



*Break free from complex and costly data encryption solutions. Experience the benefits of factory-installed, hardware-based security.*

# Changing the Landscape of Data Encryption

## Data Breach a Growing Threat

The need for strong data encryption is growing rapidly in the wake of escalating data breaches reported nationwide. The Identity Theft Resource Center recently reported a 47 percent increase in the number of data breaches in 2008 compared with the previous years. In response, regulators have raised the stakes with Massachusetts and Nevada recently passing tough new data protection laws for businesses mandating encryption of all personal information stored on laptops.

To protect against mounting business threats, C-level executives, security officers and IT managers must stop sensitive corporate data from leaking outside their organizational walls. Their search often ends with after-market encryption software, a far from ideal answer. Such solutions are vulnerable to attack, cause adverse effects on employee productivity and are complex to install within an enterprise. In the end, these hurdles have led software encryption to fall short of providing the protection and return-on-investment that organizations require to meet both their business and compliance goals.

## Why Haven't More Businesses Adopted Encryption?

Encryption (aka cryptography) is a topic that causes confusion within most IT departments. Issues such as key management, data recovery and user productivity have made many companies slow to adopt encryption. To make matters worse, most organizations rely on individual departments to be responsible for deciding how best to protect their specific applications' data. This results in fragmented and disparate solutions that

don't interoperate, each with their own policies and management infrastructures.

## Data Encryption Solutions are *Not* Created Equal

Today, there are a number of data protection methods available, including BIOS and OS passwords, ATA drive passwords, software-based full disk encryption and self-encrypting drives. Industry security best practices and most compliance regulations call for the use of both strong access controls and encryption for protecting sensitive data; and since BIOS and OS passwords do not provide any means of encryption, they are easily discredited from being secure. While ATA passwords are stronger than BIOS and OS passwords, they too can be easily defeated by someone with basic knowledge. Further, since there is no centralized management for ATA mode, proving compliance would be challenging.

Software-based full disk encryption is significantly better than ATA passwords, but remains vulnerable to software attacks and has been shown to impact user productivity due to system performance degradation and time lost for maintenance. In addition, the overhead costs associated with installing, configuring and encrypting drives can, in some cases, surpass the acquisition cost of the software itself.

## Self-Encrypting Drives & Wave Software

Self-encrypting drives offer the strongest protection available since encryption is always on, the encryption keys never leave the drive and user authentication is performed in hardware. Therefore, they're not susceptible to traditional software attacks.

Wave Systems has partnered with leading drive manufacturers Fujitsu, Hitachi, Samsung Semiconductor, Seagate Technology and Toshiba to offer the easiest-to-use and most secure self-encrypting drive (SED) solutions available. These industry-standard drives protect data where it lives — on the hard drive, by taking advantage of its closed environment to isolate data storage for stronger protection.

Wave's EMBASSY® Trusted Drive Manager is a client application that enables self-encrypting drive security features and allows for their local management. Preboot access control, password management and secure erase are just a few of the features provided.

Since self-encrypting drives and Wave Trusted Drive Manager ship factory-installed from leading PC vendors, businesses can easily add hardware-based encryption and authentication out of the box — saving time and money.

For a distributed network of self-encrypting drives, Wave's EMBASSY Remote Administration Server (ERAS) provides robust policy management of users, credentials and access rights from one central location. Through native integration with existing directory structures and policy distribution mechanisms, assigning users and policies can be performed within the directory framework — dramatically simplifying deployment.

Given the increasing threat of security breaches and the fact that both individual companies and regulators are enacting strong data protection polices, encryption is no longer optional. While security best practices call for strong access controls and encryption, the bottom line requires cost-effective solutions — don't buy another computer without a self-encrypting drive.

The advent of open standards for self-encrypting drives from the Trusted Computing Group (TCG) has created more choices for organizations looking to adopt factory-installed, hardware-based full disk encryption. Open standards and a variety of solutions should make self-encrypting drives pervasive and dispel some of the early misconceptions.

## Self-Encrypting Drive Misconceptions Dispelled

### **Myth 1:** ***Most embedded hardware security offerings are incomplete.***

Wave offers robust policy management for a wide range of encryption technologies, including self-encrypting drives from leading vendors Fujitsu, Hitachi, Samsung, Seagate and Toshiba. For organizations that choose to adopt both self-encrypting drives and software full disk encryption, Wave's ERAS, provides robust policy management for SafeNet's award-winning ProtectDrive™ encryption software — now businesses can roll out a single policy management server that works seamlessly across all of their workstations.

### **Myth II:** ***Self-encrypting drives are not universal solutions for all platforms and applications.***

The TCG specifications are designed to facilitate broad adoption of FDE solutions by creating an open, industry standard that offers improved interoperability across storage vendors, encryption technologies and platforms. Both PC OEMs and end-user organizations can now implement "off the shelf," factory-installed and interoperable hardware-based encryption solutions.

### **Myth III:** ***Enterprises will be challenged to attempt large-scale adoption of self-encrypting drives.***

Wave's ERAS supports native integration with existing directory structures. Assigning users and policies within the directory framework can significantly simplify deployment. Unlike most software encryption, this factory-integrated solution takes only minutes to configure and deploy. And, because encryption is always on, there is generally no learning curve for IT or the end user.

### **Myth IV:** ***No hardware subsystem can stand alone as a complete solution.***

No software-based encryption is a complete solution unto itself, requiring policy management for keys, users and access rights. Similarly, self-encrypting drives provide the native encryption while independent software vendors such as Wave Systems provide the robust policy management that enterprises require, including secure remote data destruction.