Documento de tecnología

Opciones de implementación del Instant Secure Erase de Seagate

Introducción

Cuando las unidades de disco duro se retiran y salen del centro de datos a manos de terceros, esto supone poner en alto riesgo los datos contenidos en esas unidades. No obstante, el departamento de informática aún debe retirar y deshechar regularmente las unidades por diversas razones, entre las que se incluye:

- Reutilización de las unidades para otras tareas de almacenamiento.
- Devolución de unidades por garantía, reparación o expiración de los contratos de arrendamiento.

La mayor parte de las unidades de disco duro quedan fuera del control de su propietario una vez que estas abandonan el centro de datos; de hecho, Seagate estima que diariamente se retiran del centro de datos alrededor de 50.000 unidades. Los datos corporativos y personales todavía residen en esas unidades, y cuando estas se retiran, aún es posible leer los datos allí almacenados. Incluso los datos grabados en muchas unidades en una matriz RAID son vulnerables al robo, puesto que basta una sola línea en las matrices actuales de alta capacidad para tener acceso a cientos de nombres y números de la seguridad social.

Opciones de implementación del Instant Secure Erase de Seagate

Complicaciones del control de unidades y costos de eliminación

En un esfuerzo por evitar la divulgación de datos y el posterior envío de las notificaciones para los clientes exigidas por las leyes de privacidad, las corporaciones han probado un sinfín de opciones para eliminar los datos en las unidades retiradas antes de que estas abandonen el lugar y puedan caer en manos inapropiadas. Los procedimientos de retiro actuales diseñados para impedir la lectura de los datos dependen en gran medida de la participación humana durante el proceso, por lo que están sujetos a fallas humanas y técnicas.

Los procedimientos de retiro utilizados actualmente presentan un gran número de desventajas de largo alcance:

- La sobreescritura de los datos en las unidades es costosa y bloquea recursos valiosos del sistema durante días. La unidad no genera ninguna notificación de que se ha completado el proceso, y la sobreescritura no cubre los sectores reasignados, por lo que los datos quedan expuestos.
- Tanto la desmagnetización como la fragmentación física de una unidad son costosas. Es difícil garantizar que la fuerza desmagnetizadora sea la más óptima para el tipo de unidad, con lo que podrían quedar ciertos datos legibles en esta. La fragmentación física de la unidad pone en peligro el medio ambiente, y ninguno de los procedimientos permite devolver la unidad por garantía o expiración de arrendamiento.
- Algunas empresas han concluido que la única manera de retirar las unidades de forma segura es guardarlas en su posesión y almacenarlas en depósitos por un tiempo indefinido. Sin embargo, este método no es realmente seguro, pues el gran número de unidades sumado a la participación humana, inevitablemente conduce al extravío o hurto de algunas unidades.
- Otras compañías prefieren contratar servicios profesionales para el proceso de eliminación, una opción costosa que implica el costo de desempeño y reconciliación de los servicios, así como de los informes internos y auditorías. Más preocupante aún, cuando se transporta una unidad hasta el lugar del servicio se ponen en riesgo los datos almacenados. El extravío de una sola unidad podría suponerle a la compañía millones de dólares para remediar la divulgación de los datos.

Los retos relacionados con el rendimiento, la escalabilidad y la complejidad han llevado a los departamentos de informática a rechazar las políticas de seguridad que requieran el uso de cifrado. Además, el cifrado ha sido visto como un procedimiento riesgoso por aquellos que no están familiarizados con la administración de claves, un proceso que le permite a una compañía asegurarse de que siempre pueda descifrar sus propios datos. Las unidades con cifrado automático (SED) resuelven estos problemas de manera integral, con lo que el cifrado para el retiro de unidades se hace fácil y asequible.

La tecnología Instant Secure Erase de Seagate hace que el retiro de la unidad sea seguro, rápido y fácil

Las unidades SED codifican todos los datos del usuario a medida que ingresan en la unidad mediante una clave de cifrado de datos almacenada de forma segura en la misma. Por consiguiente, todos los datos almacenados en SED se codifican de forma predeterminada. Cuando llega el momento de retirar o reutilizar la unidad, el propietario simplemente envía un comando a la unidad para llevar a cabo el Instant Secure Erase de Seagate (ISE). El ISE de Seagate usa la capacidad de cifrado de las unidades SED para cambiar la clave de cifrado de los datos.[1]

La eliminación cifrada segura remplaza la clave de cifrado de SED, como se muestra en la Figura 1. Una vez que se cambia la clave usada originalmente para cifrar los datos, los datos cifrados con esa clave se vuelven ilegibles e irrecuperables. De esta manera, Instant Secure Erase de Seagate destruye de forma instantánea, segura y efectiva los datos almacenados en el dispositivo y la unidad queda lista para ser descartada, reutilizada o vendida. Las unidades SED, independientemente del enfoque de implementación, reducen los gastos operativos de informática al evitar los dolores de cabeza ocasionados por el control de unidades y los costos de eliminación. La seguridad de nivel gubernamental de los datos de las unidades SED de Seagate ayuda a garantizar el cumplimiento con las normas Safe Harbor para la privacidad de los datos, sin comprometer la eficiencia informática. Además, las unidades SED simplifican el proceso de desactivación y protegen el valor del hardware en caso de devolución y reutilización al:

- Eliminar la necesidad de sobrescribir o destruir la unidad.
- Asegurar las unidades devueltas por garantía y vencimiento del arrendamiento.
- Permitir reutilizar o vender las unidades de forma segura.

Figura 1. El proceso de Instant Secure Erase de Seagate

[1] Seagate trabaja conjuntamente con diversos líderes de la industria y agencias gubernamentales para definir la regulación de la destrucción de datos mediante la eliminación criptográfica, de conformidad con la ISO (Organización Internacional de Normalización) según la ISO/IEC WD 27040.

Opciones de implementación del Instant Secure Erase de Seagate

Soluciones de Seagate según las distintas necesidades de seguridad

Todas las unidades SED empresariales de Seagate ofrecen funcionalidad de ISE de Seagate. El método empleado varía en función del nivel de seguridad implementado al poner en funcionamiento la unidad. Tenga en cuenta que cada nivel incluye las capacidades de protección de los niveles anteriores.

- Protección ante evidencia de violación de datos en reposo (FIPS 140-2 Nivel 2)
- Protección de datos en reposo
- Solo protección por reutilización (ISE de Seagate)

Figura 2. Seagate garantiza™ soluciones para todos los niveles de implementación de la seguridad

Los métodos de borrado pertinentes para cada una de estas configuraciones iniciales se detallan en la Tabla 1. Para aquellos usuarios de Seagate que usen comandos SCSI o ATA y conocimiento de codificación, también es posible desarrollar una solución propia para el empleo de las unidades SED de Seagate con almacenamiento TCG, T10 y conjuntos de comandos y especificaciones T13. Póngase en contacto con su representante de ventas de Seagate para más información.

Cómo las unidades con cifrado automático (SED) de Seagate ejecutan el Instant Secure Erase

Las unidades SED de Seagate admiten más de una forma de ejecutar el ISE de Seagate, dependiendo del conjunto de comandos y configuraciones de la interfaz de la unidad. Por ejemplo, un dispositivo con una interfaz SATA puede ofrecer opciones de borrado distintas a las de un dispositivo con una interfaz SAS. Además, la seguridad adicional y las opciones de borrado están disponibles a través del protocolo de seguridad de almacenamiento TCG compatible con SED. Tenga en cuenta que, en cualquier circunstancia, el controlador del host puede respaldar el ISE de Seagate a través de un comando compatible

1. Las unidades configuradas con protección de datos en reposo, que cuente o no con protección ante evidencia de violación, quedan habilitadas al usar los protocolos empresariales TCG.

   Un dispositivo que use el protocolo de especificaciones de almacenamiento TCG es compatible con el ISE a nivel de banda de Seagate. Además de proteger los datos del usuario mientras la unidad se encuentra en uso, el ISE a nivel de banda de Seagate permite borrar todos o una parte de los datos almacenados en el dispositivo, sin afectar otras bandas de datos de la unidad. Esta forma de borrado de datos se lleva a cabo mediante el protocolo de seguridad de almacenamiento TCG (método de borrado) en cada banda, y requiere de un software de terceros.

   Un dispositivo que use el protocolo de especificaciones de almacenamiento TCG también admite eliminación inmediata al activar el método RevertSP del protocolo de seguridad. Este tipo de borrado seguro requiere la presencia física del dispositivo para leer los 32 caracteres del PSID (ID físico de seguridad) impresos en la etiqueta y borrar de forma segura la unidad para restaurarla a su estado de fábrica original.

2. Solo se puede configurar la protección contra eliminación y reutilización en las unidades usando los comandos de seguridad ATA.

   Para borrar una unidad SED de Seagate que esté configurada con el conjunto de comandos ATA se deberán activar los comandos ATA Security Erase Prepare y Security Erase Unit ATA. Cabe señalar que esta es una implementación única del ISE de Seagate.

Opciones de implementación del Instant Secure Erase de Seagate

En la Tabla 1 se ofrece una descripción general de los métodos utilizados para implementar el ISE de Seagate en una unidad SED. Véanse las notas que le siguen a la tabla.

Tabla 1. Opciones de Instant Secure Erase de Seagate

Configuración inicial	Protección de datos en reposo, que cuente o no con protección ante evidencia de violación		Solo para protección contra reutilización	Seguridad no activada
Método de eliminación	**Protocolo de seguridad TCG** Borrar	**Protocolo de seguridad TCG** RevertSP	**Seguridad ATA** Comandos Security Erase Prepare y Security Erase Unit	**Eliminar** Conjunto de características/ Comando Eliminar
Configuración compatible	Unidades SED de Seagate con almacenamiento TCG	Unidades SED de Seagate con almacenamiento TCG	Unidades SED SATA de Seagate	Unidades SED SATA y SAS de Seagate compatibles
Alcance del borrado	Eliminación cifrada a nivel de banda	Se ejecutó una eliminación cifrada en toda la unidad	Se ejecutó una eliminación cifrada en toda la unidad	Se ejecutó una eliminación cifrada en toda la unidad
Efecto secundario	Desbloquear banda y reiniciar la contraseña de banda	La unidad SED fue restaurada al estado de fábrica predeterminado	Desbloquear unidad y desactivar seguridad ATA	No dispone de seguridad inicial para evitar borrado accidental
Control de acceso	Requiere autenticación mediante contraseña administrada por un host o predeterminada por el dispositivo	Requiere autenticación usando contraseña impresa (y código de barra) en la etiqueta de la unidad	Requiere autenticación usando contraseña(s) administrada(s) por un host	No autentificada por el diseño (si la unidad se encuentra bloqueada, esta deberá ser desbloqueada por el operador antes de la ejecución)
Ventajas	Protección de datos en reposo Validación FIPS 140-2 Nivel 2 Interfaz de administración de seguridad completa basada en las especificaciones de almacenamiento TCG	Protección de datos en reposo Validación FIPS 140-2 Nivel 2 Interfaz de administración de seguridad completa basada en las especificaciones de almacenamiento TCG	Seguridad ATA a nivel de unidad Usa comandos de seguridad ATA estándar	Ofrece borrado seguro sin gastos de gestión (por ejemplo, no requiere administración de contraseña)
Comentarios	Requiere hardware o software compatible con TCG	Requiere la presencia física de la unidad SED para leer el código de seguridad de la unidad	Utiliza comandos de seguridad ATA estándar	Es posible que se borren datos erróneos o maliciosos debido a que el comando no cuenta con protección

Notas

1. En la mayoría de los casos, el método empleado para borrar de forma segura una unidad configurada con alto nivel de seguridad también se puede emplear con configuraciones de bajo nivel de seguridad. Por ejemplo, el protocolo RevertSP puede funcionar en una unidad configurada en modo ATA, suponiendo que esta también sea compatible con el conjunto de comandos TCG (la disponibilidad de seguridad puede variar en función del modelo de la unidad).
2. El término *protección de datos en reposo* se refiere a la capacidad que tiene una unidad de cifrado automático (SED) para ofrecer protección de alto nivel de los datos en una unidad que ha sido configurada para bloquear la interfaz de datos ante accesos no autorizados mientras se encuentra conectada a un entorno informático en funcionamiento.
3. La Norma federal para el procesamiento de información (FIPS), Publicación 140-2, es una norma de seguridad informática del gobierno de EE. UU. para autorizar módulos de cifrado. Lleva por nombre *Requisitos de seguridad para módulos criptográficos (FIPS PUB 140-2, por sus siglas en inglés)* y fue publicada por el National Institute of Standards and Technology (NIST, o Instituto Nacional de Normalización y Tecnología). Esta norma establece los requisitos de seguridad que debe cumplir un módulo criptográfico utilizado dentro de un sistema de seguridad que protege datos de clase *confidencial pero sin clasificar* y *protegidos*. Las unidades FIPS de Seagate cuentan con certificación de nivel 2 (evidencia de violación). Puede encontrar más información en: www.seagate.com/docs/pdf/whitepaper/mb605_fips_140_2_faq.pdf

Opciones de implementación del Instant Secure Erase de Seagate

Cómo llevar a cabo un Instant Secure Erase (ISE) de Seagate en una unidad SED de Seagate

Existen diversas maneras de eliminar los datos actuales, según el tipo de SED y las opciones seleccionadas para borrar de forma segura el dispositivo. Están disponibles las siguientes soluciones:

- Software Seagate SeaTools™ para Windows: herramienta gratis para PC que permite diagnosticar dispositivos de almacenamiento conectados de forma interna y externa. El software SeaTools es compatible con ISE de Seagate. El software SeaTools se encuentra en www.seagate.com, en la pestaña Soporte y descargas, debajo de SeaTools – Software de diagnóstico.
- Soluciones de terceros disponibles para la venta: use Controladores RAID de LSI e Intel o una solución de administración de claves de IBM (Tivoli Key Lifecycle Manager), Wave, Winmagic, etc.
- Soluciones personalizadas/incluidas: (internas) capacidad de desarrollo integrada en el sistema o aplicación de host para respaldar el ISE de Seagate. Póngase en contacto con su representante de ventas de Seagate para más información.

Referencias

Especificaciones de almacenamiento TCG—
www.trustedcomputinggroup.org/developers/storage/specifications

Especificaciones ATA—
www.t13.org/

Especificaciones SCSI—
www.t10.org/

Software SeaTools de Seagate—
http://www.seagate.com/la/es/support/downloads/seatools/

www.seagate.com

Seagate Secure®

AMÉRICA Seagate Technology LLC 10200 South De Anza Boulevard, Cupertino, California 95014, EE. UU., +1 408 658 1000
ASIA/PACÍFICO Seagate Singapore International Headquarters Pte. Ltd. 7000 Ang Mo Kio Avenue 5, Singapur 569877, +65 6485 3888
EUROPA, ORIENTE MEDIO Y ÁFRICA Seagate Technology SAS 16-18 rue du Dôme, 92100 Boulogne-Billancourt, Francia, +33 1 41 86 10 00