WHITE PAPER:
HOW ENDPOINT ENCRYPTION WORKS

# How Endpoint Encryption Works

Who should read this paper

Security and IT administrators

# How Endpoint Encryption Works

## Content

## Introduction to Endpoint Encryption

If you're using a computer or a removable USB drive, the chances are you have sensitive data on these devices. Whether it's a computer with sensitive corporate information, or a thumb drive with government secrets, you need to ensure there is no unauthorized access to that data should the device be lost or stolen.

Endpoint encryption (which typically includes disk encryption and removable media encryption) protects this data, rendering it unreadable to unauthorized users. This paper defines endpoint encryption, describes the differences between disk encryption and file encryption, details how disk encryption and removable media encryption work, and addresses recovery mechanisms.

## What is Endpoint Encryption?

When it comes to encrypting data, there are various encryption strategies.

Disk encryption protects a hard drive in the event of theft or accidental loss by encrypting the entire disk including swap files, system files, and hibernation files. If an encrypted disk is lost, stolen, or placed into another computer, the encrypted state of the drive remains unchanged, ensuring only an authorized user can access its contents.

Some endpoint encryption solutions (like Symantec™ Endpoint Encryption) also include support to encrypt files stored on or copied to removable media devices.  As with disk encryption, removable media encryption helps prevent unauthorized access to information on lost or stolen devices (in this case the devices are USB flash drives, external hard drives (USB, FireWire, and eSATA), SD cards, and compact flash cards).  In this way, organizations can benefit from the productivity gains associated from collaboration using removable storage without putting data at risk.

## What are the differences between Disk Encryption and File Encryption?

Disk encryption typically uses one key to encrypt a hard disk, so all data is able to be decrypted when the system runs.  If you have logged into your system and leave your computer unattended, your system is unlocked and unauthorized users can access your system just as an authorized user could.

Just as an alarm system protects an entire home and a safe provides additional security, disk encryption protects the entire computer system, and file encryption provides an additional layer of security.

File encryption encrypts specific files so when a user successfully authenticates to an operating system, the contents of the file remain encrypted. An application such as Symantec™ Endpoint Encryption’s removable media capability can protect individual files and folders, prompting the user for a passphrase to permit access. File encryption requires user action while disk encryption automatically encrypts everything you or the operating system creates.

## How Disk Encryption Works

During the startup process of an operating system, a boot sequence is executed. The boot system is the initial set of operations that the computer performs when it is switched on. A boot loader (or a bootstrap loader) is a short computer program that loads the main operating system for the computer. The boot loader first looks at a boot record or partition table, which is the logical area “zero” (or starting point) of the disk drive.

Disk encryption modifies the boot sector. For example, a computer protected with Symantec™ Endpoint Encryption presents a modified pre-boot environment for the user to authenticate to the computer.

This modified pre-boot screen prompts the user for authentication credentials in the form of a passphrase (typically a longer password, often resembling a sentence). At this point, the computer may ask for additional credentials such as a smart card, token, or other two-factor authentication.

After the user enters valid authentication credentials, the operating system continues to load as normal and the user can access the computer.

Most disk encryption software operates in conjunction with the file system architecture. It filters I/O operations for one or more file systems or file system volumes.

When a drive is encrypted for the first time, it converts unencrypted drive blocks into encrypted blocks one at a time. Disk encryption allows users to continue working as normal during this initial encryption process by varying the amount CPU power assigned to the initial encryption process.

When a user accesses a file, disk encryption decrypts the data in memory before it is presented for viewing. If the user makes any changes to the file, the data is encrypted in memory and written back to the relevant disk drive block just as it would be without encryption. Decrypted data is never available on the disk.  The encryption/decryption process happens at such a speed that it appears completely transparent to the user.

## How Removable Media Encryption Works

Removable media encryption software provides the ability to encrypt files on removable storage devices.

When a user copies files of a system onto a removable storage device, each file is encrypted to a password, a shared key or a certificate. At the same time, utilities for Windows or Mac systems can be copied (if permitted by policy) allowing authorized access to data without the endpoint client installed on a machine.

This file encryption can be governed by policy, user action, or Symantec DLP.  In the case of Symantec DLP, the Endpoint Prevent software monitors users’ machines and understands when a person is moving a sensitive file off his computer.  With the integration of Symantec DLP and Symantec Endpoint Encryption, administrators can ensure files with sensitive information that are moving to removable media are encrypted rather than blocked, allowing business processes to continue in a secure manner.

To access the information, when the user inserts a removable media device like a USB drive with encrypted files into a computer system, the removable media encryption software will prompt for passphrase, and upon successful authentication, the user can access the file.

## Recovery Mechanisms: Disk Encryption

The most common cause for data recovery is a lost or forgotten passphrase. Therefore, disk encryption software must include a recovery function. There are several ways to access an encrypted system in case of a forgotten passphrase. Symantec Endpoint Encryption offers local self-recovery, a recovery token, and an administrator key among others.

Self-recovery enables users to answer pre-defined and customizable questions at boot time to gain access to an encrypted system and reset the boot passphrase without calling IT staff.

With Help Desk Recovery enabled on a client computer, the user can access the encrypted computer under two conditions: if the user forgot his password or the computer is in a lockout state at preboot (which may occur if the client computer has not communicated with the management server with a set communication interval). Help Desk Recovery makes use of a one-time password (also known as a Response Key).

Another cause for data recovery, although rare, may be data corruption resulting from hardware failure or other factors such as a data virus. Corruption of a master boot record on a boot disk or partition protected by disk encryption can prevent a system from booting. To protect and make accessible the data on encrypted client computers that cannot load a Microsoft Windows operating system, it is best practice to create a Windows Preinstallation Environment (Windows PE or WinPE) CD or USB flash drive immediately after installing the client software.

## Recovery Mechanisms: Removable Media Encryption

There are two main recovery mechanisms that can help recover encrypted files stored on removable media. If a file is encrypted with a workgroup key (used to enable sharing files) the file may be recovered by inserting the USB with the encrypted file into another computer that uses the same workgroup key. Also, if the administrator has chosen the policy to encrypt files with a recovery certificate then each file is encrypted with the public key of the recovery certificate. If the password or certificate used for encryption is lost, the administrator can use the copy of the recovery certificate with the private key to recover the encrypted file.

### About Symantec

Symantec protects the world's information, and is a global leader in security, backup, and availability solutions. Our innovative products and services protect people and information in any environment – from the smallest mobile device, to the enterprise data center, to cloud-based systems. Our world-renowned expertise in protecting data, identities, and interactions gives our customers confidence in a connected world. More information is available at www.symantec.com or by connecting with Symantec at go.symantec.com/socialmedia.

For specific country offices and contact numbers, please visit our website.

Symantec World Headquarters
350 Ellis St.
Mountain View, CA 94043 USA
+1 (650) 527 8000
1 (800) 721 3934
www.symantec.com

1/2015 21275920-3