

GLOBAL
SECURITY
INTELLIGENCE

YOUR DATA UNDER SIEGE:
DEFEND IT WITH
ENCRYPTION



CONTENTS

Your Data Under Siege: Defend it with Encryption	3
Steps Taken to Minimise Risk	5
Full Disk Encryption (FDE)	6
File Level Encryption (FLE)	8
About Kaspersky Lab	11

YOUR DATA UNDER SIEGE: DEFEND IT WITH ENCRYPTION

Keeping pace with the business demands of the enterprise can be a daunting task for IT Managers. Continually asked to do more with less, you're under pressure to implement new technologies to improve productivity and efficiency and cut costs – all while facing a growing threat from cybercrime. As if that's not enough, your workforce has become mobile – leaving the protective confines of the enterprise. A mobile workforce can make an IT department feel as if it's under siege.

According to the Ponemon Institute, 62 per cent of enterprise employees are mobile and by 2015, that figure is expected to rise to 85 per cent. As the workforce becomes more mobile, so does proprietary enterprise information, increasing the risk of data loss or theft. The robust perimeter security you put in place to protect enterprise systems and networks is no longer effective; data is no longer safe as it moves around the globe. No wonder 80 per cent of enterprise IT professionals believe that laptops and other data-bearing mobile devices pose a significant threat to enterprise networks and systems.¹

According to a study conducted by Intel, 5 to 10 per cent of all laptops will be lost or stolen within their life span. **Think about how much of your workforce is already mobile and consider this: an average of 63 per cent of them use mobile devices to access and use data in the enterprise.**

- An average of 50 per cent use them to access regulated data.
- 63 per cent of mobile data-bearing devices that are lost or stolen contain sensitive or confidential information.
- A laptop is stolen every 53 seconds.
- 63 per cent of breaches occur as a result of the use of mobile devices, including theft and unauthorised use in the workplace.²

The explosion in enterprise mobility means your proprietary corporate data is at substantial risk.

If your response to device loss or theft is to consider the cost of replacing the hardware, you're focusing on the wrong problem. Ponemon research suggests that the average cost of a lost or stolen laptop is \$49,246, with only two per cent accounting for hardware replacement costs. Eighty per cent of the cost goes to cleaning up the data leakage mess, regardless of the size of the business.

Kaspersky research has found that the average cost to the enterprise of a single serious data breach is \$649 000.³

1 & 2. Ponemon Institute, 2013 State of the Endpoint, December 2012

3. Kaspersky Lab, Global Corporate IT Security Risks: 2013, May 2013

ENCRYPTION IS AMONG THE MOST PROMISING TECHNOLOGIES FOR REDUCING THE RISK OF CRITICAL DATA LEAKAGE, BUT IT'S AT ITS MOST EFFECTIVE WHEN INCORPORATED INTO A COMPREHENSIVE SECURITY SYSTEM FOR CORPORATE IT INFRASTRUCTURE

NIKOLAY GREBENNIKOV,
CTO, KASPERSKY LAB

Factor in the ever-increasing range of government fines for data breaches, reputational damage and lost customer loyalty, and it's easy to see how the cost of losing a laptop spreads well beyond hardware replacement.

In an increasingly mobile world, enterprise intellectual property, sensitive data, and networks and systems are no longer protected by perimeter security alone. If a device is lost or stolen, the data on that device is vulnerable to theft as well, making the device a primary target for criminals. How do you protect mobile data from theft, even if the device is stolen?

THE SIMPLE ANSWER IS: ENCRYPTION!

Encryption is the process of encoding information in such a way that only authorised users can read it. In an encryption scheme, information (plaintext) is encrypted using an encryption algorithm, turning it into unreadable ciphertext. This process usually takes place with an encryption key, which specifies how data is to be encoded.

Unauthorised users may be able to see the ciphertext, but will not be able to discern anything about the original data. Authorised users, on the other hand, can decode the ciphertext using a decryption algorithm that usually requires a secret decryption key to which only they have access. An encryption scheme usually needs a key-generation algorithm to randomly produce keys.

Gartner suggests that the cost of a data breach from a lost or stolen laptop can be 70 times greater than the cost of enterprise-wide encryption,⁴ yet Kaspersky research has found that 35 per cent of enterprises are exposing their data to unauthorised access by failing to use encryption technologies.⁵

Whatever the reasons driving them, enterprises must protect their data, intellectual property and reputation. Enterprises of all functions and sectors are increasingly turning to encryption as both a pre-emptive information security measure and regulatory compliance strategy.



















There are two types of encryption that can be deployed, either independently or together: full disk encryption (FDE) and file level encryption (FLE). Kaspersky research has found that 40 per cent of enterprises are implementing FLE, with 39 per cent opting for FDE; some 33 per cent of enterprises have adopted encryption for removable media.

4. Gartner analyst John Girard, interview with Fierce Mobile IT, October 25, 2012. <http://www.fiercemobileit.com/story/laptop-data-breach-can-cost-70-times-more-firm-wide-encryption/2012-10-25>, October 25, 2012

5. Kaspersky Lab and B2B International, Global IT Risk Report: 2013, May 2013

STEPS TAKEN TO MINIMISE RISK

Kaspersky research shows that enterprises are increasingly turning to encryption as part of an effective, pre-emptive data loss prevention strategy.

Anti-Malware protection (Anti-virus, Anti-spyware)		71%	4%
Regular patch/software update management		54%	-9%
Implementing levels of access to different IT systems by privilege		52%	4%
Network structures (e.g. separation of mission-critical networks from other networks)		50%	3%
Application control (i.e. only allowing approved programs to run on devices)		45%	N/A
Policy for dealing with IT security at remote branches/offices		44%	4%
Device control (i.e. control of peripherals able to be connected to devices)		41%	N/A
Anti-malware agent for mobile devices		40%	N/A
File and folder encryption		40%	N/A
Encryption of all stored data (i.e. full-disk encryption)		39%	2%
Separate security policy for notebooks/laptops		38%	3%
Separate security policy for removable devices (e.g. USBs)		37%	0%
Encryption of business communications		37%	-1%
Auditing/verifying the IT security of third party suppliers		36%	0%
Client Management (PC Life Cycle Management)		34%	-1%
Encryption of data on removable devices		33%	2%
Separate security policy for smartphones/tablets		32%	0%
Mobile device management (MDM)		31%	-2%

N/A issues are new for 2013

Chart shows % of organisations that have fully implemented different security measures

Significantly lower YOY

Significantly higher YOY

FULL DISK ENCRYPTION (FDE)

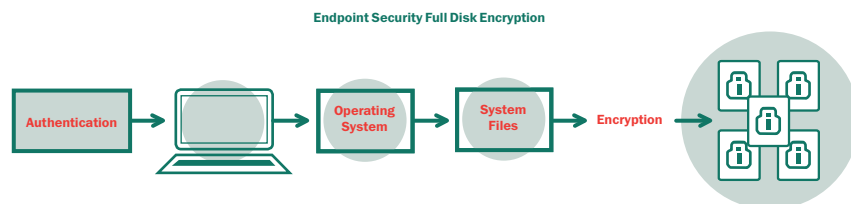
Full disk encryption (FDE) technology is one of the most effective ways any enterprise can protect its data from theft or loss. Regardless of what happens to a device, FDE allows organisations to ensure that all sensitive data is completely unreadable and useless to criminals or prying eyes.

FDE encrypts data at rest (i.e. all the data on the hard drive) from boot-up to the operating system and other installed hard drives. Essentially, every single file (including temporary files) on every single sector on the disk is encrypted. Only authenticated users can access the system, using a password, token or a combination of these. This technology can also be applied to removable media, such as USB drives. FDE supports a variety of setups and can be managed and monitored by systems administrators.

FDE uses a pre-boot scheme to operate. This means it can protect data within seconds of the power button being pressed on any device. The software encrypts all selected drives and installs an authorisation module in the boot environment. When a computer is started up, the operating system will automatically load in an encrypted environment, so encryption is enforced with almost no impact on the performance of the computer.

All encryption and decryption activity runs routinely and transparently to the end user, regardless of the software being used. Read/write operations run in this fully protected environment. Everything on the hard drive is secured, from swap space to system, page, hibernation and temporary files, which can often contain important confidential data. In the event of password loss, information can still be decrypted using private keys known only to the system administrator. FDE-enabled mobile devices can significantly reduce the risk of data breach caused by loss or theft.

FDE functionality is included in Kaspersky Endpoint Security for Business. Systems administrators can manage it centrally from the Kaspersky Security Center management console.



FULL DISK ENCRYPTION BRINGS NUMEROUS BENEFITS TO IT SECURITY:

- **Enable enforced encryption of sensitive data:** FDE removes the decision to encrypt from the end user. All files on the hard drive are automatically encrypted and password protected, including temporary files, which often contain sensitive data. There is no opportunity for end-user override.
- **Security:** FDE prevents unauthorised data access by using a login/password mechanism. When the correct login/password is presented, the system retrieves the key required to decrypt files on the hard drive. This adds an extra layer of security because data can be rendered useless immediately following the destruction of the cryptography key.
- **Centralised key management:** Encryption keys can be stored in a central location accessible only to the security administrator.
- **Centralised encryption management:** FDE systems allow all functions to be managed from a central location within the enterprise. This includes functions such as decryption key management; access control to mobile devices, lockouts, if necessary, reporting, and recovery of lost passwords.
- **Simplicity and flexibility:** FDE systems allow end-user transparency and fully automated functionality. Following successful authorisation, the encryption/decryption process takes place transparently and has no impact on user experience.
- **Centralised data recovery:** In case of lost password or damage to the data carrier, data can still be recovered and decrypted using a special centrally managed emergency recovery procedure.

While FDE does provide ample protection for data on lost or stolen devices, it does not protect data in transit – data as it is being shared between devices electronically, such as email. For this reason, many enterprises often implement file level encryption.

FILE LEVEL ENCRYPTION (FLE)

USING FLE, INDIVIDUAL FILES OR DIRECTORIES ARE ENCRYPTED BY THE FILE SYSTEM ITSELF. THIS IS IN CONTRAST TO FULL DISK ENCRYPTION, WHICH ENCRYPTS THE ENTIRE PARTITION OR DISK IN WHICH THE FILE SYSTEM RESIDES. FLE DOESN'T ENCRYPT ALL THE INFORMATION ON THE HARD DRIVE OR PORTABLE MEDIA DEVICE AS FDE DOES

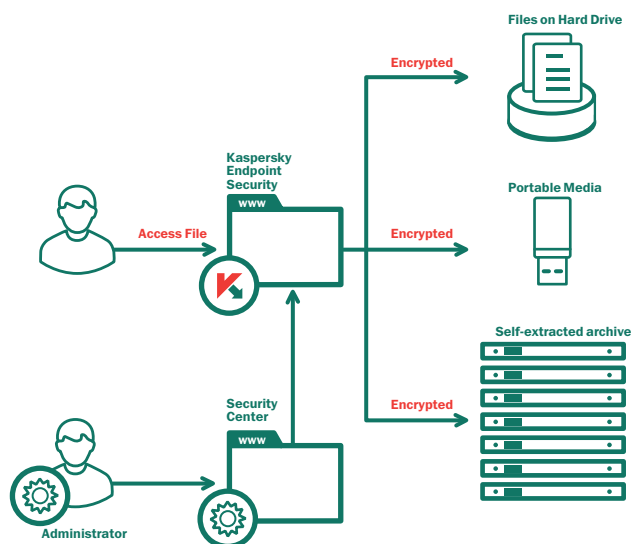
File level encryption (FLE) enables the encryption of data in specific files and folders on any given device. This makes selected information unreadable to unauthorised viewers, regardless of where it's stored. FLE allows system administrators to automatically encrypt files based on attributes such as location and file type.

Using FLE, individual files or directories are encrypted by the file system itself. This is in contrast to full disk encryption, which encrypts the entire partition or disk in which the file system resides. FLE doesn't encrypt all the information on the hard drive or portable media device as FDE does. It does, however, allow administrators to choose which data should (or should not) be encrypted, using rules that are easily implemented through a user-friendly software interface.

FLE technology allows system administrators to fully customise which files should be encrypted. This can be done manually or automatically; some solutions provide specially pre-configured tools that enable files to be encrypted easily, quickly and reliably. Granular information access policies are easily applied. For example, administrators may wish to automatically enforce encryption for financial spreadsheets but not more general ones. Encryption rules can be customised to decide what should be encrypted and when, as in the examples below:

- **Files on local hard drives:** Administrators could create lists of files to encrypt by name, extension or directory.
- **Files on portable media:** Create a default encryption policy to enforce encryption for all portable media devices. Apply the same rules to every device, or go granular and create different rules for different devices.
- **Choose what to encrypt:** FLE supports the application of different encryption rules for different situations. For example, you can choose to encrypt all files on portable devices, or new files only. You could also enable portable encryption mode to work on encrypted files being used on PCs that don't have Kaspersky Endpoint Security for Business installed.
- **Application files:** Automatically encrypt any files that are created or changed by any application.
- **Self-extracted encrypted archives:** Files added to self-extracted encrypted archives that could be decrypted with a password on PCs that don't have Kaspersky Endpoint Security installed.

FILE ENCRYPTION IS TRANSPARENT, MEANING THAT ANYONE WITH ACCESS TO THE FILE SYSTEM CAN VIEW THE NAMES (AND POSSIBLY OTHER METADATA) FOR THE ENCRYPTED FILES AND FOLDERS, INCLUDING FILES AND FOLDERS WITHIN ENCRYPTED FOLDERS IF THEY ARE NOT PROTECTED THROUGH OS ACCESS CONTROL FEATURES. FILE/FOLDER ENCRYPTION IS USED ON ALL TYPES OF STORAGE FOR END-USER DEVICES



File encryption involves encrypting individual files on any storage medium, only permitting access to encrypted data once the correct authentication has been provided. Folder encryption involves the application of the same principles to individual folders rather than specific files.

File encryption is transparent, meaning that anyone with access to the file system can view the names (and possibly other metadata) for the encrypted files and folders, including files and folders within encrypted folders if they are not protected through OS access control features. File/folder encryption is used on all types of storage for end-user devices.

File encryption is implemented via a driver-based solution with a special crypto module that intercepts all file access operations. When any user attempts to access an encrypted file (or a file located in an encrypted folder), FLE software checks that the user has been authenticated or opens a password dialogue box in the case of a self-extracted encrypted archive. Once authenticated, the software automatically decrypts the chosen file.

Because FLE decrypts a single file at a time, performance impact is minimal. File/folder encryption is most commonly used on user data files, such as word processing documents and spreadsheets. FLE solutions can't encrypt OS execution or hibernation files.

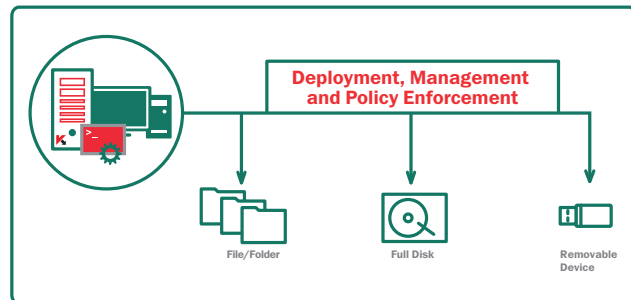
FLE delivers many benefits to IT security:

- **Flexibility:** “What and where to encrypt” custom rules (files, extensions and directories) can be created and applied to different use cases and requirements.
- **Portable media support:** Create special encryption rules for all portable media devices connected to the PC/laptop. Apply the same rules across the board or choose custom options for each unique device.
- **Transparent software encryption:** Encrypt data that is created or changed by any other software operating on the hard drive. Define access rights to encrypted files on a per-application basis or allow ciphertext-only access to encrypted files.
- **Central management:** All FLE functions can be managed from a central location, including functions such as rules management, rights management and key management.

Protect your data simply and securely with Kaspersky Encryption Technology

- FULL DISK
- FILE/FOLDER LEVEL
- REMOVABLE AND INTERNAL DEVICES

ADMINISTERED THROUGH A SINGLE MANAGEMENT CONSOLE.



SUMMARY

There's no need for today's mobile workforce to bring additional challenges as you attempt to secure enterprise data. Encryption is a logical way to secure data on vulnerable mobile devices, but can bring additional management and resource challenges. One simple way to avoid this is to implement encryption as part of a single security platform that combines fully integrated technologies and tools, such as robust anti-malware, control tools, systems management, mobile device management and encryption, into one easily managed solution. This enables complete visibility of the risks across all enterprise devices, delivered at one cost and managed from one console.

Kaspersky Endpoint Security for Business (KESB) delivers robust data protection across all devices from one console, driving down complexity and reducing the risks to your enterprise. In addition, the Kaspersky Security Network, together with our world-renowned Threat Research and Global Research and Analysis Teams (GReAT), 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, helping enterprises achieve better protection and a more pro-active stance on IT security. We focus our efforts on solving global IT security challenges – from critical infrastructure protection, enterprise mobility and secure virtualization to fraud prevention and security intelligence services.

Kaspersky never stops anticipating and preventing IT security threats - reducing enterprise risk today and in the increasingly complex future.

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.
