WHITE PAPER: WHOLE DISK ENCRYPTION

How Whole Disk Encryption Works

How Whole Disk Encryption Works

Contents

Introduction to Whole Disk 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 your home computer with family finances, your work computer with sensitive corporate information, or a thumb drive with government secrets, you want to ensure that there is no unauthorized access to that data if the device is lost or stolen.

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

What is Whole Disk Encryption

Whole Disk Encryption versus File Encryption

When it comes to encrypting data, you begin with deciding what data to protect and then you determine how to protect it.

Whole disk encryption protects a disk in the event of theft or accidental loss. Whole disk encryption encrypts 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, and only an authorized user can access its contents.

Whole disk encryption cannot protect you when you have logged into the system during startup and then leave your computer unattended. Unauthorized users could open any file on the disk. This is where file encryption comes in. Just like an alarm system protects an entire home and a safe provides additional security, whole disk encryption protects the entire system, and file encryption provides an additional layer of security. File encryption encrypts specific files and when a user successfully authorizes to an operating system, the contents of the file remain encrypted. An application such as PGP® Virtual Disk from Symantec™ can protect individual files and folders, prompting for a passphrase to permit access.

File encryption requires user action. Whole disk encryption automatically encrypts everything you or the operating system creates. File encryption does not automatically encrypt newly created or temporary files created by application software such as a Web browser.

Therefore, it is a best practice to protect your entire disk with PGP® Whole Disk Encryption from Symantec™ to ensure that data—including temporary files—remains unreadable in case of accidental loss or theft.

How it works

A boot sequence executes during the startup process of Microsoft® Windows, Apple Mac OS X, or Linux® operating systems. 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.

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

This modified pre-boot screen prompts a user for authentication credentials in the form of a passphrase (a long password that is like a sentence). At this point, the computer may ask for additional credentials such as a smart card or token.

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

Whole Disk 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.

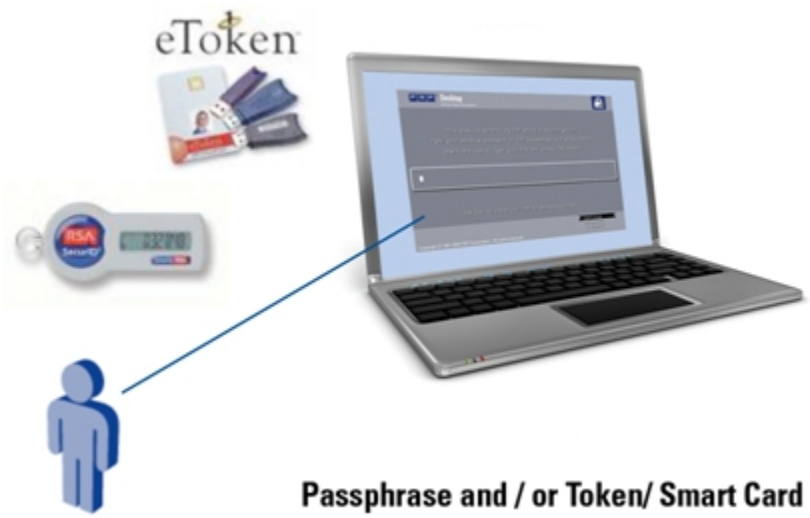

Figure 1: User authenticates with passphrase or smartcard/token

Whole Disk Encryption: Behind the Scenes

File system basics

During the boot process, the system initializes 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 whole 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 with whole disk encryption for the first time, it converts unencrypted drive blocks into encrypted blocks one at a time (Figure 2).

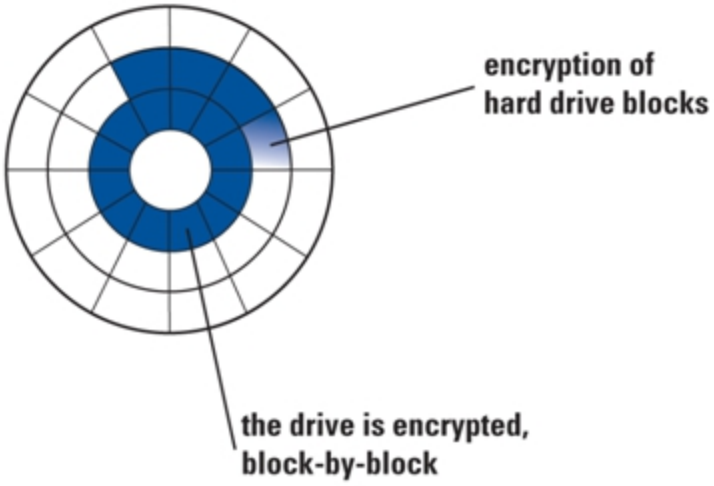

Figure 2: Drive is encrypted block-by-block

Decrypted data is never available on the disk.

When a user access a file, Whole 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 blocks just as it would be without encryption.

Because Whole Disk Encryption operates in conjunction with the file system, there is no additional wear and tear or performance impact beyond normal disk operation.

As far as the user is concerned, it's business as usual, and the underlying mechanism of encryption/decryption is completely transparent.

Whole Disk Encryption: Recovery

The most common cause for data recovery is a lost or forgotten passphrase. Therefore, whole disk encryption software must include a recovery function. There are several ways to access an encrypted system in case of a forgotten passphrase with Whole Disk Encryption, such as local self-recovery, recovery token, and 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 Whole Disk Recovery Token (WDRT) is a one-time, per-device, per-user temporary recovery set of alphanumeric characters to reset a passphrase. The administrator key 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 Whole Disk 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 Whole Disk Encryption. Whole Disk Encryption provides recovery options and does interoperate with popular backup tools. Ask your Symantec representative for information about compatibility with existing backup systems.

About Symantec

Symantec is a global leader in providing security, storage, and systems management solutions to help consumers and organizations secure and manage their information-driven world. Our software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored. Headquartered in Mountain View, Calif., Symantec has operations in 40 countries. More information is available at www.symantec.com.

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

Symantec helps organizations secure and manage their information-driven world with **security management**, **endpoint security**, **messaging security**, and **application security** solutions.

11/2010 21158817