

By George Ou

It seems as though every other month you hear about a major breach of security, with someone losing a computer containing tons of sensitive consumer information. Just within the last year, I've been inundated with "your data was exposed" letters. In mid-2005, one of the country's largest credit card companies [exposed 40 million accounts](#). The company was cut off from Visa and AMEX within weeks, putting it out of business in a flash.

With all the new breach notification laws that are in effect now, or that soon will be, any company that wants to keep its customers must do everything possible to secure its data. The [Ponemon Institute](#) conducted research showing that companies lost a significant number of customers by the second data breach and lost all their customers by the third incident.

One of the main components of keeping company data safe is the security of PCs, and especially notebooks, since they can easily be stolen. Windows Vista now offers complete data encryption security with an improved [EFS \(Encrypted File System\)](#) and the new [BitLocker feature](#). Between these two features, it's possible to cover all aspects of storage security on a Vista PC. Older versions of EFS provide only partial protection to previous versions of Windows. EFS on Windows 2000 and XP are susceptible to certain types of attacks because the Windows directory, page file, and deleted temporary files are exposed by the limitations of EFS. For example:

- ◆ Attackers with access to the Windows directory can attempt dictionary attacks to find the user's password with lightning speed, and the vast majority of passwords will fall within a day. Armed with the user's password, the system might as well be wide open.
- ◆ The page file contains clear text data, which can be exploited.
- ◆ The temporary directory used during the EFS encryption process has temporary clear text files that eventually get encrypted. These clear files are deleted, of course, but the raw data still resides on the hard drive for anyone to see.

The EFS mechanism works after Windows boots up, while BitLocker works before Windows and seamlessly operates beneath the operating system. EFS works on the file system level and encrypts at the file level based on user permissions and PKI-protected session keys; BitLocker is a low-level mechanism that encrypts an entire volume and is oblivious to the concept of users and PKI. This means that EFS offers high-level manageability, while BitLocker operates at a low level without the manageability features—but it can protect those spots EFS can't. Files encrypted by EFS can't be cracked, although the filename and directory structure is not protected. The Windows partition encrypted by BitLocker is completely scrambled so you can't even tell what the filename and directory structure is.

The only potential weakness to BitLocker occurs when a computer either wasn't shut down or is suspended, since the physical key used by BitLocker is not needed for access in those situations. But an attack is still hard to pull off. Since the PC can't be shut down, the attacker has to try to tap the RAM while the computer is running. The recommended procedure for users is to either shut down the PC or use the hibernate option because that will trigger a request for the physical BitLocker key. That key can be a TPM module on the motherboard or a generic USB that you can carry with you on a keychain. The TPM module option requires you to use a pin or password to activate, since any theft of the PC or notebook means the TPM is stolen too. The USB key, on the other hand, doesn't require a pin or password—so it's a good idea not to store that key with the notebook in the bag.

Since BitLocker won't encrypt additional hard drive volumes, whether they're logical partitions on the same physical disk or additional disks, you must use EFS to encrypt those volumes by selecting all the folders and files from the root. EFS, on the other hand, can't be used to encrypt the entire Boot partition. It can't touch the operating system files because Windows won't boot if they're EFS-encrypted. This means that EFS and BitLocker are essentially the perfect partners, compensating for each other's weaknesses.

There are exceptions, where BitLocker can be used entirely on its own if there is only one hard drive with one partition (not counting the special 1.5 GB BitLocker pre-boot partition). For home users who just want to keep things simple and load everything on a single partition with only one hard drive, just using BitLocker is perfectly

reasonable. But if there's more than one partition or more than one hard drive, EFS must be used for everything else outside the main partition Windows is installed in. To learn how to implement BitLocker for Vista Enterprise and Ultimate editions, see "[Follow these steps to secure your hard drive with Vista BitLocker.](#)"

By protecting Windows, the page file, and the temporary directory, BitLocker closes up the weaknesses that can expose EFS. By offering support for the concept of users and of PKI, which now also allows the use of physical smartcards or USB cryptographic modules, EFS can offer scalable enterprise-level manageability. Armed with BitLocker and EFS, PCs and notebooks can be secured against data theft if they're ever stolen.

Additional resources

- ◆ TechRepublic's [Downloads RSS Feed](#) **XML**
- ◆ Sign up for TechRepublic's [Downloads Weekly Update](#) newsletter
- ◆ Sign up for our [Windows Vista Report newsletter](#)
- ◆ Check out all of TechRepublic's [free newsletters](#)
- ◆ "[Protect sensitive communications and data with these simple and affordable encryption techniques](#)" (TechRepublic download)
- ◆ "[10 things you can do to protect your data](#)" (TechRepublic download)
- ◆ "[Protect your enterprise's most critical asset: Develop an effective data protection strategy](#)" (TechRepublic download)

Version history

Version: 1.0

Published: February 28, 2007

Tell us what you think

TechRepublic downloads are designed to help you get your job done as painlessly and effectively as possible. Because we're continually looking for ways to improve the usefulness of these tools, we need your feedback. Please take a minute to [drop us a line](#) and tell us how well this download worked for you and offer your suggestions for improvement.

Thanks!

—The TechRepublic Downloads Team