# BEST PRACTICE GUIDE MOBILE DEVICE MANAGEMENT AND MOBILE SECURITY.

With Kaspersky, now you can.
kaspersky.com/business

Be Ready for What's Next

KASPERSKY lab

# CONTENTS

# MOVING TARGETS: MOBILE DEVICE MANAGEMENT AND MOBILE SECURITY.

## 1. OPEN ALL HOURS

Mobile access to vital business applications and information empowers workers to be more productive, supporting increased business agility and flexibility.

But mobility comes at a price: The same features that make smart devices so useful to employees also make them attractive to hackers, data thieves, malware distributors and other criminals. In the past 12 months alone, 51 per cent of organisations globally have experienced data loss due to insecure mobile devices.[1]

It's not just about malware; the trend towards 'Bring Your Own Device' (BYOD) initiatives in companies of all sizes is contributing to an increasingly complex spread of devices across the business. At the same time, the lines between business and personal use are blurring, creating a challenging management and control environment for IT administrators.

How can you support BYOD initiatives without the headaches? How can you control what the end-user is doing when they're downloading apps in a hotel room in a different time zone? What happens when they leave their smartphone in the back of a taxi? Can you control all of this easily and from one central point? Mobile Device Management (MDM) can answer most of these questions.

## 2. MOBILE DEVICE MANAGEMENT – WHAT IS IT?

Mobile Device Management allows IT professionals to extend their 'wired' security strategy and policies to all devices, wherever they happen to be. MDM software allows IT managers to cost-effectively automate vital management and control tasks such as device configuration, software updates, backup/restore. All while ensuring the safety of sensitive business information in the event of theft, loss or end-user abuse.

## 3. CHOOSING THE RIGHT MDM SOLUTION:

### 3.1 Multi-Platform Support

Android, BlackBerry, iOS, Symbian, Windows Phone, anyone supporting BYOD initiatives will be familiar with the demands of securing and maintaining multiple platforms.

An MDM solution that supports multiple platforms is not only cost-effective, it takes the pain out of managing multiple systems. It also brings flexibility, supporting not only the devices you have today, but the brands and products you choose in the future.



1 Source reference: Ponemon: The Cost of a Lost Laptop (2009)

## 4. EFFECTIVE MDM PRACTICES

### 4.1 Strong policies

Create mobile-specific policies that clearly define, among other things:

- How the device will be deployed
- What data will be accessible by mobile workers
- Who can do what on company networks
- What procedures will be implemented in the event of device loss or theft

Define and enforce policies in a granular, flexible way – e.g. apply different policies to different users and groups, according to their needs. This level of granularity should extend to the device itself- for example, jailbroken or otherwise compromised devices can be prevented from accessing company data or remotely locked, adding an extra layer of security.

### 4.2 Containerisation

Eighty-nine per cent of people using their personal device for business purposes say they use it to access critical work information. 41 per cent say they use their personal devices at work without permission.[2]

Even the most conscientious users can inadvertently put company systems and content at risk by downloading consumer applications or accessing personal content using their device.

This is where containerisation comes in. It's a simple solution that separates personal and business content on the device, allowing IT complete control over business content and protecting it from any risks introduced by personal usage – without affecting personal data. Using containerisation, IT departments can apply security and data protection policies to a business 'container' on a personal or company-owned device – making it particularly useful in BYOD scenarios.

### 4.3 Encryption

MDM best practice should also include the option to encrypt sensitive data within the container. Encryption reinforces anti-theft strategies; forcibly encrypted data reduces the impact of any time delay in wiping a lost or stolen device.

By ensuring that only encrypted data can leave the business container on a device, organisations can guard against data leakage and support compliance requirements around data protection. Kaspersky Lab's MDM encryption technology can be automated and made completely transparent to the end user, ensuring that your security policies are adhered to.



2 Source reference: Juniper Networks, Trusted Mobility Index 2012.

### 4.4 Anti-Theft and Content Security

It's almost impossible to physically lock down small, ultra mobile devices, but you can lock down their contents and control what happens when they do go missing.

Kaspersky Lab's MDM solution includes anti-theft and content security features that can be enabled remotely, preventing unauthorised access to sensitive date. Among them:

- **SIM control:** Lock a lost or stolen phone, even if the SIM card is replaced, and send the new number to the rightful owner.
- **Device/location tracking:** Use GPS, GSM or WiFi to pinpoint device location.
- **Remote/selective wipe:** Completely erase all data on any device, or just sensitive company information.
- **Remote lock:** Prevent unauthorised access to a device; no need to wipe data.

### 4.5 Mobile Anti-Malware

You need a strategy for dealing with lost or stolen devices. But devices are at risk even when they're with authorised users. Many organisations are careful to implement anti-malware and anti-spam solutions on their fixed networks – but do little to protect their mobile devices from becoming a source of viruses or other malware.

Kaspersky Lab's mobile security technologies include a blended anti-malware solution that combines traditional, signature-based detection with proactive, cloud-assisted technologies. This improves detection rates and gives real-time protection from malware. On-demand as well as scheduled scans ensure maximum protection – automatic, over-the-air updates are essential to any MDM strategy.

### 4.6 Keeping things simple: Centralised controls

Kaspersky Lab's technologies allow administrators to manage the security of mobile devices from the same, 'single pane of glass' console they use for their network and endpoint security. This eliminates the complexity associated with separate solutions, and the multiple, often incompatible consoles that come with them. Technology sprawl makes a challenging job more complex than it needs to be.

By simplifying and automating the secure configuration of multiple devices, you not only reduce the burden on IT, but support better mobile security practices. Once your policies and ground rules are in place, centralised control can be achieved using a single click – whether you're managing 10 devices or 1,000.

### 4.7 Get the balance right

Deploying, managing and securing your mobile IT environment doesn't have to be complicated or expensive. Kaspersky Lab's MDM solution makes the secure configuration of mobile devices painless and straightforward; the mobile agent installed on devices will provide all the protection you need against current threats. IT administrators can be confident that all mobile devices are configured with their required settings and are secure in the event of loss, theft or user abuse.

It doesn't matter what size your business is, if you don't manage mobile devices properly, they'll soon become just another drain on resources, not to mention a security and data loss risk. Whether you're hoping to reduce costs by supporting a BYOD initiative or operating a strict company-owned mobile device program, the risks are ultimately the same: a growing volume of sensitive business data is sitting in employees' pockets, being left behind in taxis, stolen or lost.

What if you didn't have to trade security and data protection for mobility, enhanced productivity and simplicity? Kaspersky's mobile device management and enhanced mobile security technologies mean that you don't.

## 5. IN CONCLUSION

Organisations need intelligent security technologies to protect their data – and they also need intuitive and uncomplicated IT efficiency tools. Kaspersky Lab's 2,500 employees are driven to meet those needs for the 300 million plus systems they protect – and the 50,000 new systems a day that are added to their number.

Kaspersky MDM is a component of Kaspersky Endpoint Security for Business. Combining award-winning anti-malware, IT policy enforcement tools, centralised management and cloud-assisted protection, Kaspersky's business security products are the right choice for your organisation.

Talk to your security reseller about how Kaspersky can bring secure configuration to your mobile endpoint deployment – and more!

# SEE IT. CONTROL IT. PROTECT IT.

**With Kaspersky, now you can.**
**kaspersky.com/business**

**Be Ready for What's Next**

Kaspersky Lab ZAO, Moscow, Russia
www.kaspersky.com