

“Choosing a Mobile Device Management Vendor”

a quick checklist before finalizing your mdm decision



Introduction

If you find it difficult to manage your mobile devices effectively, this might be the right time to switch to a class of technology solution popularly known as Mobile Device Management. Recent trends have shown huge influx of mobile devices into enterprises especially in North America and Europe with the rest of the world following soon. IT operations professionals are feeling intense pressure to provide mobility support more than ever. However, leaving a mobile device unmanaged surely calls for unproductive time spent on mobile devices considering the fact that almost all modern devices provide capabilities to perform all activities including multimedia functions and gaming. Mobile devices have gone from being mostly about cell phone voice usage and e-mail to being primarily about the apps you can use on them.

According to *Forrester Research* report, Tablets & employee-owned devices are crippling Infrastructure & Operations (I&O) professionals' existing mobile strategies, tools and people resources. The burden to ensure integrity of corporate data & applications across a wide gamut of mobile devices, form factors and platforms is driving progressive firms to mark an overhaul of their enterprises by making an investment in mobile device management (MDM) solutions. There has been a 180-degree turn in the importance that is being placed on managing smart devices and the security around them, in addition to promoting and managing the application experience to get the desired employee productivity gains while still controlling corporate data. Hence, as a rule of thumb, every organization and enterprise should draw up a management strategy with the help of Mobile Device Management software which suits their needs.

An MDM solution helps to secure, monitor, manage and support mobile devices deployed across mobile operators, service providers and enterprise. While there are plenty of choices available for enterprise as an end-user, a careful analysis leaves them with just the right MDM solution which represents a suitable mix of present and future requirements of the organization. An MDM provides a central console to the enterprise to control and to protect the data and configuration settings for all the mobile devices in the network, resulting in optimized functionality and security of mobile communications network while minimizing cost and downtime.

Selecting the Right Partner

One wise decision can save you from multitude of problems in future. A thorough understanding of application needs, network capabilities and security concerns allows you to select your MDM software on the basis of the feature set it provides. Here are some important tips to consider about while making this important decision.

Type of Subscription

The first step for an enterprise to have a successful MDM is to choose how the product will be delivered to them. There are two common types available across most of the popular Mobile Device Management solution providers, SaaS (Software as a Service) and On-Premise licenses.

SaaS is provided on a cloud-based hosting environment where enterprise devices and its information is stored and managed on a shared server hosted by the MDM provider. This type can provide significant savings and benefits via lower infrastructure and support costs, faster implementation, easy application updates and more flexible configuration models thereby reducing deployment time. The main application resides in the vendor's cloud server at remote locations and the end-user has the independence of accessing the web interface on internet-enabled devices. SaaS configuration is best suited for organizations which are into Warehouse Management, Sales, and Field Service & Maintenance.

On-Premise Setups are best for enterprises which require ultra-high security and cannot rely on hosted, shared-environment as in the case of SaaS. Once it has acquired the respective licenses from the provider, the enterprise is completely responsible for managing the MDM application and the hardware required to manage the mobile devices. Since the software is stored on the company's own servers, security concerns are negligible.

Features

Selection of MDM solution provider can largely depend on the features being provided. Mobile Device Management has a different meaning to different roles within a business. However the decision should be prioritized on the quality rather than the quantity of features provided. The purpose of having a MDM for securing the enterprise's devices should be solved.

Some important features which can prove decisive in the hunt for the best MDM provider can be:

Platform Support - Most commonly used mobile OS are supported by almost all vendors.

The top ones being Android, Blackberry, iOS and Windows Mobile & CE.

Remote Configuration & Job Provisioning – An efficient remote support facility is one of the most important features. The ability to provide remote support to a device can prove very beneficial in terms of worker productivity while saving time and money spent on getting the device back to home site for troubleshooting.

Logging & Report Generation - Helps in keeping track of device activities and error tracking, if any.

Location Tracking – Helps management know the device location using GPS & network location facilities.

Messaging –Built-in messaging facilities provides an easier way to communicate with remote devices.

Mobile Asset Tracking & Management – Helps keep track of all the devices managed by MDM.

Remote Lock and Wipe – Helps protect your device and its data in case of device loss.

Network & Bandwidth usage – Mobile devices often operate in weak mobile network coverage areas, hence, an MDM solution which can operate efficiently using less network resources should be given priority while making a selection.

Security, Backup & Restore Services

Security of the device and the data on it is a matter of concern. The encryption and security mechanisms built into the software to keep user data secure while exchanging data over network gives a vendor an edge over others. Vendors providing backup and restore solutions for device information stored on cloud servers can make a vendor stand out from the crowd. Enterprises should demand transparency from application providers regarding security, encryption & authentication.

Reliability

MDM solution provider should be evaluated to ensure the services displayed and provided are reliable. Server uptime, backup and redundancy capabilities including availability of multiple data centers help in greater data availability thereby increasing productivity. The enterprise should ensure reliability of the service provider as well so that the software updates and support is provided consistently.

Ease of Usability

The server agent used for managing mobile devices and the client agent should be well built and easy to use and work seamlessly on all supported devices. UI built using good user aesthetics helps in easier usage without much end-user training required. The devices should ideally be managed through a central console which provides adequate information about the managed devices. Availability of detailed documentation about all important features helps end user to understand the software better. Some vendors also provide customer support services to sort any issues that arise.

Scalability

The vendor should support scaling its services according to the future needs of the enterprise. An MDM solution should not be restricted by technological issues thereby creating constraints in the growth of the enterprise.

Value for Money

An MDM vendor providing a good set of features sufficing an enterprise's needs at a lower cost can be termed as having a better value for the money. Competition among vendors has allowed the users to take advantage of more features at a lower price.

Customizations

An enterprise can have its own set of requirements. Few vendors allow making customizations to the MDM software according to the user's needs. But this could be a great differentiator.

Understanding Terms and Conditions

Scrutinizing the contracts with the application provider is very important to obtain the most benefit from the solution. The contract should provide terms about service & uptime guarantees, security terms, and backup-related strategies. It's also necessary to learn what happens in case the enterprise wants to switch to a different vendor or end the service contract. In case the user is not satisfied with any part of the SLA (Service Level Agreement), it must ask for a clarification and get the specifics in writing. The billing plan should be clear before finalizing on the service.

Conclusion

Mobile devices have changed the way many enterprises work, receive information, and remain competitive. The challenge is that the range of devices is growing as well as the growing trend of using personal devices for professional use, popularly known as BYOD (Bring Your Own Device). This poses a security and deployment issue for many enterprises as they try to manage these mobile devices. Mobile Device Management solutions provide an integrated approach to mobile security including company security policies, training; helps boost returns on investment of mobile device management and can rightly be called critical for all enterprises. A careful selection of an MDM solution will better enable IT staff to collect data, manage their deployed mobile devices, in-house apps as well as ensure overall fleet/device security.

ABOUT 42GEARS MOBILITY SYSTEMS

42Gears Mobility Systems Pvt. Ltd. is a software product development company based in Bangalore, India. With a growing portfolio of customers in 30 countries across the world, we develop and sell mobile device management products and solutions to enterprises. SureMDM has been solving the problems of managing, securing, supporting and tracking mobile devices deployed across the enterprises. SureLock provides an ultimate answer to all kiosk mode lockdown requirements for Smartphones, Tablets & Rugged Devices; and SureFox provides mobile browser lockdown features which work seamlessly to provide a highly secure environment for mobile platforms. Our products are actively used by customers around the world in retail, manufacturing, healthcare, government, logistics and other industries, helping them reduce Total Cost of Ownership (TCO) of mobile devices.



For more information regarding enterprise mobile device management & security, contact 42Gears Mobility Systems at www.42gears.com.