Seagate

Technology Paper

Seagate Instant Secure Erase Deployment Options

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 routinely dispose of drives 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 RAID array is vulnerable to data theft, because just a typical single stripe in today's high-capacity arrays is large enough to potentially expose the most sensitive data, such as hundreds of names and identification numbers.

Seagate Instant Secure Erase Deployment Options

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, tying up valuable system resources for days. No notification of completion is generated by the drive, and overwriting does not cover reallocated sectors, leaving that data exposed.
- 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. But this is not truly secure, as a large volume of drives coupled with human involvement inevitably leads to some drives being lost or stolen.
- 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 puts the drive's data at risk. 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.[1] The cryptographic erase securely replaces the encryption key inside the SED, as shown in Figure 1.

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 SED drives use US-government-grade data security, helping ensure safe harbour for data privacy compliance, without hindering IT efficiency. Furthermore, SEDs simplify decommissioning and preserve hardware value 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 securely

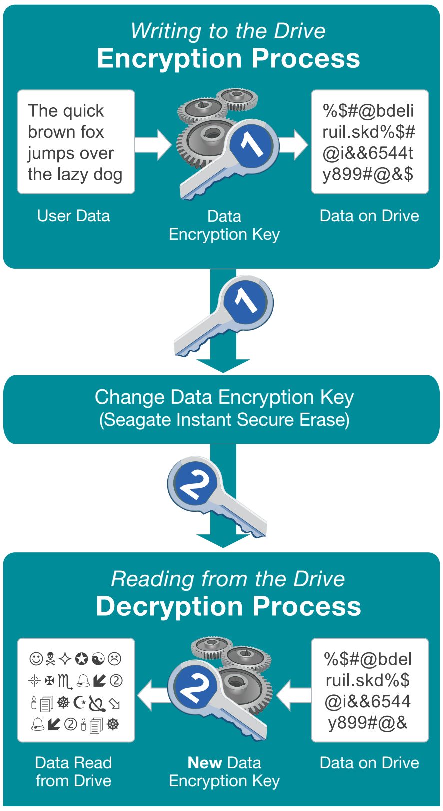

Writing to the Drive
Encryption Process
The quick brown fox jumps over the lazy dog
%$#@bdeli ruil.skd%$# @i&&6544t y899#@&$
User Data
Data Encryption Key
Data on Drive
Change Data Encryption Key (Seagate Instant Secure Erase)
Reading from the Drive
Decryption Process
%$#@bdel ruil.skd%$ @i&&6544 y899#@&
Data Read from Drive
New Data Encryption Key
Data on Drive

Figure 1. The Seagate Instant Secure Erase Process

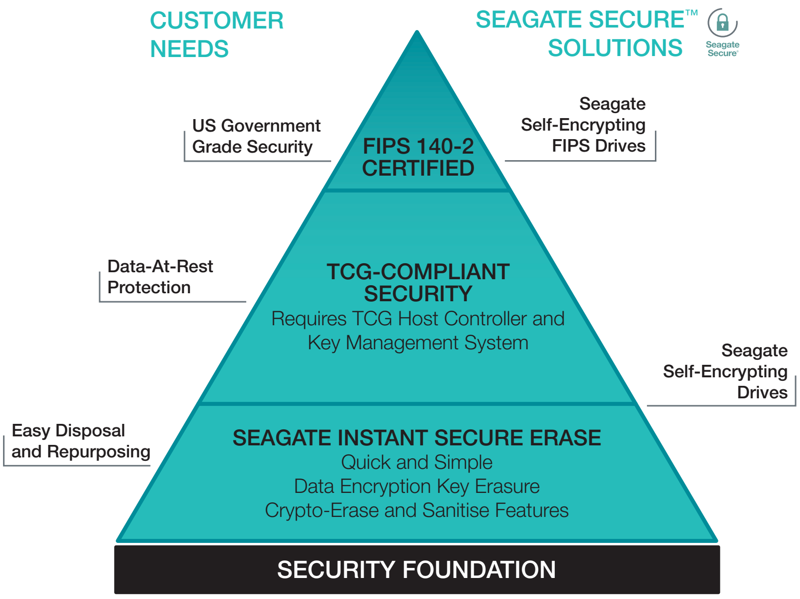
[1] Seagate is working jointly with multiple industry leaders and government agencies to finalise standardisation of data destruction using cryptographic erase; this is done within ISO (International Organisation for Standardisation) under ISO/IEC WD 27040.

Seagate Instant Secure Erase Deployment Options

Different Seagate Solutions for Different Security Needs

All Seagate enterprise SEDs provide Seagate ISE functionality. The manner in which this is achieved varies, depending on what level of security was implemented when the drive entered into use. Note that each level includes the protection capabilities of the previous levels.

- Data-at-rest and tamper evidence protection (FIPS 140-2 Level 2)
- Data-at-rest protection
- Repurposing protection only (Seagate ISE)



CUSTOMER NEEDS
SEAGATE SECURE™ SOLUTIONS
Seagate Secure
US Government Grade Security
FIPS 140-2 CERTIFIED
Seagate Self-Encrypting FIPS Drives
Data-At-Rest Protection
TCG-COMPLIANT SECURITY
Requires TCG Host Controller and Key Management System
Seagate Self-Encrypting Drives
Easy Disposal and Repurposing
SEAGATE INSTANT SECURE ERASE
Quick and Simple
Data Encryption Key Erasure
Crypto-Erase and Sanitise Features
SECURITY FOUNDATION

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

The relevant erase methods for each of these initial configurations are detailed in Table 1. For those Seagate customers with deep SCSI or ATA command and coding expertise, it is also possible to develop a proprietary solution to use Seagate SEDs with the TCG Storage, T10 and T13 command sets and specifications. Contact your Seagate sales representative for more information.

How Seagate Self-Encrypting Drives Perform Instant Secure Erase

Seagate SEDs support one or more ways of executing a Seagate ISE, depending on the drive's interface command set and configuration. For example, a device with a SATA interface may have different erase capabilities from one supporting a SAS interface. Moreover, additional security and erase capabilities are available via the TCG Storage security protocol supported by the SED. 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 tamper evidence protection, are enabled using TCG enterprise protocols.

   A device managed using TCG's Storage specification protocol supports band-level Seagate ISE. In addition to protecting user data while the drive is in use, band-level Seagate ISE allows for some or all of the data stored on the device to be erased without affecting other data bands on the drive. This method of erasing data is performed using the TCG Storage security protocol (Erase method) on each band, which requires third-party software.

   A device managed using the TCG Storage specification protocol can also be erased at once by invoking the security protocol's RevertSP method. 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 and erases the drive back securely to the original factory state.

2. Drives configured with easy disposal and repurposing protection only are 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

Table 1 provides an overview of the different methods of deploying a Seagate ISE on an SED. See notes following table.

Table 1. Seagate Instant Secure Erase Options

Initial Configuration	Data-at-rest protection, with or without tamper-evidence protection		Repurposing protection only	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	ATA drive-level 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 erase a drive securely in higher security configurations will also work when used in lower security settings. For example, the RevertSP protocol will work on a drive configured in ATA mode, assuming that 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 entitled *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 used within a security system protecting data classed as *Sensitive but Unclassified* and *Protected*. Seagate FIPS drives are certified at Level 2 (tamper evident). More information is available at: www.seagate.com/docs/pdf/whitepaper/mb605_fips_140_2_faq.pdf

Seagate Instant Secure Erase Deployment Options

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 is located at www.seagate.com in the Support and Downloads tab, under SeaTools – Diagnosis Software.
- Third-party, off-the-shelf solutions: use RAID Controllers from LSI and Intel or a full key management solution from IBM (Tivoli Key Lifecycle Manager), Wave, Winmagic, etc.
- Custom/embedded solution: (in-house) developed capability integrated into the system or host application to support Seagate ISE. Contact your Seagate sales representative for more information.

References

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

ATA Specifications:
www.t13.org/

SCSI Specifications:
www.t10.org/

Seagate SeaTools Software:
http://www.seagate.com/gb/en/support/downloads/seatools/

www.seagate.com

AMERICAS Seagate Technology LLC 10200 South De Anza Boulevard, Cupertino, California 95014, Stati Uniti, +1 408 658 1000
ASIA/PACIFIC Seagate Singapore International Headquarters Pte. Ltd. 7000 Ang Mo Kio Avenue 5, Singapore 569877, +65 6485 3888
EUROPE, MIDDLE EAST AND AFRICA Seagate Technology SAS 16–18, rue du Dôme, 92100 Boulogne-Billancourt, Francia, +33 1 41 86 10 00