技術文件

Seagate Instant Secure Erase 部署選項

序言

當汰換硬碟機而必須將硬碟機從資料中心移交至他人之手時，硬碟機上的資料便極可能會曝光。然而，基於多種理由，IT 部門仍然必須定期移除和棄置硬碟機，包括：

- 將硬碟機移到其他儲存設備另作他用
- 因保固、維修或租約到期而退回硬碟機

幾乎所有硬碟機最後都會在從資料中心移除時脫離其擁有者能控制的範圍；實際上，Seagate 估計資料中心每天會淘汰掉 50,000 台硬碟機。這些硬碟機上面都存放著公司和個人資料，而當硬碟機離開資料中心時，所包含的資料都還是可以讀取的。即使資料分置於 RAID 陣列中的多部硬碟機，資料也難免遭竊，因為即使是現今高容量陣列中的一般單一分置，也可能導致最敏感的資料曝光，例如成千上百的人名或身份字號。

Seagate Instant Secure Erase 部署選項

硬碟機控制的困難與棄置成本

為了避免資料露洞及隨後必須依照資料隱私權法律通知客戶的相關事端，公司紛紛嘗試許多方法，要先將淘汰的硬碟機上之資料悉數刪除，以免該些硬碟機在離開公司後落入不法人士手中。目前專門針對要讓資料變成不可讀取而設計的淘汰方式，在處理上一般必須大量仰賴人為操作，因此容易出現技術與人為疏失。

當前的淘汰方式尚有為數眾多且種類不一的缺點：

- 覆寫硬碟機資料相當昂貴，而且會耗用好幾天寶貴的系統資源。完成後硬碟機並不會產生通知，而覆寫也無法涵蓋重新分配過的磁區，導致資料有曝光的危險。
- 消磁或直接將硬碟機毀壞都很浪費成本。由於很難判斷各硬碟機適合的消磁強度，因此硬碟機上可能殘存可讀取的資料。毀壞硬碟機則會對環境造成傷害，而且再也無法因保固或租約結束而將硬碟機退回。
- 某些公司認為，只有將硬碟機儲存在倉庫並加以控管，才是唯一安全的淘汰方式。不過事實上這個方式並不全然安全，因為人為保存且儲存了大量資料的硬碟機，很難保證不會遺失或遭竊。
- 其他公司可能選擇僱用專業的棄置服務，不過這些服務相當昂貴，而且後續還得花費執行與協調服務以及內部報告與稽核的成本。更麻煩的是，將硬碟機運送到服務商的過程中，等於將硬碟機上的資料置於危險中。只要遺失一台硬碟機，就可能害公司為了補救資料漏洞而損失上百萬。

效能、擴充性與複雜度的挑戰，讓 IT 部門不得不回頭去面對要求使用加密的安全性策略。此外，不熟悉金鑰管理的人會覺得加密具有風險，因為這種程序必須確保公司永遠能將資料解密。加密硬碟機 (SED) 可全面解決這些問題，而且讓淘汰硬碟機的加密作業變得快速、輕鬆而且價格實惠。

Seagate Instant Secure Erase 讓硬碟機汰換過程能夠安全、快速且容易

SED 會在全部使用者資料進入硬碟機時，使用安全存放在硬碟機本身的資料加密金鑰進行加密。因此，預設會加密 SED 上儲存的所有資料。要汰換硬碟機或移作他用時，擁有者只要傳送一道指令給硬碟機，即可執行 Seagate Instant Secure Erase (ISE)。Seagate ISE 會使用 SED 的加密清除功能變更資料加密金鑰。[1] 加密清除功能會安全地取代 SED 內的加密金鑰，如圖 1 所示。一旦原本用於加密資料的金鑰有所變更，任何與所有以該金鑰加密的資料都會變得無法讀取且永遠無法回復。這樣一來，Seagate ISE 就可以立即安全且有效地銷毀裝置上儲存的資料—讓您隨時可將硬碟機汰換、重複使用或售出。不論使用的部署方式為何，SED 都可以減少 IT 作業費用，因為 IT 無需再面對硬碟機控管的難題與棄置成本。Seagate SED 硬碟機使用政府等級的資料安全性，不但能助您符合資料隱私權規範的「豁免」情況，亦不會妨礙 IT 效率。此外，SED 還簡化了汰換程序，並保存住硬體可以退回或重新利用的價值，包括：

- 免除覆寫或銷毀硬碟機的需求
- 確保可在保固期和租約到期後退還
- 讓硬碟機可以安全無虞地移作他用或售出

圖 1：Seagate Instant Secure Erase 程序

[1] Seagate 目前正與多個業界領導者和政府機關合作定案使用加密清除進行資料銷毀作業標準化；此標準化是於 ISO (國際標準組織) 之 ISO/IEC WD 27040 項目下進行。

Seagate Instant Secure Erase 部署選項

適用於不同安全需求的不同 Seagate 解決方案

所有 Seagate 企業級 SED 都提供 Seagate ISE 功能。可達到此一目標的方式有很多種，視硬碟機開始使用時所實作的安全性層級而定。請留意，每個層級都包括前一層級的防護功能。

- 核心資料與防偽保護 (FIPS 140-2 Level 2)
- 核心資料防護
- 僅限將硬碟機另作他用的防護 (Seagate ISE)

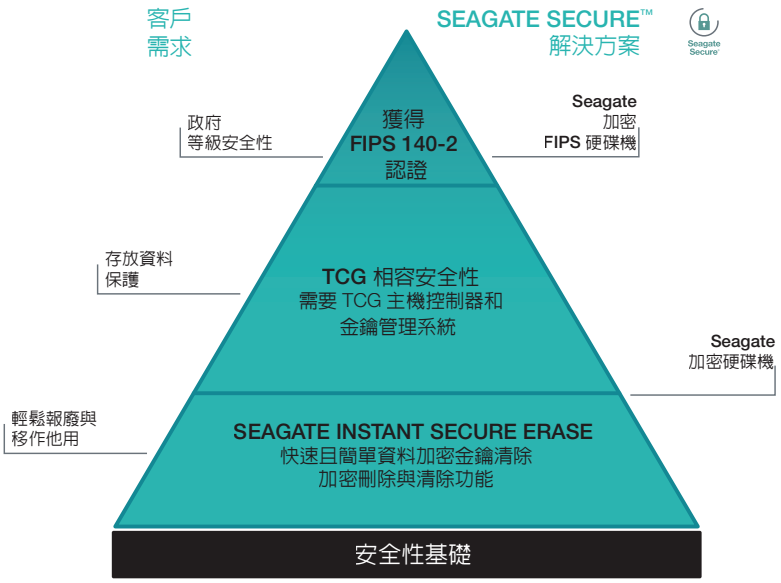

圖 2：適用於所有層級安全實作的 Seagate Secure™ 解決方案

每項初始配置的相關清除方法於表 1 中會有詳細說明。 對於具有深厚 SCSI 或 ATA 指令和編碼專業知識的 Seagate 客戶，也可以使用 TCG 儲存體、T10 和 T13 指令集與規格配合 Seagate SED，開發專利解決方案。如需詳細資訊，請連絡您的 Seagate 銷售代表。

Seagate 加密硬碟機如何執行 Instant Secure Erase

Seagate SED 支援一或多種執行 Seagate ISE 的方式，視硬碟機的介面指令集和配置而定。例如，具有 SATA 介面的裝置可能與支援 SAS 介面的裝置有不同的清除功能。此外，額外的安全性和清除功能可以透過 SED 支援的 TCG 儲存體安全通訊協定使用。請留意，在任何情況下，主機控制器都必須透過支援的指令為 Seagate ISE 實作支援。

1. 配置為核心資料防護的硬碟機 (不論是否具備防偽保護) 會使用 TCG 企業通訊協定啓用。

   使用 TCG 儲存體規格通訊協定管理的裝置會支援頻帶層級 Seagate ISE。除了在硬碟機使用時保護使用者資料之外，頻帶層級 Seagate ISE 可以清除裝置上儲存的部分或所有資料，而不影響硬碟機上的其他資料頻帶。這種資料清除方式是透過在每個頻帶上使用 TCG 儲存體安全通訊協定 (清除方法) 進行，需要使用協力廠商軟體。

   使用 TCG 儲存體規格通訊協定管理的裝置也可以透過呼叫安全通訊協定的 RevertSP 方法一次清除。此類型的安全清除需要實際持有裝置才能讀取印於標籤上的 32 字元 PSID (實體安全 ID) 並安全地清除硬碟機，使其恢復原始出廠狀態。

2. 僅配置為輕鬆報廢與移作他用防護的硬碟機會使用 ATA 安全指令啓用。

   Seagate SED 實作 ATA 指令集是透過呼叫 ATA 安全清除準備和安全清除裝置指令加以清除。請留意，這是 Seagate 的特殊 Seagate ISE 實作。

Seagate Instant Secure Erase 部署選項

表 1 提供在 SED 上部署 Seagate ISE 的不同方法概觀。請查看表格下方的附註。

表 1：Seagate Instant Secure Erase 選項

初始配置	核心資料防護，具備或不具防偽保護		僅限硬碟機移作他用時的保護	未啓用安全性
清除方法	**TCG 安全通訊協定** 清除	**TCG 安全通訊協定** RevertSP	**ATA 安全性** 安全清除準備與安全清除裝置指令	**清除** 清除功能組合/指令
支援的配置	具有 TCG 儲存體的 Seagate SED	具有 TCG 儲存體的 Seagate SED	Seagate SATA SED	支援的 Seagate SATA 和 SAS SED
清除範圍	頻帶層級加密清除	整個硬碟機的資料皆以加密方式清除	整個硬碟機的資料皆以加密方式清除	整個硬碟機的資料皆以加密方式清除
副作用	解除鎖定頻帶並重設頻帶密碼	SED 恢復為出廠預設狀態	解除鎖定硬碟機並停用 ATA 安全性	沒有避免意外清除的初始安全性
存取控管	必須使用主機管理或裝置預設密碼進行驗證	必須使用於硬碟機標籤上印出 (與條碼形式呈現) 的密碼進行驗證	必須使用主機管理密碼進行驗證	刻意設計為未驗證 (如果硬碟機已鎖定，必須由操作人員解鎖才能執行)
優點	核心資料防護 FIPS 140-2 Level 2 驗證 以 TCG 儲存體規格為基礎的全功能安全管理介面	核心資料防護 FIPS 140-2 Level 2 驗證 以 TCG 儲存體規格為基礎的全功能安全管理介面	ATA 硬碟機層級安全性 使用標準 ATA 安全指令	提供無須管理負擔 (亦即不需要密碼管理) 的安全清除
意見	需要 TCG 相容的硬體或軟體	需要實際持有 SED 以讀取硬碟機安全性代碼	運用標準 ATA 安全指令	由於指令未經防護的本質，有發生錯誤或惡意資料清除的可能性

註釋

1. 在大多數情況下，使用較高安全性配置以安全清除硬碟機資料的方法，在較低安全性設定下也可以使用，例如只要硬碟機也支援 TCG 指令集 (安全性支援可能會依硬碟機機型有所不同)，RevertSP 通訊協定就可以用於配置為 ATA 模式的硬碟機。
2. 核心資料防護這個詞是指 SED 在正常運作的電腦環境中已配置鎖定資料介面避免未經授權存取的硬碟機上提供優異資料洩漏保護功能的能力。
3. 聯邦資訊處理標準 (FIPS) 140-2 是美國政府電腦安全標準用以核可加密模組的標準。該規定的標題為加密模組安全需求 *(FIPS PUB 140-2)*，是由美國國家標準與技術局 (NIST) 所核發。 此標準會指定保護重要但非機密性與受保護級別資料之安全系統內使用之加密模組應達成之安全性需求。 Seagate FIPS 硬碟機已認證為等級 2 (防偽)；更多資訊可以在這裡找到：
   www.seagate.com/docs/pdf/whitepaper/mb605_fips_140_2_faq.pdf

Seagate Instant Secure Erase 部署選項

如何在 Seagate SED 上執行 Seagate Instant Secure Erase

根據選擇用來安全清除裝置的 SED 和選項類型，實際資料清除可以透過不同方式達成目的。以下是可使用的解決方案：

- Windows 版 Seagate SeaTools™ 軟體：免費的 PC 工具，可診斷內部與外部連接的儲存裝置。SeaTools 軟體支援 Seagate ISE。SeaTools 軟體位於 www.seagate.com「SeaTools — 診斷軟體」下的「支援與下載」標籤。
- 協力廠商現成解決方案：使用 LSI 和 Intel 的 RAID 控制器，或 IBM (Tivoli Key Lifecycle Manager)、Wave、Winmagic 等廠商的完整金鑰管理解決方案。
- 自訂/內嵌解決方案：(內部) 開發的功能整合於系統或主機應用系統以支援 Seagate ISE。 如需詳細資訊，請連絡您的 Seagate 銷售代表。

參考資料

TCG 儲存體規格—
www.trustedcomputinggroup.org/developers/storage/specifications

ATA 規格—
www.t13.org/

SCSI 規格—
www.t10.org/

Seagate SeaTools 軟體—
http://www.seagate.com/tw/zh/support/downloads/seatools/

www.seagate.com

Seagate Secure®

美洲地區 Seagate Technology LLC 10200 South De Anza Boulevard, Cupertino, California 95014, United States, +1 408 658 1000
亞太地區 Seagate Singapore International Headquarters Pte. Ltd. 7000 Ang Mo Kio Avenue 5, Singapore 569877, +65 6485 3888
歐洲、中東和非洲 Seagate Technology SAS 16–18, rue du Dôme, 92100 Boulogne-Billancourt, France, +33 1 41 86 10 00