

# ▶ KASPERSKY ENDPOINT SECURITY FOR BUSINESS

## Encryption Technology

Prevent unauthorized data access caused by device loss, theft or data-stealing malware.

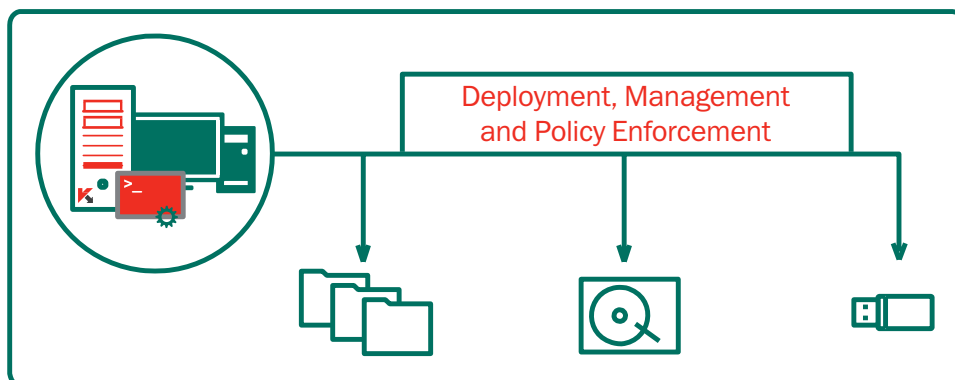
Proactive data protection and compliance is a global imperative. Kaspersky Lab's encryption technology protects valuable data from accidental loss, device theft and targeted malware attacks. Combining strong encryption technology with Kaspersky Lab's industry-leading endpoint protection technologies, our integrated platform protects data at rest and in motion.

Because it's from Kaspersky Lab, it's easy to deploy and administer from a centralized management console, using a single policy.

Prevent data loss and unauthorized information access with Kaspersky Lab's Encryption Technology:

- Full Disk Encryption (FDE)
- File/Folder Level (FLE)
- Removable and Internal Devices

ADMINISTERED THROUGH A SINGLE MANAGEMENT CONSOLE



### INDUSTRY STANDARD SECURE CRYPTOGRAPHY

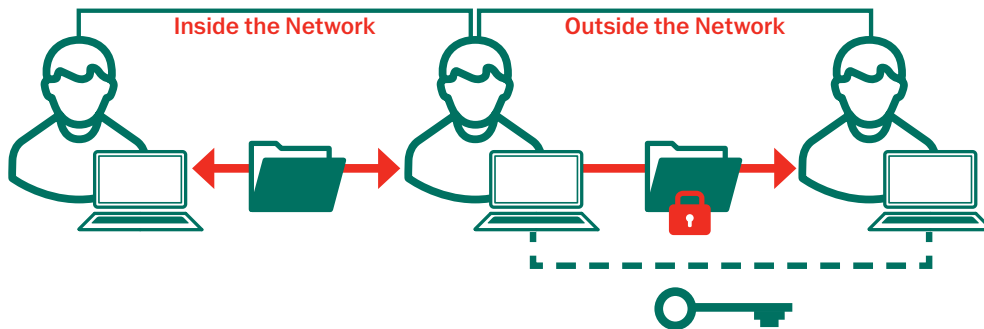
Kaspersky Lab uses Advanced Encryption Standard (AES) with 256 bit key length with simplified key management and escrow. Supports Intel® AES-NI technology, UEFI and GPT platforms.

### COMPLETE FLEXIBILITY

Kaspersky Lab offers file and folder level encryption (FLE) and full disk encryption (FDE), covering all possible use scenarios. Data may be protected on both hard drives and removable devices. 'Portable mode' enables the use and transfer of data on encrypted removable media, even on computers where encryption software is not installed – facilitating secure 'off perimeter' data exchange.

## SINGLE SIGN-ON, END USER TRANSPARENCY

From set up to daily use, Kaspersky Lab's encryption technology works transparently across all applications, without impeding end user productivity. Single sign-on ensures seamless encryption – the end user may not even be aware the technology is running.



Kaspersky Lab's encryption enables seamless, transparent file transfer between users inside and outside the network.

## ENCRYPTION FEATURES

### SEAMLESS INTEGRATION WITH KASPERSKY LAB SECURITY TECHNOLOGIES

Complete integration with Kaspersky Lab's anti-malware, endpoint controls and management technologies for true multi-layered security built on a common code base. For example, a single policy could enforce encryption on specific removable devices. Apply encryption settings under the same policy as anti-malware, device control and other endpoint security elements. No need to deploy and manage separate solutions. Network hardware compatibility is automatically checked before encryption is deployed; support for UEFI and GPT platforms is standard.

### ROLE BASED ACCESS CONTROL

In larger organizations, choose to delegate encryption management using role based access control functionality. This enables less complex encryption management.

### How to buy

**Kaspersky Encryption technology is not sold separately. It is enabled only in the 'Advanced' and 'Total' tiers of Kaspersky Endpoint Security for Business as a component of a full-featured, comprehensive security platform**

### PRE-BOOT AUTHENTICATION (PBA)

User credentials are required before the operating system even boots, providing an additional layer of security, with optional single sign-on. Kaspersky Lab's encryption technology PBA is also available for non-QWERTY keyboard layouts.

### SMARTCARD AND TOKEN AUTHENTICATION

Supports Two Factor Authentication via popular makes of smartcards and tokens, eliminating the need for additional usernames and passwords and enhancing end user experience.

### EMERGENCY RECOVERY

Administrators can decrypt data in the event of hardware or software failure. User password recovery for PBA or encrypted data access is implemented via a simple challenge/response mechanism.

### OPTIMIZED DEPLOYMENT, CUSTOMIZABLE SETTINGS

For ease of deployment, Kaspersky Lab's encryption functionality is enabled only within the 'Advanced' and 'Total' tiers of Kaspersky Endpoint Security for Business, no need for separate installation. Encryption settings are pre-defined but can be customized for common folders such as My Documents, Desktop, new folders, file extensions and groups, such as Microsoft Office documents or message archives.