SECURITY [SNAPSHOT]

Mobile Device Management:

Looking Beyond BYOD

KASPERSKY lab

Mobile Devices: Risks and Rewards

48% of businesses are worried about employees inappropriately sharing company data via the mobile devices that they bring to work.[1]

54% of businesses have had data exposed because employees have lost devices.[1]

48% of cybersecurity incidents were the direct result of employee carelessness, even more than theft of devices, which only contributed to 37% of incidents.[1]

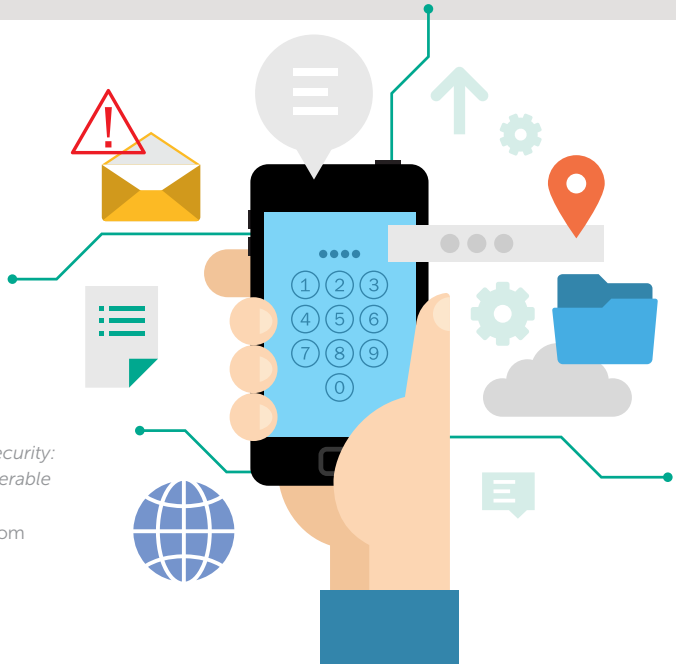
54% of companies do not feel well-protected against inappropriate sharing of data via mobile devices.[2]

53% of companies do not feel well-protected against physical loss of mobile devices.[2]

Mobile technology is changing not only how we work but how we engage with customers. With laptops essentially functioning as portable offices and everything from tablets to phones filling in the gaps, the way we do business has changed fundamentally. More and more companies are responding to the need for mobility with broader Bring Your Own Device (BYOD) policies, which both satisfy employees and cut costs.

The flip side of this is that the very same features that make mobile devices so important to employees also make them attractive to cybercriminals. Because of this, 51% of businesses agree that the increased number of devices used within their organizations makes managing security of those devices more difficult.[2]

For this reason, mobile device management is now about much more than just letting employees bring their own devices. It's about wrapping your entire network of portable devices in security that balances what employees need to do their jobs with what companies need to keep their data secure.



1. Kaspersky Lab's *The Human Factor in IT Security: How Employees are Making Businesses Vulnerable from Within*
2. *Corporate IT Security Risks Survey 2016* from Kaspersky Lab and B2B International

Choosing the Right Mobile Security Solution

There's no doubt that more and more companies are facing the need for a mobile security solution, but the task of implementing new security policies and technology—or even updating them—can be daunting.

No matter what the size of your organization, there are certain key factors you need to consider first. We recommend approaching the issue from four parts of the mobile device management (MDM) landscape:

- Users
- Devices
- Programs
- Infrastructure

Given the fact that 40% of businesses report that employees hide a security incident when it happens, it's important to start with what is always the weakest link in any security plan—your **users**. Ask your employees the following questions:

- How do they commonly use their devices?
- What data do they need to access?
- What are the needs of different departments?
- What privileges should various employees have on your network?
- Who can do what and where?
- What will you do when a device is lost or stolen?

Takeaway:
As always, it's important to know how your employees are using their devices. Salespeople may have completely different needs from your Finance staff. By understanding who does what and where, you can start to get a more complete picture of your mobile landscape.

When looking at **devices**, there are other considerations, such as:

- What kind of devices do employees need to use the most? What kinds of devices will you allow?
- How will each mobile device be deployed?
- What security constraints do you need to enforce to line up with your organization's business needs?

Takeaway:
The devices you allow in your organization will determine a large part of your security policy. Make sure they reflect not only employees' needs and wants but what customers will probably ask for.

After you determine the issues related to your users, it's important to move outside the organization to look at **programs**:

- What apps and programs do your employees need to do their work? Which ones do customers need?
- What are risky programs or apps that you want to block?

Takeaway:
You can't always get what you want. It's important to strike that balance between what employees want to use and what keeps your organization secure. Keeping out some apps and programs entirely will be a necessary part of your security structure.

Then it's time to look at the big picture of your entire **infrastructure:**

- How will the IT department manage and support mobile needs?
- What flexibility do you need to build in to allow for more devices and more apps and services that haven't even been invented yet?

Takeaway:
Change is one of the only constants on the IT landscape. Make sure you build enough flexibility into your plan to account for the inevitable growth and change both in your organization and in the world of technology.

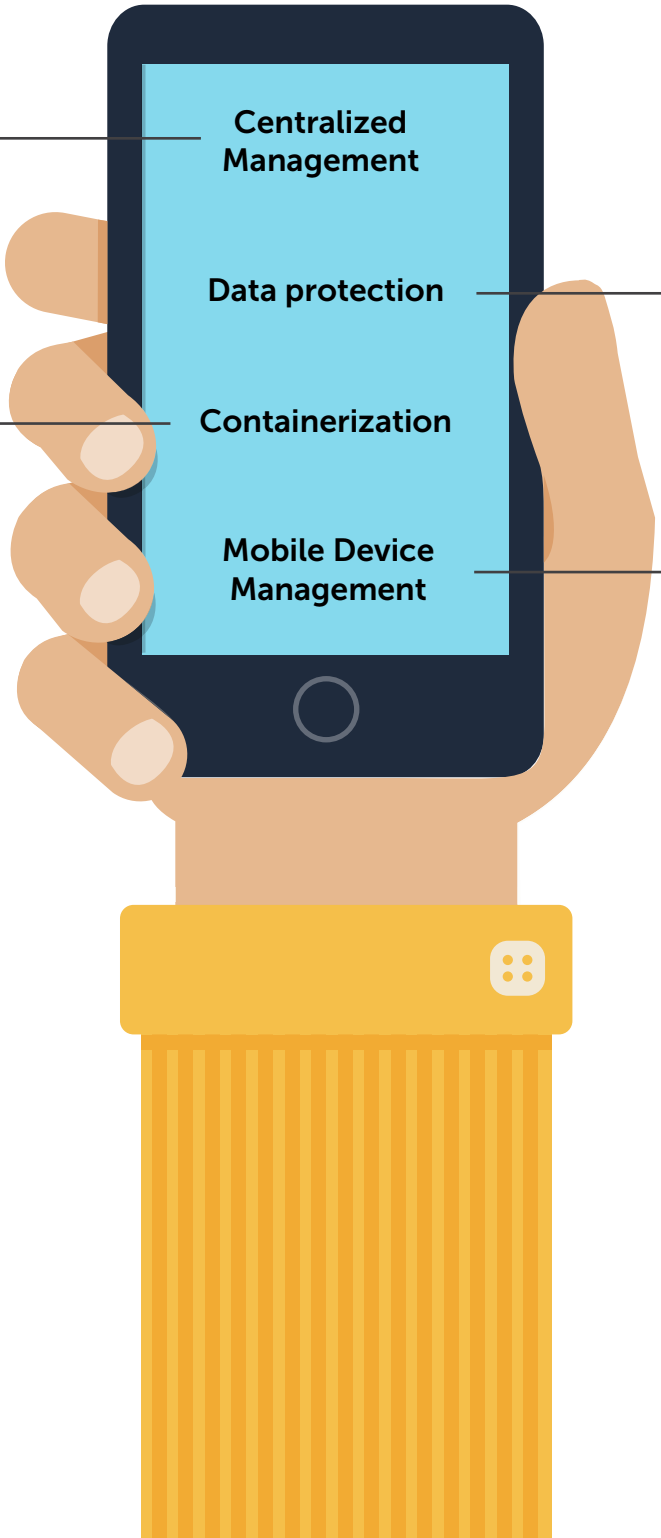
Kaspersky Security for Mobile

Kaspersky Security for Mobile ensures that the devices within your network are safe, no matter where they are, protecting them against constantly evolving mobile malware. Our **solution** allows you to gain visibility and control over the smartphones and tablets in your environment quickly and easily, from one central location and with minimal disruption.

Advantages of our Mobile Device Management product:

Kaspersky Security for Mobile allows you to manage mobile devices from the same console as other endpoint platforms: Kaspersky Security Center or Kaspersky Endpoint Security Cloud. View data on devices, create and manage policies, send commands to devices and run reports – all from one easy-to-manage, central console.

Containerization enables the separation of business and personal data on the same device. Business data stored in protected containers can be encrypted, password protected and further secured against malware. Selective wipe facilitates BYOD.



Protection of the user's personal and corporate data. If necessary, emergency response measures can be taken to prevent compromised devices from accessing company data or locking them remotely.

Set up and enable rules for passwords, encryption, Bluetooth and camera, as well as group policies for Android, iOS and Windows Phone. Run reports on the device and applications installed. Integration with all leading mobile device management platforms enables remote 'Over the Air' (OTA) deployment and control for easier usability and management of supported devices.

True Cybersecurity for Business

Kaspersky Lab's True Cybersecurity approach combines multi-layered security with cloud-assisted threat intelligence and machine learning to protect against the threats your business faces. True Cybersecurity not only prevents attacks, but also predicts, detects and responds to them quickly, while also ensuring business continuity for your organization.

Get Your Free Trial Today >

Join the conversation

Like us on Facebook

Follow us on Twitter

Join us on LinkedIn

Watch us on YouTube

Review Our Blog

About Kaspersky Lab

Kaspersky Lab is one of the world's fastest-growing cybersecurity companies and the largest that is privately-owned. The company is ranked among the world's top four vendors of security solutions for endpoint users (IDC, 2014). Since 1997, Kaspersky Lab has been an innovator in cybersecurity and provides effective digital security solutions and threat intelligence for large enterprises, SMBs and consumers. Kaspersky Lab is an international company, operating in almost 200 countries and territories across the globe, providing protection for over 400 million users worldwide. Learn more at usa.kaspersky.com.

Contact Kaspersky Lab today to learn more about Kaspersky Endpoint Security for Business and our other IT security solutions and services:
usa.kaspersky.com/business-security

usa.kaspersky.com
#truecybersecurity

AO Kaspersky Lab
500 Unicorn Park, 3rd Floor Woburn, MA 01801 USA
Tel: 866-563-3099 | Email: corporatesales@kaspersky.com