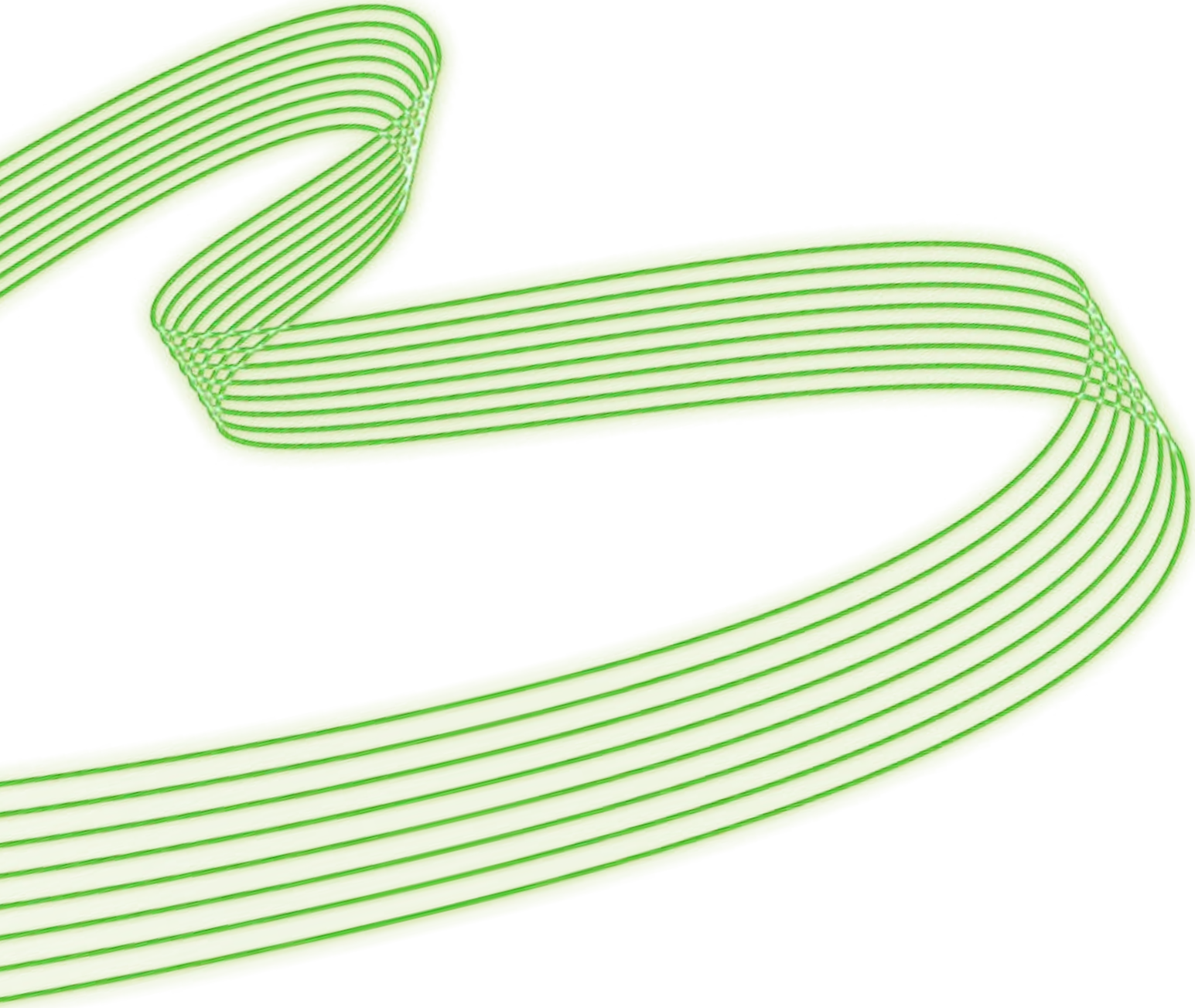

SECURITY TECHNOLOGIES FOR MOBILE AND BYOD.

A whitepaper that assesses the security technology options that are essential for protecting your network, systems and data.

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

Be Ready for What's Next

KASPERSKY lab

Executive summary

1.0

The mobile challenges

1.1 Increasing threat levels

The volume of new malware that is specifically targeting mobile devices is growing at an almost exponential rate. The nature of many of the new malware attacks is also becoming increasingly sophisticated – as cybercriminals recognise the value of the information that they can steal from mobile devices. Even though the vast majority of criminals launch attacks in order to generate revenues – either directly or indirectly – the total cost of an attack can be much higher than just stolen money. The loss of data, and the potential negative effects on a business's reputation, can also cause severe damage.

1.2 Greater demand for mobile access

At the same time, most corporations are recognising the productivity benefits that can be gained by giving their mobile workforce anytime, anywhere access to more of the business's corporate systems and data. Furthermore, with businesses and employees embracing Bring Your Own Device (BYOD) initiatives – whereby employees use their own mobile devices to perform work tasks – the security risks have increased significantly and the need for effective mobile security technologies is greater than ever.

1.3 IT and security departments have to tackle the issues

If businesses are to benefit from the potential productivity gains offered by increased mobile access – and employees are able to enjoy the convenience of BYOD – security and IT departments are faced with having to ensure their business is protected against all new mobile security threats.

The threats are increasing…
… very rapidly

In 2012, Kaspersky Lab discovered over 25 times more mobile malware than was identified in the entire six-year period between 2004 and 2010.

The use of BYOD continues to grow

In Q4 of 2012, a global study by Forrester Research Inc. found that 74% of employees use personal smartphones for business tasks.[1]

Externally… how secure is your business data?

The global study by Forrester Research Inc. in Q4 of 2012, also found that 44% of employees use smartphones for work in coffee shops or other public places, and 47% use them whilst travelling.[2]

1 & 2 Source: Forrsights Workforce Employee Survey, Q4 2012, Forrester Research, Inc.

The new security issues that mobile brings

2.0

2.1. Another route for malware to enter the corporate network

Most businesses have invested in security that protects all endpoints within their corporate network – plus firewalls that prevent unauthorised external access to corporate systems. However, enabling access – to business systems and data, from mobile devices – means smartphones and tablets will effectively cross through the protective firewall. If those devices are infected with viruses or Trojans, that will introduce security issues within the corporate network.

2.2. Dangers from mixing corporate data and personal data on one device

Whenever personal data and corporate data are stored in the same mobile device, there's the possibility of security risks. Separating corporate data and the user's personal data can help businesses to apply special security measures for their confidential or business-critical information.

For example, if the device is owned by the employee – and that employee leaves the company – data separation can make it much easier for the business to remove the corporate data from the device, without affecting the employee's personal data.

2.3. BYOD brings you even more platforms to manage

With the average employee now using two or three different mobile devices to access the corporate network, BYOD brings IT and security departments the challenge of having to implement and manage mobile security across an almost limitless range of devices and operating systems, including:

- Android
- iOS
- Windows Phone
- Windows Mobile
- BlackBerry
- Symbian

To avoid overloading the security team, it's essential that the business chooses a mobile management and security solution that simplifies the process of securing a wide range of devices and platforms.

2.4. Data theft – via vulnerabilities

Criminals are increasingly exploiting unpatched vulnerabilities within operating systems and commonly-used applications, in order to gain control of mobile devices and to steal data – including passwords for access to corporate systems.

If employees connect their mobile devices to their corporate desktops or laptops – in order to synchronise data – that introduces the possibility of data being stolen via the desktop / laptop.

Installing the latest security updates for all of the applications running on your infrastructure and your employees' devices is essential. There are security solutions that combine protection for desktops, laptops and servers – including anti-malware, application control, web control, device control, vulnerability scanning and patch management – plus mobile device security.

2.5. Risks in the employee's home

A further risk of data theft – from syncing and backup – comes from a route that's much harder for the business to control.

If your company operates a BYOD scheme, it's likely that some or all employees will be syncing their mobile devices with their home PCs or Macs. This can introduce an additional risk of data leakage. Even though the employee may only be interested in backing up their personal files and photos, they could also be downloading corporate data and passwords… from their mobile device onto their home computer as part of the sync process.

If the employee's home computer has already been infected by Trojans or spyware, this could compromise the security of corporate data. Furthermore, if the computer has unpatched vulnerabilities, cybercriminals can easily access the mobile data that's backed up, stored or synced onto the computer – regardless of the security software that's actually running on the mobile device.

This type of risk can raise serious issues regarding compliance. It's vital that the business considers how mobile devices may be used – including in the employee's home – and takes steps to ensure that sensitive data is always protected.

(For a high-level overview of compliance obligations, please see Kaspersky Lab's exclusive whitepaper – **Information Security and Legal Compliance: Finding Common Ground** by Michael R. Overly, Esq., CISA, CISSP, CIPP, ISSMP, CRISC.)

2.6. Supplementing device-level encryption

Many mobile platforms include the ability to encrypt data in order to try and ensure sensitive information cannot be accessed by criminals if the smartphone or tablet is stolen or the information is intercepted. However, there are techniques that criminals can use to decrypt data.

Thus, if the business is relying on encryption to help protect precious data, it's wise to choose a mobile security solution that can apply a further layer of encryption – in addition to the mobile device's own encryption capability.

2.7. Loss of a mobile device… means loss of corporate data

One of the key benefits of mobile devices is also one their major flaws. Because smartphones and tablets are so small and lightweight they're convenient to carry around for easy access to corporate data. However, their size and weight also means the devices are very easy to lose – or for thieves to steal.

Regardless of how much effort the business devotes to training its employees about security awareness… some devices are going to be lost or stolen. Hence, it's important to have data security remedies in place to cover such events.

Assessing the available mobile security technologies

3.0

3.1 Advanced anti-malware capabilities

Because anti-malware solutions have been available for many years, some businesses have come to regard them as 'commodity items' – with each anti-malware solution offering similar levels of protection. Unfortunately, not all anti-malware products are capable of delivering the rigorous security that businesses require today.

In the past, traditional, signature-based protection – that relied on the security vendor regularly updating its database of malware signatures – was sufficient to protect against the fairly unsophisticated threats that were prevalent. Today, signature-based methods cannot provide adequate levels of security against the vast range of new and complex threats that are being released every day. In order to provide protection against new and emerging threats, it's important to choose an anti-malware solution that offers a combination of:

• **Signature-based protection**
This is still an important element in a business's defences against malware. However, not all vendors' offerings deliver the same protection. The effectiveness of each vendor's solution will largely depend on:
– The quality of the vendor's anti-malware engine – and its ability to detect malware
– The speed and frequency with which the vendor delivers updates to its malware signature database

• **Proactive, heuristic-based protection**
In addition to signature-based methods, it's important that the security solution can also analyse behaviours – in order to protect against malicious actions undertaken by new malware programs that don't yet have a published signature.

• **Cloud-assisted protection**
The power of the cloud can add another vital layer of anti-malware security. By monitoring consenting users' systems across the world – in order to identify new and emerging threats – cloud-assisted technologies can help security vendors to deliver an extremely rapid response to new malware. Cloud-assisted security is essential for protecting businesses against zero-day and zero-hour threats.

3.2 Separating personal and corporate data

On BYOD devices, it's essential that the user's personal data and apps are totally separated from the business's mission critical programs and confidential information.

There are a number of ways in which data can be separated within a single device:

• **Smartphone / tablet virtualisation**
This technique is similar to server virtualisation – whereby several virtual machines are set up within one physical server. Mobile device virtualisation effectively makes each device act like two separate devices. In this way, corporate data / applications are totally separated from personal data / apps within the smartphone or tablet.

However, the virtualisation process uses so much of the device's computing power that the technique is not viable with current phones and tablets.

• **Separate interfaces**
Another technique involves the use of two different interfaces for the one device – one interface for corporate data and another for personal data. At first sight, this may appear to be a fairly elegant solution to the need for data separation. However, there can be major disadvantages that often make this method of operation much less convenient for users.

Even relatively simple requirements – such as the storage of contact information – can be problematic. With this method, the user may have to set up two different lists of contacts – one for personal contacts and one for work contacts. If the employee receives a work-related phone call while they're accessing personal data or apps, the phone may be unable to display the contact information for the incoming call. Because, in this example, the phone is already being used in 'personal mode', the user cannot access contact data that is held in the 'work section' of the phone.

• **Containerisation**
This third technique also successfully separates personal and corporate data. However it offers two key advantages:

– Although corporate and personal information are stored separately, there are none of the user convenience issues that can result from having two separate interfaces – such as having to switch between personal and corporate modes in order to access contact information.
– Containerisation delivers an additional layer of security for corporate data that's stored on the mobile device.

Containerisation gives administrators the ability to create containers – on the device – for all corporate applications. Data can be shared across containerised applications – but that data is not made available to non-containerised programs.

The administrator can also set specific security options for everything that's held within the corporate containers. For example, the administrator can ensure that all data within a container is automatically encrypted.

By storing all corporate data within a secure container, this technique provides a further layer of security. In addition to using the mobile device's own data encryption capabilities, the containers can also be encrypted. This makes it much harder – or virtually impossible – for the average cybercriminal to decrypt data that is held inside a secure, encrypted container.

3.3 Mobile Device Management (MDM)

Mobile Device Management can provide a convenient way for administrators to:

• Install – and uninstall – security software and other applications
• Create and manage policies and rules for corporate network access
• Manage anti-malware protection settings
• Enable data encryption
• Protect corporate data in the event of the loss or theft of a mobile device

Although MDM products have been commercially available for many years, businesses now have the option of buying fully-integrated solutions that combine mobile management features and mobile security technologies.

In the past, the only option was to buy a separate MDM product and also an anti-malware product – each from different vendors. This sometimes required a level of integration to be undertaken by the IT department. Even then, having performed the necessary integration, the need to use a combination of the two products would lead to the following issues:

- The necessity to use two separate consoles, instead of one integrated management console – so the administrator had to use:
  - One console to manage the MDM functionality
  - Another console to control the anti-malware functions

- A lack of integrated reporting functionality – with separate reports being generated by the MDM product and the anti-malware product

Even if companies have been running one of the common, standalone MDM products, there can be significant benefits from moving to one of the new integrated solutions, including:
- Ease of use – via a single console
- Integrated reporting
- Lower total cost of ownership

3.4 Over the Air (OTA) provisioning

Some MDM products give administrators the ability to deliver applications – including business and security programs – to the users' mobile devices via remote Over the Air means. This can save time, effort and money for the business.

3.5 Controlling the launch of applications

For BYOD initiatives, it's essential to recognise that some employees will have an 'application-centric' attitude towards running a wide range of non-work apps on their mobile devices. Although many applications will present no risk to corporate data, it's possible that some apps could cause security issues. Thus, it's important to choose an MDM or security solution that gives the administrator control over the launch of applications.

Application Control functions will often give the administrator a choice of policies:

- **Default Allow**

This lets any application run on the employee's device – with the exception of applications that have been blacklisted.
- **Default Deny**

This option blocks all applications from running – with the exception of applications that have been whitelisted.

Within a BYOD scheme, a Default Deny policy could be very unpopular with employees. It's likely that your choice of policy will largely depend on the nature of the information that you wish to secure.

3.6 Controlling Internet access

With the increase in the number of drive-by malware attacks – whereby users' devices can become infected, just by visiting an infected web page – controlling web access can help to prevent the leakage of corporate data or the transfer of malware to the corporate network.

Some mobile security products give administrators the ability to block malicious websites and also block access to categories of sites that:
- Contain inappropriate content, or
- Are not suitable for the work environment

3.7 Dealing with lost or stolen mobile devices

Lost or stolen mobile devices can represent a serious security risk for a business. Features that give administrators remote access to the missing device can help to minimise the security issues if the device has been used to access corporate data and systems:

• **Blocking the missing device**
As a first step, the administrator can remotely block the operation of the device. This not only prevents unauthorised access to corporate data and systems but also prevents any other use of the device.

• **Finding the device**
Some mobile security solutions can use a combination of GPS, GSM, Wi-Fi and mapping to show the approximate location of the missing device.

• **Wiping data**
If it appears that it's not going to be possible to retrieve the missing device, some security solutions provide the administrator with remotely operated commands that can delete data from the tablet or smartphone. In order to avoid possible legal liability issues – for deleting the employee's personal data – it's advisable to select a security solution that offers a choice of data wiping options:

Selective wipe
This helps administrators to delete corporate data, without affecting the user's personal data. The feature is particularly useful if:

– The user suspects that their BYOD device has been mislaid – instead of permanently lost
– The user has left the company

If the security software includes the ability to hold corporate data within secure containers, the selective wiping process can easily be restricted to the containerised data and applications.

Total wipe and device reset
This option can be used to delete all corporate and personal information on the device and to return the device to its original factory settings.

• **Accessing a mobile device if the SIM card has been changed**
To evade detection, thieves will often change the SIM card in the stolen device. However, some security solutions actively monitor for this type of action and can automatically inform the administrator of a SIM card change – and also send the new phone number to the administrator. This enables the administrator to run all of the remote blocking, locating and wiping features – despite the change of SIM card.

• **Additional anti-theft features**
Some vendors' mobile security solutions also include features that give administrators remote access to additional functions, including the ability to display a message on the device's screen – to urge anyone that's using the device to return it to the employee or the business.

Evaluating the 'invisible factors'

4.0

4.1 It's an ongoing battle… for all security vendors

All aspects of IT security are effectively a game of 'cat and mouse' between the cybercriminals and the security software vendors. As soon as vendors release new products and updates that plug the holes in IT defences, the criminals will try to:

- Identify new operating system or application vulnerabilities to exploit
- Develop new attack methods
- Find new ways to try to circumvent anti-malware technologies

At the same time, criminals are looking for new ways to enter corporate systems – and mobile devices provide one such route.

4.2. If a security vendor isn't in this 'for the long haul', can you really depend on them?

Because of the ever-changing threat scenario, it's essential that you choose an IT security vendor that is likely to keep on enhancing its corporate security offerings and continuing to deliver a rapid response to new threats and new attack vectors.

While a vendor's previous performance doesn't necessarily guarantee future service levels, it's probably one of the best indications that's available to you. In addition, you should consider the level of financial investment that each vendor makes in ongoing research and development.

Aim to shortlist only the vendors that have a good track record of:

- Developing innovative technologies that deliver additional layers of security
- Consistently being the first – or one of the first – to detect and defend against major new threats
- Winning significant industry awards and accolades

4.3 Impact on performance… long-term supportability… and adaptability

Another area that can be difficult to assess is the actual quality of the code within each security vendor's products. At first sight, this may not appear to be a vital consideration. However, the way in which the code has been developed – and how it has been adapted to include new features – can have a major effect on:

- The performance of the users' mobile devices
- The performance of your central servers
- The vendor's ability to deliver essential new features in the future

Some vendors have sought to add functionality to their basic product by acquiring other companies. While this approach can help vendors to extend the capability of their offerings, it can also result in inefficient code. Often, the vendor's development personnel will have to adapt and rework existing code in order to overcome potential incompatibilities and integration issues. This rarely results in code that is optimised for performance and ongoing flexibility.

By contrast, if you can find a vendor that has developed all of their code in-house, it's likely that the code will be highly optimised for protection that doesn't significantly impact CPU performance. With a 'smaller footprint', the code should help to preserve more of the performance of the employees' devices and the business's servers.

Furthermore – for code that's exclusively developed in-house – when the time comes for the vendor's development team to add new features, there's virtually no likelihood of integration issues. This can often mean that essential new functionality may be delivered to customers much earlier than other vendors can achieve.

Kaspersky Security for Mobile

5.0

Kaspersky Security for Mobile combines Kaspersky Lab's award-winning protection technologies and extensive MDM functionality in one, tightly integrated solution. By giving administrators greater visibility and control over mobile devices that access the corporate network, Kaspersky Security for Mobile makes it easier for businesses to benefit from rigorous, multilayer security and productivity-enhancing management capabilities.

5.1 Zero integration required

Kaspersky Security for Mobile delivers a single solution that combines:

- Mobile security
- Mobile Device Management (MDM)

5.2 Award-winning anti-malware

Kaspersky Security for Mobile protects against viruses, spyware, Trojans, worms, bots and a wide range of other threats. Its hybrid anti-malware approach combines:

- Signature-based protection
- Heuristic Analysis – for proactive detection of new threats
- Web-assisted protection, via the Kaspersky Security Network (KSN) – to respond to emerging threats within minutes instead of hours or days
- Over the Air (OTA) delivery of anti-malware updates – direct from the Kaspersky Security Network to the users' mobile devices
- Anti-spam – that can automatically filter out unwanted calls and SMS messages
- Anti-phishing – to protect users from phishing scams

5.3 Secure containers

Special containers can be set up on each mobile device – so that corporate data and applications are totally separated from the users' personal data and apps. Flexible settings for containers let administrators:

- Restrict data access
- Manage an application's access to device resources – including SMS, camera, GPS, the network and the file system
- Control how data encryption is applied within the container

5.4 Extensive Mobile Device Management (MDM)

With extensive MDM functionality, Kaspersky Security for Mobile makes it easier to manage a wide range of mobile devices and platforms. Management features include:

- Preconfigured installer – automatically generates an installation package based on your chosen policies and settings. The installation package can totally remove the need for any configuration by the user
- Over the Air delivery of security applications to users' devices – via SMS or email. To install the software, the user simply clicks the embedded link
- The ability to track deployment of security on every device – and deny access for any users that have not clicked to install the required security agent
- Support for Active Directory, Microsoft Exchange ActiveSync and Apple MDM – with a single, intuitive-to-use interface
- Backup and Restore of corporate configuration settings

5.5 Support for a wide range of platforms

Kaspersky Security for Mobile gives businesses easy management of security for a wide range of mobile platforms, including:

- Android
- iOS
- Windows Phone
- Windows Mobile
- BlackBerry
- Symbian

5.6. Application Control for Android devices

Kaspersky Security for Mobile gives administrators easy-to-configure control over the launch of applications on mobile devices – using a choice of policies:

- Default Allow – to allow running of all non-blacklisted applications
- Default Deny – to block running of all applications, unless they are whitelisted

Kaspersky is currently the only security vendor that runs its own whitelisting lab.

5.7 Web Control

For the Android platform, Kaspersky Security for Mobile lets administrators filter web access in order to:

- Block access to malicious websites
- Select categories of sites that cannot be accessed from the mobile device, including:
  - Sites with 'adult content'
  - Sports websites
  - Entertainment sites
  - Social networks
  - Online games… and more

5.8 Rooting / Jailbreak detection

When users root or jailbreak their mobile device, it strips away security provisions. Kaspersky Security for Mobile will:

- Detect rooted / jailbroken devices
- Send alerts to the administrator
- Automatically block access to containerised corporate applications

5.9 Enabling Encryption

Kaspersky Security for Mobile provides an easy-to-use interface to the mobile device's on-board encryption function – plus the ability to add a further layer of encryption, via containerisation.

5.10 Preservation of performance

Kaspersky Security for Mobile has been optimised to have minimal impact on the performance of users' devices and your central servers:

- For users' mobile devices:
  - Consumes less than 5% of the mobile device's battery power
  - Uses less than 5% of the mobile device's processor capacity

- For your IT infrastructure:
  - Negligible effect on server performance
  - Small, frequent database updates help minimise the load on servers / devices

5.11 Anti-Theft features

To protect confidential data when a phone is lost or stolen, Kaspersky Security for Mobile provides easy access to the following anti-theft functions:

- Remote locking of missing devices
- Remote find – using GPS, GSM, Wi-Fi and Google Maps
- Remote wiping of data, including:
  - Selective wiping – to wipe only corporate data
  - Device reset – to wipe all data and reset the device to its default factory settings
- SIM Watch – immediately blocks the device if the SIM card is changed, then sends the administrator the device's new phone number… so the administrator can still run the remote blocking, wiping and finding features.

5.12 Single management console – for all functions

Whereas some vendors' mobile security products require the use of several different control consoles, Kaspersky offers a single, integrated console that lets you manage:

- All mobile device security functions on thousands of mobile devices. On a single server, security can be managed for up to 50,000 devices (multiple servers can be used to manage security for larger quantities of devices)
- All Mobile Device Management (MDM) functions – for all supported platforms

In addition, the same Kaspersky console gives easy access to systems management features* and can manage a wide range of other Kaspersky security technologies*, including:

- Security for all other endpoints – including desktops, servers and virtual machines*
- A wide range of systems management functionality*

*Exact functionality depends on the tier of Kaspersky Endpoint Security for Business or Kaspersky Total Security for Business that your company purchases.

5.13 Highly-integrated… in-house developed code

All of Kaspersky's prime technologies have been developed by the company's own in-house experts – so the code that underpins Kaspersky's Mobile Security and MDM technologies is integrated and optimised to help preserve the performance of your devices and systems.

Conclusion

6.0

6.1 Why choose Kaspersky Lab?

Large corporate client-base
Over 250,000 organisations – ranging from large, multinational businesses to government organisations and small and medium-sized businesses – rely on Kaspersky endpoint security solutions.

Every day, 50,000 new endpoints come under Kaspersky protection
Across the world, Kaspersky protects over 400 million endpoints.

Worldwide capability – backed by world-class security experts
Kaspersky operates in nearly 200 countries and employs over 2,500 highly-qualified specialists that are committed to exposing, analysing and neutralising IT threats.

Benefit from a seamlessly integrated solution
Whereas many other security vendors have acquired multiple technologies and then tried to integrate them into a single solution, Kaspersky's solutions are developed by the company's own teams. Kaspersky's fully integrated approach to delivering reactive, proactive and cloud-based protection technologies – plus a wide range of systems management functionality – within a single, in-house developed architecture is unique… and we hold over 220 worldwide patents.

One management console… saves you time and money
Because all of our prime technologies have been developed by our own teams of experts, Kaspersky customers benefit from security that delivers exceptionally deep and intelligent protection… plus the added benefit of Kaspersky Security Center – a single, unified and highly granular security management console that reduces the burden on IT personnel, saves you money and gives you extraordinary visibility across your organisation.

About Kaspersky
Kaspersky Lab is the world's largest privately held vendor of endpoint protection solutions. The company is ranked among the world's top four vendors of security solutions for endpoint users. Throughout its 15-year history Kaspersky Lab has remained an innovator in IT security and provides effective digital security solutions for consumers, SMBs and Enterprises. The company currently operates in almost 200 countries and territories across the globe, providing protection for more than 300 million users worldwide.

Learn more at www.kaspersky.com/business