FDE HARD DISK DRIVE CONCERNED ISSUE.

There is some confusion around the market for FDE products from customer.

- Is hardware FDE vulnerable to the DRAM freezing attack?.
- What about passwords? Is it possible to find passwords in memory?.
- What types of encryption are vulnerable to the key theft via the memory?.
- My key is 128 to 256 bits in 1 GB (or more) of memory. Isn't this like looking for a needle in a haystack?.
- Why would someone want to steal my key? Wouldn't it be easier to just steal my data?.
- Can I change my encryption key to keep a thief from getting my data?.
- If I power off my computer, am I vulnerable to data theft?.
- Does the type of encryption matter in this theft?.
- What can I do to prevent this theft?.
- Is it possible to remove my encryption key from memory when my computer is in stand by mode?.
- How does hardware FDE help?.
- Are the 256-AES product offerings better than comparable 128-AES product?.
- Are System performance negatively impacted by encryption process?.
- Are more energy should be focused on solution-level deployment issue when put encryption engine to the rest?.
- How is it operation speed?.

This is FDE hard disk drive some performance test example on Seagate Momentus 5400 FDE.2 ST9169824AS-FDE. (Information from http://www.tomshardware.com/reviews/momentus-5400-fde,1742-3.html)

The Momentus 5400 FDE.2 follows Seagate's product naming conventions, which consists of the product family (Momentus), the speed class (5400 RPM) and the product generation (5400.3 equals the third generation). In case of the encrypted Momentus 5400 FDE.2 we're talking about the second generation of encrypted 2.5" Momentus products. The Momentus 5400 FDE.2 family is available at mainstream capacities of 80 GB, 120 GB and 160 GB, based on first-generation perpendicular magnetic recording. All of them rotate at 5,400 RPM, connect via a Serial ATA/150 interface and have 8 MB cache memory. Our test sample is the 160 GB top model, which is based on two platters. The weight of 102 g is typical for dual-platter 2.5" drives, and we measured a power consumption of up to 3.2 W maximum and 0.9 W idle. This is, not surprisingly, exactly the same as that of the drive's non-encrypting brother, the Momentus 5400.3.

In addition to the limited support - Windows XP only, with Vista not yet supported - we found some other obstacles that could prove annoying. For starters, the encryption feature and software does not seem to work with all chipsets. Information about this can be found in the readme file, but it's not obvious when browsing the product features. Our first test system was an Acer Ferrari 1000 notebook based on an integrated ATI chipset, which caused the FinallySecure software to say goodbye with a runtime error. We then decided to run the tests on a system based on an Intel G33 chipset platform, which worked properly. Although we're sure that only very few Momentus 5400 FDE.2 drives will be sold in retail - I expect most of them to be found in notebook solutions from Dell and others - **the limited chipset support could be an issue.**

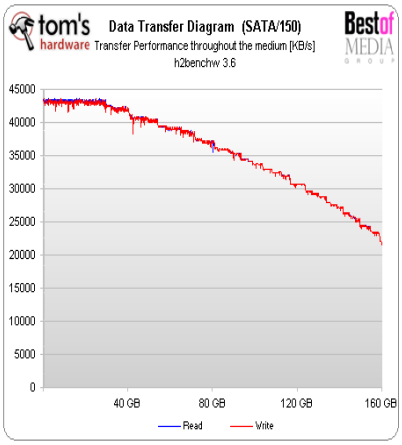
For Benchmarks

	System Hardware
Processor(s)	2x Intel Xeon Processor (Nocona core) 3.6 GHz, FSB800, 1 MB L2 Cache
Platform	Asus NCL-DS (Socket 604) Intel E7520 Chipset, BIOS 1005
RAM	Corsair CM72DD512AR-400 (DDR2-400 ECC, reg.) 2x 512 MB, CL3-3-3-10 Timings
System Drive	Western Digital Caviar WD1200JB 120 GB, 7,200 RPM, 8 MB Cache, UltraATA/100
Mass Storage Controller(s)	Intel 82801EB UltraATA/100 Controller (ICH5) Promise SATA 300TX4 Promise FastTrak TX4310 Driver 2.06.1.310
Networking	Broadcom BCM5721 On-Board Gigabit Ethernet NIC
Graphics Subsystem	On-Board Graphics ATI RageXL, 8 MB
	System Hardware
Performance Measurement	c't h2benchw 3.6 PCMark05 V1.01
I/O-Performance	IOMeter 2003.05.10 Fileserver-Benchmark Webserver-Benchmark Database-Benchmark Workstation-Benchmark
	System Software & Drivers
OS	Microsoft Windows Server 2003 Enterprise Edition, Service Pack 1
Platform Driver	Intel Chipset Installation Utility 7.0.0.1025
Graphics Driver	Default Windows Graphics Driver

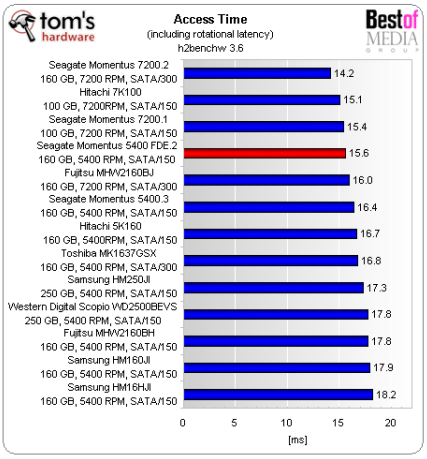
For FDE Features

	System Hardware
CPU Intel	Intel Core 2 Duo E4400 (Conroe 65nm; 2,0 GHz, 2 MB L2 Cache)
Motherboard (Intel)	Gigabyte G33M-S2H, Socket 775 (Rev. 1.0) Intel G33 Chipset
RAM	Corsair CM2X1024-8500C5 2x 1024 MB DDR2-800 (CL 5-5-5-15 2T)
DVD-ROM	Samsung SH-S183
Graphics Card	Integrated Intel GMA 3100
Sound Card	Integrated ALC889A
Power Supply	Coolermaster RS-450-ACL4 ATX 2.2, 450 Watt
	System Software & Drivers
OS	Windows XP Professional 5.10.2600, Service Pack 2
DirectX Version	9.0c (4.09.0000.0904)
Platform Drivers Intel	Version 8.3.0.1013

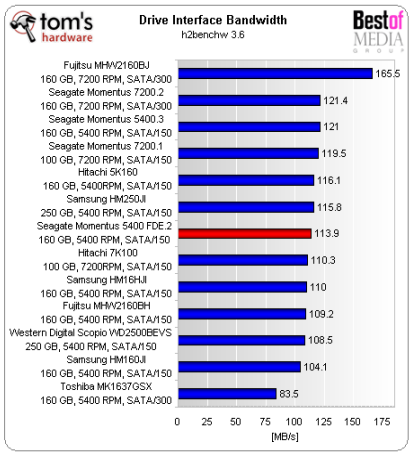
Data Transfer Diagram

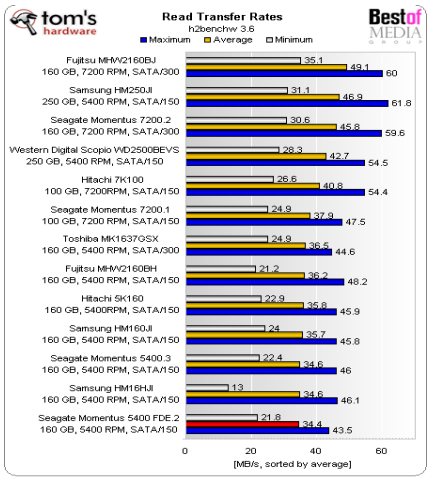


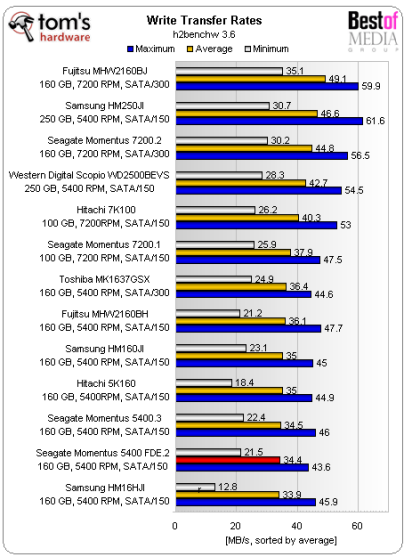
Access Time

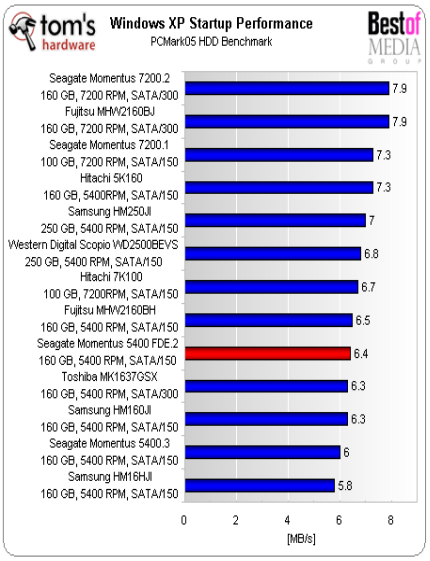


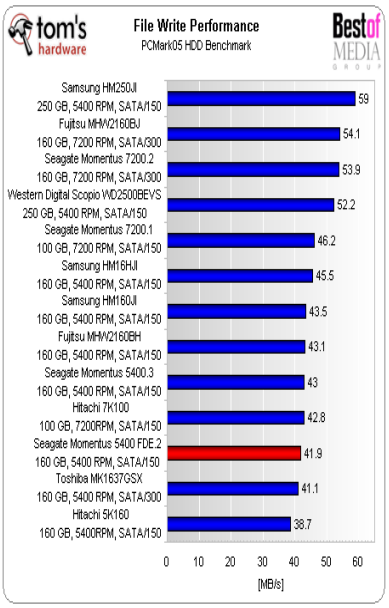
Interface Performance

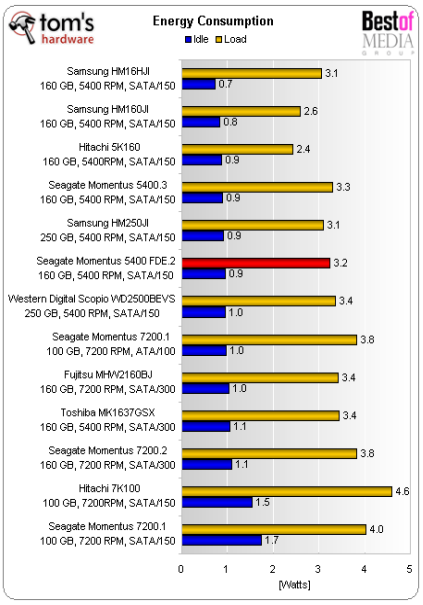


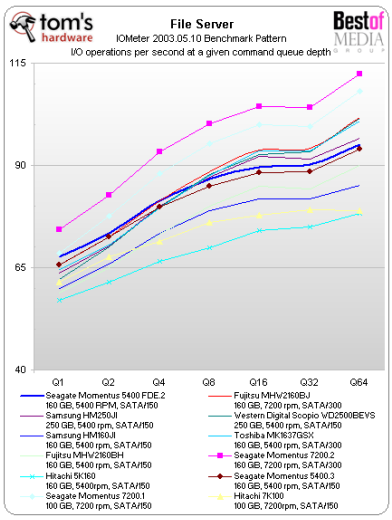


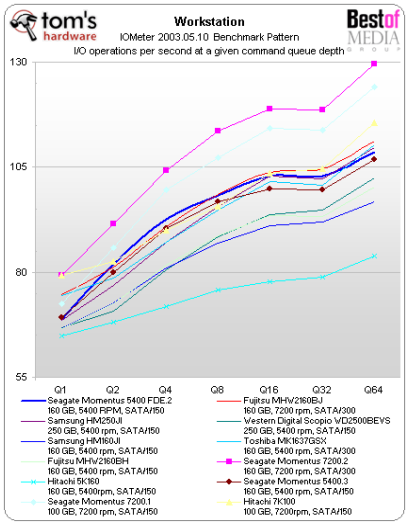












The product is fast enough, though not capable of competing with the latest 2.5" hard drives at up to 250 GB, not to mention 7,200 RPM drives or Flash-based hard drives. Everyday work with the Momentus 5400 FDE.2 is smooth, and the only handicap is the slower boot process, which we found to still be tolerable.

FDE HARD DISK DRIVE CONCERNED ISSUE CONCLUSION

- **Power consumption** : About 3.2 watts at working mode. Its quite different among another hard disk drive that have the same 5400 rpm spindle speed.
- **Read, Write transfer rate** : About 34.4 MB/s. Its transfer rate are too low when compared with another.
- **File Write Performance** : About 41.9 MB/s. Its transfer rate are too low when compared with another.
- **Command Queue depth** : highest consumption times to perform I/O operation. It will impact system performance.
- **Access Time** : About 15.6 ms. Its access time is O.K.
- **Miscellaneous issue** : Limited chip set support, RPM is concerned for Read & Write transfer rate and power consumption, Strength of cryptography(128/256 bit key length).