Samsung SED Security in Collaboration with Wave Systems

Safeguarding sensitive data with enhanced performance, robust security, and manageability

Samsung
Super-speed
Drive

wave®

SAMSUNG

Secure sensitive data economically without sacrificing performance

Ensure regulatory compliance and save costs through robust data security

The rise in workforce mobility has increased the need to protect sensitive company data and intellectual property. The security of corporate information faces greater risks of breach or loss without adequate protection. Confidential data leakages of key company and customer information can damage an organization's reputation and market position, and can also result in financial penalties.

Today, worldwide government regulations and legislation require organizations to openly disclose data breaches. Large fines and penalties may be assessed unless a business can ensure that its data is secure and safeguarded from misuse by unauthorized individuals. An example of such legislation is the 2000 Safe Harbor law, which requires that organizations protect information from loss, misuse, unauthorized access, disclosure, alteration and destruction[1].

In addition to government fines, the internal business cost of lost data can be substantial. A Ponemon study[2] surveyed 277 organizations and revealed that cost of data breach per record increased from $130 to $136 on average. The average total organizational cost of data breach is highest in the US ($5.4M) followed by Germany ($4.8M), and the associated average costs for lost business are $3.0M in the US and $1.8M in Germany.

Increase performance and security while reducing TCO with Self-Encrypting Drives

Hardware- and software-based encryption technologies are used to safeguard SSDs. Samsung offers Self-Encrypting Drives (SEDs) which are hardware-encrypted and automatically encrypt or decrypt all data transferred to and from the SSDs. SEDs provide:

- **Higher performance.** Invisible to the user, hardware encryption built directly into the drive electronics maximizes performance. In contrast, software encryption burdens the central processing unit (CPU) and lowers performance. Hardware-based SED encryption includes a built-in circuit in the controller chip that automatically encrypts all data transferred to the storage device. With hardware-based encryption, the drive controller encrypts and decrypts all data, so it eliminates the extra processor workload for transferring data and therefore, eliminates the additional CPU overhead.

- **Enhanced Security.** 256-bit hardware-based encryption and user authentication offer superior protection against data breaches, loss and theft compared to software-based encryption. Software-based encryption is vulnerable to attacks through the memory, operating system and BIOS, whereas hardware-based encryption is performed in the actual hardware, and user authentication is performed by the drive before it unlocks, independent of the operating system (OS).

- **Lower Total Cost of Ownership (TCO).** Hardware-based encryption is an easily integrated, cost-effective data security solution. In fact, SEDs offer lower TCO for encryption solutions with higher performance, lower acquisition costs, increased user productivity, simplified IT management and deployment, and lower disposal or repurposing costs.

> "Many organizations are considering drive-level security for its simplicity in helping secure sensitive data throughout the hardware lifecycle from initial setup, to upgrade transitions and disposal."
>
> *- Eric Ouellet*
> *Research Vice President, Gartner*[3]

Control SEDs throughout the organization with security management solutions

Along with the adoption of SEDs within an organization, the organization must control the use of SEDs and mitigate the use of nonstandard or rogue encryption mechanisms. The organization must manage users and systems, and provide data recovery. SED management tools and solutions enable an organization to manage SEDs with efficiency and without compatibility issues.

Keep your data safe

SAMSUNG Solid State Drive | SED | AES 256-bit Full Disk Encryption

Safeguard business information with Samsung SEDs and Wave Systems

Leverage the combination of TCG Opal-compliant Samsung SEDs and Wave Systems Software for enhanced data security and management

Samsung SEDs are compliant with the Advanced Technology Attachment (ATA) standard, a password system that restricts access to user data stored on a device. Also, in collaboration with independent software vendors (ISVs) who provide security management tools for SEDs, Samsung provides SEDs that are compliant with the TCG Opal specification, developed by the Trusted Computing Group, and the IEEE 1667 standards, as supported (for example) by Microsoft BitLocker in Windows 8.

### Get faster, more secure data encryption with Samsung SED technology

PC users expose corporate information to myriad vulnerabilities in many environments. Samsung's SED security technology safeguards sensitive data no matter where employees travel. The advanced drives include an AES 256-bit hardware-based encryption engine to ensure that users' files remain secure, even when a laptop is lost or stolen. Because it is hardware-based, the encryption engine secures corporate data faster without the performance degradation that is typically experienced with software-based encryption. Plus, it offers more secure access and compliance with advanced security standards, such as TCG Opal specification.

Safeguard access to data with Wave Cloud and Wave Embassy Remote Administration Server (ERAS)

Wave Systems is an ISV that offers secure data access control on mobile platforms, access to the cloud and safe network logon with users' personal devices. Wave System solutions augment Samsung SED security technology by Managing authorized users' access to the drives and data is where Wave comes in. Together, Samsung SEDs and Wave Systems deliver an optimal solution for managing encrypted devices for companies of all sizes.

- **Wave Cloud.** Provides remote security management without any infrastructure to install; appeals primarily to small-to-medium businesses (SMBs)
- **Wave ERAS.** Enables larger enterprises to centrally manage security while supporting more complex configurations
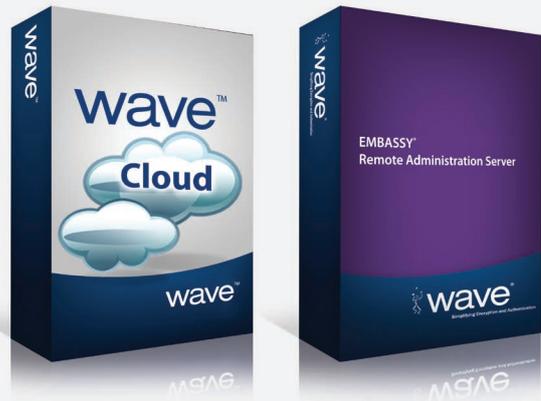
Instantly deploy endpoint encryption with Wave Cloud for enhanced data security

Deploy endpoint encryption quickly, easily and economically with Wave Cloud

Wave Cloud is the fastest, easiest way to deploy endpoint encryption. It is the world's first cloud-based service for managing SEDs and software encryption in Microsoft® Bit-Locker and OSX FileVault[4] through a single console. Wave Cloud delivers data security that is always up-to-date, works anywhere and is infinitely scalable at a low, pay-as-you-go cost.

Wave Cloud is a scalable, yet powerful software-as-a-service (SaaS) solution for data protection. It enables businesses to centrally enforce strong data encryption policies on laptops across the enterprise, but without the complexity and cost typically associated with on-site solutions.

Able to support deployment in seconds, Wave Cloud is the ideal data security solution for businesses that need data encryption without sacrificing performance, and without the requirement to set up and maintain servers. Wave Cloud provides authentication management and access control configuration through the cloud. Note that with Wave Cloud, the user does not upload any data to the cloud, rather, features such as the SSD logon experience and logon recovery methods are managed through the cloud.

Wave Cloud key benefits include:

- **Enhances security.** Wave Cloud increases device security with centralized policy enforcement, secure user recovery and protected user and device credentials.
- **Ease of use.** The solution enables the management of SED security with a simple and intuitive web interface. The Wave Cloud web application supports seamless drive provisioning and policy-based management.
- **Lowers TCO.** With Wave Cloud, organizations can deploy SEDs immediately, without the need to procure, build and test server infrastructures. Customers only pay for what they use. This pricing structure enables organizations to deploy SEDs in a capital-efficient manner.

Wave Cloud offers the following features for endpoint encryption:

- Pre-boot authentication
- Drive initialization
- User management
- Drive locking
- User recovery
- Control for external SEDs
- S3 sleep support
- Ability to deploy many drives at once with policy-based management
- Windows password synchronization
- Single sign-on (SSO)
- Active monitoring, logging and reporting of all user and device events

EMBASSY® Remote Administration Server

wave®

SAMSUNG

Easily manage security for a fleet of devices across the enterprise

Remotely activate, monitor and manage a fleet of SED devices and TPMs across the enterprise for more robust data security with Wave ERAS

Wave ERAS is a centralized management solution that provides all the tools necessary to remotely search for, initialize, configure and administer a global fleet of computers equipped with SEDs. With ERAS, businesses can centrally provision security policies to end-points across the organization, limit access of encrypted information to authorized individuals and remotely manage user and device credentials. Most importantly, ERAS provides an authority of proof, allowing organizations to demonstrate that they were, and are, compliant with regulations in the wake of a security breach.

The Wave ERAS directory-based security management solution for SEDs, TPMs and BitLocker client PCs is ideal for organizations who have the servers, personnel or infrastructure to manage data encryption and for businesses who need enhanced data security without a drop in performance.

Wave ERAS delivers centralized security management across a distributed organization. Plus, it confers real-time, policy-based security controls and proof of compliance on the network's furthest endpoints. Wave ERAS offers extensive features for SED and BitLocker management such as smart card authentication, automated user enrollment, for example. Following are Wave ERAS key benefits.

- **Enhances security.** Wave ERAS increases device security with centralized policy enforcement, secure user recovery and protected user and device credentials.
- **Comprehensive compliance with security regulations.** The solution achieves compliance through active logging, monitoring and reporting of all user and device events associated with SEDs, TPMs and BitLocker client PCs.
- **Reduces costs.** Wave ERAS minimizes IT overhead and help desk expenses associated with the setup, deployment and maintenance of device encryption and ID solutions.

Following are some features that Wave ERAS offers for centralized SED device security management:

- Pre-boot authentication
- Drive initialization
- User management

- Drive locking
- User recovery
- Control for external SEDs
- S3 sleep support
- Ability to deploy many drives at once with policy-based management
- Windows password synchronization
- Single sign-on(SSO)
- Active monitoring, logging and reporting of all user and device events
- Crypto Erase
- Common Access Card (CAC) and smart card authentication
- Secure user recovery through challenge and response protocols
- User self-enrollment and self-service password recovery
- Dual SED drive password synchronization
- Proof of compliance with data protection regulations
- Help desk portal

Wave Cloud 2014

What is Crypto Erase?

Crypto Erase[5] means to erase the encryption key stored in the SED, thus rendering the encrypted data unreadable, instantaneously. The Crypto Erase command to the SED causes the SED to erase and replace the encryption key with a new key. Since the encrypted data can no longer be read, the drive is considered sanitized. Yet, the drive will continue to operate as an SED, using the new key. Older erasure/sanitization techniques involve lengthy and error-prone drive overwriting or expensive and labor-intensive methods that destroy the drive. The U.S. government's official guide to media sanitization has recently been revised to officially recognize Crypto Erase, which is both fast and effective.

wave®

SAMSUNG

Ensure data protection the smart way with Samsung SED security and Wave Systems

Safeguard corporate data with enhanced performance, manageability and cost-efficiency

In today's mobile work environment, securing business information is more important than ever. Government regulations and prudent business practices mandate that companies ensure the protection of business and personal data, with heavy penalties and costly consequences imposed when security breaches occur. Fortunately, there's a way to ensure data security throughout the enterprise with Samsung SEDs and Wave Systems' solutions. Combined, these economical offerings help businesses of any size enhance end-point security and management without sacrificing PC performance.

Features and benefits

	Benefits
Samsung SEDs	Provides enhanced security at the hardware level; ensures higher performance and lowers TCO
Wave Cloud	Enables businesses to easily enforce and manage strong data encryption policies without the need to set up or purchase servers and reduces TCO
Wave ERAS	Provides enhanced security and regulatory compliance in a cost-effective solution that is tailored to fit the company's business needs

About Samsung Electronics Co., Ltd.

Samsung Electronics Co., Ltd. is a global leader in technology, opening new possibilities for people everywhere. Through relentless innovation and discovery, we are transforming the worlds of televisions, smartphones, personal computers, printers, cameras, home appliances, LTE systems, medical devices, semiconductors and LED solutions. We employ 236,000 people across 79 countries with annual sales of US$187.8 billion. To discover more, please visit www.samsung.com

For more information

For more information about Samsung SSD, visit
www.samsung.com/SSD

For more information about Wave Systems products, visit
www.wave.com/products

To purchase Wave Systems products, visit
www.wave.com/channel-partner-locator
to find an authorized distributor

Samsung SSD activated

[1] http://www.privacyrights.org/data-breach

[2] Ponemon Institute 2013 Cost of Data Breach Study. May 2013

[3] http://www.storagevisions.com/2013/Book/Michael%20Willett.pdf

[4] FileVault, the FileVault logo, Keychain Access, and Mac OS X are registered trademarks of Apple Inc., in the United States and other countries

[5] http://csrc.nist.gov/publications/drafts/800-88-rev1/sp800_88_r1_draft.pdf

Samsung Electronics Co., Ltd.
416, Maetan 3-dong,
Yeongtong-gu
Suwon-si, Gyeonggi-do 443-772,
Korea

www.samsung.com

2014-01