


TRUSTED STRATEGIES

Defining the Business of IT Security

FDE Performance Comparison

Hardware Versus Software Full Drive Encryption

A look at performance and other differences between hardware based self-encrypting drives and software approaches to full disk encryption for laptops

Trusted Strategies LLC
Author: Bill Bosen

February 9th, 2010

Sponsored by Seagate Technology and Wave Systems Corp.

FDE Performance Comparison: Hardware vs. Software FDE

According to recent studies, as many as 10% of laptop computers are lost or stolen each year, and most of them contain sensitive, confidential data¹. As a safeguard, many organizations are turning to FDE (Full Drive Encryption) as a means to protect their data from falling into the wrong hands. Since FDE technology encrypts everything on a PC or laptop's hard disk, security is greatly increased.

However, because the operating system, applications, and data are all encrypted, FDE takes a tremendous amount of processing power. So the performance of any FDE product is critical when selecting a solution. With today's high speed CPUs, it's germane to ask how the performance of software based encryption systems compare with hardware based options. What kind of performance penalty might one expect if installing the various FDE technologies? When deployment and operational costs are factored into the equation, is it more cost effective to deploy hardware or software?

To help answer these questions Trusted Strategies tested the performance of a number of FDE hardware and software products from industry leaders. Our objectives included determining the data throughput of commonly used applications like Microsoft office. We also wanted to test throughput for hard disk intensive procedures like system backups, virus scanning, and opening, reading, and writing large 100MB+ files used with data intensive applications. Finally, we wanted to know how encryption might effect the performance of disk heavy system processes such as startup, shutdown, and hibernation.

Products Tested

For our *FDE product testing*, we chose three well known leaders in the software space, and the leading hard disk manufacturer:

- ***McAfee Endpoint Encryption*** for PC, version 5.2.3. This is the former SafeBoot product and has been a leader in the software FDE industry for many years. McAfee acquired Safeboot in November 2007 and has since renamed it *McAfee Endpoint Encryption*.
- ***PGP Whole Disk Encryption*** for Windows, corporate desktop version, release 9.12. PGP data encryption software was one of the first solution providers in the software FDE space, and according to the company's website is currently used by more than 110,000 enterprises.
- ***Microsoft Bitlocker***, Windows Vista Ultimate, SP2. Bitlocker is included with the Ultimate and Enterprise editions of Microsoft Windows. Although BitLocker has only been around a few years, with Microsoft behind it, it's a force that can't be ignored and will certainly improve over time.

¹ Ponemon Institute, 2006 and 2009 computer security surveys *Business Risk of a Lost Laptop*

- ***Seagate Self-Encrypting Drives with Wave Systems Embassy Trusted Drive Manager:*** For the hardware based product tests, we chose *Seagate Technologies' self-encrypting drives*. Seagate was the first disk drive manufacturers to enter the encrypting hard drive marketplace. We used the Seagate *Momentum 7200 FDE* model, a well known and respected drive. To manage the Seagate self-encrypting drive we used Wave System's EMBASSY® Trust Suite software. EMBASSY enables and disables the drive's protected encryption mode, enrolls users, manages pre-boot user authentication and provides access to other unique drive features. The Seagate/Wave solution is shipped today by Dell as a factory integrated option and is the most widely distributed self-encrypting drive solution available.

Since our objective was to compare the performance of software based FDE as a *category* instead of as individual products, we've elected not to identify the performance benchmarks and scores of each specific software vendor. They are represented in the performance charts simply as *Software Product 1, 2, and 3*.

Test Platforms and Procedures

For our test platforms, we used identical Dell Latitude E6400 laptops, running Microsoft® Windows Vista™ Ultimate, Service Pack 2. These 32 bit machines were equipped with Intel® Core™ 2 Duo Processors, and 2 GB of RAM. When testing the *software* FDE products, we used standard 500 GB 7200 RPM Seagate Momentum disk drives. For the *hardware* based FDE tests, we replaced the standard Seagate Momentum disk drives with Seagate's FDE / self-encrypting drives as noted above. Other than the encryption capabilities, the two drives are identical.

We selected PCMark Vantage Professional edition to test and measure the throughput and performance of the different encryption solutions. We found the hard disk drive test suit exceptionally well designed for our needs, and while we ran performance tests on the entire system including the CPU, memory, and graphics, we concentrated on the hard disk drive test suite.

Our test procedures including freshly imaging and restoring the operating system and applications on the Dell laptops before each and every specific test, and we repeated each of the tests at least three times. The results of the three different test sets were very consistent and similar, but to give the optimum score for each product we used the best result obtained in any of the tests.

To establish a performance baseline, we first ran all of the tests on a newly imaged laptop that had no encryption enabled whatsoever, either in hardware or software. We then tested the performance of both hardware and software FDE products, and compared the results with the established performance baseline.

The specific tests conducted for each of the hardware and software solutions included the following:

- *Application Loading*: This test measured the data throughput from disk activities incurred by opening and closing the following applications - Microsoft® Word, Adobe® Acrobat® Reader, Windows® Media Player, Leadtek® Winfast® DVD, and Mozilla Internet Browser. The test involved 83% read operations and 17% write operations.
- *Modest Size File Test*: This test, consisting of 60% reads and 40% writes, measures disk activities of several common but modest size applications and files. Test activities included:
 - Opening a Microsoft® Word document, performing grammar check, saving and closing
 - Compression and decompression using Winzip
 - Encrypting and decrypting files using PowerCrypt
 - Playing WAV, MP3, and WMV files with Windows® Media Player
 - Playing a DivX video using DivX codec and Windows® Media Player
 - Viewing pictures using Windows® Picture Viewer
 - Browsing Internet files using Microsoft® Internet Explorer
 - Loading, playing and exiting a game using Ubisoft™ Tom Clancy's Ghost Recon
- *Extensive Data Read*: Measures throughput while scanning 1.8GB of files for viruses. This test is 99.5% read activity. This test is also an effective way to test the performance of data backup procedures.
- *Extensive Data Write*: Measures throughput while writing 2GB of data on the hard disk. No read operations are involved in this test.
- *System Startup*: Elapsed time and hard disk throughput and activities that occur during Windows startup procedures. The test is 90% reading and 10% writes, and contains no user activity.
- *System Shutdown*: Measures how long it takes to perform a system shutdown.
- *Hibernation Time* – Measures how long it takes for the system to hibernate and power back up. Microsoft Word, PowerPoint, and Outlook were running, with 106MB of data loaded

Performance Results: Table 1

Our first set of tests measured data throughput during system startup. As one might expect during system boot, hard disk activity during these tests was around 90% reads and 10% write activity. Since the startup procedures open a large number of relatively small files, system overhead and the associated processing tends to be the performance limiting factor or bottleneck, not encryption/decryption of the files. That being the case, the performance throughput across all five systems we tested, including the non-encrypting platform, was virtually identical. The difference in throughput between the fastest encrypting platform, the Seagate self-encrypting drive at 7.99 MB per second, and

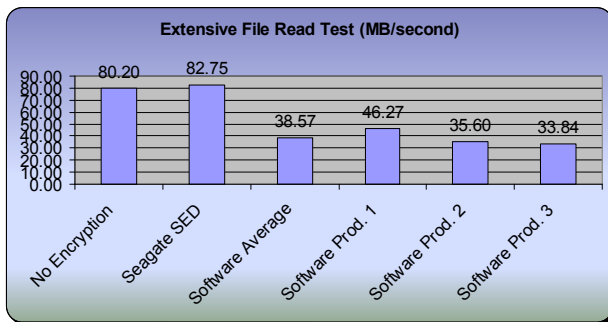
the slowest platform, one of the software products at 7.53 MB per second, was .46MB per second. Although measurable, this difference is not humanly detectable when starting up the system.

We had similar results when testing the throughput during typical, smaller sized application loading. The applications we used during these tests were common programs like Microsoft Word, Adobe Acrobat, and Internet browsers. These were all relatively small sized file operations when compared with the larger files we tested later. The difference in throughput between the various platforms for loading small applications was essentially not detectable. The same can be said of our throughput tests for reading and writing modest sized data files. The slowest software encryption product throughput was only .18MB per second behind the Seagate self-encrypting drive.

Full Disk Encryption Throughput Tests – Table 1

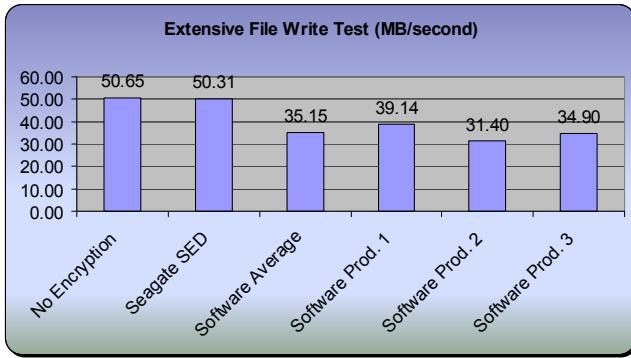
| | No Encryption | Seagate Self-Encrypting Drive | Software Encryption Average | Software Product 1 | Software Product 2 | Software Product 3 |
|--|---------------|-------------------------------|-----------------------------|--------------------|--------------------|--------------------|
| Startup Throughput (MB/second) | 7.90 | 7.99 | 7.73 | 7.87 | 7.80 | 7.53 |
| Application Loading (MB/second) | 5.89 | 5.71 | 5.51 | 5.63 | 5.50 | 5.40 |
| Modest Size File Test (MB/second) | 5.40 | 5.28 | 5.14 | 5.11 | 5.20 | 5.10 |
| Extensive Data Read (MB/second) | 80.20 | 82.75 | 38.57 | 46.27 | 35.60 | 33.84 |
| Extensive Data Write (MB/second) | 50.65 | 50.31 | 35.15 | 39.14 | 31.40 | 34.90 |

Our next test measured data throughput during extensive read operations like those performed during virus scanning, copying a large amount of data or when backing up the system. Here we saw huge differences in performance. The throughput of the software encryption products proved to be no match for the self-encrypting drives.



At 82.75 MB per second, the self-encrypting drives with their built in hardware encryption engine performed equally as well as standard disk drives, and 114% faster than the average of the three software encryption solutions we tested. The fastest software solution had a throughput of 46.27 MB per second. However, the Seagate self-encrypting drive was 79% faster

than the quickest software product, 132% faster than the next, and 144% faster than the slowest software based solution.



Our extensive file write performance tests also showed hardware encryption significantly outperforming software based encryption. Here again, the Seagate self-encrypting drive proved to be identical in performance throughput with the standard drive, and 43% faster than the average of the three software based solutions.

Next we turned our attention to the effect full disk encryption has on the time it takes to perform system startups, shutdown, and hibernation functions. As you can see from the table below, full disk encryption had little effect on system shutdown time, with the exception of one software product, which for some reason adds around 17 seconds to the time required to shut the system down.

Likewise, full disk encryption had little effect on the time it takes to hibernate. Although one software solution we tested added about 6 seconds, which most users won't find too annoying, the other products had very little effect on the time it takes to hibernate.

Recovering from a hibernation state is a different story. On average, the software solutions took nearly twice as long to recover from hibernation as the hardware based self-encrypting drives from Seagate, adding around 17 seconds. Wave Systems' pre-boot unlock of the self-encrypting drive took less than 3 seconds.

Full Disk Encryption System Startup/Shutdown Effect Tests – Table 2

| | No Encryption | Seagate Self-Encrypting Drive | Software Encryption Average | Software Product 1 | Software Product 2 | Software Product 3 |
|---|---------------|-------------------------------|-----------------------------|--------------------|--------------------|--------------------|
| Startup Time (seconds) | 37.10 | 34.47 | 47.24 | 41.49 | 52.02 | 48.22 |
| Shutdown Time (seconds) | 11.97 | 11.79 | 17.90 | 12.03 | 29.29 | 12.37 |
| Hibernate Time (seconds) | 29.16 | 28.62 | 31.14 | 28.71 | 29.61 | 35.1 |
| Hibernate Recover Time (seconds) | 21.42 | 23.22 | 40.80 | 26.37 | 41.26 | 54.76 |

Security, Implementation, and other Issues

While performance is a very important factor when selecting a full disk encryption solution, there are a number of other chief considerations. The relative security of the various technologies can be crucial for many organizations. Additionally, the time it takes to install and deploy a full disk encryption solution can be very significant, especially if hundreds or even thousands of PCs are involved. Our tests and experience with these products led us to some notable observations.

Software based encryption takes hours to install

One major observation was that software based encryption takes literally hours to install. Our first software product install took us about 25 minutes to get it installed and configured, not counting the process that encrypts the disk the first time. We did subsequent installs and configurations in about 12 minutes. However, all of the software products are time consuming to install, even after you have them mastered. One product did however, once the central policies were configured and set up, create very nice installation sets for the laptops. Although still time consuming, there were no difficult configurations or decisions to make during the end user machine installs.

The most serious deployment issue however is the actual time software solutions take to encrypt the disk the first time. Each of the software products, once installed and configured, encrypt all of the data on the disk. In the slowest products case, it took 23 hours and 46 minutes to complete the encryption on our 500 GB drives. This product offers two encryption options, one that is faster but won't guarantee system integrity if a power failure or abnormality occurs, or the slower, safer mode. We chose the latter as we believe most users or organizations would.

Another software based product took 8 hours and 9 minutes to encrypt the 500 GB drive. The company's technical support staff told us to expect about 1 hour of encryption time for every 40GB of data. Using that formula we expected it to take us 12 and ½ hours, but it actually finished in just over 8 hours. The fastest software product completed the task in 3 hours and 16 minutes.

All of the software products do the encryption completely in the background, so users can keep working and even power down their machine before the drive is fully encrypted. When the system is restarted, the background encryption process picks up where it left off and keeps right on encrypting until it is done. This is a nice feature, however until the encryption is complete the system's performance is seriously slowed. So doing anything that requires heavy file usage or processing power during the lengthy initial encryption of the drive can be painfully slow.

After all is said and done, not counting the time it takes to completely backup a system as recommended prior to installation, it took us anywhere from 3 ½ to 24 hours to finish the installation and initial encryption process for software based FDE products.

This is very different than when using a hardware approach such as a self-encrypting drive from Seagate. Since self-encrypting drives always automatically encrypts anything written to it, the operating system, applications, or any data on the drive is already encrypted as soon as it's stored on the drive. There is no need to perform the initial encryption process that software packages require. Apart from setting security policies and the key management that's necessary for every approach, the only requirement to start using a self-encrypting drive in a secure mode is to enroll authorized users, which only takes a minute or two utilizing the Wave Systems Trusted Drive Manager software.

It's scary to scramble everything on your hard disk

Another observation we experienced first hand is that it's scary to scramble everything on your hard disk. Even though we grew to be relatively comfortable with the robustness of the software encryption packages, the first few times we committed our laptops to the initial encryption process was frightening. Even though a user or administrator may have backed up their data, the thought of having something go wrong and having to restore the operating system and applications is not something users want to experience (we did have one installation that corrupted Microsoft Office and it had to be reinstalled). It's natural for users to resist the installation of software based encryption, especially those experiencing it the first time. This just isn't an issue when hardware based encryption is used. There's nothing that requires scrambling or encrypting by the operating system or an application because the drive hardware automatically encrypted everything as it was written to the disk.

Advantages of Hardware Security

While a detailed review of the security of the various FDE products was beyond the scope of this study, we felt it pertinent to comment on the generally accepted advantages of hardware based security over technologies that rely on software alone.

One of the primary drivers for laptop encryption today is to provide compliance to the various data protection laws. Unless an organization can prove that all personal or private data residing on a lost or stolen disk is securely encrypted, these laws require that, all potential victims must be notified of the possible loss of their information.

Some software based FDE solutions do a reasonable job in reporting a complete installation, and in preventing end users from removing or bypassing the data encryption on their laptops and can thus prove compliance. The extent of such controls depends of course on the specific security policies and implementation. But it is possible for some of the product's central management systems to provide reasonable proof that a given laptop's hard disk was encrypted at the time of a theft or loss.

However, not all of the software based solutions can do this. Some systems can't prove that a specific laptop's disk was ever encrypted, or that it is still being encrypted. For instance, we could find no controls in one of the software products that would prevent the end user from disabling or removing the encryption if they desired. Given the degradation in performance of software FDE, some users may elect to remove the encryption.

Since the performance of the Seagate self-encrypting drives we tested was as good as a standard drive, there is simply no incentive for users to remove or bypass the encryption, even if it were possible. Wave System's Embassy Remote Administration Server provides full audit logs of the security settings for all centrally managed self-encrypting drives for use to provide compliance to data protection laws in the event of a lost or stolen laptop. When centrally managed, Wave's client software disables all local changes to the security settings in order to maintain the integrity of the centralized audit logs

Another advantage of hardware based security is the protection of the authentication and encryption keys. By design self-encrypting drives do all of the cryptography within the disk drive controller, and unlike software FDE, the disk encryption keys are not present in the computer's CPU or memory where they are subject to theft. Likewise, authentication of

authorized user credentials is done within the protected hardware of the drive and never exposed within the memory or OS of the PC. Additionally the strength of the shadow master boot record approach used by self-encrypting drives is that the pre-boot code is highly protected and is not resident with the OS at any time. So OS attacks can't generally be used against a self-encrypting drive's pre-boot process.

Summary

Any type of full disk encryption is better than no encryption at all, but the performance advantages of self-encrypting disk drives, particularly when reading or writing large amounts of data is very compelling. The self-encrypting Seagate drive we used for these tests was as fast as a standard drive, and handled large file operations better than twice as fast as the software approaches to full disk encryption. The Wave System's self-encrypting drive management software provided access to the full range of the drive's features and security settings, including initialization of the pre-boot code and assigning users to the drive.

Another advantage of using laptops equipped with self-encrypting drives is the savings in time it takes to deploy the system. It's not necessary to initially encrypt the contents of the hard disk like software solutions require, a process that took us anywhere from 3 ½ hours to 24 hours per laptop. Organizations struggling to decide if it is more cost effective to use software solutions to encrypt existing laptops, or to upgrade to new laptops equipped with self-encrypting drives need to carefully consider the time involved and loss of performance when deploying software solutions.

Another factor in the total cost of ownership for data protection is that self-encrypting drives and the associated management drive software are being factory integrated by the PC OEMs as a primary security feature of the PC. For example, Dell currently offers Seagate self-encrypting drives and Wave's Embassy software as factory integrated features in their platforms. This provides enterprises with a single point of support, a pretested solution, and a stronger security model for the platform rather than adding encryption as a separate, aftermarket software package.

About Trusted Strategies

Trusted Strategies is the premier advisory, consulting, and market intelligence firm focused solely on the information technology (IT) security industry. Offering a unique, business-oriented perspective, Trusted Strategies provides accurate, expert, and concise market research and consulting for setting strategy and building business.

Trusted Strategies is privately held, and located in Pleasanton Calif.



Trusted Strategies LLC
Pleasanton, CA
(925) 461-1002
www.trustedstrategies.com