KASPERSKY lab

Protecting Sensitive Data with Kaspersky Encryption Technology

These days, we are seeing a constant increase in the number of cyberthreats, including targeted attacks against companies and industrial espionage. Protecting confidential information is a clear priority for businesses of all sizes. In order to resolve data security issues, it is important not only to counteract malicious programs and attacks on the corporate network, but also to prevent data leaks caused by improper employee conduct. That is why reliable security for a company's IT infrastructure must include an anti-malware solution, specialized security policies and a means of data encryption. Data encryption technologies, in particular, serve as the last line of defense and safeguard corporate data.

Encryption is one of the most in-demand security technologies. According to the results of a study conducted by Kaspersky Lab and B2B International in 2014, 33% of companies use encryption technology on workstations and 32% encrypt data stored on removable drives. These numbers demonstrate the prevalence of the two most effective data protection technologies: File and Folder Level Encryption (FLE) and Full Disk Encryption (FDE). These technologies are both designed to achieve the same goal, but use different approaches to do so. The Kaspersky Endpoint Security for Business platform from Kaspersky Lab offers clients both technologies depending on their business activities.

How encryption works

Encryption is a process by which "open" data is transformed into "closed" data, at which point it is protected against unauthorized access. The two key encryption technologies available today — FLE and FDE — tackle completely different but equally important tasks. The first protects critical data and restricts access to it, while the second rules out the possibility of any important data falling into the hands of third parties, even if a data storage device holding valuable information is lost or stolen. By using these technologies within the Kaspersky Endpoint Security for Business platform, system administrators have complete freedom to encrypt data in any volume or scope, from one file or folder to an entire hard drive, customizing automatic encryption, and so on.

The management of encryption on employee workstations is performed centrally via the unified management console Kaspersky Security Center. This supports a number of features to make life easier for system administrators, including a Role-Based Access Control function that allows for the distribution of responsibilities among several specialists. In particular, control of the Encryption settings can be delegated to the dedicated administrator. From the console, an IT specialist can track the status of encryption processes on each computer and manage every aspect of the process — even allowing or denying access to the encrypted data for specific applications.

To speed up the performance of the solution, Kaspersky Lab's Encryption technology supports the Intel Advanced Encryption Standard Instruction Set, or AES-NI. This instruction set serves to speed up the applications performing encryption and decryption using the Advanced Encryption Standard (AES).

File and folder level encryption

File and Folder Level Encryption (FLE) is used to secure critical files and folders located on a computer's hard drive or an external drive. If a company has a considerable number of workstations, selecting files or folders for encryption can be a very time-consuming process for the IT team. That is why Kaspersky Lab's corporate solution provides a wide range of options for the automatic encryption of selected data.

Using Kaspersky Security Center, the administrator of a company's local network can customize the automatic encryption of:

- Contents of selected folders on a variety of computers within the network. An administrator can set up encryption based on a file name, extension, or a directory name;
- Certain types of data, such as office documents;
- All files created by specific applications;
- Files on portable media – an administrator may create a standard encryption policy for all removable media devices or create different rules for different devices. For example, all files on portable devices, or just new files can be encrypted. A portable encryption mode can be enabled using a fixed password for working with encrypted files on a PC that is not running Kaspersky Endpoint Security.

Administrators can also enable users to work with encrypted data outside of the corporate IT infrastructure (even on systems without encryption software installed).

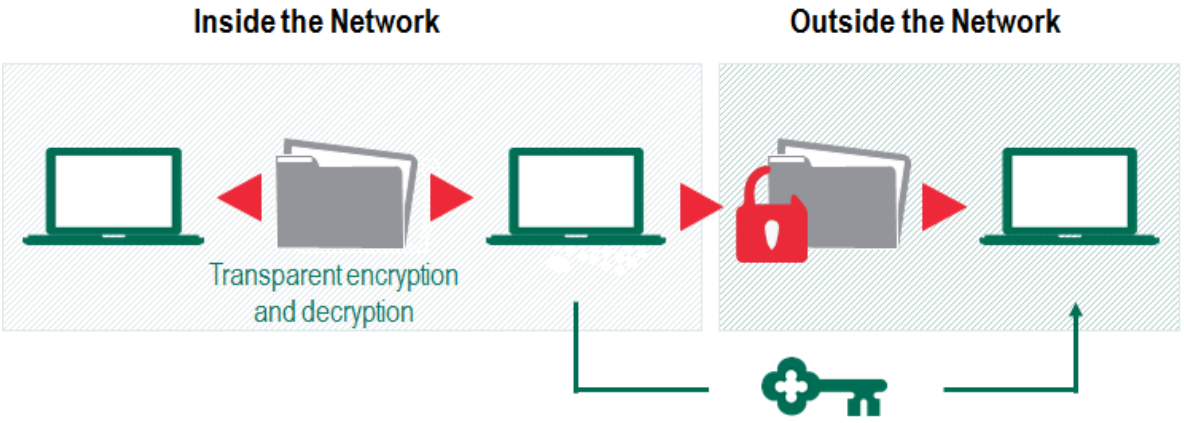

Figure 1. Encrypted data access principle

The FLE technology used in Kaspersky Lab products uses symmetric AES encryption. The AES algorithm is one of the most commonly used and reliable.

Full disk encryption

Full Disk Encryption (FDE) technology is a special data security method whereby the scope of encryption includes all of the sectors of a hard drive. This means that all of the information stored on a hard drive is secured under FDE: swap space, system files, page files,

hibernation files, and all temporary files. The technology can be used not only to secure a computer's hard drive but also to fully encrypt data on external drives. Hard drive compatibility is checked automatically prior the start of the encryption.

FDE technology supports the two widespread firmware interfaces: Basic Input-Output System (BIOS) and Unified Extendable Firmware Interface (UEFI), so that it is compatible with both the Master Boot Record (MBR) partitioning scheme and the GUID Partition Table (GPT). Before the operating system boots, a special Pre-Boot Environment (PBE) is launched that controls access to the computer. Before loading the OS, the PBE will authenticate the user, who will have to enter an ID and password. If an incorrect password is entered, the operating system will not load and the computer will be blocked until it is rebooted. To ensure keyboard compatibility, PBE supports various keyboard layouts. See the full list of layouts below.

The latest version of Kaspersky Endpoint Security for Business also supports authentication via the most popular smart cards and tokens. See the full list of compatible devices below.

In the case of a forgotten password, the challenge-response option will help users to recover their password. If pre-boot authentication is successful, the system booting process is started. Next, the FDE will decrypt as required the contents of the disk sectors containing OS files. Working within a fully encrypted environment, a user can open files, create new files and perform other actions, while the FDE technology continues to operate without interfering with user actions, encrypting and deciphering the requisite hard drive sectors 'on the fly'. These processes do not have a significant impact on the computer's performance.

In the event that a password is lost, all of the information stored on the hard drive can be decrypted using a special key that will be kept by the administrator of the company's local network and stored within Kaspersky Security Center.

Advantages

The advantages of encryption depend greatly on the technology used and the way in which it is used. The main pros for companies are relatively clear:

- Security. Using encryption will help to rule out any unauthorized access to data.
- Centralized control. With Kaspersky Security Center, an administrator can manage encryption technologies, keys, access to removable drives, and block access or restore passwords as needed.
- Simplicity. Users do not need any specialized skills to work with encrypted data.
- Support for external storage devices. It is possible to create special data encryption rules for all devices connected to a computer, or vice versa, with unique rules for each device.
- Automated encryption. The possibility to automatically encrypt files created or changed within any specific program. It is also possible to limit access to these files.
- Continual protection. Provides full data security, even in critical situations when a device or drive with confidential information is lost or stolen.

- Flexibility. Companies can customize data encryption rules to best suit their individual needs.

Availability

Full Disk Encryption and File Level Encryption technologies are parts of the following products for business users:

- Kaspersky Endpoint Security for Business Advanced
- Kaspersky Total Security for Business

Quality proven by industry experts

Forrester Research, Inc. has rated Kaspersky Lab as a Strong Performer in their evaluation of endpoint encryption solutions. According to The Forrester Wave™ Endpoint Encryption, Q1 2015, Kaspersky Lab's endpoint encryption offerings may work well for firms looking to source an all-in-one endpoint security suite at an attractive price point.

List of supported keyboard layouts

- English (UK)
- English (USA)
- Arabic (Algeria, Morocco, Tunis — AZERTY layout)
- Spanish (Latin America)
- Italian
- German (Germany and Austria)
- German (Switzerland)
- Portuguese (Brazil — ABNT2 layout)
- Turkish (QWERTY layout)
- French (France)
- French (Switzerland)

List of compatible Smart Cards and Tokens

- SafeNet eToken PRO 64K (4.2b) (USB)
- SafeNet eToken PRO 72K Java (USB)
- SafeNet eToken PRO 72K Java (Smart Card)
- SafeNet eToken 5100 (USB)
- SafeNet eToken 5105 (USB)
- SafeNet eToken 7300 (USB)
- EMC RSA SID 800 (USB)
- ruToken dongle (USB)
- Aladdin-RD JaCarta PKI (USB)
- Aladdin-RD JaCarta PKI (Smart Card)
- Athena IDProtect Laser (USB)
- Gemalto IDPrime 510 (SmartCard)
- Gemalto IDBridge CT40 (Reader)