KASPERSKY lab

KASPERSKY SECURITY FOR MOBILE

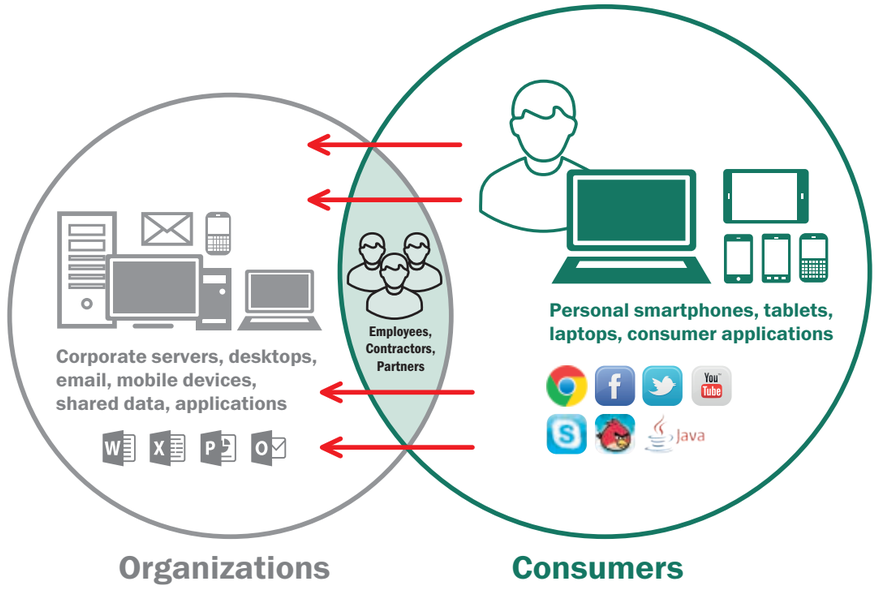
See. Control. Protect.

MOVING TARGETS

Mobile devices play a key role in connectivity and productivity. But they also introduce new risks to the business: in the past 12 months alone, 51 per cent of organizations globally have experienced data loss due to insecure mobile devices[1].

Malware and device loss or theft may seem the most obvious threats, but the trend towards Bring Your Own Device (BYOD) promises almost as many risks as benefits. Seventy-five per cent of employees choose mobile devices without any regard for security or management needs[2]. But unsecured corporate data, mixed with personal applications and files, is easily exploited. Personal devices are often shared between family members, with no regard for application security; some are even rooted or jailbroken.

And who's going to manage all these devices anyway? In today's always-on world, most information workers now use three or more devices for work — at least one of which is a smart device. That's great for productivity, but not so easy on the person tasked with ensuring their control and security.



1 Ponemon Institute, 2012
2 Forrsights Workforce Employee Survey 2012

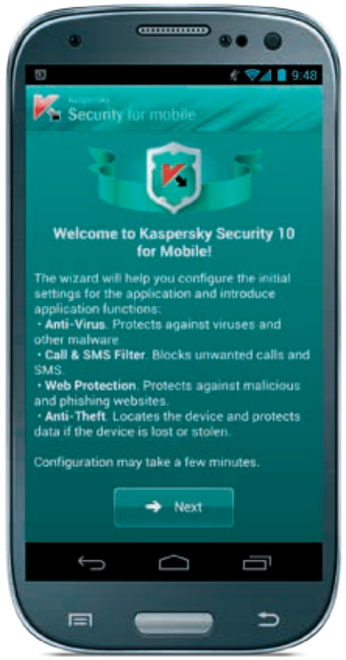
CHOOSING THE RIGHT SOLUTION

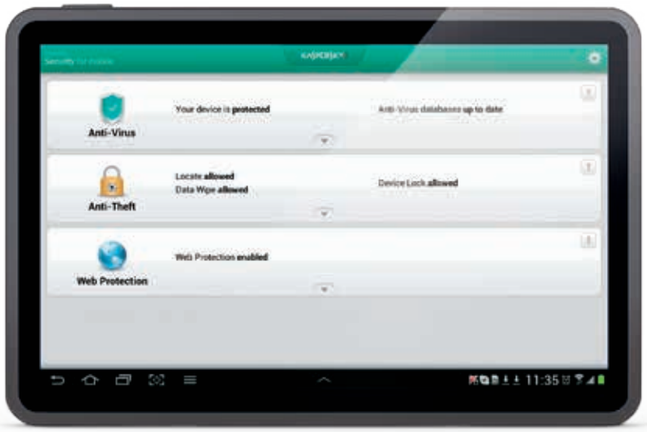
The majority of vendors on the market offer separate solutions for mobile device protection and MDM. Or they offer an additional MDM console to the major corporate IT security solution. Besides the management complexity and additional expense they incur, these solutions have another significant drawback: lack of visibility and centralized control over the mobile devices and data flow can lead to IT security gaps.

You need increased management visibility and security for mobile endpoints — without the complexity of a separate solution. Kaspersky Security for Mobile solves these problems by enabling secure configuration and deployment of smartphones and tablets using the same console as your network security — giving you the confidence that, if lost or stolen, devices are properly configured and secured.

KASPERSKY SECURITY FOR MOBILE

- Allows quick and easy enablement of all popular mobile devices
- Minimizes business risks by protecting corporate data from malware, attacks and other threats, even if the mobile devices is lost or stolen
- Optimizes expenses, providing a single solution for security and management of all mobile devices across the company





BYOD WITHOUT THE HEADACHES

BYOD entails a lot of multiplatform mobile devices. All of them need to be adjusted and protected. But most of all they need to be visible, controlled and managed. Kaspersky Security for Mobile can turn BYOD from a headache into a benefit.

Deploying, managing and securing your mobile IT environment need not be complicated or expensive. Mobile Device Management (MDM) makes secure device configuration painless and straightforward. A mobile agent installed on the device gives all the protection you need — even on employee-owned devices.

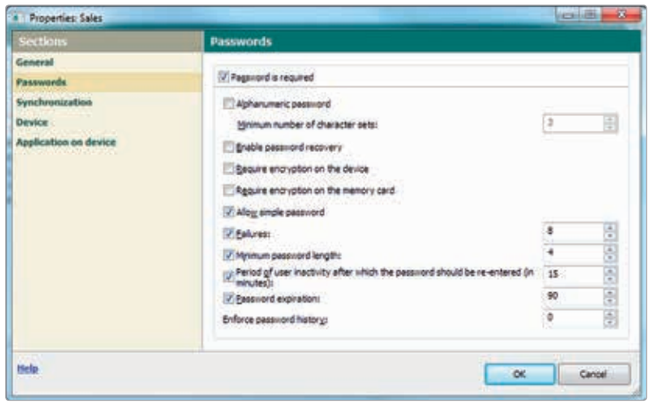
MULTIPLE PLATFORMS & SINGLE CONSOLE

Kaspersky Security for Mobile supports all popular mobile platforms — manage smartphones and tablets from a single console.

Android™ iOS Symbian BlackBerry Windows Phone Windows Mobile

MICROSOFT EXCHANGE ACTIVESYNC AND APPLE MDM SERVER

Kaspersky Security for Mobile fully supports all functionality in Microsoft Exchange ActiveSync and Apple MDM. Administrators can enforce PIN settings, define password complexity, control encryption features, prevent camera usage and manage other related features. Moreover, Kaspersky Security for Mobile can track server connections and save history. There is no need to use separate Exchange and Apple MDM consoles - all actions can be performed from Kaspersky's single management console.



SELF-SERVICE PORTAL

Set up your own corporate portal using Kaspersky Security for Mobile. Upload and deliver your own approved, secure mobile applications — and automate the application installation process, reducing administrator workload.

OTA APPLICATION DEPLOYMENT

Once uploaded, the approved applications and settings can be pushed out to end users via application links or QR codes — all from the Kaspersky Security Center. You get to ensure the security of the device without ever having to physically touch it — users simply install the software and certificates, as well as enable corporate email, themselves.

SEPARATE CORPORATE AND PERSONAL DATA

If you're allowing BYOD, you have to accept that users will engage in usage patterns you don't like: they want to download apps, play games, browse the Internet and share files. When they move to another job, their device (and the data on it) goes with them...

BYOD presents a conflict between the device owner's right to do what they want with their own property, and your company's need to protect its data. Kaspersky's containerization technology resolves this, giving everyone what they want. Here's how:

CONTAINERIZATION

Containerization is a simple solution that completely separates personal and business content on the device — the owner can continue doing whatever he likes with it, there just happens to be a small section within it — a 'corporate container' where your security policies apply.

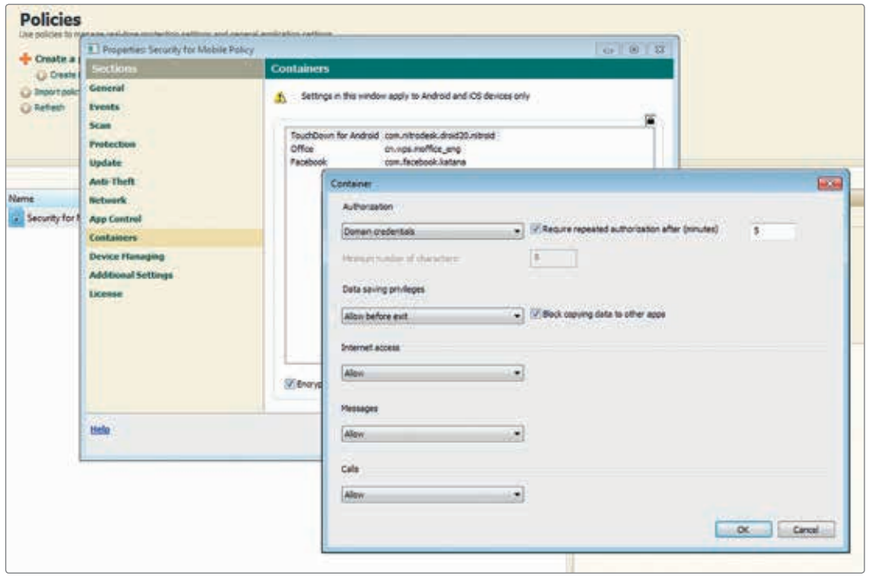
ADDITIONAL CONTAINER PROTECTION

Because the container — and data stored in it — belongs to the company, the administrator can increase its security level. For example, all data in the container can be encrypted; even if the device is lost and someone manages to unlock it, the container will remain encrypted and the corporate data will remain secured.

In addition, end user authorization can be enforced prior to application launch — even if the device is lost when a corporate application is open, data will be protected by an additional password.

WHEN EMPLOYEE IS LEAVING THE COMPANY

When your employee moves on to another company, you can make sure he doesn't take your data with him. Kaspersky Security for Mobile allows you to remote wipe the business container, removing all associated data — leaving the owner's photos, playlists, contacts and other data and settings untouched.



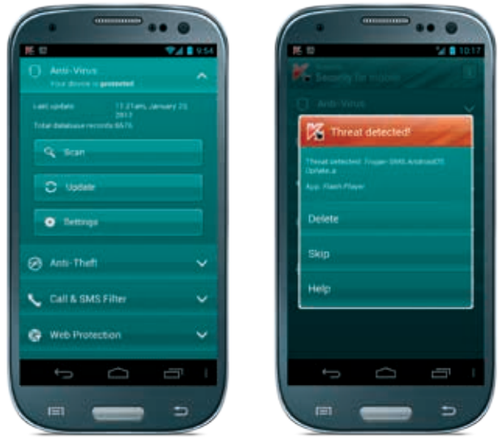
STAY ON TOP OF THREATS

Mobile devices are highly functional. And easy to lose or steal. The increasingly sensitive data they're capable of storing/sharing also has made them attractive to cybercriminals — mobile malware has increased exponentially over the past three years.

Don't make the mistake of believing that your chosen mobile operating system is somehow less vulnerable to threat — social engineering attacks such as phishing can be executed on any device. Mobile device security is just as important as other endpoint protection and should never be overlooked.

ANTI-MALWARE

Kaspersky's award-winning anti-malware technology sits at the core of everything we do. The mobile security technologies include a blended anti-malware solution that combines traditional, signature-based detection with proactive and cloud-assisted technologies, such as Kaspersky Security Network. 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.



ENCRYPTION

Kaspersky Security for Mobile allows you to enable encryption within your corporate data container, making it easy for you to protect sensitive information stored on the device. Even if the device is lost / stolen and then rooted / jailbroken — the data stored in the container remains secure.

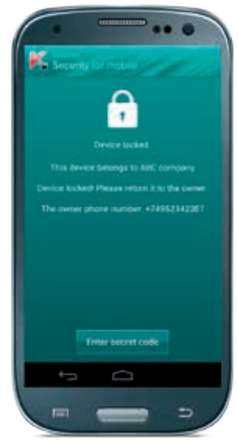
With Kaspersky, it's easy to enforce encryption technologies on the entire user device, providing additional security levels for corporate data.

ANTI-THEFT

Even if a device is lost or stolen, it need not pose any risk to the business; Kaspersky Security for Mobile can remotely block or wipe any sensitive information.

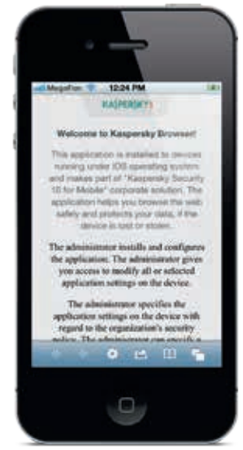
The Anti-Theft functionality includes:

- **SIM control** — lock or wipe a stolen/lost phone, even if the SIM is replaced
- **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 unauthorized access to a device; no need to wipe data



SAFE WEB BROWSING

This is underpinned by Kaspersky Secure Network — our cloud-based service offering constantly-updated reputation analysis, protecting users from phishing and malicious web sites.



KEEP CONTROL

For companies that prefer to retain ownership of mobile devices, Kaspersky offers additional control tools.

COMMON PARAMETERS OF MOBILE DEVICE SECURITY

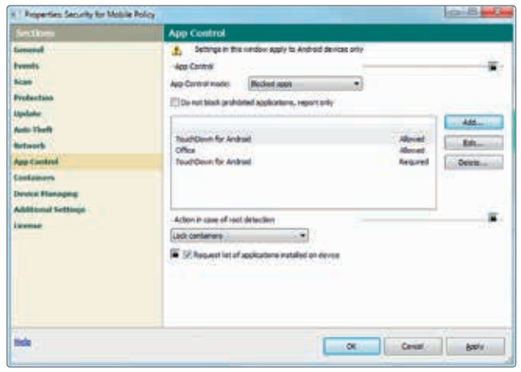
Through the Kaspersky Security Center, administrators can use Microsoft Exchange ActiveSync and Apple MDM plug-ins to, among other things: control the presence and complexity of passwords, enforce whole device encryption, disable the camera or Bluetooth features and so on.

JAILBREAK/ROOTING DETECTION

End users attempting to jailbreak a company-owned device are grounds for suspicion. Such serious IT security violations can be detected by Kaspersky Security for Mobile. In addition to administrator notification, it can automatically perform the following: block containers, selectively wipe corporate data or wipe the whole mobile device.

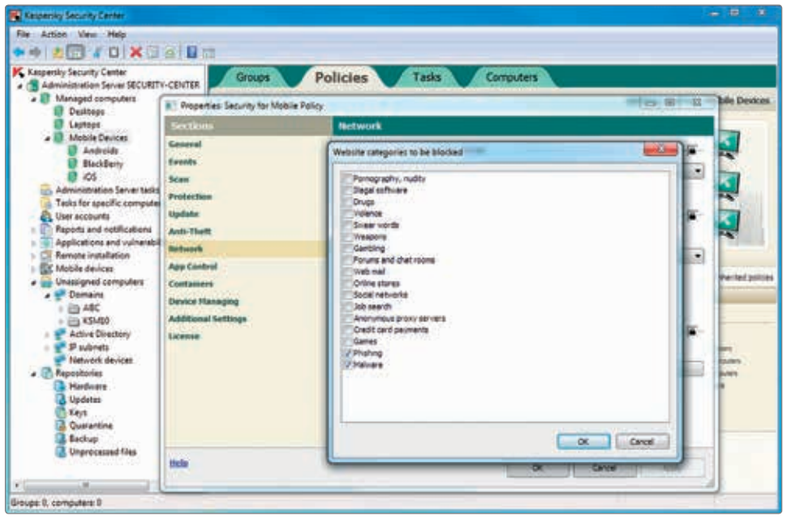
APPLICATION CONTROL

Administrators can manage and restrict application usage to company-approved ones only, while prohibiting the usage of unwanted or grey software. Enforce the installation of selected approved applications, making device functionality dependent on the presence of these. Application inactivity controls allow you to set time limits on how long any application can remain idle before re-log-in is required.



WEB CONTROL

In addition to blocking malicious sites, administrators can control access to sites that don't conform to corporate security or usage policies — e.g. social media, gambling, head hunter, adult, proxy servers or online stores.



TAKING THE PAIN OUT OF MOBILE DEVICE MANAGEMENT AND SECURITY

Now you can get one platform that gives you Mobile Device Management capabilities as well as the world's best anti-malware protection and robust control tools. All in one console and at one cost. It closes the IT security gaps, makes all mobile devices in the corporate network visible and allows you to keep the corporate data flow under control. But this isn't just about you getting separate systems or a suite of products for one price. This is about you getting one, integrated platform that reduces risk to your data, reduces the complexity of your security tools and reduces your investment.

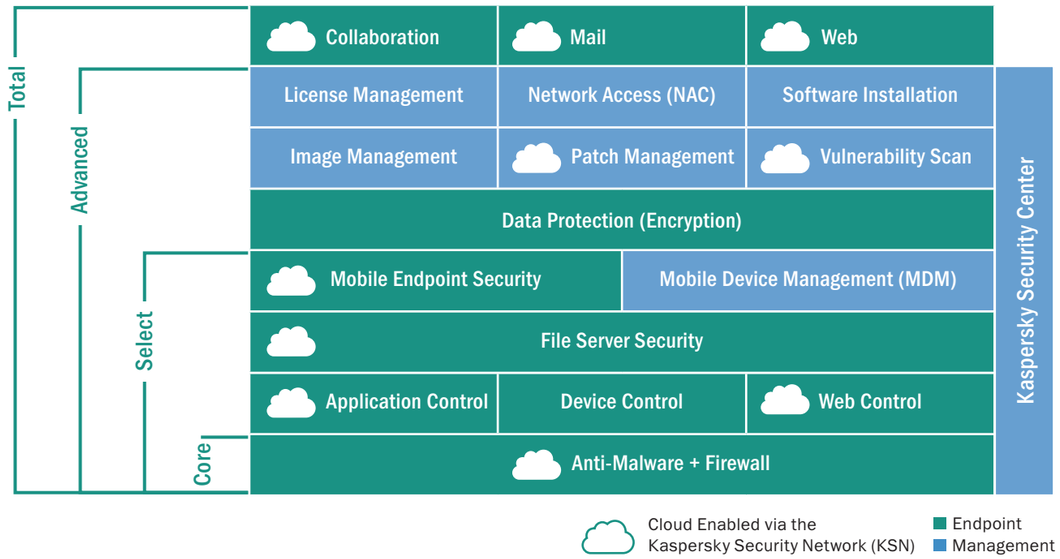
And if your goals are to protect your data, improve your efficiency, and enable and secure mobile users, this is the only way to accomplish all three.

Kaspersky Security for Mobile simplifies mobile device management, centralizing control into one easy-to-use console while providing integrated, real-time protection against threats and data loss.

See. Control. Protect.

LICENSING

Kaspersky Security for Mobile is available as a Targeted Security Solution or as part of Kaspersky Endpoint Security for Business Select, Advanced and Total.



Contact your reseller for details and pricing.
For more information, please consult **www.kaspersky.com**

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

All about Internet security:
www.securelist.com

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

KASPERSKY lab