SOPHOS

Mobile Device Management Buyers Guide

IT departments should be perceived as the lubricant in the machine that powers an organization. BYOD is a great opportunity to make life easier for your users. But convenience is always a trade-off with security. How do you strike a balance between security and productivity? In this guide we walk you through the factors you need to consider to find a mobile device management solution that best fits your needs.

Do you dare say “yes” to your users?

Mobile device management (MDM) solutions allow IT organizations to centrally manage, monitor and support mobile devices. These devices may include smartphones and tablets from several device manufacturers and OS developers. By using an MDM solution to control and protect the data and configuration settings on users’ mobile devices, you can reduce the support costs and business risks of bring-your-own-device policies (BYOD).

The right MDM solution means you can say yes to BYOD without increasing the risk of data loss and the IT workload.

BYOD risks and rewards

Companies and end users alike are realizing the benefits of BYOD policies. When employees are allowed to work on their personally owned devices, they simply get more done. The comfort associated with a device the employee knows and prefers increases productivity both inside and outside the office.

A BYOD policy can also be good for employee recruitment. Employees want to use their personal smartphones and tablets. They don’t want to be limited to what the company provides, or have to learn or carry a second device. As a result, companies that promote a BYOD policy attract tech-savvy applicants.

But as with any technology trend, there are issues that can stand in the way of benefits. BYOD brings two key challenges: data protection and management.

Data protection: With data flowing to and from devices that can be easily lost or stolen, and across public networks, protecting data becomes a paramount concern. You don’t know what data is being accessed and by whom over what channel.

Management: IT staffs need a way to control the devices used to access corporate data regardless of who owns them. And if employees are using personal devices, that means managing multiple device platforms and operating systems. This can be a significant drain on IT resources. Managing them individually is not a viable option.

What to look for in an MDM solution provider

You know you need to control and secure mobile devices. But do you know how to choose a provider? The control and security capabilities you'll find in MDM solutions are dictated by what mobile operating systems vendors allow. In fact, buyers should be wary of MDM vendors that claim they can circumvent explicit OS limitations. This is probably not true, or it applies only to jailbroken (iOS) or rooted (Android) devices. That being the case, how do you evaluate MDM solution providers? We recommend considering the following factors.

Does the provider have a flexible deployment model?

The provider should offer a choice of deployment models, including on-premise for larger deployments. While on-premise requires an upfront CAPEX investment and OPEX, these deployments are fully integrated into the organization's IT, allowing for more granular control. On-premise deployments use an EAS proxy, Active Directory, an LDAP connection, and offer backup options.

While on-premise is the most common delivery model, it's not the only option. Some MDM providers offer their software as a service. Software as a service (SaaS) is great for organizations that need to get up and running quickly. No on-site installation or maintenance is necessary, saving you time and operating expenses. And as there are no changes to the local IT environment and no hardware investment, you won't incur capital expenses.

SaaS is typically considered an option only for large organizations, but it is well suited for smaller organizations or specific user groups as well. In fact, MDM in the cloud puts mobile device management within reach of smaller organizations and user groups that require centralized control but don't have the resources to implement and manage an on-premise deployment. Companies should look for a solution that offers the scalability they need and is not over-dimensioned leading to complexity.

Is the provider's MDM solution compatible with iPhone, iPad, Android, BlackBerry and Windows Mobile?

Not all MDM solutions support every mobile device OS and platform. So it is important to consider the devices you want to support now and in the future. If you choose the wrong solution, you could end up separately managing a set of users. Administrators will have to manually control and protect the data and configuration settings on the mobile devices that are not supported by the MDM solution. This lowers your MDM return on investment and introduces risk.

Does the provider use a lightweight MDM approach or a heavyweight container approach?

There are currently two approaches to mobile security and data protection. The lightweight MDM approach secures devices through a combination of security features available in the OS and tools provided by the MDM provider. The heavyweight approach uses a proprietary "container" app that holds all the data and provides user functionality like email, calendar and document editing.

Each approach has its own advantages and disadvantages. The heavyweight approach provides full control over the capabilities of the app, like encryption, and separation of corporate and personal data. But this control comes at a price. Employees may not be pleased with the restrictions in device usability and the impact on mobile device performance and battery life. They also need training on the user interface, which is different. While selective wipe is easy with this approach, data in other apps are not protected, and you have no control over the devices' other settings.

The lightweight approach keeps the native device experience, which means less user training and better user acceptance. While administrators can control and configure more of the phone (such as camera, app store, VPN settings, etc.), those capabilities are dictated by what the mobile OS allows. However, the lightweight approach also allows administrators to manage device inventory, compliance checks and software distribution—all key to a successful BYOD policy.

Does the provider offer 24/7 global support?

Technical support issues can crop up any time of day. Your mobile device users are working around the clock, and so should your MDM vendor's tech support. Look for a vendor that provides 24/7 local language support, with knowledgeable engineers answering the phone and short wait times (if you have to wait at all). Consider those that have been independently audited and approved by SCP (Service Capability and Performance Support Standard). SCP quantifies the effectiveness of customer service and support based upon a stringent set of performance standards representing best practices in the industry.

Does the provider offer all-around security for your mobile workforce?

An MDM solution is intended to provide centralized security and management of mobile devices, but it is just one part of an overall mobile security strategy. Mobile devices are not just limited to smartphones and tablets. You also should pay attention to other ways in which employees take data out of the office such as on laptops, USB drives or even collaboration solutions such as cloud storage.

To prevent data loss, you need to be sure that sensitive information is not stored as plain text and that no applications are installed that open up the device to vulnerabilities. You need to encrypt your data everywhere and protect devices from malware. Today's companies are wise to consider how a vendor's mobile solutions integrate with these other solutions.

Ideally, a single vendor provides an integrated suite of solutions to address all of these needs. This simplifies security administration and lowers total cost. For example, you may use the enterprise app store in your MDM solution to manage apps but also force users to install antivirus software.

MDM capabilities and features

Mobile device management solutions share common capabilities. However, you'll find differences in vendors' methodologies and ease of use. As you evaluate MDM solutions, consider the following capabilities and features.

Keeping corporate data safe

The primary objective of an MDM solution is to protect corporate data. This is achieved by enforcing compliance with corporate security policies.

Before granting data access, mobile devices must be registered with the MDM solution. When a registered device connects, the MDM solution checks the device against a set of company rules like jailbreak detection, password configuration or blacklisted apps. Devices that comply with your security policies are granted access to corporate data.

Risk mitigation techniques limit or deny access to devices that do not comply. For example, users of non-compliant devices may be blocked from all network resources or receive an email notice and/or have limited data access. Some vendors also provide a self-service portal that users can log into to check their compliance status or if the device itself complies (for an OS offering this capability, as in the case of iOS and Android).

Many mobile devices have built-in security features, like device feature restrictions (no camera) and encryption (in the case of iOS and Android 4). Some lightweight MDM solutions allow you to turn on these features to further protect data.

The ability to "remote wipe" lost devices is critical and can be found in any MDM solution. It allows the admin to delete corporate data on a device that cannot be located and could be in the possession of an unauthorized user. Similarly, look for a solution that allows you to locate and lock devices from the admin web console. This allows you to find a device and prevent its use until it is back in the owner's possession. Ideally, your vendor allows users to locate, lock and wipe their own devices via a self-service portal.

Managing applications

An MDM solution may also enable organizations to manage the applications on mobile devices. By doing so, users have the appropriate tools to work smarter with minimal risk to corporate data.

Mobile application management (MAM) is primarily achieved via an enterprise app store that allows you to define the apps that users can or should have installed on their devices. This can include publicly available apps and those developed in-house.

Ideally, an MDM solution should support iOS managed apps, which became available with iOS 5. This allows companies to push apps to their users and should provide a simple way to install and delete them, including all related data, over the air from the web console.

The app store should also allow you to build a blacklist of apps that you do not want users to have on their devices. These may be applications that pose a risk to corporate data and/or user productivity.

Simplified IT administration

IT is already overburdened with provisioning, maintenance and support responsibilities. BYOD shouldn't increase user productivity at the cost of IT's. Simplified IT administration is critical, and this is where you will see the most variation when evaluating MDM solutions.

There are several ways that MDM solutions can simplify administration. Over-the-air (OTA) administration and management allows the IT organization to maintain mobile devices anytime, anywhere, so users don't have to visit the help desk. Initial setup and configuration can also be done over the air. You should also be able to automatically assign devices to existing groups from your user directory and apply the respective policies when they are registered via a self-service portal.

Centralized monitoring and control of all registered devices is a hallmark of MDM, but the ease of use and granularity of functions differ from one solution to another. Look for an MDM solution that allows you to manage all supported smartphones and tablets from one console, regardless of the operating system, service provider, network or location of the device.

If you are also using BlackBerrys, it makes sense to bring them into your MDM solution so you have the full inventory overview in one place. You should be able to track and report on all registered devices, and drill down to individual configuration settings, serial numbers, model numbers, hardware details and installed applications. A dashboard view can quickly show registered devices and whether or not they're compliant with policies. Auditing allows you to easily track changes to devices and compliance status.

Graphical reports should provide the most important data at a glance. For example, charts should show the percentage of compliant vs. noncompliant devices, managed vs. non-managed devices, corporate-owned vs. employee-owned devices, etc., rather than require you to navigate through numerous menus to find the information.

Finally, the administrative interface should be action-oriented and easy to use. Consider how many clicks are required to perform basic functions like decommissioning a device, viewing device OS distribution, and defining the OS versions supported in the app. One or two clicks maximum should be all it takes to complete these tasks.

Empower users through a self-service portal

A user self-service portal reduces the burden on IT and empowers device owners. Users can handle routine tasks themselves, such as registering their own devices and agreeing to an acceptable use policy that you define. Once registered, the MDM solution can automatically assign profiles and policies to users or groups based on their directory group membership, e.g., Active Directory. This eliminates the need for IT to be involved in any part of the device setup and configuration process.

As previously mentioned, a self-service portal extends data protection capabilities to users. They can remotely locate, lock or wipe their devices and reset their password without having to contact the help desk. This saves the help desk time, but it also improves the organization's overall security.

Device owners are typically the first to know if their device has been lost or stolen. In the amount of time it takes for a user to realize that they've misplaced a device, decide to call the help desk and for the help desk to perform the remote wipe, sensitive data could've fallen into the wrong hands. Giving users the ability to locate, lock or wipe a device themselves saves valuable time.

Finally, a user self-service portal keeps users informed of their device status, including their compliance state and, for example, why they no longer receive email. This cuts down on users contacting the help desk when the device has fallen out of compliance and email access has been blocked.

Summary

Mobile device management should enable you to manage all the devices on your network. It should also be simple to use. Use these two guidelines to find the right solution. Demo different MDM solutions and gauge for yourself their ease of use. The chart below will help you compare features and capabilities. This will help you find the vendor that can serve your company best.

What to look for in an MDM solution provider

Consideration	Options to look for
Deployment options	☐ On-premise deployment ☐ SaaS
Platforms supported	☐ iPhone & iPad ☐ Android ☐ BlackBerry ☐ Windows Mobile
MDM approach	☐ Lightweight ☐ Heavyweight
Technical support	☐ Available 24/7 global support ☐ Technicians speak local language ☐ Quality audited
Completeness of mobile security portfolio	☐ Data encryption solution ☐ Mobile malware solution ☐ Security for laptops ☐ Protection for removable media ☐ File encryption for cloud storage ☐ DLP ☐ Integrated security approach

MDM capabilities and features

Capability	Features to look for
Data protection	□ Checks devices for compliance with corporate security policies □ Offers a variety of risk mitigation techniques for non-compliant mobile devices, such as VPN blocking, email blocking, user notification, etc. □ Self-service portal where users can determine their compliance status □ Compliance status is indicated on the mobile device itself □ Admin can turn on native platform security features □ Lost devices can be located, locked or wiped from the admin console or a user self-service portal
Managing applications	□ Enterprise app store for both commercial and in-house apps □ Application blacklisting □ Over-the-air app deployment and removal
Simplified IT administration	□ Over-the-air administration and management □ Centralized management of all devices □ Dashboard view of compliance status □ Detailed graphical reports □ Easy-to-use administrative interface
User self-service portal	□ Users register their own devices □ Users can locate, lock and wipe their devices □ Users can reset their password □ Users can view compliance status

Sophos Mobile Control

Get a free 20-day trial

Your Sophos Premier Partner:
Symtrex Inc.
264 Jane Street, Toronto, Ontario M6S 3Z2
www.symtrex.com
sales@symtrex.com
866-431-8972

United Kingdom Sales:
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales:
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia & New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Boston, USA | Oxford, UK

SOPHOS