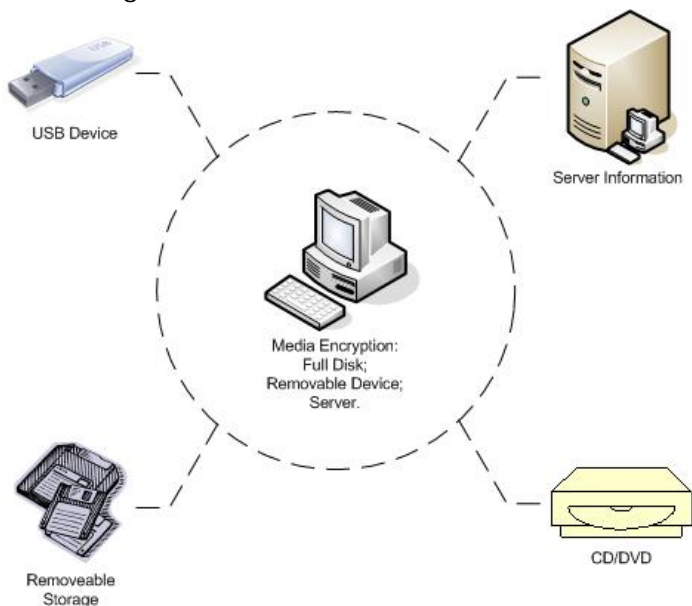




## Media Encryption

### Overview

Media Encryption refers to the encryption of data at rest, when it is stored on a storage medium. It does not apply to data in transit such as e-mail, files being transferred or interactive HTTP sessions.



Media encryption applies to physical storage devices such as magnetic disks (hard disk, floppy) or Non-Magnetic drives (USB flash memory devices) that exist as a local or networked device.

**Technology** Media encryption products are categorized by the technology used to encrypt the data: **Software or Hardware encryption**.

- **Software based encryption:** Data encryption is performed by a software application running on the host computer; it can encrypt all connected media including logical, physical and removable drives.
- **Hardware based encryption:** Data encryption requires a modified hard disk drive equipped with a hardware cryptographic chip. It only encrypts data on the local physical hard drive.

### Encryption Key

Typically a master encryption key is used to encrypt the data on the drive and is used to generate disk sector keys. The Sectors are encrypted with keys derived from the master key and the sector number which allows each sector to be encrypted and decrypted individually.

The master key is itself encrypted and protected through user credentials.

### Features

**Whole-disk** encryption products decrypt the data on the hard drive and copied in *Plaintext* to RAM; this often includes the decryption key for the hard drive itself. To ensure that data continues to be protected by whole-disk encryption, computers should be powered-off when left unattended.

**Temporary Files** are created, used and deleted by software applications. These files may not be properly deleted if the application is abnormally ended.

**Page Files** are transitory system files that in the event of a power failure may persist on the storage media.

The media encryption tool should have a **secure delete** feature to ensure that the original *Plaintext* file is destroyed after encryption.

To ensure the **data availability** the OS stores redundant copies of the data on the device, these copies are invisible to the user but may be obtained through forensic analysis; the device should be treated as if the most sensitive data remains on it.

When a computer enters '**Hibernation Mode**' data in RAM is saved to the hard drive in *Plaintext*; on resumption this data remains on the hard drive until it is **overwritten** - close sensitive files before hibernation.