



Protecting Your Business from Costly Data Theft: Why *Hardware-Based* Encryption Is the Answer

The Data Breach Epidemic Continues . . .	1
Data Encryption Choices for Businesses	2
The Hardware vs. Software Debate	2
Trusted Platform Modules and Windows Vista	3
Building Encryption into the Hard Drive	3
Conclusion	5
About Wave Systems	5

Abstract

The availability this year of the first fully encrypting hard drives for notebook PCs promises to alter how companies evaluate protection of data in the enterprise. This white paper discusses the promise of full disk encryption (FDE) hard drives and examines the key advantages of FDE for minimizing costly—and embarrassing—data breaches. Lingering concerns over performance and compatibility of software-based FDE give security lobbyists a reason to make FDE drives the bedrock of their enterprise’s data protection strategy for notebook computers. To guarantee security and performance, the FDE solution must be based in hardware, rather than software (as most FDE solutions are today). The paper also examines how file and folder encryption plays a complementary role to FDE and is vital for a complete data protection strategy.

The Data Breach Epidemic Continues

What do Starbucks, T-Mobile, Citibank and H&R Block have in common?

As with countless other businesses, each of these companies was recently forced to disclose a loss of sensitive customer data. In fact, more than 100 million data records of U.S. residents have been exposed as a result of data security breaches since 2005 alone, according to the Privacy Rights Clearinghouse. Contributing to the problem is the proliferating use of notebook PCs that end up storing increasing amounts of sensitive personal and business information. In 2006, incidents of stolen laptops and data breaches skyrocketed, resulting in lost customers, legal fees, insurance claims, counteractive measures and tarnished reputations – damages affecting the bottom line.

In June of 2006, the President of the U.S. issued a directive requiring government agencies to encrypt all sensitive data on mobile devices. In fact, thirty-seven U.S. states, the U.S. federal government and many countries worldwide have passed data protection laws. In the case of most U.S. laws, negligence equates to liability if “reasonable” security hasn’t been enacted. U.S. regulations such as the Health Insurance Portability and Accountability Act and Sarbanes-Oxley Act place

March 2007
www.wave.com

stringent controls around access to sensitive data and mandate stiff penalties for firms found out of compliance. Further legislation under consideration in one state, for example, proposes to make any entity whose sensitive customer information is stolen be liable to card-issuing banks for costs incurred due to the breach and subsequent fraudulent activity. If passed, legislation such as this could be a key step to compelling businesses to invest in stronger data security measures.

Data Encryption Choices for Businesses

Given this regulatory environment and an estimated cost of \$14 million per incident for each data breach, according to the Ponemon Institute, it's no surprise that companies are turning en masse to data encryption, the process of encoding information in such a way that only the person (or computer) with the encryption key can decode it.

Two of the most popular encryption methods are file and folder encryption and full disk encryption (FDE). File and folder encryption enables users to protect individual files, folders or volumes, including the creation of virtual secure drives that may or may not reside on the user's hard drive. Most file and folder encryption solutions also extend to shared virtual drives, which can be used by groups of users based on security policies.

With FDE, software or hardware is used to encrypt every bit of data that goes on a disk, including the operating system. One highly touted benefit of FDE is that no user action is required to specify which files to encrypt. By having an encryption solution that is "always on" and doesn't depend on manual steps by the user, the element of human error is eliminated.

FDE addresses the problem of external threats, as in the case of a laptop getting into the hands of a thief. Even if the drive is removed from the laptop and data recovery tools are used, the data will be inaccessible. However, FDE protects data, while it remains on the physical hard drive and the user has not authenticated to the system. Data is exposed when it is moved off the hard drive, or if something (like a Trojan horse) or someone accesses the data, while the system is running. That's where file and folder encryption complements FDE, by counteracting the problem of internal threats; such as, malware running while the system is being used as well as insider snooping. File and folder encryption also protects data when it is stored off the drive; such as, on a USB flash drive or a network drive. With file and folder encryption, even an IT person who has access to the data's location will not be able to view the encrypted data.

The Hardware vs. Software Debate

All FDE solutions are not created equal. The majority of FDE solutions today employ software-based encryption, which means that the highly sensitive encryption keys necessary for encryption are created using software and the computer's main processor. This leaves the keys vulnerable. And, as sophisticated hackers know, running the PC's operating system is an observable process, thereby making it possible for malware to trap encryption keys.

Other major limitations for software-based FDE are the issues of system performance and complexity. All software-based FDE affects system performance, which is typically undesirable for both users and administrators. Further disadvantages of software-based FDE are that software upgrades, backup and recovery, administration and repurposing drives can be complex and error-prone.

The first notebook hard drives that use hardware, not software, as a basis for encrypting all of the data on the drive are now hitting the market. The major drawback is that a new drive must be purchased versus installing software on an existing drive. However, the benefits are plentiful with stronger authentication measures, encryption performance that matches the throughput of the drive interface, no impact to platform performance and lower maintenance costs.

For security, total cost of ownership and performance, hardware trumps software every time.

Trusted Platform Modules and Windows Vista

When key generation and storage takes place on a dedicated hardware chip; such as, a Trusted Platform Module (TPM) on the PC motherboard or a security chip on the physical hard drive, the keys are protected from hackers or malware. Since TPM chips have emerged as a standard feature on most business-class PCs, inexpensive hardware protection built into the PC itself is becoming ubiquitous (recent estimates indicate more than 50 million TPM-equipped PCs have shipped through 2006).

Microsoft endorses the TPM in its long-awaited Vista operating system released in January. One edition of Vista comes with BitLocker, an application that encrypts the entire Windows volume and optionally utilizes the TPM. As an embedded component of the operating system, BitLocker is a natural choice for businesses looking to ease into FDE – although it is worth noting that only the Windows volume is encrypted, not necessarily the entire hard drive. When used with the TPM security chip, additional protection is provided for the system boot process. However, Vista Ultimate, the version containing BitLocker support, costs \$100 more than the more popular Vista Business version. Furthermore, BitLocker only works on Vista (not XP) and only with a version 1.2 TPM chip. Tens of millions of PCs have been shipped with version 1.1 TPM chips. These systems will not be able to use the BitLocker/TPM solution, when they are upgraded to Vista.

Building Encryption into the Hard Drive

Rather than integrating encryption with the operating system, building encryption and access control directly into the hard drive is a natural evolution for hardware-based FDE. Seagate Technology, the world's leading hard drive manufacturer with a large market share in the enterprise space, has done this with the Momentus 5400 FDE.2 drive, commercially available in the first quarter of 2007. The Seagate FDE drive creates the ideal closed security system where the encryption keys are created, used for data encryption or decryption and never leave the protection of the drive controller. With a Seagate FDE drive, trust is based on tamper-resistant hardware that transforms a hard drive from a simple data storage device into an embedded data protection system.

Seagate's pre-boot authentication supports multiple user and administrator passwords, overcoming the security vulnerability of FDE solutions that rely on shared pre-boot passwords. The chain of trust can also be extended to include remote management and central provisioning of the FDE drives across an enterprise. The strong separation of administrator and user functions by Seagate means that remote management can be strongly verified, since there are no local capabilities allowed that could have changed the drive settings, policies and access control. This feature is essential for claiming compliance to data protection laws and assessing risk for potential data loss incidents.

For deployment, the provisioning of the drive is instantaneous versus the multiple-hour process required for the initial encryption with software FDE. Besides complex deployment, another valid concern with software FDE solutions is the degradation of the PC's performance. By separating the encryption from the operating system, the Seagate drive eliminates PC performance issues and is able to operate at media speed.

Seagate's pre-boot authentication mechanism replaces weak ATA / BIOS-based password handling with a dramatically stronger password process. This integrated access to the drive makes it virtually impossible for malware to steal the pre-boot password. No root kit, virus, Trojan horse or key logger can compromise the pre-boot password because there is no operating system on which to run the malware. There are also no known hardware or software hacks to this hardware-based method of authentication, which is not the case for software FDE solutions.

Non-administrative users can only unlock the drive and change their own password making Seagate FDE drives extremely simple to use. Once a Seagate FDE drive has been set up, the user simply enters a password to unlock the drive at power-up time. The user is never prompted, bothered or required to know anything else about the underlying security that is consistently protecting the data.

Another of the many features enabled by the integration of a security chip with the hard drive is the feature of quick "disk erase." This capability allows for changing the encryption key to render the data useless, which eliminates the additional IT expense needed to clean and dispose of retired drives. During the repurposing of Momentus 5400 FDE drives, the data remains fully protected.

As data protection methods evolve, improvements occur in terms of speed, security, usability and reliability (see Figure 1). The Seagate FDE drive represents the most advanced data protection method available, and with the encryption capabilities integrated into the drive, the total cost of ownership is considerably less than software solutions.

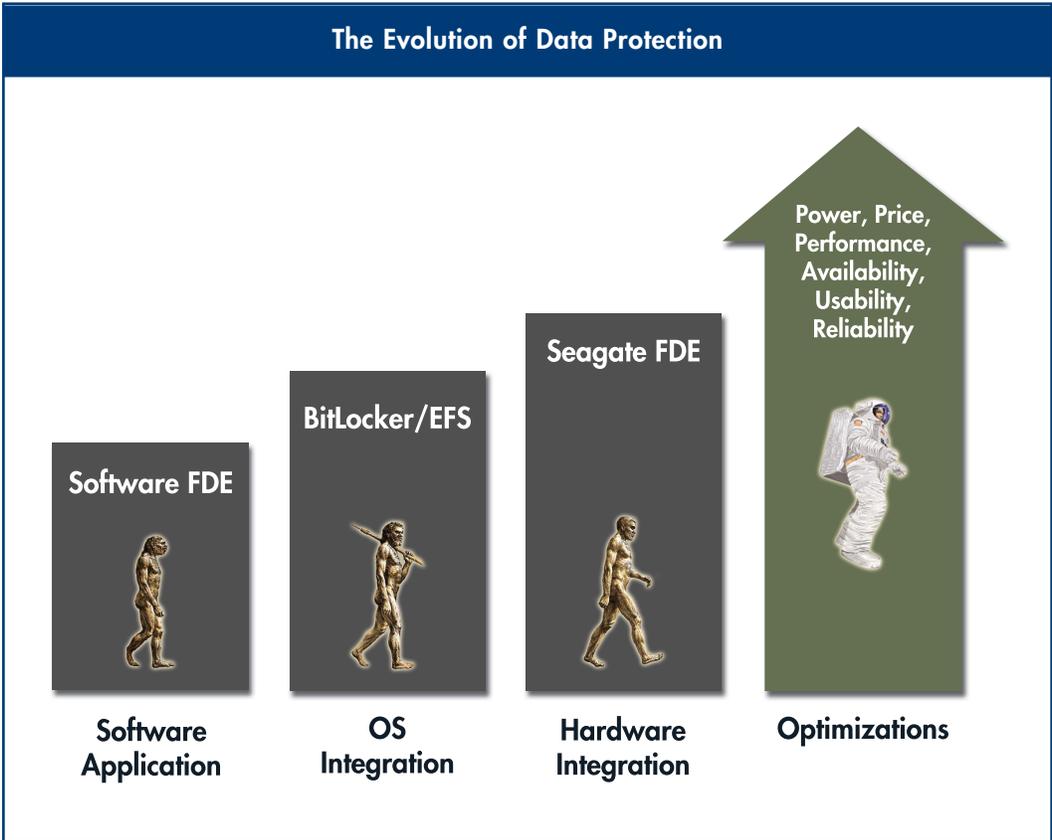


Figure 1: The Evolution of Data Protection

Conclusion

Data protection remains one of the fundamental security concerns for organizations today. Ultimately, all efforts in authentication, network access control and data security are about making sure the data that your enterprise relies upon is protected. The data protection issue is complex and choosing a technical solution is not a casual endeavor.

Often companies end up using two or more solutions to solve both external and internal threats.

The strongest encryption solutions base their trust in secure hardware. For strong data protection, deploying Seagate FDE Drives with its on-controller security chip, while adding file and folder encryption with the TPM is the best-in-class solution. With any data protection solution, centralized management and control of the backup and recovery functions is a necessary safeguard. Remote administration functions ease deployment and maintenance also aiding in regulatory compliance by validating that encryption was turned on, and not turned off, by the user.

As leaders in developing PC security software that uses hardware-based encryption, Wave Systems can help you create a hardened, yet cost-effective solution, ensuring that your organization is not the next one to make the headlines as the result of a data breach incident.



Wave Systems solves the most critical security problems for enterprises and government with solutions that are trustworthy, reliable, easy-to-use and offer a speedy return on investment. Wave's trusted computing solutions include strong authentication, data protection, advanced password management and enterprise-wide trust management services.

Wave's network management products include:

- **EMBASSY® Remote Administration Server (ERAS)** is revolutionary in enabling distributed and remote management for the millions of TPMs that have been deployed across enterprises worldwide. Additionally, ERAS enables the remote management of newly available Seagate Momentus 5400 FDE.2 drives for initialization, pre-boot authentication management, recovery, repurposing and more.
- **EMBASSY® Key Management Server (EKMS)** performs secure backup and recovery of TPM keys, associated passwords and certificates. Centralized key management is a vital component for any network of TPM-enabled PCs to ensure smooth operation in the event of hardware failure, a forgotten password or system transfer to a new user.
- **EMBASSY® Trusted Drive Manager** is the control panel for enabling the security functions of a Seagate Momentus 5400 FDE.2 hard drive. Initializing the drive's encryption features, managing the pre-boot password and backing up of secrets for recovery are a few of the functions of EMBASSY Trusted Drive Manager.
- **Document Manager** is a file and folder encryption product using the TPM as the basis for strong, hardware-based security. Document Manager allows for up to 23 virtual drives, secured by the TPM, that can be shared with other users and placed on the system's hard drive or anywhere the user has write access. Document Manager is a component of the EMBASSY Trust Suite, a collection of client applications that use the TPM for advanced PC security.

Part # 03-000224/version 1.04 Effective Date: 2007-04-30
Copyright © 2008 Wave Systems Corp. All rights reserved. Wave "Juggler" and EMBASSY logo are registered trademarks of Wave Systems Corp. All other brands are the property of their respective owners. Distributed by Wave Systems Corp. Specifications are subject to change without notice.