Solutions Review

Mobility Management

Buyer's Guide

Includes a Category Overview;
The Top 10 Questions to Ask
Plus, a Capabilities Reference of
the Leading 20 Providers for
Enterprise Mobility Solutions

INTRODUCTION:

The conversation surrounding mobility has expanded immensely over the past few years to the point where IT professionals have had to adjust their understanding of the technology. In keeping with this shifting landscape, Solutions Review has also taken the time to rethink what mobility means in 2017. While "mobile device management" was once the epicenter of the mobility discussion, many vendors now include a number of other solutions in their software offer a number of other mobility solutions that go well beyond device management.

Traditionally called mobile device management, the technology has been rebranded and is also known as Enterprise Mobility Management (EMM). While this rebranding was trivial at first, it has grown to be more significant redefining what MDM is. MDM is now a part of EMM and along with other components, works to protect every aspect of mobile, not just the device itself.

In your search for an enterprise mobility provider you will come to realize that many of the leading solutions now offer multiple and bundled mobility components including:

1. Mobile Device Management (MDM)
2. Mobile Application Management (MAM)
3. Mobile Content/Email Management (MCM/MEM)
4. Mobile Collaboration
5. Policy and Configuration Management

What makes an enterprise mobility solution even more important is the value it holds for the future of your enterprise. Computers are only becoming smaller; laptops are considered mobile devices to most of the top solutions, not just smartphones. Sooner than you realize, mobile devices in the enterprise will be a necessity as the lifestyle of the workplace begins to change. Ignore this and not only will you have less efficient workers than your competitors, but employees will seek to work other places with more favorable and modern work environments.

Mobile is also one of the most dangerous gateways for Shadow IT. Employees are going to be checking sensitive corporate data on their personal devices no matter what your policy is. The only option here is to give them the means to do so safely and securely which is entirely possible with any of these solutions.

With all these changes in technology and business practices one thing remains constant: The importance and necessity for IT managers to monitor track and secure business critical information being accessed through mobile devices. A task made even more daunting by the wide variety of mobile applications and operating systems that needs to be considered.

It is that complexity coupled with the necessity to manage and secure the range of devices that has led to growing enterprise mobility solution sophistication. Today, there are numerous companies offering solutions for a host of organizational needs and for the different end-devices being utilized within.

The *Solutions Review Enterprise Mobility Management Buyers Guide* consolidates, organizes, and presents information from the top 20 MDM service providers so you can see what they offer and what they don't, what kind of enterprise they best provide for and if they are a good fit for you.

Instead of chasing each product to web page after web page of marketing lingo and vague bullet points, Solutions Review consolidates the facts and presents them to you so you can make the best decision and move forward with the right solution and not waste your time with any of the wrong ones.

Nathaniel Lewis
Editor
Solutions Review
nlewis@solutionsreview.com
(339) 927-9244

5 Questions You Should Ask Yourself Before Selecting a Mobility Management Solution

QUESTION #1 How sophisticated is our mobile environment/ strategy?

Enterprise mobility has grown so rapidly over the past several years that mobile devices are now staples in everyday business processes that go beyond simple email and communication capabilities. Employees are accessing data and information through device centric formats and displays more and more, leaving that data more vulnerable to theft or loss. You need to understand how and at what level your organization is utilizing mobile devices.

As enterprise mobility has grown, so have the solutions that allow for mobility management. More and more technology firms are offering mobile solutions that go beyond traditional MDM and address application management, content/data management and expense management, wrapping all of these capabilities up into what the industry is referring to as Enterprise Mobility Management (EMM).

Reflect on the current status of your mobile environment and even look into the future. If your mobility management needs go beyond focusing on only the hardware and application and cost concerns that exist, than the more comprehensive EMM solution should be considered. While MDM will always be a pillar in the larger mobility solution it cannot offer all the security function needed to keep up with the growing sophistication of today's enterprise mobility environments.

QUESTION #2 How will this new level of security and management impact employees?

As Bring Your Own Device (BYOD) programs grow and mobile strategies continue to mature, the line between personal and work life becomes increasingly blurry. Any level of enterprise mobility calls for security and management, and with that comes a view into what a device is doing, where it is located and what is stored on it. Understandably, employee concerns around privacy crop up possibly leading to rejection of mobility programs or non-compliance around policy.

Every one of the mobility solutions providers in this guide have dealt with employee privacy concerns across thousands of implementation. Be sure to solicit their input and develop clear and understandable policies outlining both dos and don'ts of mobile device usage. Employees will experience benefits, productivity and convenience through increased mobility however; those benefits should not be gained at the expense of your employees trust with regard to privacy.

QUESTION #3 Do I have the internal IT resources to manage and maintain an MDM solution?

There is no arguing that most IT departments are spread thin already and adding a comprehensive enterprise mobility strategy to the mix will only compound their burden. Typically, IT will be responsible for securing devices, application and the data stored on both all the while keeping up with compliance needs and regulations such as PCI, HIPAA, HITCH and Sarbanes-Oxley. EMM solutions are meant to alleviate some of the management burden mobility brings, but first evaluate your internal team and understand what they can handle. EMM can save time, effort and money in the long run but if the right solution for you internal team and capabilities is not selected it can become clunky and cost prohibitive.

If you have employees who travel frequently, for instance, you may require a feature called Geo-fencing, which blocks or allows apps and access based on where that employee is on the globe. Also consider just whose devices you need to manage. Employees? CEOs? Students? Guests? Different kinds of end users will have different needs and present a variety of security risks requiring different capabilities from a solution.

QUESTION #4 How will we ensure compliance and decrease risk?

Monitoring tools or asset tracking can help you maintain a certain level of compliance, but some of 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 you mobile policies.

QUESTION #5 What specification will our enterprise mobility policy entail and what MDM functions will we utilize?

Answering this question will provide the dos, don't s and actual functions 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.

Remember that your enterprise mobility policy should never be a "set it and forget it" task. The policy needs to be constantly monitored, tweaked and tailored to the current environment. We can almost ensure that your mobile strategy will mature over time as technology improves, as your employees become more tech savvy and the benefits of mobility are realized. The need for new and more comprehensive security and management solution will arise and your mobile policy will need to adapt and keep pace with all those changes.

And 5 Questions You Should Ask Your Mobility Management Provider

QUESTION #6 How hard will to 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. Mobility implementations can be difficult enough on a small scale never mind looking at a large multi-unit organization. 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 do you maintain or improve the user's experience?

User experience with many MDM solutions has often come up short. A poor user experience can be more than just a nuisance for the employees of your company. If employees start finding ways around the rules you have set and technology you have implemented because they are too inconvenient, you may find yourself with security breaches you hadn't anticipated in addition to the potential for decreased productivity.

QUESTION #8 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 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 #9 What aspects of mobility do I need to manage?

Enterprise Mobility Management consists of a lot of different pieces. From the actual mobile devices themselves to the physical network and everything in between, including mobile device and application management, WLAN solutions and BYOD policies, the complexity of making all these pieces work together can overwhelm. If you can reduce that complexity by only managing what actually needs management, you can help ensure success, but doing any less could guarantee failure. Additionally, you need to consider whether to approach the process with an aim to achieve best of suite, in other words, shop for the best single solution that covers everything, or best of breed, where you look for the best solution for each particular area of mobility and then try to integrate them all together.

QUESTION #10 With the rise in BYOD, does your solution offer containerization in the even 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 EMM 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 (and BYOD) strategy and policies in accordance.
- 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.

Centrify Identity Service

Centrify is a leading provider of solutions for unifying identity management across cloud, mobile and data center IT environments. Centrify software and cloud services let organizations securely leverage their existing infrastructure to centrally manage a wide range of identity-related IT activities—such as authentication, access control, privilege management, policy enforcement and compliance—across both cloud and data center based resources.

Centrify is a complete Enterprise Mobility Management offering integrated with Identity Management. Its MDM offering allows you to automatically push email, Wi-Fi and VPN settings, and ensure device compliance. Manage passcodes, remotely lock and wipe, and leverage device posture for app SSO policy.

Solution Includes: MDM, MAM, BYOD, Identity Management

OS Support: iOS Android

Environment: Available as a cloud based solution.

Key Features

- Active Directory or Cloud-Based Device Management – Centralized administration within Active Directory or the Centrify Policy Service of all device security settings, profiles, certificates and restrictions. Group Policy-based management and enforcement of security settings, device and application Device assignment to an Active Directory user associates each device to a unique user credential in Active Directory. Automated de-provisioning occurs when an Active Directory user account is disabled or deleted. Group-based enrollment ensures only members of a specific domain or user group can enroll mobile devices.
- Self-Service and Automation- Web or mobile application-based self-service enrollment enables the rapid deployment of mobile security and management across many devices. Automated certificate enrollment secures access to Exchange, VPN and Wi-Fi connections, ensuring only assigned users can access sensitive corporate information.
- Unified Platform for Mobile Device, Mac OS X and More- Support for multiple device platforms and release levels ensures secure management across all devices. Centralizes management of your devices and systems and applications. Centrify also manages 450 versions of UNIX, Linux and Mac OS X systems and applications, providing a unified access management platform that further secures corporate resources compared to single-purpose mobile point products.

  Inventory Devices and Even Detect Jail-broken- An inventory of devices across your entire enterprise, organized by group or role, lets you easily track and enforce the status of both company-owned and user-owned devices. An inventory of applications across your entire enterprise, organized by user, group, or device OS, ensures only authorized applications are installed for the approved users.

Bottom Line

Centrify Identity Service works well with midmarket companies and manages popular mobile devices along with Mac OS X, UNIX and Linux systems. Centrify for Mobile's cloud-based service lets you centrally secure and manage smart phones and tablets using your existing Active Directory infrastructure. Centrify for Mobile uses Group Policy tools together with the Centrify Cloud Service to enforce security settings over a trusted, over-the-air connection and secure access to corporate network services. Centrify specializes in identity and access management and uses that technology as a big part of their mobile solution.

Citrix XenMobile

851West Cypress Creek Rd
Fort Lauderdale, FL 33309
United States
+1 (954) 267-3000
www.citrix.com

Citrix XenMobile is a comprehensive solution to manage mobile devices, apps, and data. Users have single-click access to all of their mobile, SaaS and Windows apps from a unified corporate app store, including integrated email, browser, data sharing and support apps. IT gains control over mobile devices with full configuration, security, provisioning and support capabilities. Deployment options give IT the choice to manage XenMobile in the cloud or on-premise.

XenMobile delivers enterprise grade EMM with role-based management, configuration, security and support for corporate and employee-owned devices. Users enroll their devices, enabling IT to provision policies and apps to those devices automatically, blacklist or whitelist apps, detect and protect against jailbroken devices, troubleshoot device and app issues, and wipe or selectively wipe a device that is lost, stolen or out of compliance.

Solution Includes: MDM, MEM, MAM, BYOD, MCM, App Wrapping, Containerization

OS Support: Windows, Mac OS, iOS, Android and Windows Phone.

Environment: Available on-premise or as a cloud based solution.

Key Features

- XenMobile Device Manager – Provides role-based management, configuration and security of corporate and user-owned devices. IT can enroll and manage devices, blacklist or whitelist apps, detect devices that are jailbroken or out of compliance and block their ActiveSync email access and do a wipe of a device that is lost, stolen or out of compliance.
- Citrix WorxHome – Available for any mobile device, WorxHome is an app that allows IT to enforce mobile settings and security while also providing access to a unified app store and live support services. XenMobile communicates with Worx Home to deliver device-specific policies and Worx-enabled app policies.
- NetScaler Gateway – NetScaler Gateway is a secure application and data access solution gives IT administrators a single point to manage access control and limit actions within sessions based on both user identity and the endpoint device, providing better application security, data protection, and compliance management.
- Mobile App Management – XenMobile App Controller manages and enables access to an organization's mobile, web and SaaS apps and ShareFile data resources. App Controller also serves as the content provider/controller for an organization's iOS, Android and HTML5 native mobile applications (including homegrown or sourced from third parties).
- StoreFront – StoreFront provides a set of service interfaces for use by Receiver that enable access to XenDesktop (which controls and delivers virtualized Windows desktops and apps). StoreFront is an optional component that extends a customer's existing XenDesktop/XenApp environment.

Bottom Line

Citrix XenMobile is a good solution for midmarket businesses because it doesn't currently have a lot of larger deployments. The Worx Mobile Apps have been proven to improve the user experience and has a high customer support rating and can create a virtual private network tunnel without the user having to manually create one. Citrix excels in MCM and has one of the most comprehensive user interfaces. Because of their VDI solution, XenMobile's integrated user experience is between applications is well reviewed.

FileWave

Established in 1992, FileWave is a leader in multi-platform device management that provides an easy, yet powerful, way to secure, manage and maintain devices, content, updates and settings.

Of FileWave's many unique features, most notably is the support for all major operating systems - macOS, Windows, iOS, Chrome OS and Android - all within *one* console. This is a major plus for any organization that needs, or will need, the ability to manage a diverse and growing population of users, devices, content, applications, accounts, etc. Additionally, all products and features are all-inclusive, ensuring IT teams have all the tools needed with no addons.

filewave

7320 E 86th Street
Suite 100
Indianapolis, IN 46256
+1 (317) 863-6282
www.filewave.com

Solution Includes: MDM, EMM, MAM, MCM, BYOD

OS Support: macOS, Windows, iOS, Chrome OS and Android

Environment: Available as on-premise or a cloud based solution

Key Features

- Multi-Platform Management – Ensures all current and future devices are fully supported within one console, eliminating the need for multiple products.
- Multi-Platform Imaging – Fully automated via a drag and drop interface makes imaging Mac and Windows devices fast and reliable. Supports direct, network and layered imaging models.
- Software/Application Deployment – Powerful deployment workflows with FileWave's patented Fileset technology provides IT teams with granular control on content distribution. Combined with FileWave's patented self-healing technology, deployments are efficient, flexible and extremely dependable.
- Patch Management/3rd Party Updates – Enables IT to easily deploy OS and 3rd party updates. Options include manual or automated settings, scheduling options, stand-alone or integration with an existing SUS (software update server) and more.
- Asset & License Management – Streamline the tracking of devices and licenses with FileWave's robust Integrated Inventory and License Management features. Get detailed reports, set alert notifications, and much more.
- Self-Service Kiosk – Empower end users to download and install pre-approved apps when they need it, without having to call IT support.
- Device Discovery, Tracking and Security – Easily scan, detect, map and/or report hardware for reporting and tracking purposes. Customize scans and reports for complete flexibility.
- Enterprise and Lightweight Infrastructure – FileWave Boosters greately reduce network traffic during deployments, ensuring a highly scalable solution for growing organizations.

Bottom Line

FileWave is a great fit for enterprise, education and government organizations of all sizes, especially those in need of a complete solution to manage a mixed environment of macOS, Windows, iOS, Chrome OS and Android. With 25 years in the industry, FileWave provides a comprehensive feature set, many of which are unique in the market.

Hypori VMI

Founded in 2011, Austin based Hypori provides Virtual Mobile Infrastructure solutions (VMI) designed to protect enterprises from the risks associated with BYOD. Hypori's VMI platform gives organizations the ability to keep data secure within the company and not exposed on the end-user's mobile device.

The solution provides users access to a virtual mobile device in the cloud from IOS, Windows and Android devices, while providing greater security and compliance for organizations. Hypori presents a user-centric mobility solution designed for all enterprises and specifically regulated industries such as government, healthcare, financial services and payments.

With Hypori's Virtual Mobile Infrastructure platform, an enterprise can keep all apps and data in the enterprise, leaving no data at risk on the end-user's mobile device. The Virtual Mobile Infrastructure platform gives access to virtual mobile devices running in the secure datacenter or cloud. The solution keeps all data and apps off the mobile device solving mobile security and management challenges.

9211 Waterford Ctr. Blvd.
Austin, TX 78758
United States
+1 (800) 789-7104
www.hypori.com

Solution Includes: MDM

OS Support: iOS, Windows, and Android.

Environment: Available in-premise or as a cloud based solution.

Key Features

- **Secure and Compliant** – With Hypori the entire mobile experience is virtualized, leaving no data at rest on the physical mobile device. Risks associated with malware, reverse engineering, and theft are eliminated. Hypori enables you to meet critical compliance requirements including Common Criteria, HIPAA and PCI.
- **Managed and Controlled** – Only develop for one OS - but distribute to many. Hyporis VMI provides a single, centralized mobile OS version on persistent virtual mobile devices. Simplify the development, deployment, testing, and support of apps with one central gold image and control point. Roll out new apps and patches instantaneously.
- **Adopted and Embraced** – No more agents, spyware and employee adoption over concerns with privacy, remote wipe and remote monitoring. The mobile thin client provides access to an entire virtual mobile environment without an intrusive agent. Drive adoption and eliminate liability from big brother policies. Easily onboard contractors with mobile access.

Bottom Line

Hypori presents a highly scalable solution completely unlike traditional MDM technologies. It takes a completely new approach to the challenge of securing, managing and driving use of mobile applications. It offers an efficient way to access important mobile applications and data without sacrificing security or user experience. Finally solve for mobility for employees and contractors on COPE and BYOD devices with no compromise.

Jamf

Jamf holds a unique spot in the world of mobility as it dedicates itself entirely to Apple devices. The company works with businesses of all sizes to easily configure, manage, and protect devices using central app deployment, remote passcode enforcement, and encryption. With Jamf, IT teams can view device details, link physical inventory to their digital records, easily export device inventory data to spreadsheets, and automatically install applications from the App Store to all of their devices. Jamf offers two versions of its solutions; Jamf Pro and JAMF Now. While Jamf Now is more geared towards smaller businesses, Jamf Pro is directed towards larger organizations, automating device management while also driving productivity and creativity. This MDM solution can be deployed through the cloud or on-premises to fit your situation.

Jamf
100 Washington Ave
Suite 1100
Minneapolis, MN 55401
+1 612-605-6625
www.jamf.com

Solution Includes: MDM, BYOD, CYOD

OS Support: macOS, iOS

Environment: Cloud Based or On-Premise

Key Features

- Device Deployment – Powerful deployment workflows to provision the perfect Mac, iPad or iPhone for every scenario. With Jamf Pro and the Apple Device Enrollment Program, automatically enroll and configure new devices without requiring hands-on support from IT. Go from new-in-box to ready-to-use without time-consuming manual configuration (or go hands-on through imaging).
- Inventory – Automatically collect user, hardware, software, and security device data or customize inventory specifications with extension attributes, such as the output of a script or the status of a third-party app. Create custom reports, alerts, and manage software licenses and warranty records. Use inventory to automate ongoing management.
- App Management –Distribute apps and content from the App Store, third-party software vendors, or B2B App Stores to an individual or group. This can be done silently, pushed on demand or published to your Jamf Pro enterprise app store. Assign apps to users or devices (no Apple ID required) and re-assign licenses as needs change. With support for native app management supported, no custom SDK or containerization is required.
- Device Management – Define settings with configuration profiles and distribute them to devices utilizing Jamf Pro. Easily apply Wi-Fi, VPN, email settings and more so users can seamlessly connect to the resources they need. Use smart targeting to trigger device management tasks automatically to specific individuals or groups based on inventory criteria.
- Self Service – More than an enterprise app catalog, Self Service transforms the IT and end-user experience. Through an intuitive interface customizable by IT, users can get instant access to resources, install apps, update configurations, and troubleshoot common issues – no help desk tickets needed.

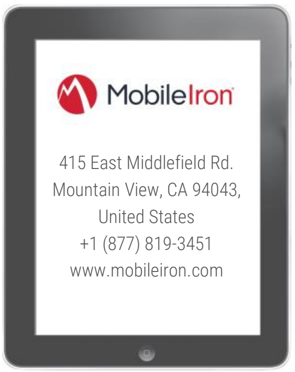
Bottom Line

Jamf is an ideal MDM solution for Apple-centric businesses whether they're hosting ten devices or hundreds. By focusing entirely on Apple, Jamf is able to ensure that end-users can receive the experience they expect from Apple. In addition, Jamf provides zero-day support and resources from Jamf Nation, the largest Apple IT management community in the world.

MobileIron EMM Platform

The MobileIron EMM Platform allows IT to secure and manage devices, apps and content providing end-users with instant access to corporate data on the mobile device of their choice. With this purpose built enterprise mobility management (EMM) platform, organizations can spend more time innovating and driving business and less time securing mobile devices.

The MobileIron EMM Platform was built to secure and manage modern operating systems in a world of mixed-use devices. It incorporates identity, context, and privacy enforcement to set the appropriate level of access to enterprise data and services. It secures and manages mobile devices, automatically provision enterprise settings such as Wi-Fi and VPN, and provide end-users with secure access to corporate email.



415 East Middlefield Rd.
Mountain View, CA 94043,
United States
+1 (877) 819-3451
www.mobileiron.com

Solution Includes: MDM, MAM, MCM, BYOD, Mobile Security, PIM, SDK, Multi OS App VPN

OS Support: Mac OS X, iOS, Android, Windows, Windows Phone and BlackBerry.

Environment: Available on-premise or a cloud based solution.

Key Features

- **Mobile Device Management (MDM) -** Enables IT to secure and manage a diverse set of mobile devices, automatically provision enterprise settings such as Wi-Fi and VPN and provide end-users with secure access to corporate email. If a device should fall out of compliance, IT can define remediation actions that will either notify the user of policy violations or selectively wipe corporate information without touching any personal data.

- **MobileIron Core -** Integrates with backend enterprise IT systems and enables IT to define security and management policies for mobile apps, content and devices. Core can be extended through APIs to integrate with the offerings of MobileIron Technology Alliance Partners.

- **MobileIron Sentry -** Manages, encrypts, and secures traffic between the mobile device and back-end enterprise systems. Sentry addresses three fundamental needs; mobile security, scalability and user experience.

- **MobileIron Content Security Service -** Addresses data loss in the cloud by providing document-level security and tight integration into an EMM platform necessary to protect enterprise content across common personal cloud services.

- **Mobile Application Management (MAM) -** Delivers, secures, and retires mobile apps. With these capabilities, IT can manage the entire application life cycle: from making the applications available to employees through the Apps@Work private enterprise app store; to securing applications on the device; containerizing corporate apps from personal apps using MobileIron AppConnect.

- **Mobile Content Management (MCM) -** IT can enable end-users to securely access and manage enterprise documents residing in a variety of content repositories, including Sharepoint, WebDav, and CIFS. MobileIron's MCM solution also ensures that corporate email attachments are encrypted and can be viewed using authorized applications.

Bottom Line

MobileIron Platform is an effective solution for any size company. They are one of the few vendors in the EMM market that has real time remote-view capacity for iOS. Their separate products for MCM and MAM are a stand out for MobileIron and are highly compatible and user friendly. Since MobileIron's only product is their EMM solutions, they're 100 percent dedicating to improving mobility which is why their individual components like Apps@Work, Docs@Work and Web@Work stand out individually while working well together.

ManageEngine Desktop Central

ManageEngine

4141 Hacienda Drive
Pleasanton, CA 94588
United States
+1 (925) 924-9500
www.manageengine.com

Desktop Central is integrated desktop and mobile device management software that helps in managing servers, laptops, desktops, smartphones, and tablets from a central location.

Automate your desktop management routines like installing patches, distributing software, managing your IT Assets, managing software licenses, monitoring software usage statistics, managing USB device usage, taking control of remote desktops, and more. It supports managing Windows, Mac and Linux operating systems.

Manage your mobile devices to deploy profiles and policies, configure devices for Wifi, VPN, Email accounts, etc., apply restrictions on using camera, browser, etc., and to secure your devices like enabling passcode, remote lock/wipe, etc.Manage all your iOS, Android and Windows smartphones and tablets.

Solution Includes: MDM, MAM, MCM, BYOD, Mobile Security, Remote Control, Asset Management, Audit and Reports.
OS Support: Android, iOS, Mac OSX, Windows, Linux

Environment: Available as a cloud based solution.

Key Features

- Device Enrollment- Over-the-Air(OTA)enrollment of devices; manually enroll mobile devices for management; bulk enrollment of mobile devices using a CSV file; authenticate enrollment with a one-time passcode and/or user's Active Directory credential.
- Profile Management- Configure policy settings to access enterprise resources; configure native e-mail client with Microsoft Exchange ActiveSync at an enterprise level. Restrict the use of camera, youtube, safari browser, etc. Provide access to corporate accounts like Email, Wi-Fi, VPN and create a logical group of devices based on department, location, or to distinguish corporate and BYOD and apply policies, restrictions and distribute Apps to all devices in the group.
- Asset Management- Get complete information about the device like device details, certificates, installed Apps, etc. and complete visibility about the devices with out-of-the-box reports.
- Application Management Manage and distribute both in-house and App Store Apps; integrate with Apple Volume Purchase Program (VPP) for hassle free distribution of commercial Apps; publish the Apps in App Catalog for users to choose and install the Apps themselves; segregate Blacklist and Whitelist of Apps
- Security Management- Enforce strict passcode to prevent unauthorized access; prevents the misuse of misplaced/lost devices; geo-location tracking to track the device; prevents data loss/theft by erasing all the device data; removes only the corporate data leaving the personal data like contacts, photos, etc. Useful for BYOD when the employee leaves the company.

Bottom Line

Manage Engine especially fitting for small businesses because the most basic version of Desktop Central is free and perfect for businesses with 25 or less employees. Other editions include Patch Edition, Professional and Enterprise each fitting for different sized businesses with different industries and needs. Desktop Central is also easy to deploy and is scalable, so upgrading is easy and all functions carry across all versions.

VMware AirWatch Enterprise Mobility Management Suite

vmware airwatch
1155 Perimeter
Center West
Atlanta, GA 30338
United States
+1 (404) 478-7500
www.air-watch.com

VMware AirWatch is an enterprise-grade mobility, productivity, identity and collaboration solution which enables end users with a seamless digital workspace for all mobility needs. AirWatch empowers IT with a future-proof mobility platform that provides flexibility to manage multiple use cases, unified management of endpoints, end-to-end security from devices to data center, and integration across enterprise systems.

An HTML5, web-based console enables organizations to enroll devices in their enterprise environment, configure and update device settings over-the-air, and secure mobile devices. The admin console gives visibility into all enrolled corporate-owned, employee owned and shared devices, regardless of platform or device type.

Solution Includes: EMM, BYOD, MAM, MEM, MBM, MCM, Mobile Security, App Wrapping, SDK, Identity Management, Container Management, Telecom Management, Multiuser Management, ACE (App Configuration for Enterprise).

OS Support: Windows, Mac, OS X, iOS, Android, Windows Phone and Symbian.

Environment: Available on-premise or as a cloud based solution.

Key Features

- True Platform Solution – Leverage a complete mobile productivity solution with Mobile Application Management, Mobile Browsing Management, Mobile Email Management, and containerized personal information management (PIM) through Boxer, the newest addition to the AirWatch product suite. Address challenges associated with mobility by providing a simplified, efficient way to view and manage all devices from the central administrator console.
- Mobile Security – Ensures your enterprise mobility deployment is secure and corporate information is protected with end-to-end security extending to users, devices, applications, content, data, email and networks. AirWatch provides real-time device details and continuous compliance monitoring to ensure your devices and corporate data are secure.
- Bring Your Own Device (BYOD) – Supports BYOD programs by enabling device choice and supporting ownership of different models without compromising mobile security and management. AirWatch provides a flexible model for asset management, policy enforcement, profile distribution, apps and content, and privacy settings for any ownership type.
- Unified Endpoint Management - Manages laptops such as Windows 10, Mac OS X, and Chrome OS devices alongside a mobile device fleet. Install and manage virtual machine applications, including VMware Fusion, on laptops using the AirWatch Catalog. These laptops are managed right alongside traditional mobile devices running iOS, Android, Windows Mobile, Blackberry, QNX and more.
- Identity Management- Extends one-touch single sign on and per-application through VMware Identity Manager (vIDM) enabled with AirWatch EMM. AirWatch integrates with vIDM to leverage your existing directory infrastructure and enforce role-based permissions, policy configurations, and device management across your entire user base.

Bottom Line

AirWatch Enterprise Mobility Management has proven its ability to handle large enterprises and is a breakaway leader in the industry. In its 2015 Magic Quadrant, Gartner cited the intuitive administrative console, with its vertical-specific administrative templates and "getting started wizards," as a contributing factor in its selection of AirWatch as a leader in Enterprise Mobility Management.

LANDESK Mobility Manager

LANDesk Mobility Manger helps IT administrators provide mobile workers access to the content and applications they need, while safeguarding corporate information. It makes mobile access easy for employees outside of the office and allows IT teams to control access to that information.

Mobility Manager is integrated with LANDESK Management Suite, so IT teams can use a single system while offering single sign-on access to users and one-click wrapping for administrators. This makes uniform delivery of policies easy and one-touch employee on-boarding a reality. You can administer policies once and propagate across all of the user's devices, which ensures consistent security for IT teams and uniform user access across devices.

LANDESK

698 West 10000 South
Suite 500
South Jordan, UT 84095
United States
+1 (801) 208-1500
www.landesk.com

Solution Includes: MDM, MAM, MEM, BYOD, App Wrapping

OS Support: Android, iOS, Mac OS X, Windows, Windows Phone and BlackBerry.

Environment: Available on-premise or a cloud based solution.

Key Features

- Secure Enterprise Mobile Applications – Offers App Wrapping to secure individual corporate applications, eliminating the need for multiple user profiles while offering single sign-on access to users and one-click wrapping for administrators. Corporate applications are secured while mobile users gain easy access to the apps that they expect—both corporate and personal.
- Scalable Mobile Management – LANDESK Fuse Mobility Manager includes capabilities that scale with your business. No longer is individual application licensing required for every mobile user in your company. Support for Apple's Volume Purchase Program makes it easy for IT teams to procure and distribute instances of iOS applications. For Android users, Samsung SAFE support ensures alignment between device and corporate security protocols, and simplified passcode and email configuration.
- Corporate App Store Experience – The LANDesk Fuse mobile application provides users a secure place to access needed corporate information. IT teams can deliver a corporate app store experience, where mobile users can launch applications and stream access to corporate data.
- Mobile Application Management – Push or pull applications to users' devices and control access to documents and other content with LANDesk Mobility Manager. You can also blacklist or whitelist applications and set rules for URL access. Wipe corporate applications selectively to maintain security in the event that a device is lost or stolen.
- BYOD and Ease of Use – LANDesk Mobility Manager helps your organization balance users' needs for productivity anywhere with IT's charter to provide secure mobility. BYOD integration allows, IT teams gain confidence that security measures are in place to safeguard corporate data consistently enterprise-wide, and mobile users benefit from a solution that respects the personal nature of their smart devices.

Bottom Line

LANDESK is a solution that fits most sized companies and does very well with larger ones. In 2012, LANDESK acquired Wavelink. These two products share the same code, but LANDESK Mobility Manager works with the LANDESK Management Suite (LDMS) which is a client management tool. Mobility Manager also offers integrated EMM and service desk. While the solution is cloud based enterprise management, LANDESK and has strong converged endpoint management

BlackBerry BES 12

BlackBerry

220 University Ave. E
Waterloo, ON N2K 0A7
Canada
+1 (519) 888-7465
us.blackberry.com

BES12 is a multiplatform EMM solution from BlackBerry that provides comprehensive device, application, and content management with integrated security and connectivity, for BlackBerry, iOS and Android. Deploy, manage and control both corporate and BYOD device users through a simple unified console.

BES12 will help you manage mobile devices for your organization to protect business information, keep mobile workers connected with the information that they need and provide administrators with efficient business tools. BES12 is the foundation to extend secure mobile productivity and collaboration within your organization beyond EMM. You can add WatchDox, WorkLife, and BBM Meetings to your organization to meet your specific needs.

Solution Includes: MDM, MAM, MDM, MCM, BYOD, VPN Authentication, APP Wrapping, Containerization, SDK

OS Support: Blackberry 10, BlackBerry OS (version 5.0 to 7.1), iOS, Android Windows Phone, Windows 10 Mobile, Windows 10

Environment: Available on-premise or as a cloud based solution.

Key Features

- Backwards Compatible – BlackBerry OS devices will be supported and the new platform provides the foundation for customers to integrate new mobile endpoints, enhanced user self-service, advanced service management, highly scalable datacenter-grade deployments, and implement active-active high availability clusters for ultimate reliability.
- Enterprise Management Agent Profile – You can use Enterprise Management Agent profiles to specify under what conditions a BlackBerry 10, iOS, Android, or Windows 10 device contacts BES12 for updates. You can assign Enterprise Management Agent profiles to users, user groups, and device groups.
- Advanced Service Management – Proactive monitoring and systems tuning delivers a complete end-to-end perspective of the BES management platform and automates problem resolution.
- Scalable Architecture – BES12 has been built from the ground up as a modern services-based architecture. It is scalable up to 25k devices per server and 150k devices per domain. Can be deployed on premise as well as through private cloud. It reduces the complexity, optimizes pooled resources, ensures maximum uptime and helps you achieve the lowest Total Cost of Ownership (TCO).
- Cross-Platform MAM, MDM and MCM – Cross-platform device, application and content management are all built into a single console. Support multiple device ownership policies at once, from BYOD to company owned personally enabled (COPE) to company owed business enabled (COBO). Comprehensive lifecycle management of apps across iOS, Android, Windows Phone and BlackBerry devices. Integrated secure connectivity provides applications with behind-the-firewall-access to your organization's resources.

Bottom Line

BlackBerry BES12 has the ability to work well for midmarket companies and larger enterprises because it is highly scalable. BES12 is also regarded to be one of the most secure solutions out there and is BlackBerry's main focus at the moment as they move away from producing devices It is a much broader expansion from BES 10 as it is now available on private cloud; public and hybrid cloud installations are currently in development.

SOTI MobiControl

SOTI

5770 Hurontario St.
Suite 1100
Mississauga, ON L5R 3G5
Canada
+1 (905) 624-9828
www.soti.net

SOTI MobiControl is an Enterprise Mobility Management (EMM) solution built on a foundation of mobile security and device management. It delivers enhanced EMM features like; application management, content management, location services and remote help. SOTI MobiControl's advanced security features enable your business to maintain full control over who is using your mobile devices and how they are using them. We ensure that all data on the device or moving between the device and your company servers remains private and secure.

SOTI unifies mobility management from a single management console, removing the complexity from managing a multi-OS, multi-vendor, and multi-purpose mobile ecosystem. SOTI provides the ability to manage mobile devices, applications, content, email, and security within an enhanced, secure, all-in-one offering.

Solution Includes: MDM, MAM, MCM, MEM Mobile Security,

OS Support: Android, iOS, Mac OS X, Windows 8 and Windows Phone.

Environment: Available on-premise or as a cloud based solution.

Key Features

- Mobile Device Management (MDM) – Manage complete mobile asset lifecycle, secure data and network integrity, integrate applications environment, optimize costs and operations management, and provide help desk support and services; standard and customized diagnostics and analytics support high-end business intelligence requirements for comprehensive mobile device asset management.
- Mobile Content Management (MCM) – Enterprise application management enables secure framework to manage mandatory, recommended and prohibited apps with on-the-fly, over-the-air, silent install and remote deployment technology.
- Mobile Application Management (MAM) – Comprehensive technical and professional services support in multiple languages; multi OS platform and device agnostic solution. Reduce complexity of onboarding, securing, monitoring, tracking and supporting a multitude of end-point devices accessing resources at anytime and from anywhere, 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.
- Remote Control & Help Desk – Lower support costs and increase device availability by remotely diagnosing and troubleshooting device issues anytime, anywhere. Our exclusive BlitFire 10X technology offers the world's fastest remote control for today's HD devices.
- AntiVirus and Malware Protection – Quarantine threats in real-time across the device file system and installed applications. Extend desktop grade antivirus and malware protection to your managed devices. MobiControl allows you to remain vigilant against evolving mobile threats.

Bottom Line

SOTI MobiControl is a good fit for larger companies or companies that need to manage a lot of devices because of they offer a lot of control. If your company is interested in or currently has a high number of Android devices, SOTI is the top vendor at securing Android devices with their SOTI MobiControl, Android for Work, with which they work closely with Google.

Sophos Mobile Control

Sophos Mobile Control (SMC) ensures each document connected to the server remains secure, allowing users to remain productive by collaborating safely. Gated entry to each file assures security anywhere and everywhere users go. Ensure compliance by maintaining control of what apps are being installed. An overview of all mobile devices in your company shows the device model, OS version and many other properties of the device.

Each file is individually encrypted making sure your data is secure. SMC also integrates with Sophos UTM, Checkpoint and Cisco, keeping the networks protected. If a device is rendered non-compliant, network access is revoked. You can also filter web access on your Android devices based on categories.

Solution Includes: MDM, MAM, MCM, MEM, BYOD

OS Support- Mac OS X, iOS, Android, Windows, Windows Phone and Blackberry.

Environment: Available on-premise or cloud based solution.

SOPHOS

3 Van de Gaaff Drive
2nd Floor
Burlington, MA 01803
United States
+1 (781) 494-5800
www.sophos.com

Key Features

- Mobile Device Management (MDM) – Manage and control iOS, Android (including Samsung SAFE), Windows 10 Windows Phone and other device types; configure device policies and deploy them over-the-air; enforce built-in security features such as passcodes and device encryption; full loss and theft protection with lock, wipe and locate; set up group-based compliance policies.
- Mobile Content Management (MCM) – Transparent encryption of each file keeps documents and data safe anywhere; leverages Sophos' Mobile Encryption app, which can be centrally managed through the SMC console; accesses content from various cloud storage providers like Dropbox, Google Drive, Microsoft OneDrive, Egnyte and various WebDAV compatible solutions.
- Mobile Application Management (MAM) – Securely distribute apps to individual users or groups; deploy iOS managed apps for added control over app data; password protect apps accessing corporate data for extra security; blacklist apps that might be risky or time-wasting; supports enterprise purchasing of apps via Apple's Volume Purchasing (VPP).
- Anti-Malware and Web Filtering for Android – Automatically scans all newly installed apps for malware; quarantines infected devices; protects users from accessing malicious websites and blocks web pages by category.
- Controlled Network Access – Constantly monitors device health and detects jailbreaks, blacklisted apps or insecure settings; integration with Sophos UTM enables admins to block Wi-Fi and VPN access based on compliance status of the device; out-of-the-box interfaces to control network access via Checkpoint and Cisco ISE.
- Mobile Email Management (MEM) – Distribute email settings, getting your users productive in minutes; control access to e-mail via a secure email gateway based on the device posture; supports email containers like Nitrodesk Touchdown; selective wipe all corporate emails, once a user leaves the company.

Bottom Line

Sophos Mobile control works best with small to midmarket businesses and is one of the few vendors to have digital rights management. It also integrates well with third party storage but does not support Samsung Knox and only supports Microsoft Certificate Services. Sophos works best with iOS and although it supports Android it has not yet adopted support of Android for Work.

Dell Enterprise Mobility Management

Software

5 Polaris Way
Aliso Viejo, CA 92656
United States
+1 (949) 754-8000
www.software.dell.com

Dell Enterprise Mobility Management (EMM) is a flexible, comprehensive mobile enablement solution that securely manages smartphones and tablets. This end-to-end mobility/BYOD solution offers security and management technology, and provides mobile device, systems, apps and content management, plus secure, remote access to corporate resources, user self-service and real-time reporting and alerts.

Simplify IT workflow with a single portal that enables you to oversee management and policy of your entire EMM footprint. Secure user identity and device connectivity, plus integrate and deploy productivity applications and services.

Solutions Includes: MDM, MAM, MCM, BYOD, SDK

OS Support: Windows, Mac OS X, iOS, Android, Windows Phone and BlackBerry.

Environment: Available on-premise or as a cloud based solution.

Key Features

- Mobile Device Management (MDM) – Simplify the management of your mobile devices with a single solution and management console for all of your endpoints, applications, and content. Dell Mobile Management also provides encryption, policy management, and secure remote access so you can rest assured that your data is protected.
- Mobile Application Management (MAM) – Get device-agnostic, remote management of corporate apps and content on corporate mobile devices. It also offers simple, secure inventory, distribution and management of apps and content across devices. It provides easy access to remote desktops, apps and content; centralized application inventory; application distribution, management and policy enforcement (public and private apps); business applications; Volume Purchase Program (VPP) support for iOS apps and devices.
- User Self-Service Portal – Enable and empower your end users with self-provisioning, management and reporting tools. A policy-driven, self-service portal allows you to define end-user rights and permissions for self-service based on individual or group membership. View current devices and register new devices; reset passwords; locate, lock, and wipe devices; view individual/group policies.
- Real-Time Reports, Alerts and Analytics – Comprehensive user-centric view shows how devices, apps and policies are combined to enable service delivery to a given user. Real-time, exceptions-based alerts allow you to focus on critical issues. Includes real-time reporting (device and application inventory, asset location, groups/users and related policies); granular events and policy compliance alerts contextually summarized events; fast searching and detailed audit trails.
- Desktop Virtualization – Desktop virtualization, or cloud-client computing, gives your IT department control over data devices and applications because data is housed in the data center instead of the mobile device. Your employees can access their applications from any device, including bring-your-own devices (BYOD), through a single network sign-on.

Bottom Line

Dell Enterprise Mobility Management is made up of endpoint management for mobile devices, Endpoint management for laptops and desktops and Dell Workspace. Dell Mobile Management, along with Dell Enterprise Mobility is great for larger companies. The Mobile Management component of Dell EMM allows IT professionals to have complete control over all devices, network access, applications and user settings.

Amtel MDM

AMTEL

900 Lafayette St. #506
Santa Clara, CA 95050
United States
+1 (408) 615-0522
www.netplustms.com

Amtel MDM from Netplus allows you to safely deploy mobile devices in the enterprise using a unified console for greater operating efficiency. Secure devices and protect access to enterprise data from corporate or BYOD devices. Deployed easily from a secure private cloud with SSAE 16 Type II compliance, Amtel by Netplus' mobile security solution is ideal for smartphone and tablet deployments in the enterprise.

Protect enterprise data with the capabilities to remotely lock and unlock lost or stolen devices and full or selective wipe of content. Set policy to restrict mobile device features such as camera or NFC at sensitive locations. By centralizing device configuration, Email server, Wi-Fi, VPN, LDAP and CalDAV settings are easily rolled out.

Solution Includes: MDM, MAM, MCM, BYOD, Mobile Security, Containerization.

OS Support: Mac OS X, iOS, Android, BlackBerry, Windows Phone and Windows.

Environment: Available as a cloud based solution.

Key Features

- Mobile Apps Management – Protect and secure enterprise apps and data with access control policies that take control over mobile apps with the ability to easily setup and manage both public and private apps. Configure whitelist policies for recommended apps and blacklist policies to restrict or block risky or time wasting apps. Easily deploy enterprise app store for distribution of in-house private apps.
- BYOD Security – Allow flexibility for users while retaining the ability to secure corporate data on personal devices. Define user profiles with access rights and restrictions, deploy over the air and manage centrally. Protect corporate data using selective wipe of container in the event of lost device or user leaving the company. User or admin alerts and reports help manage BYOD with monitoring and audit trail.
- Containerization – Containerize and protect corporate content by sharing only in secure containers. Automatically disable access and wipe container if a device is compromised, non-compliant or when user leaves the company. IT Administrators can push content updates centrally to container as well as impose corporate access control restrictions based on time of day or location of mobile device.
- Secure Enterprise Workspace – Enforce workspace restrictions on both corporate owned and BYOD mobile devices with pre-defined configuration settings for access control, content sharing and mobile app usage. With secure workspace for Android, administrators can control how users' home screens look and operate, restrict what apps can be accessed by a user and automatically hide any of the installed widgets and apps.
- Cloud-Based Mobility Management – Amtel's mobility management solution is deployed on a secure private cloud with reliable SSAE 16 Type II compliant hosting. Register and centrally configure corporate liable and BYOD devices. Authenticate users with Active Directory or secure system generated credentials. Self-enrollment is made easier by pushing a link via email, SMS, URL or QR Code

Bottom Line

Amtel MDM can be deployed from large enterprises to small businesses and nonprofits, but is most effective for midmarket enterprises. It is only available as a cloud-based solution and integrates Mobile Device Security, Mobile App Management and Mobile Content Management with Mobile Expense Management (MEM). Amtel is effective will all kinds of industries, but is mainly used for businesses with field services operations like sales, logistics and pharmaceutical companies.

Symantec Mobility: Suite

Symantec
350 Ellis St.
Mountain View CA, 94043
United States
+1 (650) 527-8000
www.symantec.com

Symantec Mobility: Suite offers a unified solution of control that enforces consistent security standards without impeding the end-user's productivity or personal privacy. By providing flexible, comprehensive tools to secure data, deliver apps and content, and protect against threats, Mobility Suite gives users what they need to be productive without compromising security or the user experience. Instead of serving as gatekeepers, enterprise IT becomes a genuine enabler of mobile business.

Mobility Suite simplifies mobility management, integrating MDM, MAM, MCM and mobile threat protection into one, single console solution. Whether your environment is standardized on corporate-owned devices, allows a choose your own device (CYOD) program, embraces BYOD, or manages a mix of these options, Mobility Suite makes it easier for enterprises to master security while maximizing productivity.

Solution Includes: MDM, MAM, MCM, BYOD, Mobile Security, App Store, App Wrapping

OS Support: Mac OS X, iOS, Android, Windows, Windows Phone and BlackBerry.

Environment: Available on-premise and as a cloud based solution.

Key Features

- Device Management – Mobility Suite includes scalable MDM capabilities, providing visibility and control over smartphones and tablets. You can easily enroll devices in your enterprise environment, configure and update device settings over-the-air, and protect mobile devices with certificate-based security. You can prevent non-compliant devices (such as jailbroken/rooted devices or devices missing required apps) from connecting to corporate assets, helping ensure compliance to internal and external security requirements.
- Application Management – Corporate apps and data are protected using a unique technology that wraps a layer of security and policy management around mobile apps, without any source code changes or SDK embedding. This technology provides granular control of corporate apps and data with dynamic per-app policies for connectivity, authentication, encryption, data access, and document/data sharing
- Symantec Sealed Program – The Symantec Sealed Program enables enterprises to confidently embrace third-party mobile apps while meeting data security requirements. The apps in the Sealed Program have been wrapped with a layer of security and management, allowing IT to define granular policies, such as encryption, authentication, and data-sharing restrictions. It delivers an ecosystem of trusted and secure third-party mobile apps, allowing you to provide a protected mobile workspace to meet your business needs.
- Threat Protection – Mobility Suite provides powerful, effective protection against malicious threats and unauthorized access to sensitive corporate information. Leveraging cutting-edge technology, research, and intelligence from Norton Mobile Insight and Symantec Security Technology and Response (STAR) experts, the suite protects Android devices from privacy and performance risks, mobile malware and fraudulent websites.

Bottom Line

Symantec Mobility: Suite does well with midmarket to larger sized companies. They are also one of the only EPP mobility vendors, which offers and extra level of security however, this may cause Symantec to be a little more expensive. Symantec has recently discontinued many of their traditional products in order to restructure their offerings. They have combined some of their products causing their Mobile Managed Suite that we covered last year to become Symantec Mobility: Suite. They also offer less inclusive device management, application management and Norton threat protection solutions individually.

Matrix42

Silverback by Matrix42 is a comprehensive, enterprise-ready mobile device and workspace management solution (Mobile Device Management). It enables simple, secure and scalable management of devices running on Apple, Google, and Microsoft operating systems all through a single interface. Strict separation of business and private (BYOD) data on company and personal devices guarantees compliance with the relevant corporate guidelines, while offering your employees complete privacy and data protection.

MATRIX42

Elbinger Straße 7
60487 Frankfurt am Main
Germany
+49 6102 816
www.matrix42.com

Matrix42's EMM solution enables you to give all your employees easy, secure access to their familiar workspaces on the mobile device of their choice (BYOD), whether company- or personally-owned. This access can be provided to hundreds of employees within hours, and without your IT staff touching a device.

Solution Includes: EMM, BYOD, MDM

OS Support: Apple iOS, MacOS, Google Android, Windows Phone, PC, Samsung

Environment: Cloud, On-Premise.

Key Features

- Mobile Device Management – Manage your mobile device environment with clientless, automated zero-provisioning, simple device registration, granular remote device wiping options respecting BYOD or corporate device ownership, and a multi-language user interface in English, French, and German.
- Mobile Application Management – Silverback's MAM feature allows for app distribution through a self-service portal or automatic push, provisioning of applications with costs using vendor specific programs, and application triggered VPN connection.
- Privacy Controls – Silverback's privacy controls protect organizations and individual users with compliance settings for users' personal applications, offer profile-based separation of business and private data and applications, and offer administrator-only access for remote wipe.
- Gmail Client Integration – Allows for a richer collaborative environment, helping you live and work better. Gmail keeps things organized and helps you get back to what matters, securely protected in the Android work profile.
- Always-On VPN – Allows users to lock corporate network activity from boot to shutdown. Enterprise admins can deploy and control VPN traffic even by defining applications. The Always-on VPN implementation has been carefully designed not to impact the battery to avoid draining
- Contact Integration with Work Profile – This feature allows for the lookup or work contacts in the phone dialer, messenger and contact apps. Incoming calls are now mapped to the work contacts to simplify the end-user to identify the caller's name.

Bottom Line

While still a relatively new player in US and UK markets, Matrix42 offers a strong mobile device management solution that can be run on Apple iOS, Google, and Microsoft operating systems. Silverback is best fit to help small and medium sized businesses with their MDM needs. The solution provides elegant design, comprehensive features, agnostic control over mobile devices, and a clean user interface.

Microsoft Enterprise Mobility Suite

Microsoft

1 Microsoft Way
Redmond, WA 98052
United States
+1 (425) 855-8080
www.microsoft.com

The Enterprise Mobility Suite is Microsoft's comprehensive cloud solution for your consumerization of IT and Bring Your Own Device (BYOD) challenges. In addition, the Enterprise Mobility Suite discount makes it cost-effective to acquire the included cloud services: Microsoft Azure Active Directory Premium for hybrid identity management, Microsoft Intune for mobile device and application management and Microsoft Azure Rights Management for information protection.

Microsoft enterprise tools and technologies can help IT maintain security across all device types, regardless of whether the devices are corporate or personal assets, and establish security measures that protect their organizations' systems, data, and networks.

Solution Includes: MDM, MAM, MCM, IAM, App Wrapping, Containerization, PIM

OS Support: Windows, Mac OS X, iOS, Android and Windows Phone.

Environment: Available on-premise or as a cloud based solution

Key Features

- Mobile Device Management – Provides a self-service company portal for users to enroll their own devices and install corporate applications. Deploy certificates, Wi-Fi, VPN and email profiles automatically once a device is enrolled, enable users to access corporate resources with the appropriate security configurations. Protect corporate data by restricting access to Exchange email and OneDrive for business documents based upon policies set by the administrator when a user tries to access resources on an unenrolled or non-compliant device.
- Mobile Application Management – Enable your workforce to securely access corporate information using the Office mobile apps. Allow administrators and device users to protect corporate information through selective wipe of managed apps and related data when a device is unenrolled, no longer compliant, lost, stolen, or retired.
- Advanced Identity Security – Monitor and protect access to your cloud applications by viewing detailed reports showing more advanced anomalies and inconsistent access patter reports. Advanced reports are machine learning-based and can help you gain new insights to improve access security and respond to potential threats.
- Self-Service Identity Management – Keep users productive with self-service password reset for both on-premise and cloud-based directories. Simplify day-to-day administration of groups and access to group-associated applications by enabling users to create groups, request access to other groups, delegate group ownership so others can approve requests and maintain their group's memberships.
- Consistent Identity – Create and manage a single identity for each user across all your directories, keeping attributes in sync and providing single sign-on for users. Provide single sign-on access to thousands of cloud-based SaaS applications and information with conditional access policies and multi-factor authentication.

Bottom Line

Microsoft Enterprise Mobility Suite is built to support any sized business or enterprise. The Enterprise Mobility Suite is a combination of Windows Intune, Microsoft Azure Rights Management and Microsoft Azure Active Directory Premium. All of these components are needed to get the full benefits of Microsoft Enterprise Mobility Suite, but they work together well and provide a solid solution. Windows 10 adds a lot of benefits and components to Microsoft EMM and almost every other EMM solution out there.

CA Technologies Mobile Device Management

technologies

520 Madison Ave.
22nd Floor
New York, NY 10022
United States
+1 (800) 225-5224
www.ca.com

CA Mobile Device Management (CA MDM) is a scalable, mobile device management solution designed to help you control and secure mobile and desktop devices as well as deploy applications. Designed to be a sustainable approach to unlocking the value of mobility, CA MDM can give IT complete deployment flexibility and provide users with productivity-enhancing Bring Your Own Device (BYOD) freedom.

This mobile device security solution is equipped with, enterprise-level application management and data security features to help you maintain a seamless mobile experience for end users—without sacrificing safety.

Solution Includes: MDM, MAM, MCM, MEM, BYOD, Mobile Security, Containerization

OS Support: iOS, Android, Samsung, BlackBerry, Windows and Windows Phone.

Environment: Available on-premise or as a cloud based solution.

Key Features

- Smart Containerization – CA MDM is powered by Smart Containerization technology to dynamically control mobile device, application and email provisioning policies at a granular level.
- Mobile Applications Management (MAM) – Complex file and software distribution for desktop management, remote management and diagnostics for Android devices, Linux/Windows client and server platform. Helps convert unmanaged mobile applications into managed applications by embedding security, supportability and control within applications.
- Scalability – CA MDM supports a wide variety of device types and environments. It preserves a familiar look and feel for both mobile and traditional Windows-based endpoints to help users get acquainted more quickly.
- Security – CA MDM uses a relay server in a demilitarized zone (DMZ). It also provides comprehensive add-on email security options that can secure both internal and external email communications within your enterprise. In the case of loss or theft, users can remotely locate, lock and wipe a lost device, reset the passcode, remove enterprise controls and unregister a device.
- BYOD – Securely manage enterprise and personal apps, content and emails separately. Gain complete BYOD freedom with an end-user option that allows the removal of CA MDM control. BYOD solutions allow enterprise productivity apps to reside on users' personal devices.
- Self-Service Portal – streamlines enrollment and provisioning of a device. It allows users to remotely locate, lock and wipe a lost device; reset the passcode; remove enterprise controls; and unregister a device. With BYOD programs, users demand the flexibility of using their device for both work and personal use with the assurance that their enterprise information is secure and their personal content is untouched by the enterprise.
- Mobile Email Management – Lets users securely access their corporate email and ensure group and policy-based controls to protect sensitive email content.

Bottom Line

CA Technologies MDM is good for enterprises and businesses of any size. CA MDM also has their own app store where you can publish corporate apps for employees to download. Content Management includes encryption to, from and on the device and there are more developments still to come; CA MDM has only been around since 2013. CA Technologies licensed SAP Afaria mobile management technology to develop CA MDM.

IBM MaaS360

1787 Sentry Parkway West
Blue Bell, PA 19422
United States
+1 (855) 611-7360
www.ibm.com

IBM MaaS360 Enterprise Mobility Management (EMM) combines device, app and content management with strong security to simplify how you go mobile. You can monitor for threats and automate compliance to maximize security without compromising the user experience. It delivers the ability to diagnose and resolve device, user or application issues in real-time from a web-based portal; offering complete IT visibility and control, and ensuring optimum mobile user productivity.

MaaS360 provides a unified mobile device management console for smartphones and tablets with centralized policy and control across multiple platforms. Dashboards deliver an interactive, graphical summary of your mobile device management operations and compliance allowing IT to report in real-time across the entire enterprise.

Environment: MDM, MAM, MCM, Mobile Security

OS Support: Android, iOS, Samsung, Amazon Fire OS, BlackBerry, Windows Phone and Symbian.

Environment: Available on-premise or as a cloud based solution.

Key Features

- Mobile Application Management (MAM) – MaaS360 simplifies mobile application management by delivering an easy-to-use enterprise app catalog with full security and operational lifecycle management of apps across mobile device platforms. Protect enterprise apps with full containerization.
- Application Security – Enables an application container for your enterprise and third-party applications with full operational and security management for iOS and Android. Enforce authentication, provide access control across MaaS360 contained applications, and configure data leak prevention (DLP) controls.
- Mobile Threat Management – Delivers a system to protect against mobile malware on iOS and Android devices. You can gain visibility of these mobile risks and remediate the threats before they compromise your enterprise data. Detect apps with malware signatures from a continually updated database, and proactively manage mobile threats in real-time.
- Mobile Enterprise Gateway – Enables collaboration while securing your content with authorization, encryption and containerization policies. It's easy to set up, configure and maintain without additional hardware in your IT environment. Protect sensitive corporate data with security policies, including authorization, encryption and data leak prevention (DLP) controls and provide access without requiring changes to your network or firewall security configuration.
- Mobile Expense Management – Enables organizations to set corporate-wide expense policies, and to proactively monitor and track mobile data and application usage. Enterprises can now optimize their mobile spend and shift the accountability more to the business and individual employees.

Bottom Line

MaaS360 can do very well for large enterprises. Since they're owned by IBM, MaaS360 is constantly being developed up to IBM standards and is compatible with other IBM products. Users have said that the interface is pleasant and easy to use for both administrators and end-users. It's recent move to offer on-premise as well as a cloud-based solution, make it appealing to a wider user base.

Wavelink Avalanche

wavelink

698 West 10000 South
South Jordan, UT 84095
United States
+1 (801) 316-9000
www.wavelink.com

Wavelink Avalanche ensures workers leverage the most from mobility, and also eases mobile deployment management for the administrator, delivering the most efficient means to update mobile applications on workers' devices. What's more, Wavelink Avalanche provides IT the flexibility to manage deployments across device types—from rugged mobile computers to consumer smart devices and tablets.

Wavelink delivers broad consumer smart device and tablet support to customers in addition to management of rugged mobile computers traditionally used by mission-critical workers. Wavelink considers all the aspects of an enterprise mobility deployment, to manage that deployment and encompass the enterprise mobility management utility that can handle not just the mobile device but all the aspects that maximize worker productivity—mobile applications and content access.

Solution Includes: MDM, MAM, MCM, Mobile Security, App Wrapping

OS Support: Mac OS X, iOS, Android, Windows and Windows Phone.

Environment: Available on-premise or as a cloud based solution.

Key Features

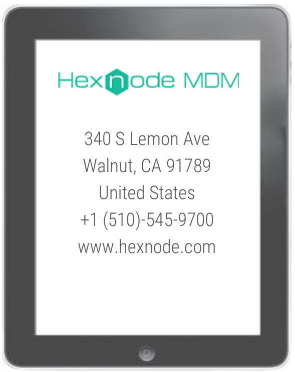
- Software & Configuration Management – Provides management support regardless of the network type, be it Wi-Fi or WWAN, including cellular networks such as GPRS, and can manage hybrid devices that transition between these different networks. Avalanche provides a variety of features and automates configuration and software package deployment, firmware distribution and other tasks to manage a large, distributed wireless LAN.
- Security – Avalanche supports a full range of wireless encryption and authentication protocols, including WEP (Key Rotation), WPA with TKIP, WPA2 with AES-CCMP, and 802.1X based EAP types such as LEAP, PEAPv0, PEAPv1, EAP-TTLS and EAP-TLS.
- Flexible Architecture – Avalanche minimizes LAN, WAN, Wireless WAN overhead and optimizes network resources. Services may be centralized, or located at the managed remote locations to suit the network topology. Client devices adjust automatically to the available bandwidth. Specific user profiles can be created which lets users across the enterprise see only what they need to see. Administrators can establish certain rights and privileges to certain users or groups, and define what level of access and usage they can perform in the console.
- Alerts & Reports – Be alerted to critical events by setting alert profiles to notify you about network resource failures, security threats or other important events. Notifications can be routed via e-mail or pager and forwarded to other enterprise network management systems such as Tivoli, HP OpenView or CA Unicenter.
- Location Based Services – Avalanche provides an accurate view of both where and how assets are being used. This feature provides detailed information regarding the location of mobile devices under management using GPS and bolsters wireless WAN management capabilities. Avalanche allows administrators to physically locate where the device was and when it was last operational.

Bottom Line

Wavelink Avalanche has a good track record with larger enterprises or companies that need to control and monitor a lot of devices. All device management is done from one web-based console that is easy to use. Phone and email-based technical support is sufficient and part of the package, any more technical support needs to be purchased separately.

Hexnode MDM

Hexnode provides a mobility management solution that simplifies mobility across each aspect of your business, ensuring that business processes, data, systems, and employees are always connected. The Hexnode MDM solution is equipped with all standard MDM features including management and provisioning tools, remote set up and configuration, application control and distribution, compliance checks, and remote lock and wipe. The solution is built on a scalable infrastructure that is able to handle increased demand while the amount of mobile devices at a company grows. The solution can be deployed with on-prem or in the cloud.



Hexnode MDM

340 S Lemon Ave
Walnut, CA 91789
United States
+1 (510)-545-9700
www.hexnode.com

Solution Includes: MAM, MCM, BYOD, Patch Management, Power Management, Asset Management

OS Support: iOS, Windows, Android

Environment: Available on-premise or as a cloud based solution.

Key Features

- Application Management – Black/white listing helps you regulate the apps coming into your enterprise. When you add apps to blacklist, Hexnode MDM identifies the devices having any blacklisted app installed as non-compliant. On whitelisting, only the whitelisted apps are acceptable. Devices with non-whitelisted apps are tagged as non-compliant.
- User-Centered Management – When it comes to managing your employee devices, the device-centric approach is not quite effective. You need to have the user above the device and not the other way around. With a strong user-centric architecture, Hexnode MDM lets you set policies for your employees and have them instantly applied to any device they use. You can easily create multi-level user polices according to your organization structure. No more wrestling with absurd device policies.
- Remote View and Control – Remotely view and manage the entire list of devices in your network. MDM dashboard renders graphical illustrations to monitor device activity data in real-time. You can view the activity summary or get detailed information on individual devices. Activity feed lets you keep track of recent stats regarding device deployment, policy creations, and enrollment.
- Configuration and Policy Management – Hexnode MDM provides an extensive set of policy controls for effective device management. From passcode policies and group policies to configurations and restrictions: you get ample control over the devices in your network. Passcode policies: Secure your content and network by enforcing strong passcode policies on the devices.
- Mobile App Distribution – Hexnode MDM allows you to centrally deploy both public apps and in house apps. You can send links or webclips of public apps to a specific user or user groups. Hexnode MDM offers creation of custom app catalogs for easily deploying and managing apps. The app catalog lets you distribute both enterprise apps and public apps. You have total control over the apps you initiated install.

Bottom Line

Hexnode provides an affordable mobility solution that is able to support a number of mobile devices all from one screen with a highly intuitive user interface. The software is capable of handling whole enterprise mobility management assisting users with the ability to centrally manage all devices, disable and restrict features, and create policies with desired configurations and assign them to specific groups.

Enterprise Mobility Glossary of Terms

- App Wrapping – Applying a management layer to a mobile app that does not change the underlying application.
- Bring-Your-Own-Device (BYOD) – An implemented policy that allows employees to use their own device to access corporate data. This device is secured by the solution and keeps corporate data away from personal data.
- Container Management – A designated and encrypted area of a device that separates sensitive corporate information from the owner's personal data and apps. The container protects the corporate data from malware that may infect the device if an employee were to download a corrupted personal app.
- Containerization – An alternative to full machine virtualization that involves surrounds an application in a container with its own operating environment.
- Desktop-as-a-Service (DaaS) – A cloud service in which the back-end of a virtual desktop infrastructure (VDI) is hosted by a cloud service provider.
- Enterprise Mobility Management (EMM) – The umbrella term for managing and securing mobile devices and all of their components including networks, apps connections.
- Identity Management – The managing and administration of identifying individuals and authenticating their identity across an enterprise and establishing boundaries based on clearance level.
- Mobile Applications Management (MAM) – The security, governance and management of apps within an EMM solution. Can also be a standalone service.
- Mobile Browsing Management (MBM) – Enables secure browsing and provides the ability to customize settings to meet business and end-user needs. Administrators can also limit browser access for certain sites for the entire network.
- Mobile Content Management (MCM) – A system that can store and deliver content and services to mobile devices, such as mobile phones, smartphones.
- Mobile Device Management (MDM) – The administrative area dealing with deploying, securing, monitoring, integrating, and managing mobile devices, such as smartphones, tablets, and laptops in the workplace. Now more specifically deals with securing the physical device. While some solutions may still be called MDM, they include MDM as part of their solution.
- Mobile Email Management (MEM) – Maximizes the efficiency of email and handles high volume email by being highly customizable
- Personal Information Manager (PIM) – A type of application software that functions as a personal organizer. This tool facilities the recording, tracking, and management of certain types of personal information.
- Software Development Kit (SDK) – Software development kit that allows for the creation of an app for the specific software package, OS, computer, etc. to use. Also known as a DevKit.
- Telecom Management – A strategic goal to create or identify standard interfaces that would allow a network to be managed consistently across all network element suppliers. This may apply to wireless communications, cable TV, as well as private and public wired networks.
- Virtual Desktop Infrastructure (VDI) – Hosting a desktop operating system within a virtual machine (VM) running on a centralized server. This is a variation on the client/server computing model, sometimes referred to as server-based computing,

About Solutions Review:

Solutions Review is a collection of technology news sites that aggregates, curates and creates the best content within leading technology categories. Solutions Review mission is connect buyers of enterprise technology with the best solution sellers.

Over the past three years, Solutions Review has launched ten tech Buyer's Guide sites in categories ranging from Cybersecurity to Wireless 802.11ac as well as Mobility Management and Business Intelligence, Data Analytics, Data Integration and Cloud Platforms.

Information for this report was gathered via a meta-analysis of available online materials and reports, conversations with vendor representatives, and examinations of product demonstrations and free trials. Solutions Review does not endorse any vendor, product or service depicted in this publication and does not advise technology users to base their vendor selection entirely on this research. Solutions Review disclaims all warranties, expressed or implied, regarding this research, including any warranties of merchantability or fitness for a particular purpose.