# Kaspersky Lab's File Level Encryption Technology

## The case for encryption

According to the Privacy Rights Clearinghouse, more than 567 million records have been compromised since 2005. In the first six months of 2012 alone, almost 14 million records were breached.[1] It seems that hardly a week goes by without news of a major data loss hitting the headlines. That's not surprising when you learn that 88 percent of organizations surveyed by the Ponemon Institute admitted to having had at least one data breach over the previous 12 months.

It's not just about the high costs of a breach (estimated at $5.5m in the US in 2011), the loss of loyal customers or the damage to your company's reputation. In most major markets, data security and privacy are now mandated by law, with many jurisdictions obliging organizations to encrypt sensitive data. In the US, for example, the State of California initiated what's become a widespread move towards obligatory encryption for any organization that uses and retains personally identifiable customer data. In the UK, the Information Commissioner's Office (ICO) has stated that data losses that occur "where encryption software has not been used to protect the data" are likely to result in regulatory action. The US Federal Trade Commission (FTC) has the authority to impose an annual 20-year audit on organizations that experience a breach but are found not to have had adequate data protection measures in place.

The Ponemon Institute has found that 75 percent of organizations implement security solutions after a data breach. Seventy percent of those organizations select encryption as their preventative measure of choice. Whatever the reasons driving them, businesses must protect their data, intellectual property and reputation. To do this, organizations of all sizes are increasingly turning to encryption as both a pre-emptive information security measure and regulatory compliance strategy.

## What is encryption?

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

Unauthorized users might be able to see the ciphertext, but will not be able to discern anything about the original data. Authorized users, on the other hand, can decode the ciphertext using a decryption algorithm that usually requires a secret decryption key. An encryption scheme usually needs a key-generation algorithm, to produce random keys.

File Level Encryption (FLE) is one of the most popular technologies that organizations are using to protect their data from unauthorized use, while mitigating the risks associated with data loss.

[1] Source: Identity Theft Resource Center 2012

# Kaspersky Lab's File Level Encryption (FLE)

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

In Kaspersky's FLE, individual files or directories are encrypted by the file system itself. This is in contrast to Full Disk Encryption (FDE) – where the entire partition or disk, in which the file system resides, is encrypted. Unlike FDE, FLE doesn't encrypt all the information on the hard drive or portable media device. It does, however, allow administrators to choose exactly what data should be encrypted (or not encrypted), using rules that are easily implemented through a user-friendly software interface.

FLE technology allows system administrators to customize which files should be encrypted. This can be done manually or automatically. Using specially preconfigured tools in Kaspersky Security Center, files can be encrypted easily, quickly and reliably. Granular information access policies are easily applied – for example, administrators may wish to enforce automatic encryption for financial spreadsheets but not for other types of spreadsheets. Encryption rules can be customized to decide what should be encrypted and when, for example:

- **Files on local hard drives:**
  Administrators could create lists of files to encrypt by name, extension or directory.

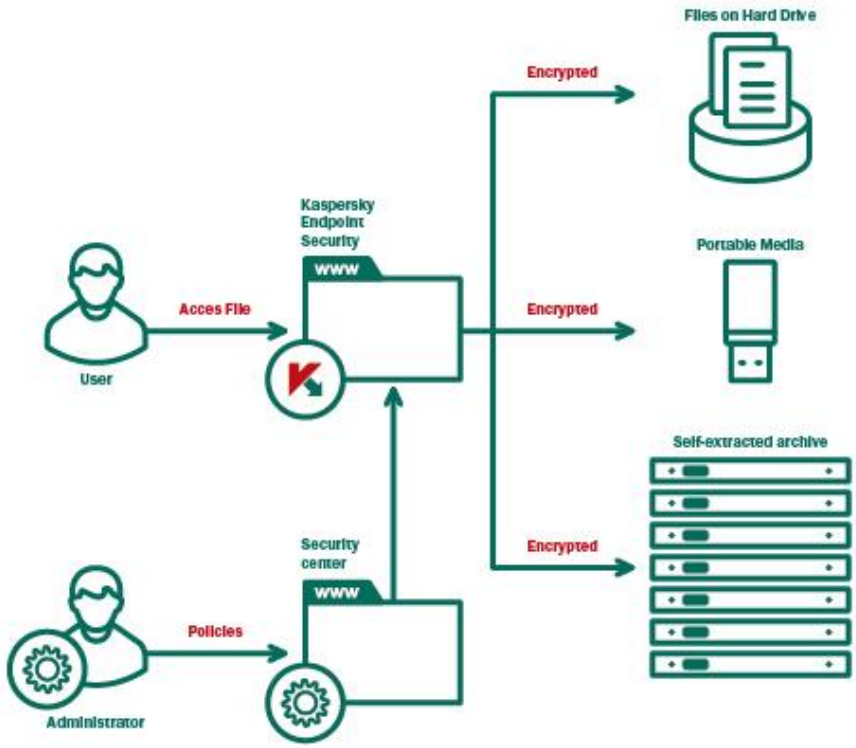
- **Files on portable media:**
  Create a default encryption policy to enforce encryption for all portable media devices. Apply the same rules to every device, or create different rules for different devices.

- **Choose what to encrypt:**
  FLE lets you apply different encryption rules in different situations – for example, you can choose to encrypt all files on portable devices, or only encrypt new files. You could also enable the portable encryption mode to work on encrypted files that are being used on PCs that don't have Kaspersky Endpoint Security 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.

Kaspersky Lab's FLE functionality scheme




Kaspersky's File Level Encryption involves encrypting individual files on any storage medium, and only permitting access to encrypted data after the correct authentication has been provided. Folder encryption applies the same principles to individual folders, rather than specific files.

File encryption is transparent. 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 Level 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, in the case of a self-extracted encrypted archive, the software will open a password dialog box. After the user has been authenticated, the software automatically decrypts the chosen file.

Because FLE decrypts a single file at a time, impact on performance 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 executables or hibernation files.

Kaspersky's FLE technology offers several options for selecting which files and folders should be encrypted. It also supports role-based rules – according to user needs and roles, encryption can be manually enabled for specific files and folders or automatically enforced, with no end-user input.

Common options include:

- Using the Kaspersky Security Center, the administrator can designate which files and folders are to be encrypted
- Automatically encrypting the contents of administrator-designated folders
- Automatically encrypting certain types of files, such as those with a particular file extension
- Automatically encrypting all files written to by particular applications
- Automatically encrypting all different data files for particular users.

## Kaspersky Lab's FLE technology uses the following cryptographic algorithms for encryption:

- AES 256 CBC/XTS/CFB8 symmetric encryption for encrypting files content, keys and self-extracted crypto containers.
- AES 56 CBC/XTS/CFB8 symmetric encryption for encrypting files content, keys and self-extracted crypto containers.

## FLE Advantages

- **Flexibility**:
  "What and where to encrypt" custom rules (files, extensions and directories) can be created and applied to different cases and requirements.
- **Portable media support**:
  Creates 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**:
  Encrypts data that is created or changed by any other software. Defines access rights to encrypted files, on a per-application basis, or allows cipher text-only access to encrypted files.
- **Central management**:
  All FLE functions can be managed from a central location via Kaspersky Security Center, including functions such as rules management, rights management and key management.

## Availability

Kaspersky's File Level Encryption technology is available in Kaspersky Endpoint Security 10 and is fully integrated with Kaspersky Security Center.