# Kaspersky Lab's Full Disk Encryption Technology

In the US alone, an estimated 12,000 laptops are lost or stolen each week. According to the Ponemon Institute, a laptop is stolen every 53 seconds; more than half of organizations had experienced data loss as a direct result of insecure mobile device use between 2011-2012.

If your first response to the above is to consider the cost of replacing the hardware, you're focusing on the wrong problem. No one wants to lose hardware, but in the event of a data loss incident, the cost of replacing the device is the least of your worries. Ponemon research suggests that the average cost of a lost laptop is $49,246, with only 2 percent accounting for hardware replacement costs; as much as 80 percent of the cost goes on cleaning up the data leakage mess, regardless of the size of the business.

Factor in the cost of reputational damage, loss of customer loyalty and the ever-increasing range of government fines for data breaches, and it's easy to see how the cost of losing a laptop extends far beyond hardware replacement. Eighty-five per cent of customers globally said they would take their business elsewhere if a business lost their personal information – 47 percent said they would take legal action.[1]

Only 34 percent of the lost laptops in the Ponemon survey were encrypted. However, Gartner suggests that the cost of data breach from a lost or stolen laptop can be 70 times more than the cost of organization-wide encryption.

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

FDE encrypts 'data at rest', i.e., all the data on the hard drive and the module which authorizes software installation at the boot up. Essentially, the operating system loads safely in an encrypted environment, with every single file (including temporary files) on every single sector on the disk being encrypted. Only authenticated users can access the system, using a password, token or combination of these. FDE can also be applied to removable media, such as USB drives. FDE supports a variety of setups and can be managed and monitored through a centralized security center.

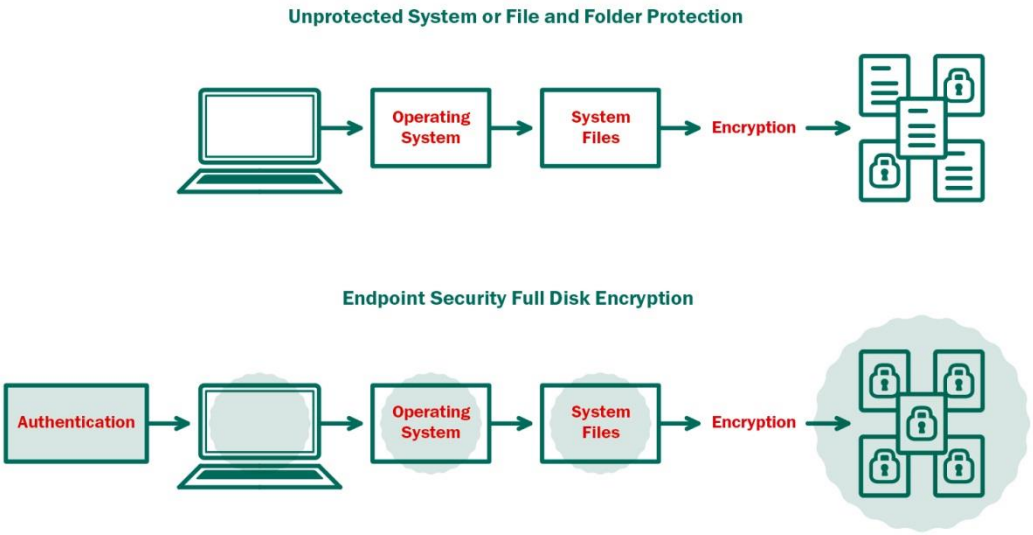
## How Kaspersky Lab's Full Disk Encryption Works

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 system administrator can personally install the software, or can do so using the Kaspersky Security Center. The software encrypts all selected drives and installs an authorization module in the boot environment. When the computer is started up, the operating system will automatically load within an encrypted environment – encryption is enforced, with almost no impact on the performance of the computer.

[1]Newspoll survey, November 2011

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 confidential data.** In the event of password loss, information can still be decrypted from the Kaspersky Security Center by using private keys that are only known by the system administrator. FDE-enabled mobile devices can significantly reduce the risk of data breach that results from loss or theft.

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




## Kaspersky's FDE Benefits

- **Enables enforced encryption of sensitive data**:
  By implementing FDE, organizations can enforce encryption, without depending on end users to make decisions about which items should be encrypted. 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**:
  By using a login/password mechanism, FDE prevents unauthorized access to data. When the correct login/password is presented, the system retrieves the key that's required to decrypt files on the hard drive. This adds an extra layer of security, because data can be rendered useless if the cryptography key is destroyed.

- **Centralized key management**:
  All encryption keys are stored in the Kaspersky Security Center, which can only be accessed by the security administrator.

- **Centralized encryption management**:
  FDE systems allow all functions to be managed from a central location within the organization. This includes functions such as decryption key management, access control to mobile devices, lock-outs (if necessary), reporting and recovery of lost passwords.

- **Simplicity and flexibility**:
  FDE offers end-user transparency and fully automated functionality. Following successful authorization, the encryption/decryption process takes place transparently and has no impact on the user experience.

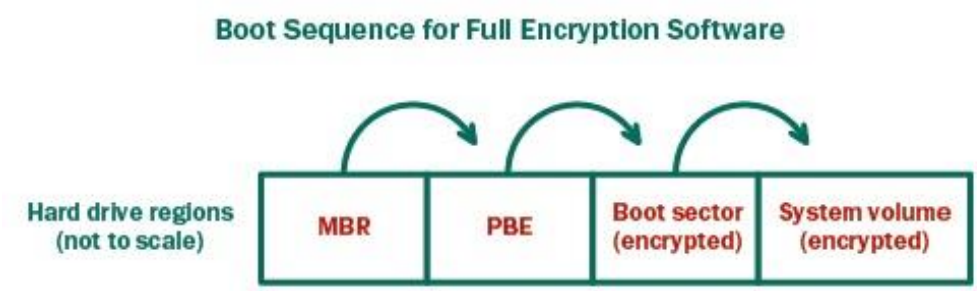
- **Centralized data recovery**:
  In the event of password loss or damage to the data carrier, data can still be recovered and decrypted using a special centrally managed emergency recovery procedure.

## Availability

Full Disk Encryption (FDE) is available in Kaspersky Endpoint Security 10 and is fully integrated with the Kaspersky Security Center.

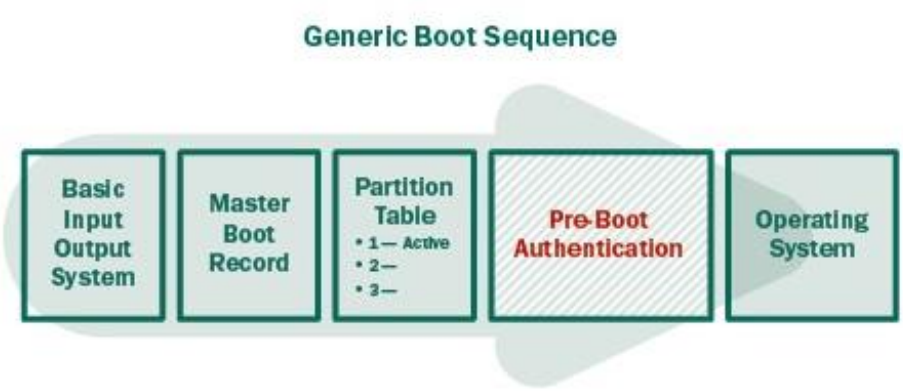
## Detailed Technology Description

**How FDE works (generic technology)**




FDE software works by redirecting a computer's master boot record (MBR – a reserved area or space that determines which software will be executed when a computer boots) to a special pre-boot environment (PBE) that controls the computer. Before FDE software is installed, the MBR usually points to the computer's primary OS. The PBE prompts the user to authenticate using an ID and password, before decrypting and booting into the OS. This is known as pre-boot authentication (PBA).

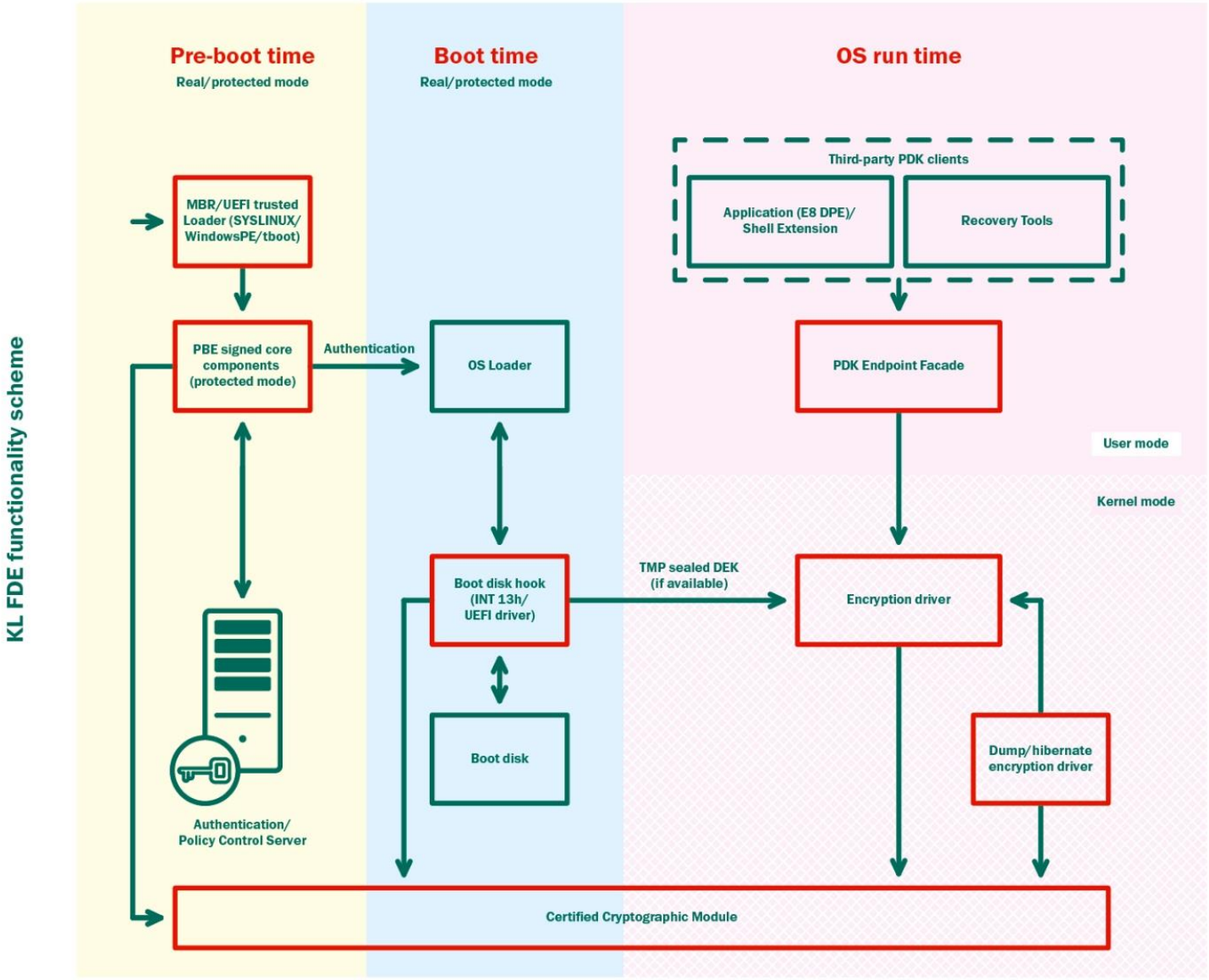
**Pre-boot authentication (PBA)** serves as an extension of the BIOS or boot firmware and guarantees a secure, tamper-proof environment external to the operating system – as a trusted authentication layer. PBA requires a user to authenticate before the operating system loads. In other words, on a system with PBA installed, the user is prompted for a user ID and password before the system boots up. After the user successfully logs in, the operating system starts. If the user enters the wrong user ID and password, the operating system won't load and the computer locks up.




After successful PBA occurs, the FDE software decrypts the boot sector for the OS and the boot loader begins to load the OS. While the OS is loading, the FDE software decrypts the OS files (which are stored in the system volume) as needed. After the OS has finished booting, the user provides OS authentication and can use the computer normally.

When the user needs to open encrypted files, save new files or perform other operations involving the hard drive, the FDE software transparently decrypts or encrypts the necessary sectors of the hard drive in operative memory. This may marginally increase the time needed to open or save files, but any delay should generally only be noticeable for particularly large files. On an FDE-protected computer, users will typically notice a delay of at least a few seconds when booting the computer or shutting it down. Delays may also occur when using hibernation features, because the FDE software has to encrypt or decrypt the large hibernation file (which includes a copy of the computer's memory) that is stored on the hard drive. The length of delay is dependent on memory size, hard drive size and speed, plus other factors.

**Kaspersky Lab's FDE functionality scheme**




**Kaspersky Lab's FDE Emergency recovery**

If a user forgets their PBA password, a PBA 'challenge-response' procedure is executed. A pre-boot agent creates a challenge sequence (5 lines, 17 symbols). The user informs the system administrator about the challenge value. Using the challenge sequence value, the system administrator creates a response sequence and sends this value to the user. This response sequence value could be used in the PBA authorization interface to change the password.

What if the data carrier (HD or portable media) is damaged? Data can still be recovered using Kaspersky Lab's FDE recovery tool to access a key that is stored in the Kaspersky Security Center vault. The damaged data carrier can be recovered manually, sector by sector, using a special recovery utility.

## Kaspersky Lab's FDE Features

- FIPS-approved algorithm XTS-AES 256-bit for disk encryption.
- 'Transparent' disk encryption in both setup and work phases.
- Removable disk encryption.
- Ability to boot OS from totally encrypted boot disk.
- Pre-boot authentication (PBA).
- Audits successful and unsuccessful attempts to pass PBA.
- Remote recovery of password (helpdesk support).
- Ability to recover disk data in case of hardware failures.
- Single Sign-On (SSO). Users can automatically log on to Windows, using pre-boot credentials.
- Centralized management via the Kaspersky Security Center.



KASPERSKY lab