TRUSTED STRATEGIES

Full Drive Encryption with Samsung Solid State Drives

A performance and general review of Samsung's new self-encrypting solid state drives.

Trusted Strategies LLC
Author: Bill Bosen

November 2010

Sponsored by Samsung Electronics

Full Drive Encryption Using Samsung Solid State Drives

The new Samsung self-encrypting sold state drives are as fast as their standard SSDs, and offer a much faster and better full drive encryption (FDE) solution than installing software encryption with a traditional, rotating hard disk drive (HDD).

One of the big trends in cybersecurity is encrypting sensitive data on laptops and other portable devices. As our world becomes increasingly mobile, we take more and more of our sensitive data with us where it is subject to loss or theft. Encryption of that data is the best defense and the technology is gaining wide acceptance and adoption. In some industries or applications, government or industry regulations, such as breach notification laws, are progressively mandating that data must be encrypted. These regulations, along with the ever-growing security vulnerabilities and threats, are driving this important trend.

For many years, it has been possible to use software tools to encrypt hard drive data. Storage drives capable of automatic encryption within their own hardware are relatively new, but have many advantages over software implementations. At Trusted Strategies, we have been heavily involved in drive encryption technologies for 20 years, and it is exciting to see the recent advancements and developments in hardware-based drive encryption.

In an earlier paper, we studied and reported on using *self-encrypting hard drives* for full drive encryption (see Trusted Strategies' "FDE Performance Comparison – Hardware Versus Software Full Drive Encryption"). That report was focused on traditional self-encrypting *rotating* hard disk drives. However, in this report, we are presenting the findings of an additional study regarding *self-encrypting SSDs (solid state drives)*. In particular, we obtained and tested the new Samsung 128GB SSD with FDE (Full Drive Encryption). We were very eager to have this new state-of-the-art technology in our hands and put it through our series of tests.

Objectives

Our analysis had several objectives. Encryption requires a great deal of processing, and because FDE products encrypt everything on the device, including the operating system, the encryption performance is extremely important. So, our initial objective was to evaluate the performance of the device. Since most FDE implementations to date have used software encryption products like Microsoft's BitLocker, McAfee Endpoint Encryption, TrueCrypt, or others, we wanted to compare how the Samsung self-encrypting SSD performed when compared with a typical software-encrypting product.

Of course, we also wanted to compare how the Samsung self-encrypting SSD compared with their own standard, non-encrypting SSD. We were intent on determining what performance penalties, if any, one would encounter by going with the self-encrypting SSD over the standard SSD.

Another objective was to take a look at the security, deployment issues, manageability, and user experience of the device. While performance is a critical component to evaluate, if an organization's full drive encryption project is too difficult to deploy or manage, the entire effort will suffer or perhaps fail altogether. So, this was another area we wanted to explore.

Products Tested

The self-encrypting hardware products we evaluated included:

- Samsung 2.5" 128GB Standard SSD, Model MZ-5PA1280/0D1. The performance of this device was tested as-is with no encryption, and then again with software encryption added.
- Samsung 2.5" 128GB SSD with FDE, Model MZ-5PA1280/0D7 with FDE 1034. This is Samsung's self encrypting SSD.
- Although certainly not an apples to apples comparison, to establish some sort of a performance baseline, we also tested the standard, non encrypting 2.5" *rotating* 7200 RPM HDD (hard disk drive) that came stock in our test platform. The performance of this stock hard disk drive was tested as-is with no encryption, and then again with software encryption added.

For the software encrypting products, we tested 4 industry leaders. Although there were big differences in the management and deployment issues of these various products (especially in the time it took to do the initial drive encryption), once installed, the performance among the different software contenders was relatively similar for most operations. Ultimately, for our comparison with the SSD alternatives, we elected to report on the software encryption product that was most representative of the lot. It was consistently one of the best software performers in most areas, and tended to have our favorite features and options.

Since our objective was to evaluate the performance of SSD encryption against software encryption performance in general and not to single out the weaknesses of any particular product, we have opted not to name the software vendor. But you can take at least some comfort in the knowledge that it was one of the leading software products. We could have reported on any of the software products and the performance results would not have varied enough to make much difference when compared with the performance of the SSD devices.

Test Platforms and Procedures

For our test platforms, we used identical Dell Latitude E6410 laptops, running Microsoft® Windows 7 Professional - 64 bit. These machines were equipped with Intel® Dual Core vPro i5-540M Processors running at 2.53GHz with 4 GB of RAM. This platform was, of course, outfitted with the different drives we tested.

When testing the *software* FDE products, we tested both the standard 250 GB 7200 RPM drive that came stock on the Latitude along with software encryption added, and the standard non-encrypting Samsung SSD with software encryption added. For the *hardware*-based FDE tests, we used Samsung's self-encrypting SSD as noted above.

All in all, we tested the performance of 5 different platform configurations:

1. The stock Dell Latitude E6410 with its traditional rotating hard disk drive. No encryption whatsoever.
2. The Dell Latitude E6410 configured with Samsung's standard non-encrypting SSD. Again, no encryption whatsoever.
3. The Dell latitude E6410 with its traditional rotating hard disk drive plus *software full disk encryption.*
4. The Dell Latitude E6410 configured with Samsung's standard non-encrypting SSD *plus software full drive encryption.*
5. The Dell Latitude E6410 configured with Samsung's *self encrypting SSD*

Our performance test objectives included determining the data throughput of commonly used applications like those within Microsoft Office, Internet browsing, picture viewing, and the like. We also wanted to test throughput for drive intensive procedures like system backups, virus scanning, audio and video editing, and opening, reading, and writing large 100MB+ files used with data-intensive applications. Finally, we wanted to know how encryption might affect the performance of drive-heavy system processes such as startup, shutdown, and hibernation.

In addition to our own test procedures, we used *PassMark's Performance Test 7* benchmarking software to test and measure the throughput performance of the different encryption solutions. We found PassMark's drive test suite exceptionally well-designed for our needs. While we ran performance tests on the entire system, including the CPU, memory, and graphics, we concentrated on the drive test suites.

Our test procedures included freshly imaging and restoring the operating system and applications before each and every specific test. We also repeated each of the tests at least three times, and included the mean of the three or more tests.

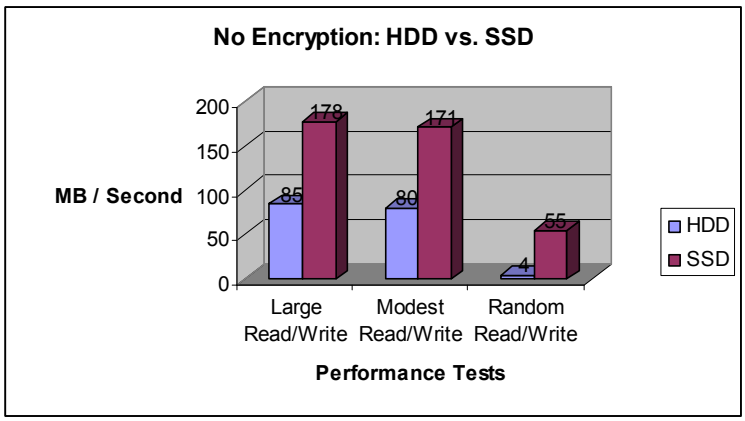
The specific tests conducted for each of the platform configurations included the following:

- *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 drive 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
- *Large Scale Data Read*: This test measures throughput while reading 2 GB of files. This test is 99.5% read activity. This test is also an effective way to test the performance of data backup procedures.
- *Large Scale Data Write*: Measures throughput while writing 2 GB of data onto the drive. No read operations were involved in this test.
- *System Startup*: Elapsed time, 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.

Performance Results:

Our baseline tests used no encryption at all on either the traditional HDD, or on the non-encrypting SSD. When comparing these two test results, as expected, the SSD was significantly faster than a traditional rotating hard disk drive. In fact, it was more than twice as fast as the HDD for large scale read/write operations, 7 times faster for modest sized files, and up to 13 times faster for highly randomized read/write activity. *See Full Drive Encryption Throughput Tests – Table 1.*



The differences were startling. The SSD was significantly faster than we expected.

Full Drive Encryption Throughput Tests – *Table 1*

	Stock HDD No Encryption	Samsung SSD No Encryption	Stock HDD with Software Encryption	Samsung SSD with Software Encryption	Samsung Self Encrypting SSD
Startup Throughput (MB/second)	7.90	82.50	6.97	47.90	95.33
Application Loading (MB/second)	7.03	48.33	5.77	30.77	60.37
Modest Size File Test (MB/second)	6.13	41.13	5.00	26.77	50.40
Large Scale Data Read (MB/second)	84.67	178.00	52.88	70.23	169.33
Large Scale Data Write (MB/second)	79.60	170.80	49.50	63.60	164.50
Random R/W (MB/second)	4.07	54.77	2.51	29.57	54.50
PassMark Overall Disk Rating	608.53	1457.50	380.10	590.70	1404.23

Self-encrypting SSD as fast as standard SSD

Next we examined the results to see how the self-encrypting SSD compared with the standard non-encrypting SSD. Other than the hardware encryption, these two devices appear to be exactly the same model. The self-encrypting SSD has the added hardware to accelerate the encryption and provide robust security, but otherwise the specs of the two drives are indistinguishable.

Our tests showed that the Samsung self-encrypting SSD had nearly identical performance when compared with the non-encrypting SSD. So, organizations choosing the self-encrypting hardware will see virtually no degradation in performance over the non-encrypting device. For large scale data reading, the encrypting SSD achieved an impressive 169.33 megabytes per second. This was nearly as fast as the non-encrypting SSD which achieved 178.0 MB per second. Large scale writing throughput was also very similar at 164.50 MB/second for the encrypting SSD vs. 170.80 for the standard SSD.

This performance consistency was also true for heavily randomized read/write activity where the encrypting SSD scored 54.50 MB/second and the standard SSD was measured at 54.77 MB/second. It is interesting that the optimization and hardware acceleration of the self-encrypting SSD performs so well that it is actually slightly faster in a couple of areas. Although probably not noticeable in typical use, the self-encrypting SSD outperformed the standard SSD during startup, application loading, and working with small to modest files. In our tests, shutting down the system configured with encryption did take a little over 2 seconds longer than shutting down the non-encrypting system. See *Full Drive Encryption System Startup/Shutdown Tests – Table 2*. Overall, the self-encrypting SSD performed as well as the standard SSD.

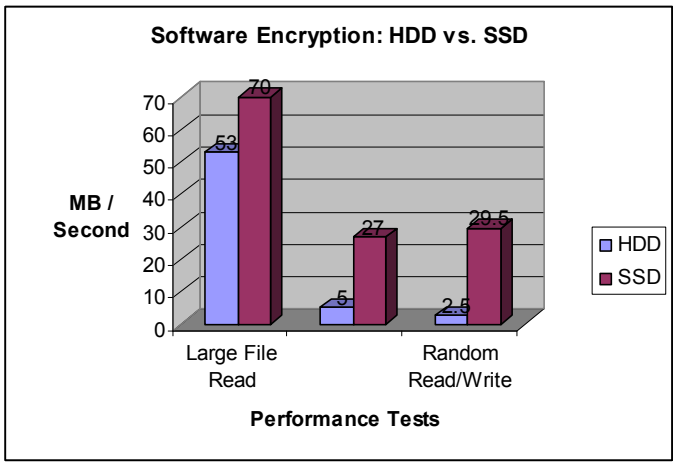
Full Drive Encryption System Startup/Shutdown Tests – *Table 2*

	Stock HDD No Encryption	Samsung SSD No Encryption	Stock HDD with Software Encryption	Samsung SSD with Software Encryption	Samsung Self Encrypting SSD
Startup Time (seconds)	56.02	42.53	58.88	47.71	42.92
Shutdown Time (seconds)	14.50	8.66	15.18	12.12	11.25
Hibernate Time (seconds)	18.95	14.15	19.25	15.68	15.64
Hibernate Recover Time (seconds)	35.27	32.60	38.08	39.42	31.43

If using software encryption - SSD is significantly faster than HDD

With the performance advantages of hardware encryption, we believe most enterprises will migrate to hardware-based full drive encryption during the next 3 years. However, some organizations might be contemplating a continuation of their software encryption programs for a period of time, wondering when the correct time to convert to hardware encryption will be. So, to help answer that question, we tested the performance options of using software full drive encryption with SSDs, versus doing so with traditional HDDs.

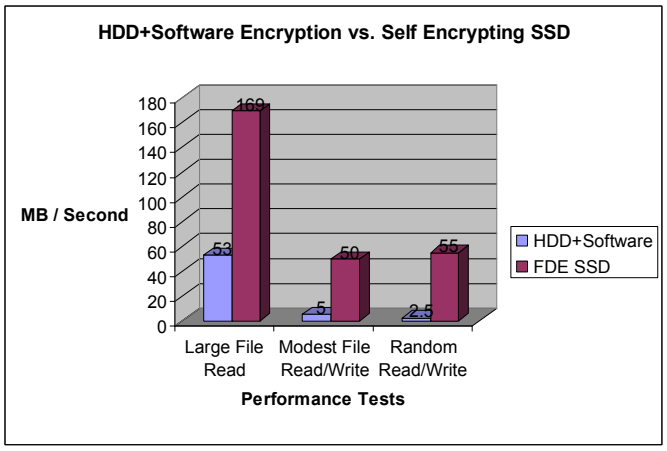
As one might expect, software encryption turned out to be much faster when installed on a PC with a SSD instead of a traditional hard disk drive (HDD). The throughput for large scale data reading was clocked at 70.23 MB/second for the standard SSD plus software encryption versus 52.88 MB/second for the PC with a traditional hard drive and software encryption. Large scale data writes showed a similar advantage for the SSD configuration at 63.50 MB/second versus 49.50 MB/second.



The SSD advantages become even more pronounced when considering the performance of random read/write activities or the throughput for smaller file sizes. For these operations, the SSD was at least 5 times faster than the HDD, and sometimes as high as 11 times faster. Our test machine configured with a traditional HDD and software encryption ran the random read/write test at 2.51 MB/second. When the SSD with software encryption added was tested, it achieved 29.57 MB/second. That's better than 11 times faster than with the traditional hard disk drive configuration.

Self-encrypting SSD over 3 times faster than HDD with software encryption

As noted previously, most implementations of full drive encryption today rely on software encryption packages installed on platforms with traditional rotating hard disk drives. We wanted to examine the performance gains an organization might see if they upgraded to hardware-based encryption using self-encrypting SSD technology. So, we analyzed the performance difference between systems doing encryption in software on a traditional HDD, and those performing encryption within the hardware of self encrypting SSDs.

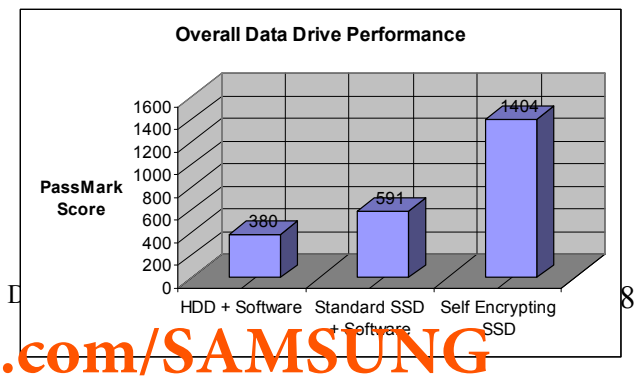


The results of our tests showed obvious performance advantages of the self-encrypting SSD configuration over software encryption on a traditional HDD-based PC. The HDD platform using software encryption achieved 52.88 MB/second throughput in our large scale data read test. The self-encrypting SSD ran over 3 times faster, clocking in at 169.33 MB/second throughput. For random read/write operations, the system with a HDD and software encryption ran at a meager 2.51 MB/second, whereas the self-encrypting SSD was over 21 times faster at 54.50 MB/second. And the self-encrypting SSD was 10 times faster doing operations with modest file sizes.

Overall, the SSD-based system significantly out-performed the software-based solution in every test, including system startup and shutdown, hibernation and recovery, application loading, and all other operations. PassMark, one of the benchmarking systems we used, calculated an overall score for all drive performance tests it conducted. The HDD system with software encryption scored 380. The system equipped with the self-encrypting SSD scored 1404, well over 3 times faster than a software approach with traditional rotating disk drives.

Self-encrypting SSD - Fastest overall encryption

When compared with the other alternatives tested, our results showed that the fastest encryption was achieved by the Samsung self-encrypting SSD.



The traditional HDD with software encryption scored 380 on our overall PassMark drive performance test. The SSD with software encryption was almost twice as fast with a score of 591. The self-encrypting SSD achieved the highest score of 1404.

Security, Implementation, and other Issues

As important as performance is when selecting a full drive encryption solution, the relative security and costs to implement and maintain an organization's full drive encryption program is very important. Here again, the new Samsung drives we evaluated in this report have distinct benefits over software approaches.

One major advantage of hardware-based security over software-based solutions is the way the authentication and encryption keys are protected. Self-encrypting drives perform all cryptography within the hardware-protected drive controller. Unlike software FDE, the drive encryption keys are not present in the computer's CPU or memory where they are subject to theft.

Another nice feature of hardware-based security as implemented in the self-encrypting SSD and associated management software is that the encryption is always on, even when an equipped laptop is first purchased. And, there is no way for users to disable or remove the protection. This not only helps ensure data is encrypted at all times, but makes it much easier to prove compliance with encryption regulations.

Additionally, the time it takes to install and deploy a full drive encryption solution can be very significant, especially if hundreds or even thousands of PCs are involved. Software-based encryption takes hours to install on a typical laptop with a 128GB or larger drive. We installed one software encryption package on a 500GB drive that took almost 24 hours to complete the installation. Multiply that by the number of laptops in a large organization and the implementation hassles become very significant.

Contrast that with the thought of purchasing a laptop with an encrypting drive already installed. In this latter case, all one needs to do is add authentication credentials and they are all set.

Summary

The performance advantages of self-encrypting drives, particularly solid state devices, are very compelling. The self-encrypting SSD we tested from Samsung was just as fast as their non-encrypting SSD, so there is no performance penalty for protecting the enterprise's laptops with encryption. And, when compared with the alternative of using full drive encryption software on a platform equipped with a traditional rotating hard disk drive, the Samsung SSD is faster by far.

Another advantage of using laptops equipped with self-encrypting drives as opposed to add-on software encryption packages is the savings in time it takes to deploy the system. It is not

necessary to initially encrypt the contents of the drive 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. We came away very impressed with the Samsung SSDs.

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