KASPERSKY ENDPOINT SECURITY FOR BUSINESS

Encryption Technology

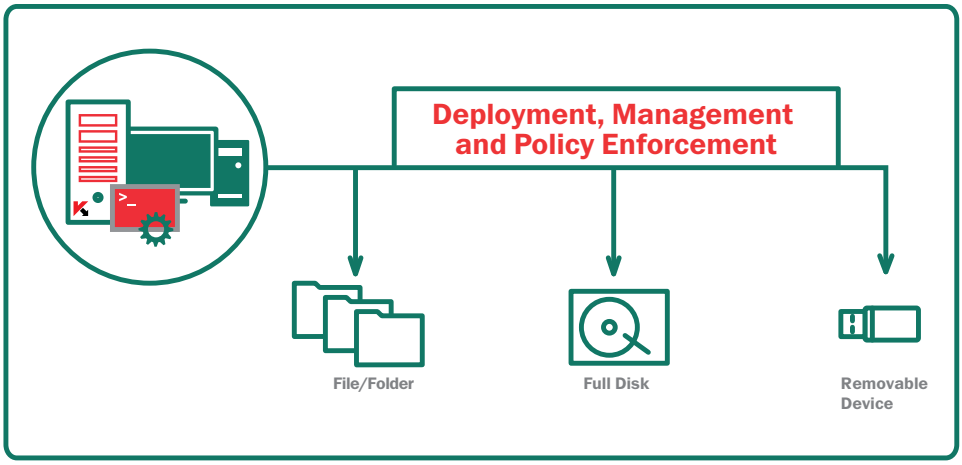
Encryption prevents unauthorized data access in the event of accidental PC or media loss.

Kaspersky Lab's encryption technology protects valuable data from accidental loss due to misplaced or stolen devices. The solution combines strong encryption organically integrated with Kaspersky's industry leading endpoint protection technologies. Because it's from Kaspersky, it is easy to deploy and administer from a centralized management console using a single policy.

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.



INDUSTRY-PROVEN SECURE CRYPTOGRAPHY

Kaspersky employs an AES encryption algorithm with 256 bits of key length.

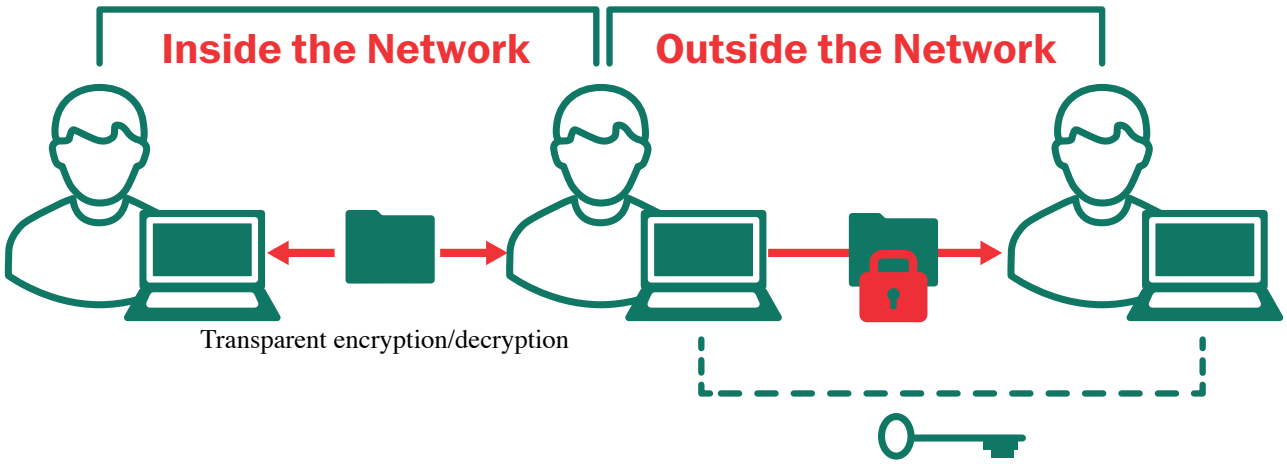
FLEXIBILITY IN CHOOSING ENCRYPTION METHOD

To cover all possible usage scenarios, both file and folder level encryption (FLE) and full-disk encryption (FDE) methods are available for data protection on hard drives and removable devices.

TRANSPARENCY FOR END-USERS

Kaspersky Lab's encryption technology remains transparent for all applications at all times, including at set-up. Operating with protected information on-the-fly, it does not interfere with end-user productivity. A single-sign-on to the encrypted system enhances user transparency.

During a file transfer, Kaspersky Encryption is seamless and transparent to the user inside the network. Data intended for external users can be packaged into password-protected containers. The password can be sent to the recipient for decryption using a seperate channel.



ENCRYPTION FEATURES:

INTEGRATED CODEBASE
Because all functions for multi-layered endpoint protection are in one single piece of software, there is no need to deploy and manage separate solutions for anti-malware protection, endpoint controls and encryption.

INTER-CONNECTED AND ORGANICALLY INTEGRATED POLICIES
The integrated codebase allows the administrator to create single policies. For example: IT can allow only approved removable media to be connected, and can also force an encryption policy on the same device (combining policies for device control and encryption technologies).

CUSTOMIZABLE "OUT-OF-THE-BOX" SETTINGS
Encryption settings are predefined (but can be customized) for common folders such as My Documents and Desktop, new folders, file extensions, and groups of file extensions (i.e. Microsoft Office documents, email message archives).

ADMINISTRATIVE EMERGENCY CENTRALIZED KEY
Means the security administrator can decrypt data on drives in the event of a hardware or software failure.

USER PASSWORD RECOVERY
Allows the user to recover the pre-boot password or access encrypted data via a challenge/response mechanism.

How to buy

Kaspersky encryption technology is not sold separately, but is enabled in these tiers of **Kaspersky Endpoint Security for Business**:

- Endpoint Security, Advanced
- Kaspersky Total Security for Business

NOT ALL FEATURES ARE AVAILABLE ON ALL PLATFORMS.
For details, please consult **www.kaspersky.com**

KESB-ET/Version 0.1/Nov12/Global

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