KASPERSKY lab

BEST PRACTICES

Mobile Security

www.kaspersky.com

YOUR GUIDE TO MOBILE SECURITY BEST PRACTICES.

Mobile threats are increasing exponentially.

Over a **12** month period, Kaspersky Lab security products reported **3.5** million malware detections on the mobile devices of over **1** million users.[1]

Mobile devices are essential pieces of business kit. But as their capabilities grow, the associated data security risks have increased. You know that securing an increasingly mobile and geographically distributed workforce that has embraced social media and cloud-based technologies is not easy. But it is possible to say 'Yes' to the mobile technologies, including BYOD, which are so critical to improved productivity, without opening new doors to security breaches.

The very features that make smart devices so useful in the workplace also make them attractive to hackers, data thieves, malware distributors and other criminals. And that's before you've factored in the ease with which they're stolen or left behind in taxis and airport security check-in trays.

Kaspersky Lab research has found that an average of 23 per cent of organizations have experienced mobile device theft; 19 per cent have experienced data loss because of it, with 14 per cent reporting the inappropriate leaking or sharing of information via mobile devices.[2]

With the average cost of a security breach now running at $50k for a small-to-medium-sized business[3], it's no wonder that 38 per cent of IT security professionals have made the protection of confidential data against leakages a top priority.[4]

Bring your own danger?

It's not just about malware or theft; the trend towards 'Bring Your Own Device' (BYOD) in companies of all sizes is contributing to an increasingly complex spread of smartphones and other devices across the business. As the lines between business and personal use blur, they create an IT management and control headache all of their own. When your job is to keep everyone as productive as possible and to maintain data security, mobile is something of a double-edged sword – 69 per cent of IT security professionals view mobile devices as the greatest risk to regulated, sensitive data.[5] And more than half of employees aged 21-31 say they would circumvent any company policy banning the use of personal devices.[6]

1 Securelist, http://securelist.com/analysis/publications/66978/mobile-cyber-threats-a-joint-study-by-kaspersky-lab-and-interpol/ October 2014.
2 Kaspersky Lab, Global IT Security Risk Report 2014.
3 Kaspersky Lab, IT Security: Fighting the Silent Threat, 2013.
4 Kaspersky Lab, IT Security Risk Report, 2014.
5 Ponemon Institute, Risk of Regulated Data on Mobile Devices and in the Cloud, 2013.
6 Forbes, http://fortune.com/2013/10/21/employees-really-want-to-use-their-personal-devices-at-work/

How can you support BYOD without the headaches? How can you control what end users do 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 manage all of these eventualities easily and from one central point?

Mobile Device Management (MDM) and Mobile Application Management (MAM) can answer most of these questions...

1. EMBRACE MOBILE DEVICE MANAGEMENT

Mobile Device Management (MDM) enables the extension of a 'wired' security strategy and policies to all devices, wherever they happen to be. Using MDM software, you can cost-effectively automate vital management and control tasks such as device configuration, software updates and backup/restore. All while ensuring the safety of sensitive business information in the event of theft, loss or end-user abuse.

What to look for in an MDM solution

- Multi-platform Support

  Securing and maintaining multiple devices and platforms is a challenge. An MDM solution that supports multiple platforms with a unified interface and integrated policies is not only cost-effective, it takes the pain out of managing multiple systems while enabling flexibility across current and future devices.

- The Ability to Create Strong Policies

  To follow a Best Practice approach to Mobile Device Management you will need to create mobile-specific policies that clearly define, among other things:

  - How the device will be deployed
  - What applications are allowed to run
  - Who can do what on company networks
  - What procedures will be implemented in the event of device loss or theft

  Your policy definitions should include some granularity and flexibility – e.g. applying different policies to different users and groups, according to their needs. Extend this granularity to the device itself – for example, preventing jail-broken or otherwise compromised devices from accessing company data, or locking them remotely – and you have a further layer of security.

2. MAKE FULL USE OF MOBILE APPLICATION MANAGEMENT

Mobile Application Management (MAM) is concerned with the delivery to, administration and control of applications software on end-users' smartphones and tablets. If fact, any effective Enterprise Mobility Management (EMM) solution should ideally include the management of applications and application data as well as device firmware and configuration settings, so MAM can be seen as complementary to MDM, and even as a subset.

While device loss or theft is clearly a far greater issue for smartphones and tablets than it is for their fixed workstation counterparts, applications remain a primary route for malware infection on all endpoints, including mobile devices. In addition, the deployment of apps has become central to mobile device usage, while the quality and volume of leisure and entertainment apps downloaded to an employee-owned mobile device is not within your professional control.

An MAM solution needs to separate corporate and personal data, allowing to you apply additional security policies to business applications on the device. This separation is achieved through containerization.

Containerization

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 containerization comes in. It's a simple solution that separates personal and business content on the device, giving you complete control over business data and protecting it from any risks introduced by personal device usage.

Security and data protection policies can be applied to applications secured in a business 'container' on a personal or company-owned device – making it particularly useful for BYOD. Kaspersky Lab's 'selective wipe' feature means that, when an employee leaves the company, taking their own device with them, it's possible to delete the contents of the container or containers, including all sensitive, business-related data, from their phone, without affecting personal data.

Container encryption capability adds a further layer of protection to your a mobile security strategy. In line with best practices for mobile anti-theft protection, 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 container on a device, you can guard against data breaches, supporting compliance requirements around data protection. Kaspersky Lab's mobile device encryption technology can be automated; user transparency ensures compliance with security policies. It's also possible for the entire mobile device to be encrypted using Kaspersky Lab's MDM capabilities.

3. ACTIVATE ANTI-THEFT AND CONTENT SECURITY

Physically locking down small, ultra-mobile devices is almost impossible – but you can lock the data on them and control what happens when devices go missing.

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

- **Remote lock**: Prevent unauthorized access to a device; no need to wipe data.
- **Device/location tracking**: Use GPS coordinates to pinpoint the device location on a map – tinformation that can be sent to the device owner.
- **SIM Control**: Lock a lost/stolen phone, even if the SIM is replaced; send new number to rightful owner.
- **Remote/selective wipe**: Completely erase all data on any device, or just sensitive company information.
- **Alarm & mugshot**: Make mobile device thieves aware that you are aware of them – you can even instruct the stolen phone to photograph them for identification purposes.

4. ...AND EMPOWER YOUR USERS

One way of potentially reducing the time-delay in activating anti-theft security measures above is to empower users to do this for themselves. Using a self-service portal, the employee can react immediately to the loss of a device, wherever he or she is. First, an attempt can be made to find the device by locating in on the map, making a screenshot or sending the alarm signal to it. If this doesn't help, the user can block it and wipe the corporate profile or entirely remove all the data from the lost smartphone or tablet.

By encouraging employees to take responsibility for activating anti-theft controls themselves, the natural tendency to delay a little longer in the hope that the device may turn up, rather than immediately 'owning up' to you and your team, is counteracted. This makes for faster activation times and improved security, as well as creating one less headache for you.

Kaspersky Lab's self service portal, incidentally, also allows users to register their devices onto the corporate network, relieving you of yet another administrative task.

5. FIGHT MOBILE ANTI-MALWARE

Devices are at risk from attack even when they're not lost or stolen. It's surprising how many businesses insist on having anti-malware and anti-spam protection for their fixed networks, but do little to enforce the same strategy on their mobile devices.

It is worth noting that many MDM solutions offer essentially reactive protection via containerization – Kaspersky Lab's mobile security technologies include a robust anti-malware, anti-spam and anti-phishing engine supported by cloud-assisted technologies to detect and block attacks in real time, before reaching the device, rather than relying entirely on the container to form a protective barrier.

On-demand and scheduled scans also help ensure maximum protection – automatic, over-the-air scans and updates are essential capabilities of any effective MDM strategy.

6. CHOOSE CENTRALIZED MANAGEMENT

Thirty-four per cent of SMBs have integrated mobile devices into their IT systems in the past year – a rate almost identical with larger businesses.[7] Kaspersky Lab's technologies allow you to manage the security of mobile devices from the same console you already use for network and endpoint security. This spares you the additional work and frustrations associated with separate solutions and the multiple, often incompatible control consoles that come with them.

Larger organizations with highly structured IT departments may also want to ensure that any control center is capable of supporting Role Based Access Control (RBAC), so that administrative responsibility for mobile devices or for applications control, for example, can be allocated to a specific individual within the team.

7. MAKE EFFICIENCY SAVINGS THROUGH AUTOMATION

By simplifying and automating the secure configuration of multiple devices, you not only reduce the burden on IT, you also support better mobile security practices. Many tasks falling to the mobile security administrator, such Windows or PKI based Certification, can be automated securely and effectively. Larger organizations may opt for further simplification through the use of technologies like Kerberos Key Distribution Center.

Management through a web portal has clear advantages if you are on the move, while a self-service user portal, as we have seen, empowers the user to take a level of personal responsibility.

Once your policies and ground rules are in place, centralized deployment can be achieved through a single click, whether you're managing 10 devices or 1000.

7 Kaspersky Lab, IT Security Risks Report 2014.

FINALLY....

Deploying, managing and securing a mobile IT environment doesn't have to be complicated or expensive. Kaspersky Lab's Enterprise Mobility Management solution makes it painless and straightforward for you configure the security of mobile devices painless and straightforward; a mobile agent installed on devices will provide all the protection you need against current threats. All mobile devices are configured with IT-sanctioned settings, completely securing them in the event of loss, theft or user abuse.

When it comes to mobile device security and data breach protection, size doesn't matter – regardless of how many users and devices you're managing, if you don't control them properly they'll soon become a drain on resources – not to mention a security breach risk.

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


Twitter.com/
Kaspersky


Facebook.com/
Kaspersky


Youtube.com/
Kaspersky

Kaspersky Lab, Moscow, Russia
www.kaspersky.com

All about Internet security:
www.securelist.com

Find a partner near you:
www.kaspersky.com/buyoffline

KASPERSKY lab