	Unsupported
VPN Support	Supported
DLP Integration	N/A
Integrate AD/LDAP	Unsupported
Whitelisting Applications	Supported
Encryption Data-at-Rest	Unsupported
Server in DMZ	Unsupported
Data in DMZ	Unsupported
Granular Level	Unsupported
SAFE Program	Supported
Differing Mobile Policies	Unsupported

Supported Unsupported

Mobile Active Defense Mobile Enterprise Compliance and Security Server

2014 DCIG Buyer's Guide — Mobile Data Management

DCIG Scores and Rankings

OVERALL SCORE	Management	Operating Environment	User Experience	Security and Compliance	Support
28.50	9.00	3.50	4.00	12.00	0.00
GOOD	GOOD	BASIC	BASIC	GOOD	BASIC

MANAGEMENT

Provision Platforms	✓
Policy Restriction	✗
Hardware Inventory	✓
Device Ownership	✗
Customizeable Dashboard	✗
Bulk Device Management	✗
Policy Alerts	✓
Administrator Deployment	✓
Device Change	✗
Deploy Multiple Groups	✗
Combined Group	✗
Automatic Provision	✗
SSAE-16	✗
Database Instance (Total #)	0
Solution Options (Total #)	0
Device Change (Total #)	0
Notifications (Total #)	0
Dedicated Database	✗
Backup and Recovery	✗
Software Inventory	✗
Apple VPP	✓
Corporate v. Personal	✗
Single Console	✓
Change Propagations	✗

OPERATING ENVIRONMENT

Deployment Options (Total #)	1
Solution Integration (Total #)	1
Cloud and On-Premise Same	✗
Full MDM Functionality	✗
Third Party Solution	✓
DMZ Replication	✗
High Availability	✓
Secure Communications	✗
Remote Troubleshooting	✗
Corporate App Store	✗
MDM Server	✗
Location Services	✗
Single Cluster Configuration	0
Windows 8	✓
Windows 8 Plan	✗

SUPPORT

Annual Downtime	✗
Support Staff Availability	✗
Methods of Support	✗
Phone Support Hours	✗
Not Under Contract Support	✗
Not Under Contract Availability	✗
Support Forum	✓

SECURITY AND COMPLIANCE

Cloud Based	✗
PKI Certificate	✗
SIEM Integration (Total #)	0
DLP Integration (Total #)	0
Geo-Fencing	✗
Detect Security Requirements	✓
Jailbroken	✗
Selective Wiping	✓
Strong Password	✓
Two-Factor Authentication	✗
Device Encryption	✗
Choose Enforcement	✓
Blacklisted Applications	✗
Rooted Device Detection	✗
Manage Anti-Virus	✗
Auto-Deletion	✗
VPN Support	✓
DLP Integration	✗
Integrate AD/LDAP	✗
Whitelisting Applications	✗
Encryption Data-at-Rest	✗
Server in DMZ	✗
Data in DMZ	✗
Granular Level	✗
SAFE Program	✗
Differing Mobile Policies	✗

✓ Supported ✗ Unsupported

MobileIron
Advanced Mobile Management

DCIG Scores and Rankings

OVERALL SCORE	Management	Operating Environment	User Experience	Security and Compliance	Support
116.00	34.00	21.00	13.00	44.00	4.00
BEST-IN-CLASS	BEST-IN-CLASS	BEST-IN-CLASS	EXCELLENT	BEST-IN-CLASS	EXCELLENT

MANAGEMENT

Provision Platforms	✓
Policy Restriction	✓
Hardware Inventory	✓
Device Ownership	✓
Customizeable Dashboard	✓
Bulk Device Management	✓
Policy Alerts	✓
Administrator Deployment	✗
Device Change	✓
Deploy Multiple Groups	✓
Combined Group	✗
Automatic Provision	✓
SSAE-16	✓
Database Instance (Total #)	2
Solution Options (Total #)	3
Device Change (Total #)	3
Notifications (Total #)	4
Dedicated Database	✓
Backup and Recovery	✗
Software Inventory	✓
Apple VPP	✓
Corporate v. Personal	✓
Single Console	✓
Change Propagations	✗

OPERATING ENVIRONMENT

Deployment Options (Total #)	3
Solution Integration (Total #)	3
Cloud and On-Premise Same	✓
Full MDM Functionality	✓
Third Party Solution	✗
DMZ Replication	✗
High Availability	✓
Secure Communications	✓
Remote Troubleshooting	✗
Corporate App Store	✓
MDM Server	✓
Location Services	✓
Single Cluster Configuration	100,000
Windows 8	✓
Windows 8 Plan	✓

SUPPORT

Annual Downtime	00:52:60
Support Staff Availability	24×7×365
Methods of Support	Dispatch Technician Onsite/Email/Phone/ Remote Monitoring/ Web Chat
Phone Support Hours	24×7×365
Not Under Contract Support	8AM EST to 8PM PST
Not Under Contract Availability	Business Day Local
Support Forum	✓

SECURITY AND COMPLIANCE

Cloud Based	✓
PKI Certificate	✓
SIEM Integration (Total #)	8
DLP Integration (Total #)	7
Geo-Fencing	✓
Detect Security Requirements	✓
Jailbroken	✓
Selective Wiping	✓
Strong Password	✓
Two-Factor Authentication	✓
Device Encryption	✓
Choose Enforcement	✓
Blacklisted Applications	✓
Rooted Device Detection	✓
Manage Anti-Virus	✓
Auto-Deletion	✓
VPN Support	✓
DLP Integration	✓
Integrate AD/LDAP	✓
Whitelisting Applications	✓
Encryption Data-at-Rest	✓
Server in DMZ	✗
Data in DMZ	✗
Granular Level	✓
SAFE Program	✓
Differing Mobile Policies	✗

✓ Supported ✗ Unsupported

Motorola Mobile Services Platform v4

2014 DCIG Mobile Data Management Buyer's Guide

DCIG Scores and Rankings

OVERALL SCORE	Management	Operating Environment	User Experience	Security and Compliance	Support
41.25	12.00	4.75	10.00	14.50	0.00
GOOD	GOOD	GOOD	EXCELLENT	GOOD	BASIC

MANAGEMENT

Provision Platforms	✓
Policy Restriction	✗
Hardware Inventory	✓
Device Ownership	✗
Customizeable Dashboard	✗
Bulk Device Management	✓
Policy Alerts	✓
Administrator Deployment	✓
Device Change	✗
Deploy Multiple Groups	✗
Combined Group	✗
Automatic Provision	✗
SSAE-16	✗
Database Instance (Total #)	0
Solution Options (Total #)	0
Device Change (Total #)	0
Notifications (Total #)	0
Dedicated Database	✗
Backup and Recovery	✗
Software Inventory	✗
Apple VPP	✗
Corporate v. Personal	✗
Single Console	✓
Change Propagations	✗

OPERATING ENVIRONMENT

Deployment Options (Total #)	1
Solution Integration (Total #)	0
Cloud and On-Premise Same	✗
Full MDM Functionality	✗
Third Party Solution	✗
DMZ Replication	✗
High Availability	✗
Secure Communications	✗
Remote Troubleshooting	✓
Corporate App Store	✓
MDM Server	✗
Location Services	✗
Single Cluster Configuration	0
Windows 8	✗
Windows 8 Plan	✗

SUPPORT

Annual Downtime	✗
Support Staff Availability	✗
Methods of Support	✗
Phone Support Hours	✗
Not Under Contract Support	✗
Not Under Contract Availability	✗
Support Forum	✗

SECURITY AND COMPLIANCE

Cloud Based	✗
PKI Certificate	✓
SIEM Integration (Total #)	0
DLP Integration (Total #)	0
Geo-Fencing	✗
Detect Security Requirements	✗
Jailbroken	✓
Selective Wiping	✓
Strong Password	✓
Two-Factor Authentication	✗
Device Encryption	✓
Choose Enforcement	✗
Blacklisted Applications	✗
Rooted Device Detection	✗
Manage Anti-Virus	✗
Auto-Deletion	✗
VPN Support	✓
DLP Integration	✗
Integrate AD/LDAP	✗
Whitelisting Applications	✓
Encryption Data-at-Rest	✓
Server in DMZ	✗
Data in DMZ	✗
Granular Level	✗
SAFE Program	✗
Differing Mobile Policies	✗

✓ Supported ✗ Unsupported

OpenPeak Advanced Device and Application Management (ADAM)

DCIG Scores and Rankings

OVERALL SCORE	Management	Operating Environment	User Experience	Security and Compliance	Support
26.50	7.00	1.50	10.00	8.00	0.00
BASIC	BASIC	BASIC	EXCELLENT	BASIC	BASIC

MANAGEMENT

Provision Platforms	Supported
Policy Restriction	Unsupported
Hardware Inventory	Supported
Device Ownership	Unsupported
Customizeable Dashboard	Unsupported
Bulk Device Management	Unsupported
Policy Alerts	Unsupported
Administrator Deployment	Unsupported
Device Change	Unsupported
Deploy Multiple Groups	Unsupported
Combined Group	Unsupported
Automatic Provision	Unsupported
SSAE-16	Unsupported
Database Instance (Total #)	0
Solution Options (Total #)	0
Device Change (Total #)	0
Notifications (Total #)	0
Dedicated Database	Unsupported
Backup and Recovery	Unsupported
Software Inventory	Unsupported
Apple VPP	Unsupported
Corporate v. Personal	Unsupported
Single Console	Supported
Change Propagations	Unsupported

OPERATING ENVIRONMENT

Deployment Options (Total #)	1
Solution Integration (Total #)	0
Cloud and On-Premise Same	Unsupported
Full MDM Functionality	Unsupported
Third Party Solution	Unsupported
DMZ Replication	Unsupported
High Availability	Unsupported
Secure Communications	Unsupported
Remote Troubleshooting	Supported
Corporate App Store	Supported
MDM Server	Supported
Location Services	Unsupported
Single Cluster Configuration	0
Windows 8	Unsupported
Windows 8 Plan	Unsupported

SUPPORT

Annual Downtime	Unsupported
Support Staff Availability	Unsupported
Methods of Support	Unsupported
Phone Support Hours	Unsupported
Not Under Contract Support	Unsupported
Not Under Contract Availability	Unsupported
Support Forum	Unsupported

SECURITY AND COMPLIANCE

Cloud Based	Unsupported
PKI Certificate	Supported
SIEM Integration (Total #)	0
DLP Integration (Total #)	0
Geo-Fencing	Unsupported
Detect Security Requirements	Supported
Jailbroken	Supported
Selective Wiping	Supported
Strong Password	Supported
Two-Factor Authentication	Unsupported
Device Encryption	Unsupported
Choose Enforcement	Unsupported
Blacklisted Applications	Unsupported
Rooted Device Detection	Unsupported
Manage Anti-Virus	Unsupported
Auto-Deletion	Unsupported
VPN Support	Unsupported
DLP Integration	Unsupported
Integrate AD/LDAP	Unsupported
Whitelisting Applications	Supported
Encryption Data-at-Rest	Supported
Server in DMZ	Unsupported
Data in DMZ	Unsupported
Granular Level	Unsupported
SAFE Program	Unsupported
Differing Mobile Policies	Unsupported

Supported Unsupported

RIM Blackberry Enterprise Service 10

MOBILE DATA MANAGEMENT 2014 DCIG BUYER'S GUIDE

DCIG Scores and Rankings

OVERALL SCORE	Management	Operating Environment	User Experience	Security and Compliance	Support
-	-	-	-	-	-
RANK	RANK	RANK	RANK	RANK	RANK

MANAGEMENT

Provision Platforms	✓
Policy Restriction	✗
Hardware Inventory	✓
Device Ownership	✗
Customizeable Dashboard	✗
Bulk Device Management	✗
Policy Alerts	✗
Administrator Deployment	✗
Device Change	✗
Deploy Multiple Groups	✗
Combined Group	✗
Automatic Provision	✗
SSAE-16	✗
Database Instance (Total #)	0
Solution Options (Total #)	0
Device Change (Total #)	0
Notifications (Total #)	0
Dedicated Database	✗
Backup and Recovery	✗
Software Inventory	✗
Apple VPP	✗
Corporate v. Personal	✗
Single Console	✓
Change Propagations	✗

OPERATING ENVIRONMENT

Deployment Options (Total #)	1
Solution Integration (Total #)	0
Cloud and On-Premise Same	✗
Full MDM Functionality	✗
Third Party Solution	✗
DMZ Replication	✗
High Availability	✗
Secure Communications	✗
Remote Troubleshooting	✗
Corporate App Store	✗
MDM Server	✗
Location Services	✗
Single Cluster Configuration	0
Windows 8	✗
Windows 8 Plan	✗

SUPPORT

Annual Downtime	✗
Support Staff Availability	✗
Methods of Support	✗
Phone Support Hours	✗
Not Under Contract Support	✗
Not Under Contract Availability	✗
Support Forum	✓

SECURITY AND COMPLIANCE

Cloud Based	✗
PKI Certificate	✓
SIEM Integration (Total #)	0
DLP Integration (Total #)	0
Geo-Fencing	✗
Detect Security Requirements	✗
Jailbroken	✗
Selective Wiping	✓
Strong Password	✓
Two-Factor Authentication	✗
Device Encryption	✓
Choose Enforcement	✗
Blacklisted Applications	✗
Rooted Device Detection	✗
Manage Anti-Virus	✗
Auto-Deletion	✗
VPN Support	✗
DLP Integration	✗
Integrate AD/LDAP	✗
Whitelisting Applications	✗
Encryption Data-at-Rest	✗
Server in DMZ	✗
Data in DMZ	✗
Granular Level	✗
SAFE Program	✗
Differing Mobile Policies	✗

✓ Supported ✗ Unsupported

DCIG

SAP (Sybase) Afaria

DCIG Scores and Rankings

OVERALL SCORE	Management	Operating Environment	User Experience	Security and Compliance	Support
46.25	11.25	11.25	5.00	15.75	3.00
GOOD	GOOD	EXCELLENT	BASIC	GOOD	EXCELLENT

MANAGEMENT

Provision Platforms	✓
Policy Restriction	✓
Hardware Inventory	✓
Device Ownership	✗
Customizeable Dashboard	✗
Bulk Device Management	✗
Policy Alerts	✗
Administrator Deployment	✓
Device Change	✓
Deploy Multiple Groups	✗
Combined Group	✗
Automatic Provision	✓
SSAE-16	✓
Database Instance (Total #)	1
Solution Options (Total #)	2
Device Change (Total #)	1
Notifications (Total #)	2
Dedicated Database	✓
Backup and Recovery	✗
Software Inventory	✗
Apple VPP	✗
Corporate v. Personal	✗
Single Console	✗
Change Propagations	✗

OPERATING ENVIRONMENT

Deployment Options (Total #)	2
Solution Integration (Total #)	3
Cloud and On-Premise Same	✗
Full MDM Functionality	✓
Third Party Solution	✓
DMZ Replication	✗
High Availability	✓
Secure Communications	✓
Remote Troubleshooting	✗
Corporate App Store	✗
MDM Server	✗
Location Services	✗
Single Cluster Configuration	0
Windows 8	✓
Windows 8 Plan	✗

SUPPORT

Annual Downtime	✗
Support Staff Availability	24×7×365
Methods of Support	Email/Phone/ Remote Login/ Remote Monitoring
Phone Support Hours	24×7×365
Not Under Contract Support	✗
Not Under Contract Availability	✗
Support Forum	✗

SECURITY AND COMPLIANCE

Cloud Based	✗
PKI Certificate	✓
SIEM Integration (Total #)	0
DLP Integration (Total #)	0
Geo-Fencing	✗
Detect Security Requirements	✓
Jailbroken	✓
Selective Wiping	✓
Strong Password	✓
Two-Factor Authentication	✗
Device Encryption	✓
Choose Enforcement	✗
Blacklisted Applications	✓
Rooted Device Detection	✓
Manage Anti-Virus	✗
Auto-Deletion	✗
VPN Support	✓
DLP Integration	✗
Integrate AD/LDAP	✓
Whitelisting Applications	✓
Encryption Data-at-Rest	✓
Server in DMZ	✗
Data in DMZ	✗
Granular Level	✗
SAFE Program	✓
Differing Mobile Policies	✓

✓ Supported ✗ Unsupported

Silverback Mobile Device Management

DCIG Scores and Rankings

OVERALL SCORE	Management	Operating Environment	User Experience	Security and Compliance	Support
27.00	6.00	4.00	7.00	10.00	0.00
BASIC	BASIC	GOOD	GOOD	BASIC	BASIC

MANAGEMENT

Provision Platforms	✔
Policy Restriction	✖
Hardware Inventory	✔
Device Ownership	✖
Customizeable Dashboard	✖
Bulk Device Management	✖
Policy Alerts	✖
Administrator Deployment	✖
Device Change	✖
Deploy Multiple Groups	✖
Combined Group	✖
Automatic Provision	✖
SSAE-16	✖
Database Instance (Total #)	0
Solution Options (Total #)	0
Device Change (Total #)	0
Notifications (Total #)	0
Dedicated Database	✖
Backup and Recovery	✖
Software Inventory	✖
Apple VPP	✖
Corporate v. Personal	✖
Single Console	✔
Change Propagations	✖

OPERATING ENVIRONMENT

Deployment Options (Total #)	3
Solution Integration (Total #)	0
Cloud and On-Premise Same	✖
Full MDM Functionality	✖
Third Party Solution	✖
DMZ Replication	✖
High Availability	✖
Secure Communications	✖
Remote Troubleshooting	✖
Corporate App Store	✖
MDM Server	✔
Location Services	✖
Single Cluster Configuration	0
Windows 8	✖
Windows 8 Plan	✖

SUPPORT

Annual Downtime	✖
Support Staff Availability	✖
Methods of Support	✖
Phone Support Hours	✖
Not Under Contract Support	✖
Not Under Contract Availability	✖
Support Forum	✖

SECURITY AND COMPLIANCE

Cloud Based	✖
PKI Certificate	✔
SIEM Integration (Total #)	0
DLP Integration (Total #)	0
Geo-Fencing	✖
Detect Security Requirements	✖
Jailbroken	✖
Selective Wiping	✔
Strong Password	✔
Two-Factor Authentication	✖
Device Encryption	✖
Choose Enforcement	✔
Blacklisted Applications	✖
Rooted Device Detection	✖
Manage Anti-Virus	✖
Auto-Deletion	✖
VPN Support	✔
DLP Integration	✖
Integrate AD/LDAP	✖
Whitelisting Applications	✖
Encryption Data-at-Rest	✖
Server in DMZ	✖
Data in DMZ	✖
Granular Level	✖
SAFE Program	✖
Differing Mobile Policies	✖

✔ Supported ✖ Unsupported

Smith Micro Software Enterprise Device Management

DCIG Scores and Rankings

OVERALL SCORE	Management	Operating Environment	User Experience	Security and Compliance	Support
15.75	5.00	1.75	4.00	5.00	0.00
BASIC	BASIC	BASIC	BASIC	BASIC	BASIC

MANAGEMENT

Provision Platforms	✗
Policy Restriction	✗
Hardware Inventory	✓
Device Ownership	✗
Customizeable Dashboard	✗
Bulk Device Management	✗
Policy Alerts	✗
Administrator Deployment	✓
Device Change	✗
Deploy Multiple Groups	✗
Combined Group	✗
Automatic Provision	✓
SSAE-16	✗
Database Instance (Total #)	0
Solution Options (Total #)	0
Device Change (Total #)	0
Notifications (Total #)	0
Dedicated Database	✗
Backup and Recovery	✗
Software Inventory	✗
Apple VPP	✗
Corporate v. Personal	✗
Single Console	✓
Change Propagations	✗

OPERATING ENVIRONMENT

Deployment Options (Total #)	1
Solution Integration (Total #)	1
Cloud and On-Premise Same	✗
Full MDM Functionality	✗
Third Party Solution	✓
DMZ Replication	✗
High Availability	✗
Secure Communications	✗
Remote Troubleshooting	✗
Corporate App Store	✗
MDM Server	✗
Location Services	✗
Single Cluster Configuration	0
Windows 8	✗
Windows 8 Plan	✗

SUPPORT

Annual Downtime	✗
Support Staff Availability	✗
Methods of Support	✗
Phone Support Hours	✗
Not Under Contract Support	✗
Not Under Contract Availability	✗
Support Forum	✗

SECURITY AND COMPLIANCE

Cloud Based	✗
PKI Certificate	✓
SIEM Integration (Total #)	0
DLP Integration (Total #)	0
Geo-Fencing	✗
Detect Security Requirements	✗
Jailbroken	✗
Selective Wiping	✓
Strong Password	✓
Two-Factor Authentication	✗
Device Encryption	✗
Choose Enforcement	✗
Blacklisted Applications	✗
Rooted Device Detection	✗
Manage Anti-Virus	✗
Auto-Deletion	✗
VPN Support	✗
DLP Integration	✗
Integrate AD/LDAP	✗
Whitelisting Applications	✗
Encryption Data-at-Rest	✗
Server in DMZ	✗
Data in DMZ	✗
Granular Level	✗
SAFE Program	✗
Differing Mobile Policies	✗

✓ Supported ✗ Unsupported

Sophos Mobile Control

DCIG Scores and Rankings

OVERALL SCORE	Management	Operating Environment	User Experience	Security and Compliance	Support
69.50	20.00	11.50	12.00	26.00	0.00
EXCELLENT	EXCELLENT	EXCELLENT	EXCELLENT	EXCELLENT	BASIC

MANAGEMENT

Provision Platforms	Unsupported
Policy Restriction	Unsupported
Hardware Inventory	Supported
Device Ownership	Supported
Customizeable Dashboard	Unsupported
Bulk Device Management	Unsupported
Policy Alerts	Supported
Administrator Deployment	Unsupported
Device Change	Unsupported
Deploy Multiple Groups	Supported
Combined Group	Unsupported
Automatic Provision	Supported
SSAE-16	Unsupported
Database Instance (Total #)	0
Solution Options (Total #)	0
Device Change (Total #)	0
Notifications (Total #)	0
Dedicated Database	Unsupported
Backup and Recovery	Supported
Software Inventory	Supported
Apple VPP	Supported
Corporate v. Personal	Supported
Single Console	Supported
Change Propagations	Unsupported

OPERATING ENVIRONMENT

Deployment Options (Total #)	2
Solution Integration (Total #)	3
Cloud and On-Premise Same	Unsupported
Full MDM Functionality	Unsupported
Third Party Solution	Supported
DMZ Replication	Unsupported
High Availability	Supported
Secure Communications	Unsupported
Remote Troubleshooting	Unsupported
Corporate App Store	Unsupported
MDM Server	Unsupported
Location Services	Unsupported
Single Cluster Configuration	0
Windows 8	Supported
Windows 8 Plan	Unsupported

SUPPORT

Annual Downtime	Unsupported
Support Staff Availability	Unsupported
Methods of Support	Unsupported
Phone Support Hours	Unsupported
Not Under Contract Support	Unsupported
Not Under Contract Availability	Unsupported
Support Forum	Supported

SECURITY AND COMPLIANCE

Cloud Based	Unsupported
PKI Certificate	Supported
SIEM Integration (Total #)	0
DLP Integration (Total #)	0
Geo-Fencing	Unsupported
Detect Security Requirements	Supported
Jailbroken	Supported
Selective Wiping	Supported
Strong Password	Supported
Two-Factor Authentication	Unsupported
Device Encryption	Supported
Choose Enforcement	Supported
Blacklisted Applications	Supported
Rooted Device Detection	Supported
Manage Anti-Virus	Supported
Auto-Deletion	Unsupported
VPN Support	Supported
DLP Integration	Unsupported
Integrate AD/LDAP	Unsupported
Whitelisting Applications	Supported
Encryption Data-at-Rest	Supported
Server in DMZ	Unsupported
Data in DMZ	Unsupported
Granular Level	Unsupported
SAFE Program	Supported
Differing Mobile Policies	Unsupported

Supported Unsupported

SOTI MobiControl

DCIG Scores and Rankings

OVERALL SCORE	Management	Operating Environment	User Experience	Security and Compliance	Support
24.00	3.00	3.00	9.00	9.00	0.00
BASIC	BASIC	BASIC	GOOD	BASIC	BASIC

MANAGEMENT

Provision Platforms	✔
Policy Restriction	✘
Hardware Inventory	✔
Device Ownership	✘
Customizeable Dashboard	✘
Bulk Device Management	✘
Policy Alerts	✘
Administrator Deployment	✔
Device Change	✘
Deploy Multiple Groups	✘
Combined Group	✘
Automatic Provision	✔
SSAE-16	✘
Database Instance (Total #)	0
Solution Options (Total #)	0
Device Change (Total #)	0
Notifications (Total #)	0
Dedicated Database	✘
Backup and Recovery	✘
Software Inventory	✘
Apple VPP	✘
Corporate v. Personal	✘
Single Console	✘
Change Propagations	✘

OPERATING ENVIRONMENT

Deployment Options (Total #)	1
Solution Integration (Total #)	1
Cloud and On-Premise Same	✘
Full MDM Functionality	✘
Third Party Solution	✘
DMZ Replication	✘
High Availability	✘
Secure Communications	✘
Remote Troubleshooting	✘
Corporate App Store	✘
MDM Server	✘
Location Services	✘
Single Cluster Configuration	0
Windows 8	✘
Windows 8 Plan	✘

SUPPORT

Annual Downtime	✘
Support Staff Availability	✘
Methods of Support	✘
Phone Support Hours	✘
Not Under Contract Support	✘
Not Under Contract Availability	✘
Support Forum	✘

SECURITY AND COMPLIANCE

Cloud Based	✘
PKI Certificate	✔
SIEM Integration (Total #)	0
DLP Integration (Total #)	0
Geo-Fencing	✘
Detect Security Requirements	✔
Jailbroken	✔
Selective Wiping	✔
Strong Password	✔
Two-Factor Authentication	✘
Device Encryption	✘
Choose Enforcement	✘
Blacklisted Applications	✘
Rooted Device Detection	✘
Manage Anti-Virus	✘
Auto-Deletion	✘
VPN Support	✘
DLP Integration	✘
Integrate AD/LDAP	✘
Whitelisting Applications	✔
Encryption Data-at-Rest	✘
Server in DMZ	✘
Data in DMZ	✘
Granular Level	✘
SAFE Program	✘
Differing Mobile Policies	✘

✔ Supported ✘ Unsupported

Symantec Mobile Management Suite

DCIG Scores and Rankings

OVERALL SCORE	Management	Operating Environment	User Experience	Security and Compliance	Support
104.00	28.50	19.00	14.00	38.50	4.00
RECOMMENDED	RECOMMENDED	RECOMMENDED	RECOMMENDED	RECOMMENDED	EXCELLENT

MANAGEMENT

Provision Platforms	✔
Policy Restriction	✔
Hardware Inventory	✔
Device Ownership	✔
Customizeable Dashboard	✔
Bulk Device Management	✔
Policy Alerts	✔
Administrator Deployment	✖
Device Change	✔
Deploy Multiple Groups	✔
Combined Group	✖
Automatic Provision	✔
SSAE-16	✖
Database Instance (Total #)	1
Solution Options (Total #)	3
Device Change (Total #)	3
Notifications (Total #)	4
Dedicated Database	✖
Backup and Recovery	✖
Software Inventory	✔
Apple VPP	✔
Corporate v. Personal	✔
Single Console	✔
Change Propagations	✖

OPERATING ENVIRONMENT

Deployment Options (Total #)	2
Solution Integration (Total #)	3
Cloud and On-Premise Same	✔
Full MDM Functionality	✔
Third Party Solution	✖
DMZ Replication	✖
High Availability	✔
Secure Communications	✔
Remote Troubleshooting	✔
Corporate App Store	✔
MDM Server	✔
Location Services	✔
Single Cluster Configuration	0
Windows 8	✔
Windows 8 Plan	✔

SUPPORT

Annual Downtime	✖
Support Staff Availability	24×7×365
Methods of Support	Dispatch Technicial Onsite/eMail/Phone/ Remote Login Problem Resolution
Phone Support Hours	24×7×365
Not Under Contract Support	8AM EST to 8PM PST
Not Under Contract Availability	✖
Support Forum	✔

SECURITY AND COMPLIANCE

Cloud Based	✖
PKI Certificate	✔
SIEM Integration (Total #)	1
DLP Integration (Total #)	1
Geo-Fencing	✔
Detect Security Requirements	✔
Jailbroken	✔
Selective Wiping	✔
Strong Password	✔
Two-Factor Authentication	✔
Device Encryption	✔
Choose Enforcement	✔
Blacklisted Applications	✔
Rooted Device Detection	✔
Manage Anti-Virus	✔
Auto-Deletion	✔
VPN Support	✔
DLP Integration	✔
Integrate AD/LDAP	✔
Whitelisting Applications	✔
Encryption Data-at-Rest	✔
Server in DMZ	✖
Data in DMZ	✖
Granular Level	✔
SAFE Program	✔
Differing Mobile Policies	✖

✔ Supported ✖ Unsupported

Tangoe Mobile Device Management

DCIG Scores and Rankings

OVERALL SCORE	Management	Operating Environment	User Experience	Security and Compliance	Support
80.75	23.00	14.75	12.00	29.00	2.00
EXCELLENT	EXCELLENT	EXCELLENT	EXCELLENT	EXCELLENT	GOOD

MANAGEMENT

Provision Platforms	Supported
Policy Restriction	Supported
Hardware Inventory	Supported
Device Ownership	Supported
Customizeable Dashboard	Supported
Bulk Device Management	Supported
Policy Alerts	Supported
Administrator Deployment	Supported
Device Change	Supported
Deploy Multiple Groups	Supported
Combined Group	Supported
Automatic Provision	Supported
SSAE-16	Supported
Database Instance (Total #)	Supported
Solution Options (Total #)	2
Device Change (Total #)	1
Notifications (Total #)	2
Dedicated Database	Supported
Backup and Recovery	Unsupported
Software Inventory	Supported
Apple VPP	Supported
Corporate v. Personal	Supported
Single Console	Supported
Change Propagations	Supported

OPERATING ENVIRONMENT

Deployment Options (Total #)	3
Solution Integration (Total #)	3
Cloud and On-Premise Same	Supported
Full MDM Functionality	Supported
Third Party Solution	Supported
DMZ Replication	Unsupported
High Availability	Supported
Secure Communications	Supported
Remote Troubleshooting	Supported
Corporate App Store	Supported
MDM Server	Supported
Location Services	Supported
Single Cluster Configuration	0
Windows 8	Supported
Windows 8 Plan	Unsupported

SUPPORT

Annual Downtime	Unsupported
Support Staff Availability	24×7×365
Methods of Support	Email/Phone/ Remote Login/ Remote Monitoring
Phone Support Hours	24×7×365
Not Under Contract Support	Supported
Not Under Contract Availability	Unsupported
Support Forum	Supported

SECURITY AND COMPLIANCE

Cloud Based	Unsupported
PKI Certificate	Supported
SIEM Integration (Total #)	0
DLP Integration (Total #)	0
Geo-Fencing	Supported
Detect Security Requirements	Supported
Jailbroken	Supported
Selective Wiping	Supported
Strong Password	Supported
Two-Factor Authentication	Supported
Device Encryption	Supported
Choose Enforcement	Supported
Blacklisted Applications	Supported
Rooted Device Detection	Supported
Manage Anti-Virus	Supported
Auto-Deletion	Supported
VPN Support	Supported
DLP Integration	Unsupported
Integrate AD/LDAP	Supported
Whitelisting Applications	Supported
Encryption Data-at-Rest	Supported
Server in DMZ	Unsupported
Data in DMZ	Unsupported
Granular Level	Supported
SAFE Program	Supported
Differing Mobile Policies	Supported

Supported Unsupported

Trend Micro Mobile Security

DCIG Scores and Rankings

OVERALL SCORE	Management	Operating Environment	User Experience	Security and Compliance	Support
19.75	6.00	1.50	4.00	8.25	0.00
BASIC	BASIC	BASIC	BASIC	BASIC	BASIC

MANAGEMENT

Provision Platforms	✓
Policy Restriction	✗
Hardware Inventory	✓
Device Ownership	✗
Customizeable Dashboard	✗
Bulk Device Management	✗
Policy Alerts	✗
Administrator Deployment	✓
Device Change	✗
Deploy Multiple Groups	✗
Combined Group	✗
Automatic Provision	✗
SSAE-16	✗
Database Instance (Total #)	0
Solution Options (Total #)	0
Device Change (Total #)	0
Notifications (Total #)	0
Dedicated Database	✗
Backup and Recovery	✗
Software Inventory	✗
Apple VPP	✓
Corporate v. Personal	✓
Single Console	✓
Change Propagations	✗

OPERATING ENVIRONMENT

Deployment Options (Total #)	1
Solution Integration (Total #)	0
Cloud and On-Premise Same	✗
Full MDM Functionality	✗
Third Party Solution	✓
DMZ Replication	✗
High Availability	✗
Secure Communications	✗
Remote Troubleshooting	✗
Corporate App Store	✗
MDM Server	✗
Location Services	✗
Single Cluster Configuration	0
Windows 8	✓
Windows 8 Plan	✗

SUPPORT

Annual Downtime	✗
Support Staff Availability	✗
Methods of Support	✗
Phone Support Hours	✗
Not Under Contract Support	✗
Not Under Contract Availability	✗
Support Forum	✗

SECURITY AND COMPLIANCE

Cloud Based	✗
PKI Certificate	✗
SIEM Integration (Total #)	0
DLP Integration (Total #)	1
Geo-Fencing	✓
Detect Security Requirements	✓
Jailbroken	✗
Selective Wiping	✓
Strong Password	✓
Two-Factor Authentication	✓
Device Encryption	✗
Choose Enforcement	✗
Blacklisted Applications	✗
Rooted Device Detection	✗
Manage Anti-Virus	✓
Auto-Deletion	✗
VPN Support	✓
DLP Integration	✓
Integrate AD/LDAP	✗
Whitelisting Applications	✗
Encryption Data-at-Rest	✗
Server in DMZ	✗
Data in DMZ	✗
Granular Level	✓
SAFE Program	✗
Differing Mobile Policies	✗

✓ Supported ✗ Unsupported

Product Rankings Dashboard

Airwatch Mobile Device Management

	OVERALL SCORE	MANAGEMENT	OPERATING ENVIRONMENT	USER EXPERIENCE	SECURITY AND COMPLIANCE	SUPPORT
Best-in-Class						
Recommended						
Excellent						
Good	X	X	X			
Basic				X	X	X

Amtel Mobile Lifecycle Management

	OVERALL SCORE	MANAGEMENT	OPERATING ENVIRONMENT	USER EXPERIENCE	SECURITY AND COMPLIANCE	SUPPORT
Best-in-Class				X		X
Recommended	X	X			X	
Excellent			X			
Good						
Basic						

BoxTone Mobile Device Management

	OVERALL SCORE	MANAGEMENT	OPERATING ENVIRONMENT	USER EXPERIENCE	SECURITY AND COMPLIANCE	SUPPORT
Best-in-Class						
Recommended						
Excellent						
Good	X	X		X	X	
Basic			X			X

Capricode SyncShield

	OVERALL SCORE	MANAGEMENT	OPERATING ENVIRONMENT	USER EXPERIENCE	SECURITY AND COMPLIANCE	SUPPORT
Best-in-Class						
Recommended						
Excellent						
Good						
Basic	X	X	X	X	X	X

Citrix XenMobile (Zenprise)

	OVERALL SCORE	MANAGEMENT	OPERATING ENVIRONMENT	USER EXPERIENCE	SECURITY AND COMPLIANCE	SUPPORT
Best-in-Class						
Recommended						
Excellent						
Good			X	X		
Basic	X	X			X	X

Excitor DME Mobile Device Manager

	OVERALL SCORE	MANAGEMENT	OPERATING ENVIRONMENT	USER EXPERIENCE	SECURITY AND COMPLIANCE	SUPPORT
Best-in-Class						
Recommended		X				
Excellent	X		X	X	X	X
Good						
Basic						

FancyFon Software FAMOC

	OVERALL SCORE	MANAGEMENT	OPERATING ENVIRONMENT	USER EXPERIENCE	SECURITY AND COMPLIANCE	SUPPORT
Best-in-Class						
Recommended						
Excellent						
Good					X	
Basic	X	X	X	X		X

Fiberlink MaaS360 Mobile Device Management

	OVERALL SCORE	MANAGEMENT	OPERATING ENVIRONMENT	USER EXPERIENCE	SECURITY AND COMPLIANCE	SUPPORT
Best-in-Class						
Recommended						
Excellent				X		
Good	X	X	X		X	
Basic						X

Fixmo EMP

	OVERALL SCORE	MANAGEMENT	OPERATING ENVIRONMENT	USER EXPERIENCE	SECURITY AND COMPLIANCE	SUPPORT
Best-in-Class						
Recommended					X	
Excellent	X	X	X	X		X
Good						
Basic						

Good Technology Good Mobile Manager

	OVERALL SCORE	MANAGEMENT	OPERATING ENVIRONMENT	USER EXPERIENCE	SECURITY AND COMPLIANCE	SUPPORT
Best-in-Class						
Recommended						
Excellent						
Good						
Basic	X	X	X	X	X	X

IBM MobileFirst Management

	OVERALL SCORE	MANAGEMENT	OPERATING ENVIRONMENT	USER EXPERIENCE	SECURITY AND COMPLIANCE	SUPPORT
Best-in-Class						
Recommended						
Excellent						
Good						
Basic	X	X	X	X	X	X

The Institution REVIVAL Mobile Management

	OVERALL SCORE	MANAGEMENT	OPERATING ENVIRONMENT	USER EXPERIENCE	SECURITY AND COMPLIANCE	SUPPORT
Best-in-Class						
Recommended						
Excellent						
Good	X		X	X	X	
Basic		X				X

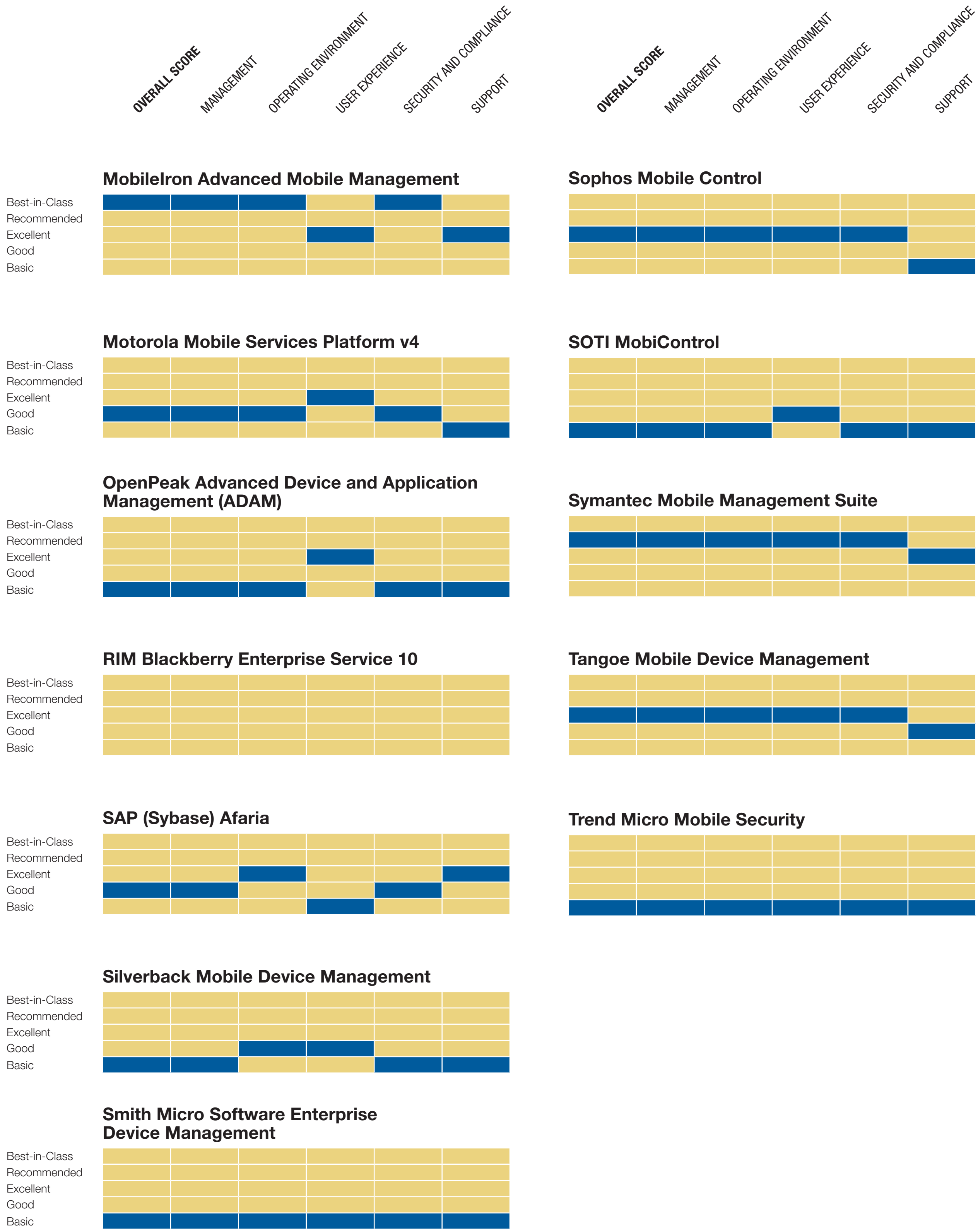
McAfee Enterprise Mobility Management

	OVERALL SCORE	MANAGEMENT	OPERATING ENVIRONMENT	USER EXPERIENCE	SECURITY AND COMPLIANCE	SUPPORT
Best-in-Class						
Recommended						
Excellent						
Good			X		X	
Basic	X	X		X		X

Mobile Active Defense Mobile Enterprise Compliance and Security Server

	OVERALL SCORE	MANAGEMENT	OPERATING ENVIRONMENT	USER EXPERIENCE	SECURITY AND COMPLIANCE	SUPPORT
Best-in-Class						
Recommended						
Excellent						
Good	X	X			X	
Basic			X	X		X

Product Rankings Dashboard (continued)



APPENDIX

Appendix A—Definitions, Explanations and Terminology

Definitions, Explanations and Terminology

This section contains brief definitions and/or explanations of the terms used in the development of the data sheets found in the *DCIG 2014 Mobile Data Management Buyer's Guide.*

Management

Provision Platforms

The process of allocating access rights and privileges which are subsequently monitored and tracked to ensure the security of an enterprise's resources.

Policy Restriction

Authorization requirements needed to access a network system remotely from a home computer, smartphone or other compatible devices. Also must comply with all security procedures, federal and state laws and regulations along with company rules.

Hardware Inventory

An up-to-date hardware (things you can actually touch) list which includes manufacturer, model, device type, processor, physical memory installed, operating system, located in a central repository.

Device Ownership

Who controls the mobile device issued or brought to work. The device may be owned by either the corporation or the employee.

Customizable Dashboard

Products that allow users to create fully customizable dashboard that helps transform monitored data into immediate feedback for the enterprise IT department. The dashboard can be modeled and scaled to meet IT management needs using widgets.

Bulk Device Management

The ability to manage multiple devices from a single location to enable control of software settings such as: user locale, phone button template, and login user ID which are used to monitor and control devices on the network.

Policy Alerts

When mobile device management policy violations are alerted on and updates are visible on the dashboard or sent to the Administrator.

Administrator Deployment

Trusted agents within the organization who have complete and unrestricted access to perform software deployment in mass to all servers and/or devices in the organization. This role is usually given to two to three trusted users to help prevent potential lockouts that could occur.

Device Change

Administrator device change propagations are sent automatically to all devices, groups and users.

Deploy Multiple Groups

The ability for an administrator to create a policy and deploy across multiple groups.

Combined Group

When a third group is necessary for users to gain policies from multiple groups.

Automatic Provision

Also called self-service provisioning, is the ability to deploy an information technology or telecommunications service by using pre-defined procedures that are carried out electronically with no human intervention.

SSAE-16

Statement on Standards for Attestation Engagements (SSAE) No. 16, titled "Reporting on Controls at a Service Organization," was finalized by the Auditing Standards Board of the **American Institute of Certified Public Accountants (AICPA)** in January 2010.

Database Instance (Total #)

The term "instance" is typically used to describe a complete database environment. It is most commonly used to differentiate multiple instances of the same database running in the same software environment. The number specifies the number of different supported elements available. The specific elements supported for each product are available by accessing the *2014 DCIG Mobile Data Management Interactive Buyer's Guide* (IBG).

Appendix A—Definitions, Explanations and Terminology (continued)

Solution Option (Total #)

A file structured storage, or compound, file stored in a binary format. User information can be saved in streams which may be named to help identify the information later. Can be used to store user preference settings and is created automatically. The number specifies the number of different supported elements available. The specific elements supported for each product are available by accessing the *2014 DCIG Mobile Data Management Interactive Buyer's Guide* (IBG).

Device Change (Total #)

Refers to the ability for the MDM solution automatically propagate device changes. The number specifies the number of different supported elements available. The specific elements supported for each product are available by accessing the *2014 DCIG Mobile Data Management Interactive Buyer's Guide* (IBG).

Notifications (Total #)

The sum of alert messages sent to mobile manager. The number specifies the number of different supported elements available. The specific elements supported for each product are available by accessing the *2014 DCIG Mobile Data Management Interactive Buyer's Guide* (IBG).

Dedicated Database

Refers to a specific database reserved for serving a specific need.

Backup and Recovery

Refers to the various strategies and procedures involved in protecting an organization's database against any potential data loss and subsequently reconstructing the database after any kind of data loss occurs.

Software Inventory

Details of software installed in a computer. The Software details include Software Name, Version, Manufacturer and Usage statistics.

Apple VPP

Apple's Volume Purchase Program (VPP) allows for multiple downloads of the same document by certain institutions or a single download discount to qualified individuals.

Corporate v. Personal

These terms are common to the bring-your-own-device (BYOD) movement. *Corporate* indicates the device is owned and issued by the organization, whereas *personal* means the user has provided their own device for work use.

Single Console

Meaning that organizations use one single toolset to manage Linux, Macintosh, and Windows computers.

Change Propagations

The distribution of software changes in a methodical manner across all devices employed on the network without Administrator intervention.

Any numerical responses in the management category of the data sheets refer to how many differing solutions the vendor supports. For more information on which solutions are supported please see the 2014 DCIG Mobile Data Management Interactive Buyer's Guide (IBG).

Operating Environment

Deployment Options (Total #)

When a MDM company issues a command that can be changed or refined in the area of installing, testing and implementing a computer system or application. The number specifies the number of different supported elements available. The specific elements supported for each product are available by accessing the *2014 DCIG Mobile Data Management Interactive Buyer's Guide* (IBG).

Solutions Integration (Total #)

In business computing a total solution is one that contains all products and services in one delivery that meets a specific function or provides one solution or system to solve multiple problems. The number specifies the number of different supported elements available. The specific elements supported for each product are available by accessing the *2014 DCIG Mobile Data Management Interactive Buyer's Guide* (IBG).

Cloud and On-Premise Same

Whether an organization chooses to store their data in the cloud or on-premise, the MDM company can manage data all the same.

Full MDM Functionality

Indicates the MDM provider can offer an organization all the major functions needed to manage their mobile devices.

Appendix A—Definitions, Explanations and Terminology (continued)

Third Party Solution
A third-party entity that the MDM company uses to manage and distribute remote, cloud-based data backup services and solutions to organizations from a central data center.

DMZ Replication
Stands for Dematerialized Network Zone, DMZ is a computer or small sub-network that sits between a trusted internal network, such as a corporate private local-area network (LAN), and an untrusted external network, such as the public Internet. It also offers the process of creating and managing duplicate versions of a database for organizations.

High Availability
Also known by the abbreviation HA, this refers to the availability of redundant resources in a computer system in the case of component failures which minimizes the possibility of a single point of failure.

Secure Communications
This indicates an encrypted transmission of data from one device to another that cannot be viewed by other devices unless they have the identical encryption technology.

Remote Troubleshooting
Refers to the ability to identify and correct anomalies with data files, devices and other resources from another device at a different location.

Corporate App Store
An in-house, online application store that enables authorized users to download apps directly to their approved devices.

MDM Server
Mobile data management offered over a computer or device on a network that manages network resources.

Location Services
The ability to use information from cellular, wireless, or a Global Positioning System to determine the devices approximate location.

Single Cluster Configuration
Refers to the number of supported devices in a single 2-node server cluster configuration.

Windows 8
An operating system developed by the Microsoft Corporation for use on personal computers, laptops, tablets, and other devices. The Windows 8 operating system officially debuted on October 26th, 2012.

Windows 8 Plan
Planned development path to support the Windows 8 platform.

AD/LDAP/Active Sync
An automatic synchronization of the Active Directory (AD) and Lightweight Directory Access Protocols (LDAP) which mitigates the need for a separate database of users and groups. If a user is added to the domain or is removed from a group then software will automatically synchronize this information without any human intervention from the system administrator.

Support

Annual Downtime
The cumulative total of all time during a calendar year that the MDM provider is not up and running.

Support Staff Availability
When and to what extent the MDM company's staff is available for support.

Methods of Support
The means by which a MDM company offers support services to organizations.

Phone Support Hours
Times and days when a MDM company is able to offer support via the telephone.

Not Under Contract Support
This indicates an option to forgo contracted help/support from the MDM company.

Not Under Contract Availability
This indicates an option chosen by the organization to forgo the MDM provider being available to them for support, etc.

Support Forum
Help offered by the MDM company in the form of a forum of individuals contributing assistance to one another.

24x7x365

This indicates if phone support is available ***24*** hours a day, ***7*** days a week, ***365*** days out of the year.

Dispatch Technician/Onsite/Email/Phone/Monitoring/Remote Monitoring/ Remote Login/Remote Login Problem Solving /Web Chat

Methods of support offered by a MDM company.

8AM EST to 8PM PST

Indicates the hours of service offered by a MDM company are from 8AM Eastern Standard Time (EST) until 8PM Pacific Standard Time (PST).

Business Day Local

Indicates hours of service offered by a MDM company that are in accordance with the typical local businesses that surround the company.

Security And Compliance

Cloud Based

Provides direct access to cloud storage and which cloud providers are offered as available options. The total number of cloud providers supported is listed here.

PKI Certificate

Stands for Public Key Infrastructure (PKI), a system of digital certificates, Certificate Authorities, and other registration authorities that verify and authenticate the validity of each party involved in an Internet transaction.

SIEM Integration (Total #)

Security Information and Event Manager (SIEM) is a set of tools used by IT professionals and system administrators to manage multiple security applications and devices, and to respond automatically to resolve security incidents. The number specifies the number of different supported elements available. The specific elements supported for each product are available by accessing the *2014 DCIG Mobile Data Management Interactive Buyer's Guide* (IBG).

DLP Integration (Total #)

Data Loss Prevention Integration refers to the all encompassing solution to identify, monitor and protect data that is in use (being used by an end-user), in motion (being transferred over a network), or at rest (stored on a storage device). This done by a contextual analysis of the data to ensure protection of proprietary data during its use and transmission over a network. The number specifies the number of different supported elements available. The specific elements supported for each product are available by accessing the *2014 DCIG Mobile Data Management Interactive Buyer's Guide* (IBG).

Geo-Fencing

This indicates a virtual perimeter for a real-world geographic area. This technology employs the use of the global positioning system (GPS) or radio frequency identification to define geographical boundaries.

Detect Security Requirements

Indicates the solutions ability to detect devices outside a company's security requirements.

Jailbroken

Slang term used to describe the user gaining access to an iPhone's private file system to override some of the device's restrictions. *Jailbreaking* also enables an iPhone user to install third-party applications.

Selective Wiping

When a device manager selects specific applications or data to delete.

Strong Password

Indicates a user or device monitor creating a password that is difficult to hack.

Two-Factor Authentication

Indicates a security feature that uses two forms of identification in order to access a network system or application through a mobile device.

Device Encryption

When a device's data is translated into a secret code for security purposes.

Choose Enforcement

Indicates when an organization chooses to enforce certain policies.

Blacklisted Applications

Refers to applications for mobile devices that an organization has deemed to be not authorized on the network.

Rooted Device Detection

Indicates the ability for a system to track whether a mobile device has the capability and has already been rooted—meaning it has been "superused" by the user.

Manage Anti-Virus

Indicates the MDM provider can manage the Anti-Virus system in use.

Auto-Deletion

This is when a MDM company sets up a program to automatically eliminate certain data and applications from mobile devices.

VPN Support

Indicates assistance offered through a Virtual Private Network (VPN) which is a network constructed by using public wires to connect nodes.

DLP Integration

Data Loss Prevention Integration refers to the all encompassing solution to identify, monitor and protect data that is in use (being used by an end-user), in motion (being transferred over a network), or at rest (stored on a storage device). This done by a contextual analysis of the data to ensure protection of proprietary data during its use and transmission over a network.

Integrate AD/LDAP

This refers to the process of integrating with Active Directory (AD) and Lightweight Directory Access Protocol (LDAP).

Whitelisting Applications

Refers to applications for mobile devices that an organization has deemed to be authorized or approved on the network.

Encryption Data-at-Rest

This means protecting data that's not moving through networks. The protection in this case is offered via encryption.

Server in DMZ

Indicates data on a computer or device on a network that manages network resources that is in a Dematerialized Network Zone (DMZ).

Data in DMZ

Indicates data on a computer or device that is in a Dematerialized Network Zone (DMZ).

Granular Level

Used to describe safeguards to ensure compliance at the level of the individual user which is a very detailed level.

SAFE Program

SAFE represents a Samsung Enterprise solution for their mobile devices that includes the necessary security and feature enhancements suitable for business use.

Differing Mobile Policies

Refers to the managing of differing mobile policies based on.

Any numerical responses in the security and compliance category of the data sheets refer to how many differing solutions the vendor supports. For more information on which solutions are supported please see the 2014 DCIG Mobile Data Management Interactive Buyer's Guide (IBG).

Appendix B—Mobile Data Management Provider Contact Information

Mobile Data Management Provider Contact Information

AirWatch, LLC
1155 Perimeter Center West, Suite 100
Atlanta, GA 30338
United States
info@air-watch.com
+1.404.478.7500
http://www.air-watch.com/

Amtel, Inc.
900 Lafayette St., Suite 506
Santa Clara, CA 95050 USA
+1.408.615.0522
http://www.amtelnet.com

BlackBerry
295 Phillip Street
Waterloo, Ontario
Canada N2L 3W8
+1.519.888.7465
http://www.rim.com/

Boxtone
8825 Stanford Boulevard, Suite 200
Columbia, MD 21045 USA
+1 410.910.3300
+1 410.910.3344
http://boxtone.com

Capricode
Yrttipellontie 10
FIN-90230 OULU, Finland
info@capricode.com
+358 40 3012 300
http://www.capricode.com

Citrix Systems, Inc.
4988 Great America Parkway
Santa Clara, CA 95054
+1.408.790.8000
http://www.citrix.com/

Excitor
Spotorno Allé 12
DK-2630 Taastrup
marketing@excitor.com
+45 70 21 68 00
http://www.excitor.com/

IBM Corporation
1 New Orchard Rd
Armonk, NY 10504-1722
callserv@ca.ibm.com
+1.800.426.4968
http://www.ibm.com/storage

Iron Mountain, Inc.
745 Atlantic Ave. Fl 6
Boston, MA 02111
+1.617.535.4766
http://www.ironmountain.com/

McAfee, Inc.
2821 Mission College Blvd.
Santa Clara, CA 95054
+1.866.622.3911
http://www.mcafee.com/

Mobile Active Defense, Inc.
435 Rock Springs Road N.E.
Atlanta, GA 30324
+1.877.425.6623
http://www.mobileactivedefense.com/

MobileIron
415 East Middlefield Road
Mountain View, CA 94043
+1.650.919.8100
+1.877.819.3451
http://www.mobileiron.com/

Motorola Solutions, Inc.
1303 East Algonquin Road
Schaumburg, Illinois 60196 USA
+1.847.576.5000
http://www.motorolasolutions.com/

Mobile Data Management Provider Contact Information continued

OpenPeak
1750 Clint Moore Road
Boca Raton, Florida 33487
+1.561.893.7800
http://openpeak.com/

SAP AG - Walldorf
Dietmar-Hopp-Allee 16
(früher: Neurottstraße)
69190 Walldorf
Phone: +49 (0)6227 / 7-47474
http://www.sap.com/index.epx

SilverbackMDM
Aurora Place
88 Phillip Street
Level 31
Sydney, NSW 2000
Phone: +61 2 8211 2702
http://silverbackmdm.com/

Smith Micro Software, Inc.
51 Columbia
Aliso Viejo, CA 92656
+1 949-362-5800
http://www.smithmicro.com/

Sophos, Inc.
3 Van de Graaff Drive, 2nd Floor
Burlington, MA 01803 USA
+1.781.494.5800
http://www.sophos.com/en-us/

SOTI
5770 Hurontario Street,
Suite 1100, Mississauga,
Ontario L5R 3G5 Canada
sales@soti.net
+1.905.624.9828
http://www.soti.net/

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043
+1.650.527.8000
http://www.symantec.com/

Tangoe, Inc.
35 Executive Blvd
Orange, CT 06477
+1.203.859.9300
+1.877.571.4737
http://www.tangoe.com/

The Institution JSPM AB
Kungsbroplan 1
112 27 Stockholm
Sweden
+46 705 83 00 03
http://www.theinstitution.se/

Trend Micro Inc.
10101 N. De Anza Blvd
Cupertino, California 95014
+1.408.257.1500
+1.800.228.5651
http://www.trendmicro.com/

Appendix C—Author Contact Information

Author Contact Information

DCIG, LLC
7511 Madison Street
Ralston, NE 68127
+1.402.884.9594

CONTACT

Howard Haile
howard.haile@dcig.com

WEBSITE
www.dcig.com