KASPERSKY lab

GLOBAL
SECURITY
INTELLIGENCE

SECURITY TECHNOLOGIES FOR MOBILE AND BYOD

Essential security technology options for protecting enterprise networks, systems and data

#EnterpriseSec
kaspersky.com/enterprise

CONTENTS

THE MOBILE CHALLENGES

INCREASING THREAT LEVELS

The volume of new malware specifically targeting mobile devices is growing at an exponential rate. New malware attacks are also becoming increasingly sophisticated – as cybercriminals recognise the value of the information that they can steal from mobile devices. While the vast majority of criminals launch attacks in order to generate revenue – 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.

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, as businesses and employees embrace Bring Your Own Device (BYOD) initiatives – where employees use their own mobile devices to perform work tasks – the security risks are significantly increased, so the need for effective mobile security technologies is greater than ever.

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 to enjoy the convenience of BYOD – security and IT departments must ensure that the business is protected against all new mobile security threats.

THE NEW SECURITY ISSUES THAT MOBILE BRINGS

ANOTHER ROUTE FOR MALWARE INTO THE CORPORATE NETWORK

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

THE DANGERS OF MIXING CORPORATE AND PERSONAL DATA ON ONE DEVICE

Whenever personal and corporate data are stored on the same mobile device, there's a potential security risk. Separating corporate data and the user's personal data can help businesses to apply specific security measures to their confidential or business critical information on the device.

If, for example, the device is owned by an employee who leaves the company, separating the data can make it much easier for the business to remove the corporate data from the device without affecting the employee's personal data.

BYOD MEANS EVEN MORE PLATFORMS TO MANAGE

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

- Android
- iOS
- 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.

VULNERABILITIES LEAD TO DATA THEFT

Cybercriminals 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 to corporate systems.

Installing the latest 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.

RISKS IN THE EMPLOYEE'S HOME

A further risk of data theft – from syncing and backup – is 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 loss. Even though the employee may only be interested in backing up their personal files and photos, they could also be unintentionally 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's exclusive whitepaper – Information Security and Legal Compliance: Finding Common Ground by Michael R. Overly, Esq., CISA, CISSP, CIPP, ISSMP, CRISC.

SUPPLEMENTING DEVICE-LEVEL ENCRYPTION

Many mobile platforms include the ability to encrypt data in order to ensure sensitive information cannot be accessed by criminals if the smartphone or tablet is stolen or the information is intercepted. However, there are techniques criminals can use break some encryption algorithms. 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 –to help protect precious data.

LOSS OF A MOBILE DEVICE, COULD MEAN LOSS OF CORPORATE DATA

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

Regardless of how much effort the business devotes to educating its employees about security awareness, some devices are going to be lost or stolen. It's important to have data security remedies in place to cover these eventualities.

ASSESSING THE AVAILABLE MOBILE SECURITY TECHNOLOGIES

ADVANCED ANTI-MALWARE CAPABILITIES

Because anti-malware solutions have been available for many years, some businesses have come to regard them as 'commodity items' – assuming that all anti-malware solutions offer 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, relying on the security vendor regularly updating its database of malware signatures, was sufficient to protect against the fairly unsophisticated threats of the time. Today, signature-based methods cannot provide adequate security against the vast range of new and complex threats that are being released daily. To protect against new and emerging threats, it's important to choose an anti-malware solution that offers a combination of the key components of protection:

Signature-based protection

This is still an important element in a business's defences against malware. But not all vendor solutions deliver the same protection. The effectiveness of each 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 the behaviour of software – 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.

SEPARATING PERSONAL AND CORPORATE DATA

On BYOD devices, it's essential that the user's personal data and applications 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 virtualization

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

However, the virtualization 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 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. 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 applications, the phone may be unable to display the contact information for the incoming call. Because the phone is in use in 'personal mode', the user cannot access contact data that is held in the 'work section' of the phone.

Containerisation

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.

This third technique also 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 – like having to switch between personal and corporate modes in order to access contact information.
- Containerisation delivers an additional layer of security for the corporate data that's stored on the mobile device.
- 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. It is virtually impossible for the average cybercriminal to decrypt data that is held inside a secure, encrypted container.

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 MDM solution and separate anti-malware – from a different vendor – which often required a level of integration by the IT department. Even once it was integrated, a combination of the two products typically meant:

- Using 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 companies running one of the common, standalone MDM products, can expect 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

OVER THE AIR (OTA) PROVISIONING

Some MDM products allow administrators to deliver applications, including business and security programs, remotely via OTA to users' mobile devices.

This can significantly reduce administrative time and effort, saving the business money.

CONTROLLING THE LAUNCH OF APPLICATIONS

Some employees will always have an 'application-centric' attitude towards running a wide range of non-work apps on their mobile devices.

Although many applications present no risk to corporate data, some do cause security issues. It's important to choose a MDM or security solution that gives the administrator control over the launch of applications.

Application Control functions 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. But your choice of policy may depend primarily on the nature of the information that you wish to secure.

CONTROLLING INTERNET ACCESS

'Drive-by' malware attacks, where a user's device can become infected just by visiting an infected web page, are increasing. 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 as well as blocking access to categories of sites that:

- Contain inappropriate content, or
- Are not suitable for the work environment

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 damage if the device attempts 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, or 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 this action, automatically notifying the administrator of a SIM card change and supplying the new phone number. This enables the administrator to run all remote blocking, locating and wiping features despite the change of SIM card.

Additional anti-theft features

Some vendors' mobile security solutions include features that give administrators remote access to additional functions, such as the ability to display a message on the device's screen urging anyone using the device to return it to the employee or the business.

EVALUATING THE 'INVISIBLE FACTORS'

IT'S AN ONGOING BATTLE… FOR ALL SECURITY VENDORS

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

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 to choose an IT security vendor that continuously enhances its corporate security offerings and delivers a rapid response to new threats and new attack vectors in the long term.

While a vendor's previous performance doesn't necessarily guarantee future service levels, it's probably one of the best indicators 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

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 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 to deliver protection without significantly impacting 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.

If code is exclusively developed in-house, when new features are added, there’s virtually no likelihood of integration issues. This can result in essential new functionality being delivered to customers much earlier than when this is not the case.

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, multi-layered security and productivity-enhancing management capabilities.

KASPERSKY SECURITY FOR MOBILE

COMPREHENSIVE

Kaspersky Security for Mobile delivers a single solution that combines:

- Mobile security
- Mobile Device Management (MDM)

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

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

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

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 Mobile
- BlackBerry
- Symbian

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

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

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

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 containerization.

PRESERVATION OF PERFORMANCE

Kaspersky Security for Mobile has been optimised for minimal impact on the performance of users' devices and the business's 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

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.

SINGLE MANAGEMENT CONSOLE – FOR ALL FUNCTIONS

While some vendors' mobile security products require several different control consoles, Kaspersky offers a single, integrated console to 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*

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.

*Exact functionality depends on the tier of Kaspersky Endpoint Security for Business or Kaspersky Total Security for Business

WHY CHOOSE KASPERSKY LAB?

There are many reasons why Kaspersky is trusted and used by enterprises all over the world. Here are just some of them:

- Eugene Kaspersky, our CEO, is the world's foremost, respected, influential security expert.
- We are trusted by and have partnerships with the world's premier law enforcement and government agencies – such as Interpol and CERTS.
- The Kaspersky Security Network, gives us the broadest view of millions of threats from every corner of the world. This intelligence allows us to see and often predict security incidents.
- Our Threat Research and Global Research and Analysis Teams (GReAT) are renowned as leading threat experts – strategically located in 16 countries around the world, providing unparalleled depth of analysis and understanding of all kinds of threats, from common malware, to targeted attacks and the most sophisticated cyber weapons.
- We have a long-standing reputation of making the first and most relevant security discoveries.
- We are the world's largest privately held IT security company whose R&D teams are solely focused on technology quality and innovation, rather than being constrained only by short-term, market-driven profit expectations.
- We are recognised as the industry leader in IT security technologies, demonstrated by the fact that Kaspersky is consistently awarded top scores in more independent tests than any other security software vendor.
- Kaspersky Lab has been identified as a Leader in the three most prominent and influential global analyst vendor assessments (Gartner, Forrester and IDC).

About Kaspersky Lab

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 more than 16-year history Kaspersky Lab has remained an innovator in IT security and provides effective digital security solutions for large enterprises, SMBs and consumers. Kaspersky Lab, with its holding company registered in the United Kingdom, currently operates in almost 200 countries and territories across the globe, providing protection for over 300 million users worldwide.

Learn more at kaspersky.com/enterprise

* The company was rated fourth in the IDC rating Worldwide Endpoint Security Revenue by Vendor, 2012. The rating was published in the IDC report "Worldwide Endpoint Security 2013–2017 Forecast and 2012 Vendor Shares (IDC #242618, August 2013). The report ranked software vendors according to earnings from sales of endpoint security solutions in 2012.