BitLocker for Windows 7

“A full disk-encryption feature that can save your valuable data.”

by Pete Choppin

BitLocker Drive Encryption is a full disk-encryption feature included with the Ultimate and Enterprise editions of Microsoft's Windows Vista and Windows 7 desktop operating systems, as well as the Windows Server 2008 and Windows Server 2008 R2 server platforms. It is designed to protect data by providing encryption for entire volumes. By default it uses the Advanced Encryption Standard (AES) encryption algorithm in Cipher Blocking Chain (CBC) mode with a 128-bit key.

Since its introduction with the original shipping release of Windows Vista, BitLocker has undergone a regular series of improvements. The initial version of this technology was conceived as full-disk encryption—that is, it will encrypt any entire partition, not just parts of it —that works both online and offline (i.e., at boot time and when the drive is disconnected) thanks to integration with underlying Trusted Platform Module (TPM) 1.2 (and higher) chipsets. (BitLocker can also utilize a USB memory key or an alphanumeric password if TPM hardware isn't present.)

With the introduction of BitLocker in Windows Vista, it wasn't very popular. This might be because it is available only for Windows Vista Ultimate and Windows Vista Enterprise. But the main reason probably is that it is complicated to set up.

Windows 7 BitLocker (available in the Ultimate and Enterprise editions) is now far easier to configure and install, and no longer requires manual partitioning or even a separate tool: You can simply right-click a drive in Explorer and choose "Turn on BitLocker" from the context menu that appears. And there's no need to create a special partition, because it's already here: Windows 7 creates a hidden partition for this very purpose during setup. Windows 7 also adds Data Recovery Agent (DRA) support for all protected disk volumes so that enterprises can store recovery data in Active Directory and recover volumes if needed. Windows 7 also extends BitLocker support, for the first time, to removable storage devices. This feature is called BitLocker To Go, which we will discuss later.

Why Use BitLocker?

BitLocker Drive Encryption helps protect your data by creating a small partition on the drive as well as encrypting the contents on the drive itself. If your hard drive or system is lost or falls into the wrong hands, your data will be protected.

Not only can you store your recovery key for BitLocker to a thumb drive or a smart card, but even if your laptop and thumb drive are both stolen, the thief would still need to know your password to unlock the drive. This adds an additional layer of security that is nearly unrivaled.

Unlike the Encrypting File System, which allows you to encrypt individual files, BitLocker Drive Encryption encrypts the entire drive, meaning the second you move a file into the drive, it is automatically encrypted, and when you move a file off of the drive, it becomes unencrypted. This makes it much easier to manage your encrypted files so you never have to double check to make sure every important file is encrypted.

You can even access a drive locked with BitLocker Drive Encryption over a Windows network, as long as you have the encryption password. You can also set a drive to automatically unlock right when you log into your computer.

Setting up BitLocker in Windows 7

In Windows Vista, setting up BitLocker was a troublesome procedure, forcing you to manually shrink your current partition and create a BitLocker partition. Microsoft then created the BitLocker Drive Preparation Tool, most likely after realizing that the current method was a bit too technical for new users. In Windows 7, however, the BitLocker Drive Preparation is fully integrated into the Control Panel and does most, if not all, of the work for you (see Figure 1).

Figure 1. BitLocker Control Panel in Windows 7.

You can encrypt a drive right from Windows Explorer—simply right click on the drive, and choose Turn on BitLocker. After going through the setup process you can choose a password and your drive will be fully encrypted.

You can also modify more advanced settings from within the Group Policy Editor. To do this, navigate to Administrative Templates/Windows Components/BitLocker Drive Encryption to see specific settings that can be modified. From here, you can modify settings for fixed data drives, operating system drives and removable data drives, as well as general settings like how to recover BitLocker-protected drives.

One notable setting allows you to configure the use of passwords, being able to set passwords, and minimum password complexity allowed. You can also now modify settings for the pin used in Windows Startup and can choose how long the pin should be (up to 20 characters), as well as enabling extra characters such as symbols, uppercase and lowercase letters, and numbers.

Unlike with Vista, BitLocker for Windows 7 creates only a small 100MB partition that is fully hidden so an individual cannot accidentally or purposefully overwrite or delete the partition. While you can see the partition in Disk Management, it is well secured to ensure nothing happens to lower the integrity of the protection.

Another nice security feature is the use of a "recovery key"—a 40-digit code provided specifically as a means to access your data if there is a problem with your system or you lose your PIN. You can save the recovery key to a USB drive or a local file, or you can print it out.

Is BitLocker Right For You?

BitLocker Drive Encryption is a great, fully integrated way of protecting your hard drives from unauthorized use. However, while the encryption is powerful, it can be a bit over the top for users who don't fully require the encryption.

For example, if you forget your thumb drive key for your laptop, you could end up with a locked machine and be unable to access it until you recover it. Because of this, day-to-day use can be a bit bothersome with extra work just to get into your own system.

All that aside, for those who require heavy protection, such as enterprise users or users with very important or confidential data, BitLocker Drive Encryption can be a very valuable asset to save you, and possibly your company, time and money when fighting unauthorized access.

BitLocker Drive Encryption does its job very well, and in my opinion has risen above alternative encryption systems, both paid and free.