Abstract
This white paper describes how Seagate® Momentus® 5400 FDE.2 hard drives provide best-in-class data protection for lost or stolen laptops. The paper also introduces DriveTrust™ technology—the foundation for Momentus 5400 FDE.2 hard drives with full-disk encryption—and presents a business case for hardware-based security throughout the enterprise.

Mobile Computing Increases Data Security Risks
A laptop computer is standard issue for today’s information worker. But while mobile computing is a boon for productivity, the number of large data security breaches has dramatically increased as a result. The reason is simple: laptops are more easily lost or stolen than desktop systems. And as laptop disk drives grow in capacity, these systems can carry vast amounts of potentially sensitive information.

In response to these trends, federal and state governments in the United States have implemented legislation with costly penalties for companies that lose unencrypted personal data. As of January 2007, thirty-four U.S. states require companies to publicly disclose data security breaches or notify affected customers. The U.S. government enforces the Sarbanes-Oxley Act and the Health Insurance Portability and Accountability Act (HIPAA), putting pressure on publicly traded companies, and firms that do business with them, to shore up data management. Governments outside the United States have implemented similar measures.

These government regulations, together with growing public awareness about data security and privacy, mean that a lost or stolen laptop could cost a company millions of dollars and significantly harm its brand image. Industry experts estimate
a single data security breach costs an average of US$14 million in direct expenses (such as legal fees and customer notification), indirect costs (such as lost productivity) and opportunity costs (such as customer loss and customer recruitment).

Benefits of Hardware-Based Full-Disk Encryption

Seagate addresses the issue of laptop data security with the Momentus 5400 FDE.2 hard drive, which combines a Serial ATA interface and capacities up to 160 GB with full-disk encryption. Because encryption is recognized as a best practice for protecting private data, many states offer a “safe harbor” to companies that can prove the data on lost or stolen hard drives was encrypted. Seagate Momentus 5400 FDE.2 hard drives help companies comply with privacy laws because encryption is always on and cannot be circumvented by users, as in many software-based products.

From a technical standpoint, the Momentus 5400 FDE.2 hard drive’s encryption solution is more secure than software-based encryption solutions because it is sealed off from other elements of the computing system. Where software-based products rely on the computer operating system, full-disk encryption uses specialized hardware circuitry within the drive. This isolation makes it nearly impossible for data thieves to exploit operating system vulnerabilities to compromise the encryption. And even if data thieves have physical access to the disk, they cannot locate the key, because it is never stored in the clear. Rather, the key is mixed with user credentials and stored in that form in hidden memory on the drive.

The Momentus 5400 FDE.2 hard drive offers a compelling laptop data security solution from both a technical and business standpoint. The main benefits include:

- **Transparent encryption**—Momentus 5400 FDE.2 hard drive encryption is easy to use and requires minimal setup. When turning on their computer—before the operating system boots up—users simply submit their credentials and the drive automatically encrypts all data written to it. (Credentials can include passwords, USB tokens or biometrics.) Users never need to think about using the encryption solution because it runs continuously and encrypts all hard-drive data, not just particular files or folders. And unlike software-based products, Momentus 5400 FDE.2 hard drive encryption does not require labor-intensive installation, initial encryption processes or configuration.

- **Strong authentication**—The Momentus 5400 FDE.2 hard drive combines the most advanced cryptographic technologies to protect data, including standards published by the U.S. National Institute of Standards and Technology. Secure Hash Algorithm-1 (SHA-1) is used for authentication and RSA for public-key encryption. To encrypt data and render it unreadable by potential thieves, the Momentus 5400 FDE.2 hard drive uses the 128-bit Advanced Encryption Standard (AES) algorithm.

- **No performance penalty**—Unlike software-based encryption products that rely on the central processing unit to encrypt data, the Momentus 5400 FDE.2 hard drive uses a specialized chip inside the hard drive to encrypt data at full interface speed so there is no noticeable performance penalty.

- **Lowest total cost-of-ownership compared with software-based encryption**—the Momentus 5400 FDE.2 hard drive enhances existing data security frameworks without adding extensive administrative burdens for corporate IT departments. Because it is seamless to integrate and requires minimal configuration, the Momentus 5400 FDE.2 hard drive helps save time and money. The drive supports cryptographic key-management and password-management tasks, and also works with Seagate partner solutions for advanced enterprise-management needs. And because Momentus 5400 FDE.2 hard drives offer fast cryptographic erase, they eliminate complicated and expensive disposal processes.
DriveTrust Brings Laptop Security to a New Level

The Momentus 5400 FDE.2 hard drive takes advantage of DriveTrust technology from Seagate, which implements security on the hard drive itself to offer a best-in-class data protection solution compared to software-based products. With DriveTrust, the drive introduces a number of unprecedented features that strengthen enterprise data security at its weakest points and simplify IT administration.

- **Cryptographic erase**—Government entities and large corporations spend millions of dollars to ensure that sensitive data is not recovered from discarded or repurposed hard drives. By simply changing the encryption key on a Momentus 5400 FDE.2 hard drive, IT administrators instantaneously render all stored data unintelligible. Compared to traditional overwrite and erase techniques, the drive’s cryptographic erase function is much simpler, dramatically faster, more secure, less expensive and less prone to human error.

- **Pre-Boot Authentication**—Because it is not dependent on the computer operating system, the Momentus 5400 FDE.2 hard drive engages its security function before the operating system boots up. Users have five chances to enter the correct password. (Third-party solutions can easily replace password authentication with smart card readers or biometrics.) Upon the fifth failure, the drive shuts down and the user must restart the computer to try again. Because the computer operating system will not boot up without authentication, potential data thieves cannot exploit software vulnerabilities to compromise security.

- **Emergency Password Recovery**—Password management for encryption is cited by IT leaders as a major barrier to the adoption of full-disk encryption solutions. The Momentus 5400 FDE.2 hard drive offers centralized management capabilities to ease administrative tasks in case of upgrades, repurposing or lost passwords. Besides the ability to create a master password, the drive supports escrowed passwords so that data recovery services can retrieve data from the drive. In addition, the Momentus 5400 FDE.2 hard drive works with third-party solutions that make it easy for administrators and users to create and back up passwords.

- **Enterprise Management Tools**—Seagate provides independent software vendors (ISVs) with a software development kit (SDK) they can use to take advantage of DriveTrust technology in their applications. For example, these applications include security management software solutions that simplify enterprise deployments and make it easier for IT administrators to manage hard-drive usage policy and security settings.

- **Security providers**—Every hard drive reserves a portion of its disk capacity for internal system memory. DriveTrust uses some of this space to create security providers (secure partitions) that are both logically and physically separated from the rest of the disk drive memory, with strong conditional access controls. The Momentus 5400 FDE.2 hard drive uses these exclusive security providers to store sensitive data, including cryptographic keys. DriveTrust-equipped disk drives can make security providers exclusively available to applications that present the proper credentials. ISVs can make use of this capability to build strong authentication functions into their applications.

**Trusted Computing for the Enterprise**

Seagate believes that grounding security functions where data lives—in the disk drive—can make enterprise data security stronger and easier to manage. Looking beyond full disk encryption for laptops, Seagate believes DriveTrust holds the potential to improve security for networked storage, portable storage devices, desktops and other computers that utilize disk drives. In each of these scenarios, DriveTrust-equipped disk drives act as a toolbox of hardware-based security functions, or what security experts dub a “cryptographic service provider.” In short, DriveTrust takes advantage of the hard drive’s isolated operations to serve as a platform for hardware-based security.
Seagate is a pioneer in storage-based security, but is not alone in its efforts. Seagate is an active board member and leader in the Trusted Computing Group (TCG), a not-for-profit industry organization helping to develop and promote open, vendor-neutral trusted computing standards. Seagate developed DriveTrust technology in conjunction with the company’s work as chair of the TCG’s Storage Work Group. DriveTrust is consistent with the TCG’s Core Storage Specification, which is currently in final draft form. This consistency helps ensure DriveTrust-enabled drives like the Momentus 5400 FDE.2 hard drive will fit into broader, trusted computing efforts.

In addition to its standards work, Seagate is collaborating with ISVs and technology providers on applications that take advantage of DriveTrust technology. For example, DriveTrust-equipped disk drives allow applications to store cryptographic keys on the disk drive, eliminating the need for key escrowing and simplifying credential management. Using the Seagate-provided SDK mentioned earlier, enterprise IT departments and third-party software developers can integrate the DriveTrust platform into their solutions. Seagate envisions DriveTrust-equipped disk drives working with BIOS software, biometrics and companies’ existing investments in the TCG’s Trusted Platform Module. Some potential applications of DriveTrust technology in an enterprise setting include:

- **Hardware-based security for biometric authentication data**—Biometric authentication is cutting-edge technology that verifies users, but what happens if these biometric credentials are compromised? DriveTrust technology allows software applications to store biometric data in security providers on hidden portions of the hard drive for the best possible security.

- **Secure credentials and user data for multi-user computers**—By taking advantage of the security providers on DriveTrust-equipped disk drives, organizations can securely manage user accounts for shared computers. For example, a financial institution could provide an entire office access to a shared computer while storing each user’s account information separately and securely.

- **Centralized authentication and credentialing for DriveTrust-equipped drives in multiple-drive environments**—The TCG Storage Work Group is developing standards that will allow enterprises to implement policy-driven authentication across their networked or array-based storage infrastructure, backed with DriveTrust hardware-based security. This base-level protection will complement other security measures implemented higher up the storage architecture.

- **Enterprise management of USB-attached external hard drives through drive pairing and encryption**—USB-attached external hard drives pose a serious risk to IT security because people can discretely copy and walk away with gigabytes of data in a matter of minutes. IT departments can utilize drive-pairing functionality, enabled through DriveTrust, so that department computers only work with authorized external hard drives.

**Conclusion**

Laptop security is the weak link in overall enterprise data security. Without an always-on, full-disk encryption solution to protect data on lost or stolen laptops, organizations risk losing millions of dollars in legal fees and customer notifications, not to mention customer goodwill. The Seagate Momentus 5400 FDE.2 hard drive offers an easy-to-manage, cost-effective solution to the laptop security challenge.

Moreover, the innovative DriveTrust security platform enables organizations to take advantage of hardware-based security functions that strengthen existing security frameworks. With security functions rooted in the hard drive, potential data thieves can no longer exploit software vulnerabilities to compromise security.

Seagate continues to pioneer drive-based security and make the technology available to ISVs and solution providers with the goal of making the overall computing environment more secure for business.
Resources

To learn more about the Seagate Momentus 5400 FDE.2 hard drive, visit: www.seagate.com/www/en-us/products/laptops/momentus/momentus_5400_fde.2/.

To read about the TCG Storage Work Group, visit: www.trustedcomputinggroup.org/groups/storage/.

For more information about DriveTrust technology, read these white papers:

