Seagate Instant Secure Erase Deployment Options

Technology Paper

Introduction

When hard drives are retired and moved outside the data centre into the hands of others, the data on those drives is put at significant risk. Nevertheless, IT departments must still remove and dispose of drives routinely for a variety of reasons, including:

- Repurposing drives for other storage duties
- Returning drives for warranty, repair or expired lease agreements

Nearly all hard drives are placed outside their owners' control when the drives are eventually removed from the data centre; in fact, Seagate estimates that 50,000 drives are retired from data centres daily. Corporate and personal data resides on such drives, and when they do leave the data centre, the data they contain is still readable. Even data that has been striped across many drives in a storage system configured with RAID data protection is vulnerable because a single stripe in today's high-capacity arrays is large enough to store hundreds of names, social security numbers, and other personal and highly-sensitive data.

Drive Control Headaches and Disposal Costs

In an effort to avoid data breaches and the ensuing customer notifications required by data privacy laws, corporations have tried a myriad of ways to erase the data on retired drives before they leave the premises and potentially fall into the wrong hands. Current retirement practices designed to make data unreadable generally rely on significant human involvement in the process, and are thus subject to both technical and human failure.

The drawbacks of today's drive retirement practices are both numerous and far-reaching:

- Overwriting drive data is expensive, taking up valuable system resources for days. No notification of completion is generated by the drive, and overwriting will not cover reallocated sectors on the drive, thus leaving that data exposed.

Seagate Instant Secure
Erase Deployment Options

- Degaussing or physically shredding a drive is costly. It is difficult to ensure that the degauss strength is optimised for the drive type, potentially leaving readable data on the drive. Physically shredding the drive is environmentally hazardous, and neither practice allows the drive to be returned for warranty or expired lease.

- Some corporations have concluded that the only way to retire drives securely is to keep them in their control, storing them indefinitely in warehouses. However, this is not truly secure, as a growing volume of drives coupled with human involvement inevitably leads to some drives being lost or stolen. In fact, a 2014 Cost of Data Breach Study by the Ponemon Group revealed that the most common cause of a data breach was a malicious insider or criminal attack.

- Other companies choose to hire professional disposal services, an expensive option which entails the cost of reconciling the services as well as internal reports and auditing costs. More troubling, transporting a drive to the service provider introduces another risk since the drive might be lost or stolen in transit. Just one lost drive could cost a company millions of pounds in remedies for the breached data.

Challenges with performance, scalability and complexity have led IT departments to push back against security policies that require the use of encryption. In addition, encryption has been viewed as risky by those unfamiliar with key management, a process for ensuring that a company can always decrypt its own data. Self-Encrypting Drives (SEDs) resolve these issues comprehensively, making encryption for drive retirement fast, easy and affordable.

Seagate Instant Secure Erase Makes Drive Retirement Safe, Fast and Easy

SEDs encrypt all user data as it enters the drive, using a data encryption key stored securely on the drive itself. Therefore, all data stored on an SED is encrypted by default. When it is time to retire or repurpose the drive, the owner simply sends a command to the drive to perform a Seagate Instant Secure Erase (ISE). Seagate ISE uses the SED's cryptographic erase capability to change the data encryption key. Crypto-erase methods, such as Seagate ISE, are now endorsed by ISO (International Organization for Standardization) and NIST (National Institute of Standards and Technology) as the preferred method of data sanitisation because "[it] can be performed with high assurance much faster than with other sanitisation techniques".[1] The cryptographic erase securely replaces the encryption key inside the SED, as shown in Figure 1.
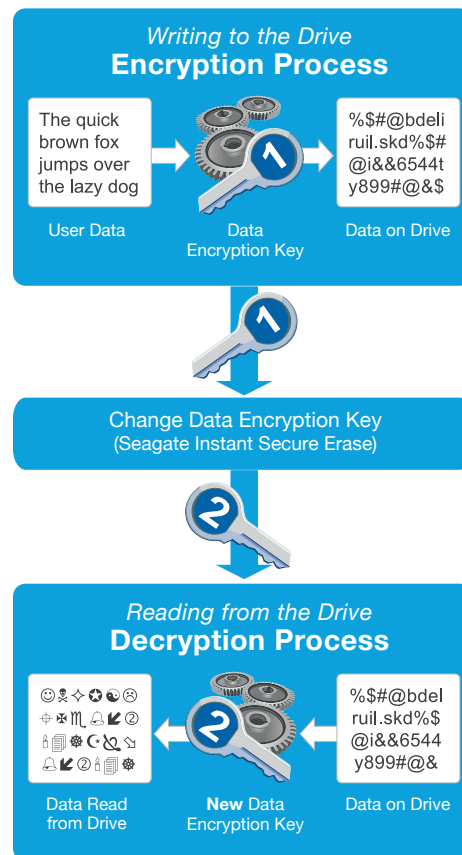

Figure 1. The Seagate Instant Secure Erase Process

Once the key originally used to encrypt the data is changed, any and all data encrypted with that key becomes unreadable and can never be recovered. In this way, Seagate ISE instantly, securely and effectively destroys the data stored on the device, making the drive ready for retirement, reuse or sale. SEDs, regardless of the deployment approach used, reduce IT operating expenses by freeing IT from both drive control headaches and disposal costs. Seagate's government-grade data security helps ensure data privacy compliance without hindering IT efficiency.

Furthermore, SEDs simplify decommissioning and preserve hardware investments for returns and repurposing by:

- Eliminating the need to overwrite or destroy the drive

- Securing warranty and expired lease returns

- Enabling drives to be repurposed or sold with the reassurance that former data is not exposed.

Seagate Instant Secure Erase Deployment Options

Different Seagate Solutions for Different Security Needs

- Two types of Seagate Secure drives are available. Customers can select standard SEDs or models with Federal Information Processing Standard (FIPS 140-2) certification for additional security. Both include the Seagate Instant Secure Erase feature that allows customers to quickly and securely erase the contents of their drives in seconds, a valuable feature not available with non-encrypting drives.
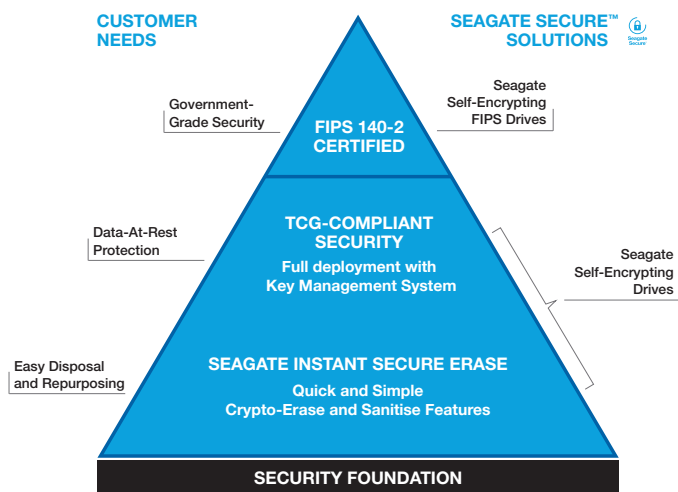

Figure 2. Seagate Secure™ Solutions for All Levels of Security Implementation

How Seagate Self-Encrypting Drives Perform Instant Secure Erase

Seagate SEDs support several methods to execute a Seagate ISE depending on the drive's interface command set and configuration. The most secure method is to use the cryptographic erase option available through the drive's SED Trusted Computing Group (TCG) security protocol. In addition to its superior security, this method is fast and easy. Customers can also erase drives with the legacy data overwrite command methods, but these are largely considered less secure and can be very time consuming. Table 1 lists these and other data erasure methods. Note that in all circumstances the host controller must implement support for Seagate ISE via a supported command.

1. Drives configured with data-at-rest protection, with or without the advanced FIPS 140-2 tamper-evidence protection, are enabled using TCG security protocols.

   An SED managed using TCG's Storage specification protocol supports band-level cryptographic erasure (crypto erase). In addition to protecting user data while the drive is in use, band-level crypto erase allows for parts or all of the data stored on the device to be erased without affecting other data bands on the drive. This electronic erase method requires third-party software available from a variety of Seagate partners.

   An SED managed through the TCG Storage specification protocol can also be erased entirely by invoking the protocol's RevertSP command. This type of secure erase requires physical possession of the device in order to read the 32-character PSID (Physical Secure ID) printed on the label to securely erase the data and configure the drive to its original factory state.

2. Drives not configured with full data at rest protection can be enabled using ATA Security commands.

   A Seagate SED implementing the ATA command set is erased by invoking the ATA Security Erase Prepare and Security Erase Unit commands. Note that this is a Seagate unique implementation of Seagate ISE.

Seagate Instant Secure Erase Deployment Options

SEAGATE

Table 1 provides an overview of the different methods to erase data from an SED. See notes below the following table:

Table 1. Seagate Instant Secure Erase Options				
Initial Configuration	**Data-at-rest protection, with or without tamper-evidence protection**		**Limited security enabled**	**No security enabled**
Erase Method	**TCG Security Protocol** Erase	**TCG Security Protocol** RevertSP	**ATA Security** Security Erase Prepare and Security Erase Unit commands	**Sanitise** Sanitise Feature Set/Command
Supported Configuration	Seagate SEDs with TCG Storage	Seagate SEDs with TCG Storage	Seagate SATA SEDs	Supported Seagate SATA and SAS SEDs
Erase Scope	Band-level cryptographic erase	Entire drive is cryptographically erased	Entire drive is cryptographically erased	Entire drive is cryptographically erased
Side Effect	Unlocks band and resets band password	SED goes back to factory default state	Unlocks drive and disables ATA Security	No initial security to prevent accidental erasure
Access Control	Authentication required using host-managed or device's default password	Authentication required using password printed (and bar-coded) on drive label	Authentication required using host-managed password(s)	Unauthenticated by design (if drive is locked, drive must be unlocked by the operator before execution)
Benefits	Data-at-Rest Protection FIPS 140-2 Level 2 validation Full-featured Security Management interface based on TCG Storage specifications	Data-at-Rest Protection FIPS 140-2 Level 2 validation Full-featured Security Management interface based on TCG Storage specifications	Drive-level security Security uses standard ATA Security commands	Provides secure erase with no management overhead (i.e. no password management required)
Comments	Requires TCG-compatible hardware or software	Requires physical possession of the SED to read the drive security code	Leverages standard ATA Security commands	Possibility of erroneous or malicious data erasure due to unprotected nature of command

Notes

1. In most situations the method to securely erase a drive in higher security configurations will also work when used in lower security settings, as an example, the RevertSP method will work on a drive configured in ATA mode assuming the drive also supports the TCG command set (security support may vary by drive model).

2. The term *data-at-rest protection* refers to the ability of an SED to provide very strong protection against data compromise on a drive that has been configured to lock the data interface against unauthorised access while in a functioning computer environment.

3. The Federal Information Processing Standard (FIPS) Publication 140-2 is a US Government Computer Security Standard used to accredit cryptographic modules. It is titled *Security Requirements for Cryptographic Modules (FIPS PUB 140-2)* and is issued by the US National Institute of Standards and Technology (NIST). This standard specifies the security requirements that will be satisfied by a cryptographic module utilised within a security system protecting *Sensitive but Unclassified and Protected* class data. Seagate FIPS drives are certified at Level 2 (tamper evident); more information is available at: http://www.seagate.com/files/www-content/solutions-content/security-and-encryption/en-us/docs/faq-fips-sed-mb605-3-1411us.pdf

Seagate Instant Secure Erase Deployment Options

SEAGATE

How to Perform a Seagate Instant Secure Erase on a Seagate SED

Based on the kind of SED and option chosen to erase the device securely, actual data erasure can be achieved in different ways. The following solutions are available:

- Seagate SeaTools™ software for Windows: free tool for PCs to diagnose both internally and externally connected storage devices. SeaTools software supports Seagate ISE. SeaTools software can be downloaded from www.seagate.com in the Support and Downloads tab, under SeaTools – Diagnosis Software.

- Third-party key management software applications from Seagate partners, such as IBM (Tivoli Key Lifecycle Manager), Wave, Winmagic, etc.

- Custom/embedded solution to integrate Seagate ISE capabilities into systems or host applications. Contact your Seagate sales representative for more information.

- Linux users may use HDPARM (command line utility for the Linux operating system) if they want to issue their own SATA commands.

References

TCG Storage Specifications:
www.trustedcomputinggroup.org/developers/storage/specifications

ATA Specifications:
www.t13.org/

SCSI Specifications:
www.t10.org/

Seagate SeaTools Software:
www.seagate.com/www/en-us/support/downloads/seatools

Seagate Secure®

seagate.com