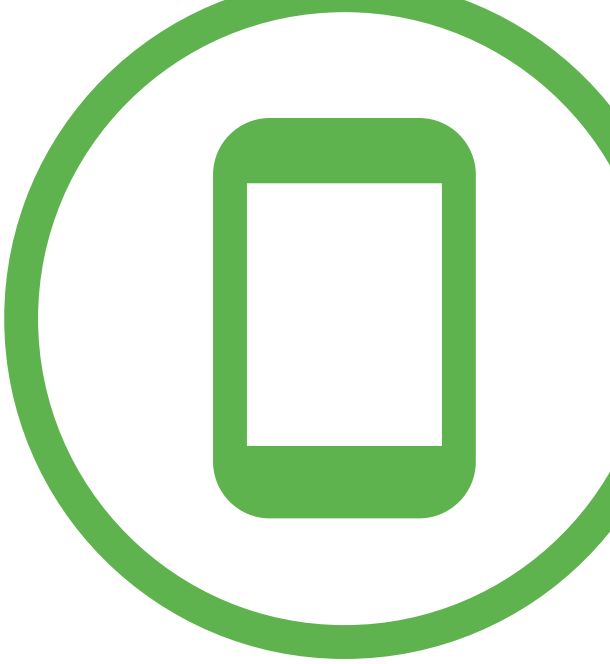
SOPHOS
Security made simple.



Mobile Device Management Buyers Guide

IT Resource Management vs. User Empowerment

Business leaders and users are embracing mobility and enjoying the flexibility and productivity—leading to rising mobile device usage. As a result, the average knowledge worker carries three devices. Corporate IT departments are saddled with the responsibility to achieve a balance between corporate data security and end user productivity, all the while managing scarce IT resources.

An essential part of BYOD is allowing users to choose their preferred devices and platforms. According to recent research, the mobile market has quickly become a three-way race with Android and iOS commanding more than 80% of market share and Windows 8 Phone gaining momentum (see chart below). Standardizing mobile platform can potentially reduce IT complexity but with this trend, it is not likely to happen in the near future. The platform diversity only exacerbates IT's resource issue. Many IT professionals are evaluation mobile device management (MDM) systems to help them managing BYOD and shield them from the complexity.

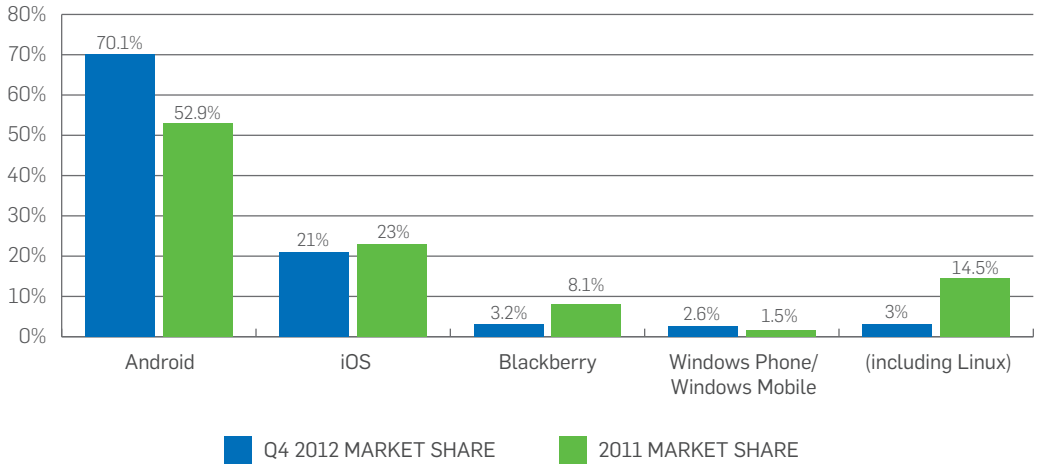


Figure 1 Mobile OS market share 2011 and 2012

This MDM buyers guide will walk you through the process of selecting the right mobile device management solution that fits your company's BYOD objectives. It explains how an effective MDM system can support an organization's workforce mobility strategy, ensure compliance, and provide central management of devices and apps while supporting easy administration. Plus, the guide includes a detailed to table to compare features across the major MDM vendors.

Compliance and Policy Enforcement

An MDM solution protects corporate data by enforcing compliance with corporate security policies. Compliance checks ensure that only registered devices that meet your policies have full access to corporate data.

End users who want to access corporate data using their mobile devices should understand that data access comes with a responsibility to comply with corporate mobility policy. IT professionals can use features of MDM solutions for enforcement and risk mitigation.

Before granting data access, mobile devices must be registered. When a registered device connects, the MDM system checks the device against a set of company rules like jail-breaking, password configuration or blacklisted apps. In addition to the standard compliance check, some MDM solutions allow you to embed corporate mobility policy on a self-service portal to ensure users understand and accept the policy before access is granted.

Also, since users may own and use multiple mobile devices to access corporate data, your solution should allow you to set up group and user-based compliance rules. If your organization has mixed device ownership, you might want to create separate rules for your corporate devices and those owned by your users.

Risk Mitigation

Smart IT professionals can leverage MDMs for risk mitigation measures. You'll also be able to put some teeth into the enforcement of your mobility policy. Risk mitigation actions can be set according to the severity of a policy breach. For minor cases, you may want to simply inform the users. Or you can block non-compliant devices from accessing data or receiving corporate email. If your data is at risk, a remote wipe, either for the full device or a selective wipe of the company's data, may be the only viable option.

Risk mitigation is easier for the IT team if the MDM system has some automated responses configured, which are executed in case of a compliance issue, without the admin interaction. Examples include blocking email delivery, informing the user and/or the admin, or triggering a malware scan. Automatic user notification of any compliance issues can significantly Reduce IT's workload. Users can self-correct most of the issues—without having to call the IT help desk.

Data and Content Security

An MDM solution is intended to provide centralized security and management of mobile devices in order to protect corporate data stored on the devices, and data that these devices have access to. A comprehensive mobility strategy must cover all aspects of mobile users and their interaction with corporate data.

Many mobile operating systems have built-in security features such as device restrictions (disable camera) and encryption. Your MDM solution should allow you to controls these functions to protect data.

The ability to "remote wipe" lost devices is critical and can be found in most MDM solutions. It allows the admin to locate, lock and/or delete corporate data on a device. Ideally, use a solution that allows users to locate, lock and wipe their own devices via a self-service portal. This not only reduces IT's work load but also enhances efficiency. Ultimately, your user should be the first one to know if his or her device is lost or stolen and can take immediate action.

In addition to securing data stored on the devices, IT need to be aware of how do the users access, transfer and collaborate on corporate content. Do they send documents to themselves by email, or do they use cloud-based file sharing? To prevent data loss, you need to encrypt your data everywhere and protect devices from malware. 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, consider an encryption solution that encrypts data before it is uploaded to a cloud-based file share, and still allows mobile devices with the right credentials to interact with the content stored in the cloud.

Mobile Malware Protection

Malicious or “leaky” apps and mobile malware are among the top security concerns for IT professionals. Knowing how important it is to have full control over your mobile protection, choose a solution that gives you the option to integrate mobile security apps into your MDM console and fully manage all aspects of security from one console.

In addition, since the web is the main infection vector, mobile security with web protection for Android users is highly recommended. Below is a short list of recommended functions in an MDM solution’s mobile security app that allow you to:

- Manage malware protection
- Trigger a scan when the mobile security app is out of date
- Automatically block outdated or infected devices
- Block or allow suspicious or potentially unwanted apps (PUAs)
- Protect your Android users from malicious websites
- Protect users from annoyances like text and call spam

Security Features at a Glance

Security Vendors with MDM

✓= YES X = NO

Feature	Sophos	Symantec	McAfee	Kaspersky	Trend
COMPLIANCE CHECK & ENFORCEMENT					
Allow or disallow jailbreaks / rooted devices	✓	✓	✓	✓	✓
Check for side-loading	✓	✓	✓	X	✓
Enforce minimum allowed OS version	✓	✓	✓	X	✓
Enforce device encryption	✓	✓	✓	✓	✓
Whitelist or Blacklist apps	✓	✓	✓	✓	✓
Enforce mandatory apps	✓	✓	✓	✓	X
RISK MITIGATION FEATURES					
Ability to block email access based on compliance status	✓	✓	✓	X	X
Notify administrator	✓	✓	✓	✓	✓
Ability to control network admission	✓	✓	X	X	X
Automatically execute mitigation actions	✓	✓	✓	X	X
DEVICE, DATA AND CONTENT SECURITY					
Locate, lock and wipe	✓	✓	✓	✓	✓
Corporate wipe	✓	✓	✓	✓	✓
MOBILE MALWARE PROTECTION FEATURES (INTEGRATED INTO MDM)					
Scan apps on install	✓	✓	X	X	✓
Ability to remotely trigger anti malware scan	✓	✓	X	X	✓
Block malicious apps (malware)	✓ (SMSec 3.0)	✓	X	X	X
Secure web browsing	✓	✓	X	X	✓
VENDOR'S COMPLETE SECURITY SOLUTION/ INTEGRATION CAPABILITIES					
Complete security vendor	✓	X Mobile Suite, but no complete EP+Mobile Suite	✓ Via EPO	✓	✓

Security Features at a Glance

Pure MDM Vendors

✓= YES X = NO

Feature	Sophos	Airwatch	MobileIron	Good Technology
COMPLIANCE CHECK & ENFORCEMENT				
Allow or disallow jailbreaks / rooted devices	✓	✓	✓	✓
Check for side-loading	✓	✓	✓	✓
Enforce minimum allowed OS version	✓	✓	✓	✓
Enforce device encryption	✓	✓	✓	✓
Whitelist or Blacklist apps	✓	✓	✓	✓
Enforce mandatory apps	✓	✓	✓	✓
RISK MITIGATION FEATURES				
Ability to block email access based on compliance status	✓	✓	✓	✓
Notify administrator	✓	✓	✓	✓
Ability to control network admission	✓	✓	✓	X
Automatically execute mitigation actions	✓	✓	✓	✓
DEVICE, DATA AND CONTENT SECURITY				
Locate, lock and wipe	✓	✓	✓	✓
Corporate wipe	✓	✓	✓	✓
MOBILE MALWARE PROTECTION FEATURES (INTEGRATED INTO MDM)				
Scan apps on install	✓	X	X	X
Ability to remotely trigger anti malware scan	✓	X	X	X
Block malicious apps (malware)	✓ (SMSec 3.0)	X	X	X
Secure web browsing	✓	✓	✓	✓
VENDOR'S COMPLETE SECURITY SOLUTION/ INTEGRATION CAPABILITIES				
Complete security vendor	✓	X	X	X

Light Touch vs. Heavy-Handed

Almost all MDM solutions on the market address security, device and app management, and compliance issues. However, the approach to security can be divided into two camps—light touch and heavy-handed.

Vendors that use the light touch approach leverage the device's native capabilities. However, there is some discrepancy in the capabilities depending on what the OS allows. The benefit is that the "agent" provides a "native" user experience.

In addition, let's not forget the fact that mobile device manufacturers and mobile OS developers are innovating at lightning speed. We can already see a lot of new features that address security coming up in the latest crop of mobile devices. If you are choosing this light touch approach, new security features may become available with OS refreshes. It is a good idea to make sure that you select a vendor that is agile and can keep up with the speed of new mobile devices and OS features.

The heavy-handed approach represents the category of solutions that use "containerization" to isolate applications that access corporate data from other applications.

Since email, calendar and contacts are the most popular mobile applications, most containerization vendors focus on delivering a separate email client, calendar and contacts. However, the trade-off for the user is the usability of their device, because this approach tends to drain the battery faster.

Your end user is one person, trying to use a personal mobile device to achieve work-life balance as efficiently as possible. Because this containerized approach has negative effects on the user's native device experience (low battery life), it shouldn't be a surprise that few end users support this approach.

Before you select one of these approaches, IT professionals need to carefully consider the balance between risk and usability. Unless your company is on the extreme side of risk intolerance, the containerized approach may not be the best choice.

Central Management of Mobile Devices and Applications

The reality of BYOD is that end users are willing to give up some level of control of their personal mobile devices in order to gain flexibility, efficiency and productivity. At the same time, corporate IT professionals need to maintain a level of control in order to properly manage BYOD and ensure security. This may include having the ability to enforce corporate policy, maintain visibility on which devices are brought into the corporate network, what applications are installed on the device, and how content is accessed and shared.

Mobile Device Management

Whether you deploy mobile devices or your employees bring their own, it is important to keep track of all the devices on your network. Select the MDM solution that provides an easy way to manage the mobile devices in your environment throughout their full lifecycle. From the initial setup and enrollment, right through to decommissioning. In addition, you will also need tools to help you with device inventory and reporting. Clear dashboards that provide device information at a glance, with structured tables or pie charts, show you all the devices and their status, such as their ownership, platform and compliance status.

Mobile Application Management

Give your employees the tools to do their jobs. In the BYOD world, this may translate to proliferation of mobile apps. The mobile appltent (MAM) module included in your MDM solution can help you manage apps. For example, pushing required enterprise mobile applications, whitelisting acceptable apps, and blacklisting risky apps.

Enterprise App Store

An enterprise app store allows you to directly supply your users with recommended and required apps on their mobile devices. Both your company-developed apps and commercial app store apps can be offered for download on the user's mobile device, where they can click to trigger the installation.

In addition, an enterprise app store allows you to:

- Safely distribute recommended or company-developed apps
- Define software packages in the admin console and push them to individual devices, groups or platforms
- Distribute iOS-managed apps to users and delete them and all their data, if required
- Avoid users going to non-market app stores
- View a full list of apps installed on each device

Administration

With so many different mobile devices to manage, you need a simple solution to keep your users working without increasing IT's burden.

Self-Service Portal

We advise you to select an MDM solution that comes with a built-in self-service portal. This reduces IT workload and empowers your users to do many common tasks themselves. After all, they would be the first to know if they bought a new device and wish to use it for work, or if a device is lost or stolen. Your self-service portal should provide end users with a simple step-by-step process for common tasks.

A self-service portal allows users to:

- Register their own devices and agree to the company's mobility policy
- See their compliance status in the self-service portal and on their devices
- Receive guidance to help them become compliant
- Remotely locate, lock or wipe their devices and reset their passcode

Configuration and Maintenance

The ease of installation, configuration and maintenance should also be evaluated during your selection. A system with over-the-air setup and configuration from a web console can speed up deployment and reduce IT workload.

Here is a quick checklist to gauge the simplicity of configuration, management and maintenance of your MDM.

- How quickly can the systems be set up and running?
- Can the system automatically assign profiles and policies to users or groups based upon their AD group membership?
- Does it have the ability to automatically set the device status for compliance state and whether the user is allowed to receive email?
- Can you configure your all your devices including iOS, Android and Samsung SAFE devices directly in the MDM system? Or are you required to use the separate iPhone Configuration Utility?
- Is the workflow optimized, and how easily can you find the data you need to manage devices and policies?
- Can you deploy policies over-the-air?
- Can you manage your mobile devices anytime, anywhere?
- How is the interface design? Does it display information in a way that allows you to find the data quickly and mitigate problems in a few clicks?
- Does the system support the Simple Certificate Enrollment Protocol (SCEP), providing the certificates both corporate- and employee-owned mobiles need to access your network and other resources?

Can Your MDM Vendor Do This?

You should consider other factors when selecting your MDM vendors. Ask your vendor these questions:

1. Flexibility of deployment. Does your MDM vendor offers both on-premise management and a cloud-managed option?
2. User-based licensing. With each user bringing multiple mobile devices (smartphone, tablet) to work, licensing cost can easily get out of control. Does your MDM solution provider charge per device (per-node), or offer a user-centric pricing concept?
3. Support. Does your vendor provide 24/7 support?
4. Long-term viability. MDM is still a relatively new with a lot of smaller, start up vendors. You want to check if your vendor is viable for the long run or will it be likely acquired by other players.
5. Ability to innovate. Evaluate your vendor on their speed of innovation and adoption. The mobile device manufacturers are innovating at a much faster pace. Is your MDM vendor agile enough to take advantage of what the latest OS has to offer? For example, Windows Phone 8, Samsung SAFE, or KNOX by SAFE?
6. Complete IT Security. Does your vendor provide complete IT security? And can it provide adjacent and integrated IT security solution for your overall company IT security

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

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com

Boston, USA | Oxford, UK

bg.7.13v1.sNA

SOPHOS
Security made simple.