SOPHOS
Security made simple.

CLASS NETWORKS

Enterprise Mobility Management Buyers Guide

IT Resource Management & Mobile Data Protection vs. User Empowerment

Business Leaders and users are embracing mobility and enjoying the flexibility and productivity these devices provide. The average knowledge worker carries three devices - which means there's a significant increase in mobile device usage in the workplace. Corporate IT departments are saddled with the responsibility to achieve a balance between corporate data protection and end user productivity, all while managing scarce IT resources.

An essential part of Bring Your Own Device (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). Standardising mobile platforms 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 evaluating Enterprise Mobility Management (EMM) solutions to help them manage the influx of mobile devices and shield them from the inherent complexity of BYOD.

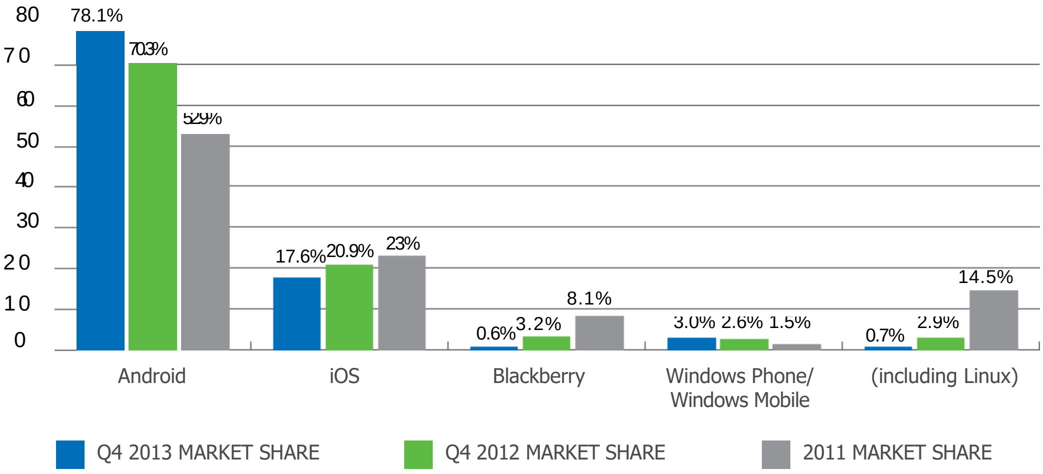

Figure 1 Mobile OS market share 2011–2013. Source: IDC Worldwide Mobile Phone Tracker, February 12, 2014

This EMM buyers guide will walk you through the process of selecting the right mobile solution to fit your company’s Bring Your Own Device (BYOD) objectives. It explains how an effective EMM system can support an organisation’s workforce mobility strategy, ensure compliance, protect corporate data and provide centralised management of devices and apps while supporting easy administration. Plus, the guide includes a detailed table to compare features across the major mobile security vendors.

Protect Corporate Data

An EMM solution is intended to provide centralised 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 mobile security 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 EMM solution should allow you to control these functions to protect data.

The ability to handle lost devices is critical and can be found in most EMM 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 workload but also enhances efficiency. Ultimately, your user will be the first one to know if his or her device is lost or stolen and should take immediate action.

In addition, IT needs to be aware of how users store, maintain, and collaborate on corporate content on a mobile device. According to a Sophos study, 46 percent of organisations embrace cloud storage providers as a method of collaborating on corporate content, yet over 60 percent of these organisations fail to encrypt the data that shared within the cloud on these mobile devices. In order to prevent data loss, data protection cannot end at the office door. Content must be protected anywhere and everywhere these devices go, and individual file encryption is essential to ensure that a malicious user cannot get access to sensitive company data. An EMM solution that provides transparent encryption of each file lets you rest assured that your documents and data remain safe—not just in the office, but everywhere your users go.

Compliance and Policy Enforcement

An EMM 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 fully-functioned EMM solutions for enforcement and risk mitigation.

Before granting data access, mobile devices must be registered. When a registered device connects, the EMM system checks the device against a set of company rules like jailbreaking, password configuration or blacklisted apps. In addition to the standard compliance check, some Enterprise Mobility Management (EMM) 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 organisation 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 mitigate risk and put some teeth into the enforcement of their mobility policy with an Enterprise Mobility Management solution. 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 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 EMM system has pre-configured and automated responses which are executed in the event of a compliance issue without the need for admin intervention. Examples include blocking email delivery, informing the user and/or the admin, or applying a lockdown profile. 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.

Integrated Security: Anti-malware and Web Protection

Mobile devices are simply tiny computers travelling everywhere with users; hence, mobile devices need the same level of robust, integrated antivirus protection, which includes both protection against mobile malware & web filtering for Android devices.

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 EMM solution to protect against mobile malware:

- Automatically scan all newly installed apps for malware
- Quarantine infected devices
- Protect users from accessing malicious websites and block web pages by category

Network Access Control

In order to reduce the risk of data breaches, an EMM solution should constantly monitor device health and control network access accordingly. An EMM solution should constantly detect jailbreaks, blacklisted apps or insecure settings and assess device health, integrating with network security providers to revoke access to WiFi and/or VPN should a device be rendered non-compliant. Ideally, both the network security and EMM solution would come from a single vendor to provide a complete security portfolio.

Security Features at a Glance

Security Solution Providers with EMM

✓= YES X = NO

Feature	Sophos	Symantec	McAfee	Kaspersky	Trend
DATA PROTECTION AND MOBILE ENCRYPTION					
Locate, lock and wipe	✔	✔	✔	✔	✔
Corporate wipe	✔	✔	✔	✔	✔
Individual File Encryption	✔	✗	✗	✗	✗
COMPLIANCE AND POLICY 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					
Ability to block email access based on compliance status	✔	✔	✔	✗	✗
Notify administrator	✔	✔	✔	✔	✔
Ability to control network admission	✔	✔	✗	✗	✗
Automatically execute mitigation actions	✔	✔	✔	✗	✗
ANTI-MALWARE AND WEB PROTECTION					
Scan apps on install	✔	✔	✗	✔	✔
Ability to remotely trigger anti malware scan	✔	✔	✗	✔	✔
Block malicious apps (malware)	✔	✔	✗	✔	✔
Categorial Web Filtering	✔	✗	✔	✔	✔
Secure web browsing	✔	✔	✔	✔	✔
NEWORK ACCESS CONTROL					
Network Access Control	✓	✓	X	X	X
Complete security vendor	✓	X Mobile Suite, but no complete EP+Mobile Suite	✓ Via EPO	✓	✓

Security Features at a Glance

Pure EMM Solution Providers

✓ = YES X = NO

Feature	Sophos	Airwatch	MobileIron	IBM (Fiberlink)
DATA PROTECTION AND MOBILE ENCRYPTION				
Locate, lock and wipe	✓	✓	✓	✓
Corporate wipe	✓	✓	✓	✓
Individual File Encryption	✓	✗	✗	✗
COMPLIANCE AND POLICY 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				
Ability to block email access based on compliance status	✓	✓	✓	✓
Notify administrator	✓	✓	✓	✓
Ability to control network admission	✓	✓	✓	✓
Automatically execute mitigation actions	✓	✓	✓	✓
ANTI MALWARE AND WEB CONTROL				
Scan apps on install	✓	✓	✓	✓
Ability to remotely trigger anti malware scan	✓	✓	✓	✓
Block malicious apps (malware)	✓	✓	✓	✓
Categorical Web Filtering	✓	✓	✓	✓
Secure web browsing	✓	✓	✓	✓
NEWORK ACCESS CONTROL				
Network Access Control	✓	✓	✓	✓
Complete security vendor	✓	✗	✗	✗

Central Management of Mobile Devices, Content, E-Mail and Applications

The BYOD reality 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, company 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 company policy, maintain visibility on which devices are brought into the company network, what applications are installed on the device, and how content is accessed and shared.

Mobile Device Management (MDM)

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 EMM 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 Content Management (MCM)

Ensure your data protection does not end at the office door. Mobile Encryption on the devices brought into your organisation helps ensure that each document remains secure while allowing users to remain productive and collaborate safely. By extending a robust encryption solution onto your mobile devices, you ensure that IT has control over the way in which content is maintained and shared within the cloud; for example, if a malicious user gets access to an employee's dropbox account, having individual file encryption allows you to rest assured that the malicious user cannot access any of the company content without key access.

Mobile Email Management (MEM)

Secure company email access is essential, especially in a BYOD environment. MEM enables comprehensive security for your corporate email infrastructure by distributing email settings, getting your users productive in minutes, and by controlling access to email via a secure email gateway based on the device health. Moreover, it is important to be able to selectively wipe all company emails once a user leaves the company.

Mobile Application Management (MAM)

Giving your employees the tools to do their jobs makes good business sense, but in the BYOD world, this may result in the proliferation of a variety of mobile applications. The mobile application (MAM) module included in your EMM solution should help you manage them all, and enable you to push the required enterprise mobile apps, whitelist acceptable apps, and blacklist the risky ones.

Integrated Security

Android devices are particularly susceptible to malware, and it is important to protect the devices -- and your network -- with an EMM solution that offers integrated anti-malware, web protection, and network access control. These solutions can help protect Android users from data-stealing malware, and from accessing malicious websites.

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 EMM solution that comes with a comprehensive 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
- Decommission their device

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 EMM.

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 your EMM solution have the ability to automatically render a device compliant and have control over whether a user is permitted to access/receive corporate email?
- Can you configure all your devices including iOS, Android and Samsung SAFE devices directly in the EMM 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 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?

Deployment Options

We encourage users to select an EMM solution that offers a variety of deployment options to suit their needs, including:

- On-premise: software you install and manage on your own servers on-site. This version allows you to keep all data in-house.
- SaaS: allows you to do all administration via the web-based console without the need to install or update software.

For those organisations seeking a simple, integrated web-based console and robust security for Mobile, please call 0800 160 1920 or visit www.classsnetworks.com/IT Security.

Can Your EMM Provider Do This?

You should consider other factors when selecting your EMM providers. Ask these questions:

1. **Flexibility of deployment.** Does your EMM provider offer 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 costs can easily get out of control. Does your EMM provider charge per device (per-node), or offer a user-centric pricing concept?
3. **Support**. Does your EMM solution provider offer 24/7 support?
4. **Data Protection.** With content increasingly shared and maintained on mobile devices, it is important to ensure that the EMM provider you choose offers mobile encryption to secure the corporate data.
5. **Long-term viability.** EMM is still relatively new with a lot of smaller, start up solution providers. You want to check if your provider is viable for the long run or likely to be acquired by other players.
6. **Additional security for Android devices.** You want to ensure your EMM provider offers additional anti-malware and web protection capabilities to protect Android devices.
7. **Ability to innovate.** Evaluate your EMM solution provider on their speed of innovation and adoption. Mobile device manufacturers are innovating at an incredible pace. Is your EMM provider agile enough to take advantage of what the latest OS has to offer? For example, Windows Phone 8, Samsung SAFE, or KNOX by SAFE?
8. **Complete IT Security.** Does your EMM provider provide complete IT security? And can it provide adjacent and integrated IT security solutions for your overall company IT security?

Class Networks are Certified Architects of Sophos Threat Management Systems. Sophos products help secure the networks used by 100 million people in 150 countries and 100,000 businesses, including Pixar, Under Armour, Northrop Grumman, Xerox, Ford, Avis, and Toshiba.

Class Networks works with over 1,000 organisations in the voluntary sector providing business technology communications solutions. We have been the Trusted Supplier Partner for the NCVO, SCVO and WCVA for nearly twenty years.

Please call 0800 160 1920 or email visit www.classnetworks.com or email contacts@classsnetworks.com.

Class Networks Mobile Control

Class Networks, Givon's House, Givon's Grove, Leatherhead, Surrey, KT22 8LY