Mobile Device Management

Buyers Guide

A compilation and capabilities reference summary of the top 24 solution providers in Mobile Device Management

Released by Solutions Review
4/1/2013
INTRODUCTION: In this Buyers Guide Solutions Review has chosen to highlight Mobile Device Management because we believe the recent explosion of mobile devices has caused a seismic shift in how IT executives need to think about their networks. The end user – maybe employees, maybe students – is demanding access to networks via mobile devices and the amount of applications and data they expect to access is growing at an alarming rate.

In a recent survey conducted by Info Week; 80% of polled IT professionals say tablets are growing in organizational importance, 64% of organizations are adopting custom applications for business practices and 65% are predicting an increasing in employee owned end-device utilization within the organization.

With all these changes in business practices and emerging technology one thing remains constant. The importance and even necessity for IT managers to monitor track and secure business critical information that is being accessed through this new technology, Mobile Device Management (MDM). While that task is daunting enough the variety of end devices and platforms those devices run on just add to the complexity of this requirement.

It is that variety coupled with the necessity to manage and secure the range of devices that has lead to the increase in software offering MDM solutions. There are numerous companies offering solutions for the different organizational needs for the different end-devices being utilized within.

The Solutions Review 2013 MDM Buyers Guide is an attempt to consolidate, organize, and present that information for your convenience. Without bias, opinion or editorializing we highlight some of the top MDM solutions providers offering strictly the facts. Who they are and what they offer with visibility into their entire solution set.

Matthew Adamson
Editor
Solutions Review
madamson@solutions-review.com
(339) 927-9237

“The recent explosion of mobile devices has caused a seismic shift in how IT executives need to think.”
5 Questions You Should Ask Yourself Before Selecting a Mobile Device Management Solution

QUESTION #1 *What type of mobile devices will we support?*

With so many new device options for corporate issued devices and the surge in BYOD programs it is important to understand which devices you are going to support, and ultimately allow corporate access to. While you want to provide options for employees it is important to draw a line in the sand and not allow anything and everything for fear of spreading your IT department to thin. A quality over quantity approach may be a good thing to consider when asking this question.

QUESTION #2 *What is the best mobile architecture for our organization?*

There are a number of things to consider when addressing this issue. First you need to consider what your current IT infrastructure looks like and then structure your MDM evaluation around what is already in place. Not the other way around. Also you will need to address cloud-based solutions vs. on-premise solutions, hosted vs. self supported and the scalability of the MDM solutions as your mobile device population grows.

QUESTION #3 *How will information be access, where will it live, and do we need varying levels of access or risk profiles?*

When accessing information and corporate data on your mobile devices how and where that information is stored will vary on a case by case basis. Will it be stored on the device itself or will it be accessed remotely? Compliance or auditing requirements, as well as fear of lost or stolen devices will help you make that determination. If the level of data is extremely sensitive or compliance and auditing requirements are so strict, utilizing said devices as viewing platforms only may be considered rather than storing data directly on the device. Considering who is accessing what and the need for certain individuals to access certain information will determine if you need to set separate levels of access or risk profiles.

QUESTION #4 *What specification will our enterprise mobility policy entail and what MDM functions will we utilize?*

Answering this question will provide the dos and don'ts and actual functions that your mobile devices can perform. These security policies will be the backbone of your mobile strategy and have a major impact on the safety of your corporate data. You will want to look at and determine how each of these functions will impact your mobile strategy, data security and device utilization: Password policy control, device and data encryption, port control (Wi-Fi, Bluetooth, camera) remote lock/unlock/wipe, asset tracking, device configuration (VPN, email), application delivery and control, black/white listing and audit, monitoring and reporting.

“Will corporate data be stored on the device itself or will it be accessed remotely?”
QUESTION #5  **How will we ensure compliance and decrease risk?**

Monitoring tools or asset tracking can help you maintain a certain level of compliance, but sometime these functions are more reactive then proactive. Waivers, forms and policy agreements are typically needed before access to the network and corporate data is granted. To truly ensure compliance and policy integrity we believe that communication and education is the best policy. Through seminars, courses or information sessions you can clearly outline, define and reinforce policies and guidelines. By laying everything out on the table and communicating rules and regulations directly to the end users you can feel better about there being a true understanding of your mobile policies.

And 5 Questions You Should Ask Your Potential Mobile Device Management Providers Before Selecting a Solution

QUESTION #6  **How hard will it be to integrate your MDM solution into my existing infrastructure?**

Once you figure out the type of architecture that might work best it is important to understand how that architecture will be implemented into your current infrastructure. As stated before, the architecture and integration should fit into what is currently in place and already helping you to achieve your overall objectives, not vice versa. MDM implementations can be difficult enough on a small scale never mind looking at a large multi-unit organization so that is why it is important to truly understand how a MDM solution will integrate with what is currently in place and what the entire implementation process looks like before getting started. Look for solutions with simple installation requirements, distributed control, and scalability suitable for your organizations size and structure.

QUESTION #7  **How flexible is the MDM architecture and solution?**

Technology is continually changing and that has never been more the case than with today’s mobile devices. New operating systems, device features or capabilities seem to enter the market on a monthly basis. These devices are actually evolving faster than the MDM solutions that enterprises are using to manage and secure them. That is why it will be very important for you to find out how adaptable, flexible and scalable a provider’s solution is. Choosing a solution that isn’t designed to be flexible will become a real problem as new mobile devices become part of the mix. Keep in mind your needs for the future as switching solutions may prove to be a barrier.

QUESTION #8  **What resources will the MDM solution require on the client side?**

If the MDM system requires any significant percentage of the storage or processing capability on the client side, the solution could be problematic with mobile devices that are running other high performance demand apps or have limited storage. The point of a MDM solution is to provide the management and security needed in order to take advantage of mobility in your organization. If the solutions relies heavily on client storage and data usage it can hinder performance, thus negating the benefits that come with enterprise mobility.
QUESTION #9  What level of support will provider for regulatory compliance, auditing and reporting standards?

This question may not be necessary for all MDM users, but for those in regulated industries it is a critical question to ask. You will need to fully understand how comprehensive auditing and reporting features are and if they meet current requirement for your organization and industry. You will also want to understand the process of or how a solutions provider would plan on meeting possible future regulatory demands. Flexibility is a key in regards to this issue as well.

QUESTION #10  With the rise in BYOD does your solution offer containerization in the event remediation activities are needed?

BYOD offers great options for employees, but it can also present a tough mix of personal and corporate data for IT to have to manage. In the instance of device exceptions (conditions that indicate tampering, client side MDM failure, etc.) actions such as remote wiping or locking may need to be taken. On a device where data is not separated in corporate and personal containers all can be lost, Solutions offering containerization can help prevent some of the issues organizations face when allowing for BYOD.

And a few more MDM Strategy and Issues to Keep in Mind:

- Determine the type of devices that the company or organization will support whether that company/organization issued or employee own devices.
- Be sure to align the chosen devices with the level of security need to secure and protect data and make sure they can handle that level.
- Create strong policies and security standards. Enforce policies and standard but be sure to communicate those clearly to employees.
- Remember to keep in mind legal implications and structure the MDM strategy and policies in accordance.
- Understand what business tool employees in a company/organization’s specific mobile environment need and structure access and security accordingly.
- Do not expect 100% acceptance and be ready to communicate, educate and train on best practices and device capabilities.
- Structure you MDM strategy to allow it to scale and adapt – technology is ever changing.

Below is a list and Summary Information on 24 of the Top Mobile Application Development Platform Solution Providers. If you have any questions regarding this list or the topic of Mobile Device Management, please feel free to contact us at (339) 927-9234.
# Table of Contents: Mobile Device Management Solution Providers

<table>
<thead>
<tr>
<th>Provider</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Absolute Software</td>
<td>7</td>
</tr>
<tr>
<td>AirWatch</td>
<td>8</td>
</tr>
<tr>
<td>AmTel</td>
<td>9</td>
</tr>
<tr>
<td>Boxtone</td>
<td>10</td>
</tr>
<tr>
<td>Citrix</td>
<td>11</td>
</tr>
<tr>
<td>Excitor</td>
<td>12</td>
</tr>
<tr>
<td>Fiberlink (MaaS360)</td>
<td>13</td>
</tr>
<tr>
<td>Fixmo</td>
<td>14</td>
</tr>
<tr>
<td>Good Technology</td>
<td>15</td>
</tr>
<tr>
<td>IBM</td>
<td>16</td>
</tr>
<tr>
<td>Kaseya</td>
<td>17</td>
</tr>
<tr>
<td>LANDesk</td>
<td>18</td>
</tr>
<tr>
<td>Mobile Active Defense</td>
<td>19</td>
</tr>
<tr>
<td>McAfee</td>
<td>20</td>
</tr>
<tr>
<td>Mformation</td>
<td>21</td>
</tr>
<tr>
<td>MobileIron</td>
<td>22</td>
</tr>
<tr>
<td>Notify</td>
<td>23</td>
</tr>
<tr>
<td>OpenPeak</td>
<td>24</td>
</tr>
<tr>
<td>Sophos</td>
<td>25</td>
</tr>
<tr>
<td>SOTI</td>
<td>26</td>
</tr>
<tr>
<td>Sybase</td>
<td>27</td>
</tr>
<tr>
<td>Symantec</td>
<td>28</td>
</tr>
<tr>
<td>Tangoe</td>
<td>29</td>
</tr>
<tr>
<td>Widepoint</td>
<td>30</td>
</tr>
</tbody>
</table>
FROM THE COMPANY: Absolute Software Corporation was founded in 1993 on the idea that individuals and businesses should be able to track, manage, and secure their mobile computers regardless of the physical location of the device.

Absolute Manage for Mobile Devices allows you to remotely manage the iOS, Android, and Windows Phone devices in your deployment. Now you can wirelessly (over 3G or Wi-Fi) configure, query, and even wipe or lock managed devices.

Absolute Manage for Mobile Devices is available stand-alone or as a component within Absolute Manage.

OS SUPPORT: iOS, Android, Symbian, Windows Phone 7, Window Desktops, MAC Desktops

MDM FEATURES:

**Apps Management:**

Track installed apps. Build device records using custom data fields. Publish a list of approved apps onto each device and provide a single-click download/install process for users. Silently install/remove apps using management APIs. Apps by Absolute provide you with a variety of apps so you can geographically track devices and perform security and administrative tasks from an iPad; manage in-house apps; and apply strict security controls for the sharing of files and media using the AbsoluteSafe app. Includes support for the Apple App Store Volume Purchase program.

**Security, Change & Configuration Management:**

Set longer, more complex passwords for enterprise level security. Lock a device, clear a password, and wipe a device clean to factory settings. Manage and deploy profiles to configure email, restrict apps, set up VPN, disable the camera, and deploy web clips. Use policy-locked configuration profiles to stop non-compliant devices (jailbroken, blacklisted apps installed) from accessing company email and networks. Schedule policies so users have a defined window of time to access secured documents and corporate networks. Send customized messages and communicate with the end user wirelessly.

**Asset Inventory:**

Gather hardware and software data points for analysis. Display data such as serial numbers, Mac addresses, installed apps, telephone numbers, and other data with custom views, searches, and reports. Integrate your mobile device data with third party applications such as Microsoft SCCM.

**BYOD:**

Use the automated employee enrolment process to onboard employees and their personally owned devices, eliminating the manual IT work associated with BYOD programs. Record employee opt-in and direct a copy of each confirmation to Human Resources. Automatically assign BYOD-specific policies to ensure these devices only access corporate networks and data if they are compliant.

A link to an overview of the Absolute Software MDM solutions can be followed here.
AirWatch was founded in 2003 by John Marshall and Alan Dabbiere. They believed mobile technology would completely revolutionize the way companies do business. Based in Atlanta with offices worldwide, AirWatch is privately held and financially backed by its executive team.

AirWatch is the leader in enterprise-grade Mobile Device Management, Mobile Application Management and Mobile Content Management solutions designed to simplify mobility. More than 2,000 customers across the world trust AirWatch to manage their most valuable assets: their mobile devices, including the apps and content on those devices. Our solutions are comprehensive, built on a powerful yet easy to use platform by leaders in the mobile space.

**OS SUPPORT:** iOS, Android, Blackberry, Symbian, Mac OS X, Windows Mobile, Windows Phone 7

**MDM FEATURES:**

**Multi-OS Management:**

Managing a diverse mobile fleet of Android, Apple, BlackBerry, Symbian, Windows Mobile and Windows Phone devices raises many challenges for enterprises. AirWatch enables organizations to leverage the latest mobile devices with a comprehensive mobility solution that manages all mobile assets regardless of operating system, carrier, network or location.

**Multi-Tenant Solution:**

Within large enterprises, IT departments have to meet the requirements of different users based on role, function or geography. AirWatch’s multi-tenant architecture enables IT administrators the ability to create tiers within the AirWatch console to represent each of these groups, for simplified management of devices.

**Seemless Enterprise Integration:**

AirWatch can authenticate device users through a basic authentication progress or by integrating directly with enterprise directory services (LDAP). For enterprises using Microsoft Exchange Active Sync, AirWatch has the ability to configure and secure access to enterprise email, calendar and contacts. AirWatch also supports corporate VPN settings, Wi-Fi and much more.

**Secure Enterprise Access:**

AirWatch developed the concept of role-based access control to ensure only authorized console users are able to view and manage enterprise assets. Custom roles provide the ability to restrict the device groups an IT administrator can manage. More specifically, console roles also control the depth of device management features and capabilities available to that user. For another added level of security, console log in credentials are integrated with enterprise directory services, authenticating users before logging in.

A link to an overview of the AirWatch MDM solutions can be followed here.
FROM THE COMPANY:

Founded in 2001, Amtel is a global mobile device management (MDM) & telecom expense management (TEM) vendor, addressing the challenges companies face in managing mobile devices and telecommunications expenses. Amtel developed the industry's first integrated private cloud based secure MDM and TEM solution, allowing companies of all sizes to securely manage mobile devices and telecom expenses from a single platform. Provided as a convenient and cost effective SaaS platform, Amtel TIMS solution is available with SSAE 16 Type II compliant hosting offering the highest level of data security and reliability as compared to other MDM & TEM vendor companies.

A SaaS model provides clients a secure and customized application at an affordable price point. An optional Amtel Gateway for Active Directory & Active Sync integration can reside behind corporate firewall for added security.

The Amtel solution features the ability to segregate personal information from corporate data, selective wipes, encryption, remote lock, etc. It also includes secure document management, segregate Whitelisted & Blacklisted Market Apps, create Enterprise App store for in-house Apps etc for major mobile device platforms.

OS SUPPORT:

iOS, Android, Blackberry, Symbian, Windows Mobile, Windows Phone 7

MDM FEATURES:

Mobile Device Security and Content Management:

Amtel's mobile device management (MDM) solution is the first modular platform that is organically developed with integrated security management, content management and expense management solutions. Amtel delivers this platform as secure Software-as-a-Service (SaaS) solution with quick implementation. Solution is designed to handle both Corporate liable & BYOD Bring-your-own-device types.

Mobile Lifecycle Management:

Amtel's mobile management suite of services can help enterprises reduce 10 to 40% of their mobility expenses. The award winning TIMS platform (Telecom Information Management System), along with professional services help in streamline & manage mobile services at an organization.

Telecom Expense Management:

Amtel's Telecom Expense Management solution using the award winning TIMS platform (Telecom Information Management System), can help enterprises eliminate 10 to 40% of their telecom expenses. The solution is hosted using SAS 70 Type II certified program to deliver the highest level of security available today.

A link to an overview of the Amtel MDM solutions can be followed here.
FROM THE COMPANY:

Founded in 2005, BoxTone is a global Enterprise Mobility Management (EMM) Software and Services provider headquartered in Columbia, Maryland, USA. Our platform of enterprise-grade, plug-and-play software modules is used by more enterprises, public sector entities and managed service providers (MSPs) than any other to ensure that their iPhone, Pad, Android, BlackBerry and Windows Phone device platforms are continuously maintaining optimal services levels, at the lowest cost and risk.

Delivered by our EMM experts, BoxTone software uniquely brings proactive IT Service Management (ITSM) best practices together with Mobile Application Performance Management (MPM), Mobile Device Management (MDM) and Mobile User Management technologies into a single unified management console.

OS SUPPORT: iOS, Android, Blackberry, Symbian, Windows Mobile

MDM FEATURES:

BoxTone Enterprise Mobility Management (EMM) platform delivers centralized control of all mobile devices and tablets including iPhone, iPad, Android and BlackBerry, as well as the apps that run on them. Built to CIO and CISO specifications, BoxTone aligns mobility management with core IT services, extending existing resources and processes to fully secure, manage and govern mobility on par with all other critical IT systems. Powered by patented real-time automation, BoxTone addresses the full mobile lifecycle—mobile device management (MDM), mobile support management, mobile operations management and mobile business management.

Mobile Device Management:

Enterprise-grade Mobile Device Management (MDM) designed to help your organization rapidly and securely deploy mobile devices, tablets and applications, powered by automated policy, compliance, configuration and application management to ensure lowest cost and risk.

Mobile Support Management:

Automated service desk and user self-service to help make your Level 1 Service Desk staff instant mobility management experts to speed issue resolution, improve first call closure (FCS) rates and reduce mobile support costs.

Mobile Operations Management:

Real-time automated monitoring, performance dashboard, alerting and system tuning to help Operations and Engineering IT staff get proactive and deliver the exceptionally high mobile service levels your end users demand, at the lowest cost and risk to the organization.

Mobile Business Management: Sophisticated analysis and reporting to help you track and analyze mobility ROI and TCO to drive continuous improvement, no matter how many mobile devices, applications and platforms you deploy.

A link to an overview of the Boxtone MDM solutions can be followed here.
On December 5 2012 Citrix announced today that it has closed the acquisition of Zenprise, a leading innovator in mobile device management (MDM). Citrix has integrated the Zenprise offering for mobile device management, with its Citrix CloudGateway™ and Me@Work™ solutions for managing mobile apps and data.

“Citrix is the cloud computing company that enables mobile workstyles - empowering people to work and collaborate from anywhere, accessing apps and data on any of the latest devices, as easily as they would in their own office - simply and securely. Citrix products are in use at more than 260,000 organizations and by over 100 million users globally.”

OS SUPPORT: iOS, Android, Blackberry, Symbian, Windows Mobile

MDM FEATURES: Mobile Device Management

XenMobile MDM is a mobile device management solution that delivers role-based management, configuration and security for both corporate and employee-owned devices. Upon user device enrollment, IT can provision policies and apps to devices automatically, blacklist or whitelist apps, detect and protect against jailbroken devices, and wipe or selectively wipe a device that is lost, stolen or out of compliance.

Configure

Configure both corporate and bring-your-own device (BYOD) settings and integrate with IT resources in a centralized, role-based way that’s integrated with enterprise directories like Microsoft Active Directory.

Provision

Enable users to self-service enroll, select apps from an app catalog, and perform some self-help functions, and empower administrators to provision policies and apps automatically over-the-air to users.

Secure

Take security action in the event of loss, theft, or user departure. The solution keeps an audit trail of administrator actions and integrates with enterprise security systems for threat correlation and analysis.

Support

Provide help desk functions, remote support, and troubleshooting for mobile users.

Monitor and Report

Monitor and report on device and app inventory, device status, and security and compliance status.

A link to an overview of the Citrix XenMobile solution can be followed here.
FROM THE COMPANY: Founded in 2001, Excitor is a provider of secure mobile device management, mobile email and mobile application solutions. The company develops and sells DME (Dynamic Mobile Exchange) to organizations globally. With sales and implementation offices and partners across Europe, North America, Asia Pacific, the Middle East and Africa, Excitor counsels enterprises of all sizes about mobilizing their respective workforces.

“Excitor DME is the perfect business solution for working securely with corporate email, calendar, contacts, to dos, news feeds, HTML5 applications and intranets - all secured within a container on the device, without risk of leaking data to other apps and without the need to install and configure a full VPN. DME is ideal for bring-your-own-device (BYOD).”

OS SUPPORT: iOS, Android, Windows Mobile, Windows Mobile

MDM FEATURES: DME’s Mobile Device Management addresses all of these areas and equips you to effectively mobilize your company, without compromising existing security policies.

With DME’s Mobile Device Management you gain complete control over your organization’s mobile fleet. It enables you to:

- Deploy applications to your users’ phones
- Administer your mobility solution
- Support your users
- Secure your organization’s data
- Deploy DME AppBox Apps

Or manage Corporate Data with DME Secure Container

DME offers more than mobile device management capabilities. Using the DME Secure Container application, you give your employees secure access to their corporate email, calendar, address book, RSS feeds, and business apps - and therefore create a true separation between what is corporate compliant and what is personal. Read more about DME Mobile Email & PIM and DME AppBox to find out how to enable a secure container on personal devices or corporate-owned devices.

Mobile Device Management for iOS

DME delivers full mobile device management capabilities for iPhone, iPad and iPod Touch. Using the Simple Certificate Enrollment Protocol (SCEP), DME can now manage and monitor iOS devices without any particular user involvement. Some of the useful aspects of this feature include the ability to update device setting profiles, obtain critical device information, block some apps and remote wipe not just the corporate partition but the whole device if required.

A link to an overview of the Excitor MDM solution can be followed here.
FROM THE COMPANY:

In 2008 Fiberlink announced the world’s first “Mobility-as-a-Service” solution, the MaaS360 Platform and has expanded to include the complete suite of Enterprise mobile devices including smartphone and tablets. Today they manage over 1 million devices in over 700 global companies.

Fiberlink’s unique cloud-based technology and delivery model are the foundation for our Mobility-as-a-Service platform. MaaS360 changes the game for how IT manages, views, and controls all enterprise devices, from desktops and laptops to smartphones and tablets. In a market with so many vendors jumping on the mobile device management bandwagon, Fiberlink’s history of managing enterprise mobile computing devices for over a decade translates to best practices that accelerate deployment, eliminate risk and simplify enterprise device management for IT.

OS SUPPORT: iOS, Android, Blackberry, Symbian, Windows Mobile, Windows Phone 7, Windows Desktops, MAC Desktops

MDM FEATURES:

Mobile Device Management:

Every organization needs to see and control the mobile devices entering their enterprise, whether they are provided by the company or part of a Bring Your Own Device (BYOD) program. MaaS360 mobile device management (MDM) is the fastest and most comprehensive way to get devices configured for enterprise access and to secure corporate data on smartphones and tablets.

Mobile App Management:

MaaS360 simplifies mobile application management by delivering an easy to use enterprise app catalog with full operational and security lifecycle management of apps across mobile device platforms.

- Enterprise App Catalogs for iOS and Android Devices
- Web-based Management Console
- Mobile App Lifecycle Management
- Mobile App Security & Compliance Management
- Mobile Cloud API & Software Development Kit
- Mobile App Distribution Cloud

Document Management:

MaaS360 empowers your users by giving them access to business documents on mobile devices while providing total visibility and control.

Mobile Expense Management:

MaaS360 for mobile expense management enables organizations to set corporate-wide expense policies, and to proactively monitor and track mobile data and application usage.

A link to an overview of Fiberlink’s MaaS360 MDM solution can be followed here.
FROM THE COMPANY:

Founded in 2009, Fixmo Inc. is the mobile risk management (MRM) company that helps organizations identify, mitigate and manage the risks associated with mobile devices in the workplace. The company’s MRM solutions enable protected and compliant mobile computing, helping organizations embrace a wide range of mobile devices and applications while maintaining system integrity, protecting confidential data and proving regulatory compliance.

Fixmo’s MRM technology has been developed as part of a Cooperative Research and Development Agreement (CRADA) with the U.S. National Security Agency (NSA).

“Fixmo’s MRM solutions enable organizations to support a wide range of mobile devices and embrace the “bring your own device” (BYOD) trend by taking a holistic approach to MDM, corporate data security, mobile application management (MAM), malware prevention, IT compliance reporting and more.”

OS SUPPORT: iOS, Android, Blackberry

MDM FEATURES:

Mobile Risk Management:

Fixmo’s mobile security and risk management solutions enable enterprises to support corporate-liable and personal-liable devices while addressing their requirements for device management, corporate security, private data protection, corporate compliance and audit ability.

Mobile Device Management:

Fixmo MDM helps you manage your growing fleet of corporate-owned and personal-liable mobile devices across the workplace through Configuring and Securing Your Devices, Managing Users and Device Lifecycle including Mobile Application Management Services.

BYOD:

Fixmo helps you overcome limitations through a secure encrypted workspace on personal-liable devices that are controlled and managed by IT. Fixmo SafeZone is a virtual container for corporate data and apps that gives IT back the control they need to keep their corporate data protected and controlled. With Fixmo SafeZone all corporate data – including email, documents and custom apps – stays encrypted and contained in a secure workspace on personal devices while Fixmo Sentinel manages device-level and container-level security policies from a single federated management console.

A link to an overview of the Fixmo MDM solution can be followed here.
Established in 1996 and headquartered in Sunnyvale, California, Good Technology's services are used by major organizations, including 50 of the Fortune 100 as well as enterprise customers in 90+ countries operating on over 200 carriers.

Mobile security is about more than just passwords and policies. It’s about making sure all of your sensitive corporate and employee data will remain safe in transit and at rest – on whichever devices your employees choose to use.

That’s why Good’s secure device management solutions offer true data loss prevention by encrypting your information at the device and app level. No matter what your enterprise security goals may be, our mobile device management and secure application development software can help.

OS SUPPORT: iOS, Android, Symbian, Windows Mobile, Windows Phone 7, Windows Desktops

MDM FEATURES:

Your Own Device (BYOD) programs:
Dramatically reduce your organization's telecom expenses by securing employee-owned mobile devices and allowing them to be used for work purposes.

Data Loss Prevention:
Prevent the loss of sensitive corporate and employee data by encrypting data over the air, on devices, and within apps.

Mobile Data Management:
Protects critical corporate data and apps on your employees’ iOS, Android, and Windows Phone devices.

Secure Collaboration:
Boost employee productivity by offering secure access to collaboration tools such as email, calendar, PIM, browser, and file management.

Secure Document Management:
Deliver the application-level encryption and data protection your employees need to share documents safely.

Secure Business Intelligence:
Rapidly build, deploy, and manage secure mobile apps that enable remote business intelligence.

Secure Social Business:
Offer secure iOS device management and data loss prevention capabilities through social mobile applications.

A link to an overview of the Good Technology MDM solution can be followed here.
FROM THE COMPANY: IBM, headquartered in Armonk, New York, is the largest technology and consulting employer in the world, with approximately 427,000 employees serving clients in 170 countries.

The IBM mobile device management solution is delivered through the IBM Tivoli Software service management brand of the IBM Software Group. IBM mobile device management solutions and services enable companies to confidently gain visibility and manageability over employees’ mobile devices.

IBM® Endpoint Manager for Mobile Devices provides a completely integrated approach for managing, securing, and reporting on laptops, desktops, servers, smartphones, tablets, and even specialty devices such as point-of-sale terminals. This provides customers with unprecedented real-time visibility and control over all devices employees use in their job functions; reducing costs, increasing productivity, and improving compliance.

Endpoint Manager for Mobile Devices helps you address the issues of security, complexity and bring own device (BYOD) policies that challenge support for an increasingly mobile workforce.

OS SUPPORT: iOS, Android, Blackberry, Symbian, Windows Mobile, Windows Phone 7, Windows Desktops, Desktops, Linux Desktops

MDM FEATURES:

End Point Management for Mobile Devices:

IBM Tivoli® Endpoint Manager—built on BigFix® technology—helps you achieve smarter, faster endpoint management. It combines endpoint and security management into a single solution that enables your team to see and manage physical and virtual endpoints—servers, desktops, roaming laptops, and specialized equipment such as point-of-sale devices, ATMs and self-service kiosks.

Mobile Enterprise Services:

Reduce management costs and complexity, and achieve rapid ROI with services that help you plan, enable, support and scale anytime, anywhere access to enterprise content from converged mobile devices.

Telecom Expense Management Services:

Telecom expense management (TEM) services can help you quickly gain visibility into your communications spend patterns and identify areas for short term and long term savings.

A link to an overview of the IBM MDM solution can be followed here.
Founded in 2000, Kaseya is a global provider of IT Systems Management software. Kaseya solutions empower individual consumers, SMBs, large corporations and IT service providers — to proactively manage and control IT assets remotely from one integrated Web-based platform. Kaseya solutions are trusted by IT service providers and a wide variety of industries including: banking, consumer packaged goods, education, financial services, government, healthcare, military, real estate, retail and transportation. The company is privately held with over 30 offices in more than 20 countries.

Kaseya extends robust IT policies to mobile devices by treating them as computers rather than souped-up cellular phones. These systems are getting more powerful every production cycle, and in many organizations they are starting to replace desktops and laptops at all levels of the company. It is important that this next generation of computing devices is maintained, updated, secured and protected at the same level as last generation devices.

OS SUPPORT: iOS, Android

MDM FEATURES:

Consolidated Dashboard:

Kaseya Mobile Device Management allows IT organizations to manage mobile devices from the same Kaseya IT Automation Framework as desktops, laptops and servers. The central Kaseya dashboard gives IT organizations the visibility they need to efficiently, consistently and reliably track, update and back up mobile devices.

Mobile Device Management:

Kaseya’s MDM solution allows you to:

- Automate email configuration and settings to one or many devices
- Collect detailed inventory information in a central repository that can be easily accessed by administrators and technicians for fast resolution while providing a complete network view
- Track location of mobile devices based on location history or in real time
- Force Alarm sound on device to help track lost device
- Lock, wipe and reset lost or stolen devices

Visibility for Seamless Problem Resolution:

Because of the unique architecture of cellular networks and proprietary hardware platforms, administrators can push out the Kaseya agent to mobile management device application through text messages or a Web link. Once installed, the administrator has complete hardware and software visibility into the device, including serial number, operating system, firmware status, installed applications and other inventory data.

A link to an overview of the Kaseya MDM solution can be followed here.
FROM THE COMPANY:

Founded in 1985, LANDesk Software is a provider of systems lifecycle management, endpoint security, and IT service management solutions for desktops, servers and mobile devices across the enterprise. LANDesk is headquartered in Salt Lake City, Utah, with offices located in the Americas, Europe and Asia Pacific.

In June 2012, LANDesk announced it had acquired Wavelink, a leading provider of mission critical mobility management solutions. “The acquisition of Wavelink will further strengthen LANDesk management solutions and enable the company to provide true end-to-end mobile management. LANDesk will maintain the Wavelink brand and product lines. “

OS SUPPORT: iOS, Android, Windows Desktops, MAC Desktops, Linux Desktops

MDM FEATURES: System Lifecycle Management:

LANDesk Management Suite provides all the client management tools you need to manage and control PCs, Macs, laptops, servers, software assets, mobile devices and more—regardless of location—from a single, intuitive console.

Endpoint Security Management:

LANDesk® Security Suite software offers a multi-layered approach to security that makes it easy to safeguard data and preserve productivity by securing enterprise devices. We secure IT resources from core and network servers to desktops, laptops and portable storage media—preventing data leakage, viruses, malware, spyware and other malicious attacks.

Mobility Manager:

Its core functionality of discovery, inventory, and wiping devices provides perfect balance between those responsible for making IT policy and security, and those who need to stay productive outside your firewall in the cloud.

- Discover the devices within the environment and prevent unmanaged devices from connecting to the network.
- Know which users are consuming corporate data and what devices they’re using
- Extend corporate management and security to out-of-policy devices
- Wipe data using a single user-based policy from devices that are lost or stolen or when someone leaves your organization
- Improve business processes for reclaiming corporate IT assets and proprietary information—as in the case of employee termination
- When used with LANDesk Management Suite organizations can manage mobility devices from the same console you your other hardware and software assets, security, and lifecycle management.

A link to an overview of the LANDesk MDM solution can be followed here.

M.A.D. Partners’ mission is to create innovative, high quality and easy to use security solutions for smartphones, pads and tablets.

“The Mobile Enterprise Compliance and Security (MECS) Server is unique in its ability to truly lock down iPhones, iPads as well as smartphone and tablet devices, to the extent required by the security-aware and compliance regulated organization – while not changing the user experience or causing any noticeable latency whatsoever.

The MECS Server extends existing enterprise and network security policies across mobile platforms with complete encryption, geolocation and granular firewall controls and a suite of anti-virus, malware, content filtering and device management tools.

OS SUPPORT: iOS, Android, Symbian, Windows Mobile

MDM FEATURES: Mobile Active Defense locks down, secures and puts your iPhones, iPads, Androids, other smartphones and tablets into regulatory compliance. By employing the most stringent security standards and enforcement mechanisms, the (MECS) Server enforces policy across your entire mobile enterprise. MECS gives you device management, security controls, remediation, compliance and centralized administration over your mobile workforce.

M.A.D. Enterprise Solution:
- iPhone & iPad Security and Mobile Compliance
- Smartphone Content Filtering and Policy Enforcement
- Zero Footprint on the Smartphone
- Email Security
- Smartphone Firewall

M.A.D. Carrier Solution:
- Reclaim “Last Mile” Bandwidth
- Anti-virus, detects and eliminates malware
- Transparent to subscribers

M.A.D. Consumer Solution:
- Protects users from ID Theft attacks
- Anti-virus, detects and eliminates malware
- Protect all of your email accounts

A link to an overview of the Mobile Active Defense MDM solution can be followed here.
From the Company:

Founded in 1987, McAfee is a wholly owned subsidiary of Intel Corporation and is the world’s largest dedicated security technology company.

In 2010, McAfee announced an agreement to acquire Trust Digital, a privately-held online security company that specialized in security for mobile devices. The acquisition allowed McAfee to extend its services beyond traditional endpoint security and move into the mobile security market.

“McAfee provides a complete mobile security solution that embraces mobile device diversity. McAfee Enterprise Mobility Management (McAfee EMM) brings the same level of security and control to mobile devices that IT applies to laptops and desktops, including the ability to identify, tag, and assign policies to both employee- and business-owned smartphones and tablets.”

Os Support:

iOS, Android, Blackberry, Symbian, Windows Mobile, Windows Phone 7, Windows Desktops, MAC Desktops, Linux Desktops

MdM Features:

McAfee EMM combines secure mobile application access, anti-malware, strong authentication, high availability, a scalable architecture, and compliance reporting in a seamless system. Integration with McAfee ePolicy Orchestrator (McAfee ePO) enables IT to implement persistent policies and ease compliance management — while protecting devices and the corporate network from malware. McAfee EMM also helps drive down mobile device management and support costs and overall TCO by leveraging your enterprise’s existing data center infrastructure and IT network, including directory services, Wi-Fi, VPN, and PKI.

Mobile Security:

Properly configures mobile devices to match corporate security policies and enforces compliance prior to network access. Provides malware protection for Android with McAfee VirusScan Mobile for Enterprise. Secures corporate email, calendar and contacts from personal data with McAfee Secure Container. Both are available with McAfee EMM to be distributed as a recommended app.

Easy Deployment and Configuration:

Eases mobility management by automating the configuration and connectivity of VPN, Wi-Fi, PKI, and native email sync. Personalization features equip the device with a user’s unique credentials to allow access to user-specific application services and enforcement of role-based policies. Bulk group provisioning helps administrators to quickly enable large groups of corporate users.

Scalable Mobile Security Architecture:

Seamlessly manages a few or thousands of mobile devices over a geographically dispersed data network, while efficiently assisting users when problems arise.

A link to an overview of the McAfee MDM solution can be followed here.
FROM THE COMPANY:


Mformation offers a complete solution that enables mobile operators, managed service providers (MSPs) and enterprises to remotely manage, support and secure all types of mobile devices across all network types.

“Mformation Service Manager™ and Mformation Enterprise Manager™ suites are the most complete, flexible and integrated mobile device management software solutions in the industry, supporting end-to-end management across the broadest possible range of endpoints, from mobile devices to connected computing devices and machines. More than 500 million devices are under the management of Mformation’s device management solutions.”

OS SUPPORT:

iOS, Android, Blackberry, Symbian, Windows Mobile, Windows Phone 7

MDM FEATURES:

MFORMATION Service Manager:

Mformation Service Manager is a carrier-grade platform that supports more than 25,000 different types of mobile devices, computing devices and connected machines. The solution scales up to support the largest global operators, can be deployed into multiple network environments, and complies with key industry standards.

MFORMATION Enterprise Manager:

Mformation Enterprise Manager™ enables the enterprise to centrally manage a myriad of connected devices and applications in a uniform manner. IT staff can remotely manage and secure the company’s mobile data across all of the different device platforms in use by employees today.

Cloud-Based Enterprise MDM:

MEM: CloudPlus provides an Mformation-hosted, turnkey, cloud-based MDM solution that enables MSPs, MEAPs and ISVs to access the core MDM functionality required by their enterprise customers on the key devices used within the enterprise, without having to deploy and implement a solution within their own network.

MFORMATION Enterprise Manager SDK:

The Mformation Enterprise Manager SDK is designed for MSPs, MEAPs and ISVs who want to integrate Mformation’s enterprise MDM capabilities into an existing MEAP platform or ITSM framework. The SDK provides an exhaustive library of enterprise MDM APIs, supporting documentation, sample use cases, WSDLs and SOAP integration layers.

A link to an overview of the Mformation MDM solution can be followed here.
MobileIron is a California-based Mobile IT innovator delivering software and cloud solutions to help businesses secure and manage mobile apps, data, and devices. Established in 2007 the company has thousands of customers in over 30 countries.

Available as an on-premise or a cloud solution, MobileIron was purpose-built to secure and manage mobile apps, content, and devices for global companies.

“MobileIron’s mission is to be the core enabling platform for Mobile IT. We are focused on delivering the technology, education, and best practices our customers need to stay ahead of rapidly evolving business and user requirements, to accelerate mobile adoption, and to power true business innovation.”

**OS SUPPORT:** iOS, Android, Blackberry, Symbian, Windows Mobile

**MDM FEATURES:**

**Mobile Device Security:**

MobileIron’s Mobile Device Security Solution provides enterprises with visibility into what’s on a smartphone and how it’s being used, letting both IT and users better secure data and control without compromising privacy, even on employee-owned phones.

**Bring Your Own Device (BYOD):**

BYOD holds tremendous promise across multiple dimensions. While many organizations look at it as a possible way to reduce costs, the real value of a well-designed BYOD program is increasing employee satisfaction and productivity, while speeding up the rate of technology adoption in enterprises.

**Enterprise Mobility:**

True enterprise mobility means supporting multiple devices and operating systems across an organization, while providing IT administrator’s visibility and control of corporate data. MobileIron, enterprises gain true multiplatform management of industry-leading mobile devices: iOS, BlackBerry, Windows, Android and Symbian.

**Wireless Expense Management:**

MobileIron’s wireless expense management solution offers companies access to real-time voice, data usage, including full visibility into operator performance data. Based on Mobile Activity Intelligence, MobileIron’s solution gives IT, finance, and the end-user a detailed view of phone usage cost drivers and service quality.

**Mobile App Management:**

One of the unique benefits of MobileIron is the integrated ability for managing mobile apps for business users. The built-in Enterprise App Storefront provides both the tightest security and best end experience for the distribution and delivery of mobile applications company-wide.

A link to an overview of the MobileIron MDM solution can be followed here.
FROM THE COMPANY: Founded in 2002, OpenPeak designs end-to-end managed systems and solutions that enable Enterprises, SMBs, and Education, Healthcare and service providers to provision and manage their customer’s mobile devices and applications remotely.

“OpenPeak’s Advanced Device and Application Management (ADAM) mobility management suite is comprised of three components: SANCTION, SECTOR, and OPENSHOP. Each component can be deployed individually to complement pre-existing device and network management configurations, or together as a complete end-to-end Device, Application, and Profile Management solution.

OS SUPPORT: iOS, Android, Windows Mobile, Windows Phone 7

MDM FEATURES: Advanced Device and Application Manager:

Provides comprehensive mobile device and application management as a cloud hosted service. ADAM’s capabilities include pushing and removing apps, setting policies for passwords, configuring VPNs, defining policies, and locking and wiping a device remotely.

Sanction Device Management:

Can be deployed as a stand-alone device management solution or in tandem with other products within OpenPeak’s ADAM platform to provide a complete end-to-end solution. This includes full separation of work and personal workspaces, the ability to push applications and content, revoke problem applications on specific devices, and manage configuration bundles that can be distributed to a large group of devices.

Bring Your Own Device Environment:

Designed for the bring-your-own-device environment, SECTOR is a powerful personal device application that separates “work” and “personal” profiles via a PIM container for company-approved applications on individual-liable devices.

Secure Enterprise Application Store:

OPENSHOP brings together developers, enterprises and service providers in a secure and customizable marketplace. It alleviates enterprises from having to roll out their own application store for in-house apps.

Enterprise App Suite:

Fully integrated Personal Information Manager (PIM) for iOS and Android devices consists of secure individual applications for corporate Email, Contacts, Calendar, Tasks and Notes that are easily accessible from the device’s. SPECTRUM combines all of these corporate information tools into one single, simple, and secure application that conveniently synchronizes using Exchange ActiveSync or IMAP.

A link to an overview of the OpenPeak MDM solution can be followed here.
FROM THE COMPANY: Founded in 1994, Notify Technology Corporation is an independent software vendor (ISV) who has specialized in wireless mobility solutions and services for the past 10 years. Notify’s products including NotifyLink, NotifySync and NotifyMDM support all major smartphone and tablet platforms independent of wireless carrier or network.

“NotifyMDM provides organizations of any size, real-time visibility and control over a variety of mobile devices regardless of operating system, liability, carrier, or email platform. Whether on-premise or in the cloud, NotifyMDM provides a number of features including policy creation, compliance management, device statistics, audit tracking, app management, file sharing, and report generation, all from a single administrative console.”

OS SUPPORT: iOS, Android, Blackberry, Symbian, Windows Mobile, Windows Phone 7

MDM FEATURES: Notify MDM:

NotifyMDM provides organizations of any size, real-time visibility and control over a variety of mobile devices regardless of operating system, liability, carrier, or email platform. Whether on-premise or in the cloud, NotifyMDM provides a number of features including policy creation, compliance management, device statistics, audit tracking, app management, file sharing, and report generation, all from a single administrative console.

NotifyLink On-Premises:

Notify Technology has designed the NotifyLink On-Premise mobility solution as a means to provide wireless access and management of Email, Calendar, Contacts and Tasks (PIM) suitable for any size organization. Notify’s On-Premise solution can integrate seamlessly into an organization’s existing network while offering the broadest possible wireless device support of almost any enterprise solution on the market today.

NotifyLink On-Demand:

NotifyLink On-Demand provides organizations with a simple, fast, and cost effective solution to their immediate mobility needs. Notify Technology has designed NotifyLink On-Demand as a means to provide wireless access and management of Email and PIM information for any size organization.

NotifySync:

NotifySync provides BlackBerry users secure, real-time, wireless synchronization of Email and PIM with their ActiveSync Server. NotifySync provides a single solution supporting any BlackBerry over a variety of wireless networks such as CDMA/1XRTT/EVDO, GSM/GPRS/EDGE/3G-HSDPA or any 802.11x network.

A link to an overview of the Notify MDM solution can be followed here.
FROM THE COMPANY:

Founded in 1985, Sophos is focused on delivering the best IT security and data protection for businesses. “We produced our first encryption and antivirus products back in the 1980s. And today our products protect over 100,000 businesses and 100 million users, in more than 150 countries. We understand what it takes to keep your business secure—that’s why we’re recognized by analysts and customers alike as leaders in what we do.”

Sophos Mobile Control is available as a subscription license or as part of the SophosComplete Security Suite, which combines endpoint, data, email, web, server and mobile protection in one license. Sophos plans further integration of its mobile products in future releases, for example, with the integration of Sophos Mobile Control into Sophos UTM and reporting for both Sophos Mobile Security and Sophos Mobile Encryption in Sophos Mobile Control.

OS SUPPORT: iOS, Android, Blackberry, Symbian, Windows Mobile, Windows Phone 7

MDM FEATURES:

Sophos Mobile Control:

- Lets you turn on the built-in security features of iOS (iPhone/iPad), Android, BlackBerry and Windows Mobile 6.x devices, including any OS encryption or password protection.
- Provides remote over-the-air lock. And can help to locate or wipe lost devices, all from the central web console.
- An Enterprise App Store means you can enable users with the tools they need to work smarter as well as block listing apps that might be risky.
- Ensures that only registered devices that meet your policies—like minimum required password length—can access corporate email by using Exchange Active Sync Proxy.
- We’re regularly checking so you can see if devices aren’t compliant and remove their access to company resources if you need to.
- Deploys security updates and policies over the air through the web portal, letting you maintain mobile devices anytime, anywhere—so users don’t have to visit the Help Desk.
- Monitors and controls security features on mobile devices from a centralized, web-based console.
- Lets you prove your corporate compliance with easy inventory and reporting tools.
- Tracks and reports on all registered devices, letting you drill down to their individual configuration settings, serial numbers, model numbers, hardware details and more.
- Allows users to register their own devices and agree to an acceptable use policy you define, meaning they can use their personal phone—and you can make sure it’s secured.
- Lets users choose to remotely locate, lock or wipe their devices and reset their passcode without having to contact the Help Desk.
- Set the device status, its compliance state and if the user is allowed to receive email.
- Now available for download in the Android Market and Apple App Store.

A link to an overview of the Sophos MDM solution can be followed here.
FROM THE COMPANY:

Founded in 1995, SOTI develops industry-leading technology that solves the unique challenges of Managing, Supporting, Securing and Tracking remote mobile and desktop computing devices.

“Today over 80,000 customers around the world in retail, manufacturing, healthcare, government, logistics & numerous other industries rely on SOTI software products within the mobile device management industry. Companies strive to reduce costs by enabling the central management, security & support of remote mobile field-forces.”

SOTI MobiControl is a comprehensive enterprise mobility solution for managing your entire fleet of mobile assets irrespective of the operating system, OEM device, Telecom service provider and network type. The centralized, web-based management console provides total visibility and full control of your corporate, shared and personally-owned mobile devices.

OS SUPPORT:

iOS, Android, Blackberry, Windows Mobile, Windows Desktops

MDM FEATURES:

**Multi-Platform Web Console:**

MobiControl's Web Console provides administrators an intuitive tool to perform daily mobile management functions and provides a central and convenient way

**Helpdesk Tools:**

MobiControl equips support personnel with powerful remote control and helpdesk tools to diagnose and fix problems efficiently.

**Device Provisioning:**

MobiControl's group policies make it easy to automatically deploy software and data to devices in the field in real-time over any network (WiFi, cellular, cradled, etc.).

**Location Services:**

MobiControl's Location Services provides the ability to locate, track and gather information on the movement of your GPS enabled devices, no matter where they are in the world.

**Asset Management:**

MobiControl allows support personnel to track hardware and software assets at any time. Dynamic grouping management allows devices to be automatically grouped based on organizational structures or locations.

**Alerts:**

MobiControl's Alerts proactively monitors device-side and server-side system events and triggers immediate notifications to keep administrators informed on live mobile activity.

A link to an overview of the SOTI MDM solution can be followed here.
FROM THE COMPANY:

Founded in 1994, Founded in 1984, Sybase (An SAP Company) is an industry leader in delivering enterprise and mobile software to manage, analyze and mobilize information. The company has 40,000+ enterprise customers and 91 of the Fortune 100 rely on Sybase.

“SAP Afaria's software platform delivers centralized control of all mobile devices and tablets including iPhone, iPad, Android and BlackBerry, as well as the apps that run on them. With keeping technology in mind, SAP Afaria offers Enterprises the flexibility to deploy on premise or partner hosted. Ensure your mobile data and devices are protected – with Afaria's Enterprise Mobility Management solution.”

OS SUPPORT: iOS, Android, Blackberry, Symbian, Windows Mobile, Windows Desktops, Linux Desktops

MDM FEATURES: SAP Afaria:

Data and content is backed up and can be deleted if a device is lost or stolen. Sensitive data on devices is encrypted, and security policies are centrally enforced. IT can be confident that sensitive company information is secure outside the office. Afaria provides the tools to solve complex management tasks simply and effectively. IT has full control of the devices and applications deployed with the flexibility to manage even away from the central console.

IT can add, update or remove applications, data and content without the users' involvement and can ensure mobile workers have the correct software and data in the field. Your users can be confident that the data on their devices is up-to-date and reliable. All management tasks can be done regardless of bandwidth available, thanks to Afaria's optimization capabilities. Applications managed with Afaria have continuous, consistent availability and performance. All management activity happens in the background, leaving the user undisturbed.

Afaria for iOS 4 and iOS 5:

Afaria, a Mobile Device Security and Application Management Solution, enables businesses to effectively manage the proliferation of both personally-liable and corporate-liable iPhone and iPad devices, while providing a high degree of security to meet the strictest corporate standards. With iOS5 Apple delivers critical new MDM features for the enterprise – Afaria supports most new features today and will support all MDM features in our upcoming release.

Sybase Enterprise Solutions for Android:

Android adoption in the enterprise continues to expand rapidly as employees are demanding IT departments provide access to enterprise resources like email, CRM and other mission-critical corporate data. Sybase is working to make sure that this vision becomes a reality. By addressing the critical issues enterprises must consider before they allow new mobile devices or new mobile platforms into their environment, Sybase is leading the way in enabling Android adoption.

A link to an overview of the SAP Afaria MDM solution can be followed here.
FROM THE COMPANY: Founded in 1982, Symantec is a global leader in providing security, storage and systems management solutions to customers from consumers and small businesses to the largest global organizations.

“Symantec Mobile Management Suite is a comprehensive mobile business enablement solution designed to addresses a diverse set of enterprise mobility needs. With scalable device management, innovative application management and trusted threat protection technology, Mobile Management Suite provides all the capabilities needed for enterprises to enable, secure and manage mobile devices, applications and data.”

OS SUPPORT: iOS, Android, Blackberry, Symbian, Windows Mobile, Windows Phone 7, Windows Desktops, MAC Desktops, Linux Desktops

MDM FEATURES: Symantec Mobile Management Suite includes three products in the areas of device management, application management, and threat protection.

Symantec Mobile Management (SMM) 7.2 is a scalable MDM platform that enterprises can rely on to enable, secure and manage mobile devices. SMM enables enterprise-wide mobile email and application rollouts, safeguards mobile data and devices and provides comprehensive visibility and control of the mobile environment. Built on an enterprise-proven and globally deployed platform, SMM provides the scalability and robustness for enterprises to mobilize with confidence. Supports iOS, Android and Windows Phone platforms.

Symantec App Center Enterprise Edition (formerly Nukona) is an easy-to-use mobile application and content management solution that secures all corporate data on mobile devices. In addition to enabling distribution and management of apps and content, App Center uniquely enables enterprise grade security on a per-app basis, without requiring any source code changes or SDK embedding. App Center is available in on-premise and SaaS versions.

Symantec Mobile Security offers comprehensive protection for Android and Windows based mobile devices against malicious threats while ensuring compliance with regulatory requirements. Mobile Security provides award-winning antivirus technology, advanced firewall, and SMS anti-spam features to ensure mobile assets and maintenance of compliance policies.

A link to an overview of the Symantec MDM solution can be followed here.
FROM THE COMPANY:

Founded in 2000, Tangoe is a provider of Communications Lifecycle Management (CLM) software and related services to a wide range of global enterprises. Tangoe currently supports more than 500 active clients, many of them large multinational corporations.

“Tangoe MDM’s rules-based framework provides automatic deployment of business-critical applications and control of devices based on user/device criteria. Deployment rules can include different application policies for corporate-liable and individual liable devices, secure download via WiFi (and not via cellular) connectivity, and minimums for battery life and available memory.”

OS SUPPORT: iOS, Android, Blackberry, Symbian, Windows Mobile, Windows Phone 7, Windows Desktops

MDM FEATURES: Tangoe’s MDM Enterprise App Portal provides employees with an on-demand, consumer-style app store experience for secure Over the Air (OTA) deployment from either their Android or iOS (including iOS 5) device (via SSL) or the Tangoe MDM Self Service Portal. IT administrators can control the licensing, distribution, and management of approved enterprise and third-party applications, which decreases security threats from malware. Also, devices that are identified as jailbroken or rooted can be automatically prevented from accessing the Enterprise App Portal.

Comprehensive Control for Device Deployment:

As part of Tangoe's end-to-end managed mobility services, Tangoe delivers integrated device provisioning, configuration, security, monitoring, management, and support for devices owned by your company and employees.

Secure Application Lifecycle Control:

Employees are demanding access to enterprise resources and consumer applications that raise productivity and support real-time collaboration. Securely empower them with public and custom-built IT approved apps for business, employee, and shared devices including apps for iOS, Android, BlackBerry, and Windows Mobile.

Global Enterprise Mobility Control:

Tangoe is the first to provide an integrated solution. Approved devices for purchase, respective of employee, are automatically linked to the Self Service Portal for secure provisioning in the employee’s user profile.

Telecom Expense Management:

Tangoe rTEM offers bill shock prevention, roaming control, and cost optimization for today's leading smart devices. rTEM is the only SaaS-based solution with real-time tracking and monitoring of your entire mobile fleet.

A link to an overview of the Tangoe MDM solution can be followed here.
FROM THE COMPANY: WidePoint Solutions Corporation (WSC) is a leading provider of communications lifecycle management services, technology, and solutions.

Based on SAP’s Afaria award winning software, our MDM solutions combine best in class MDM software and infrastructure support services help desk and logistics support to provide a complete wireless management lifecycle ecosystem.

We deliver every element required for Managed Mobility Services: MDM, MLM, Logistics, Help Desk, and TEM Spend Management (with optimization and contract negotiation) in a hosted, secure, scalable, high availability environment with all services available 24 x 7 x 365.

Choose from a single offering delivered SaaS to a customized, completely outsourced business process. WidePoint Solutions offers fast, accurate customer friendly implementation that gives you the flexibility to exploit the mobile revolution without being distracted from your strategy by having to build the complex infrastructure required for support and control.

OS SUPPORT: iOS, Android, Blackberry, Symbian, Windows Mobile, Windows Desktops, Linux Desktops

MDM FEATURES: WidePoint Solutions delivers visibility into consumption, Business Intelligence, policy implementation and user support through its technology and Help Desk services. Managed Mobility Service is supported by comprehensive web-based software tools supporting the delivery of high quality service, extensive reporting, and visibility to optimize and simplify mobility, security and logistics management.

WidePoint Solutions’ portal is a superior tool for Managed Mobility Services. This includes cloud based MDM, available for rapid deployment, that gives you complete control of your mobile devices; Mobile Expense and inventory management, Rate Plan Optimization; and managed procurement to secure, green disposal lifecycle management.

WidePoint Solutions Central provides enterprise branded Help Desk services supporting hundreds of device types and including cell phones, EVO devices, air cards, smart phones and tablets.

WidePoint Solutions LogistiX™ offers complete inventory management, warranty and non-warranty repairs, re-purposing, overnight replacement, lost/stolen/broken replacement programs, custom kitting, inventory optimization and program rollout.

WidePoint MDM enables all the key mobile device management elements: Application Management, Business and Personal Containerization, Configuration Management, Exchange Server Policies, Hardware and Software Inventories, Password Policy, and Security Management.

A link to an overview of the Widepoint MDM solution can be followed here.