WHITE PAPER:
HOW DRIVE ENCRYPTION WORKS

How Drive Encryption Works

Who should read this paper

Security and IT administrators

Content

Introduction to Drive Encryption

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

Drive encryption, also known as disk encryption, protects this data, rendering it unreadable to unauthorized users. This paper describes the differences between drive and file encryption, details how drive encryption works, and addresses recovery mechanisms.

What is Drive Encryption

Drive Encryption versus File Encryption

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

Drive encryption protects a disk 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.

Drive encryption cannot however, protect your data when you have logged into the system during startup and leave your computer unattended. In this case, your system has been unlocked, and unauthorized users can access your system just as an authorized user could. This is where file encryption comes in.

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

File encryption encrypts specific files so that when a user successfully authorizes to an operating system, the contents of the file still remain encrypted. An application such as Symantec™ File Share Encryption can protect individual files and folders, prompting the user for a passphrase to permit access. File encryption requires user action while drive encryption automatically encrypts everything you or the operating system creates. File encryption can also be paired with an encryption policy server which allows IT administrators to create and deliver encryption rules across an organization, including automatically encrypting files from various applications and/or folders.

How it Works

During the startup process of Microsoft® Windows, Apple® OS X, or Linux® operating systems 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.

Drive encryption modifies the zero point area of the drive. A computer protected with Symantec™ Drive Encryption presents a modified “pre-boot” environment (Figure 1) to the user.

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.

Drive encryption software also provides the ability to encrypt removable storage media such as USB drives. When you insert an encrypted USB drive into a computer system, it prompts for passphrase, and upon successful authentication, you can use the USB drive.

Drive Encryption: Behind the Scenes

File System Basics

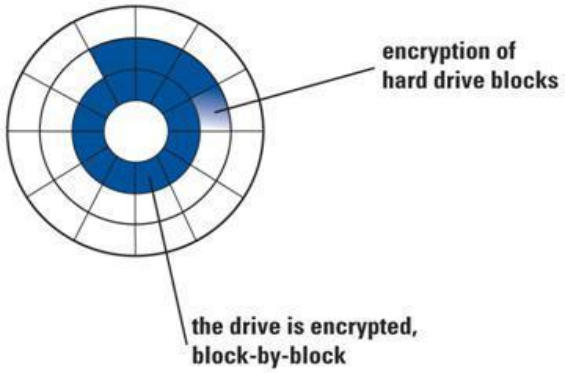
During the boot process, the system initializes the computer's file systems.

When a user requests access to a file (i.e., creates, opens, or deletes a file), the request is sent to the operating system input/output (I/O) manager, which forwards the request to the file system manager. The file system manager processes data in blocks.

Life with Encryption: Business as Usual

Most drive 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 with drive encryption for the first time, it converts unencrypted drive blocks into encrypted blocks one at a time. Drive 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, Drive 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.

Drive Encryption: Recovery

Whole Disk Encryption: Recovery

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

Local 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 ever calling IT.

The Drive Recovery Token (DRT) is a one-time, per-device, per-user temporary recovery set of alphanumeric characters to reset a passphrase.

The administrator key, held by administration, is stored on a tamper-proof smart card or token.

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 drive encryption can prevent a system from booting. To avoid these kinds of errors, it is best practice to create a recovery CD and then backup a drive before encrypting it with drive encryption. Drive encryption provides recovery options and does interoperate with popular backup tools. Ask your Symantec representative for more information about compatibility with existing backup systems.

About Symantec

Symantec protects the world's information and is the 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 industry-leading 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