Informe técnico

HP Secure Erase

Borra tu información confidencial de manera segura y efectiva de las unidades de estado sólido (SSD)

Índice

HP Secure Erase es un recurso muy importante para los administradores informáticos encargados de proteger información confidencial, y además es un componente clave del sistema de seguridad de HP.
HP Secure Erase facilita la reparación de unidades de estado sólido locales (SSDs por sus siglas en inglés) conforme a los estándares de fábrica antes de eliminarlos o reciclarlos.

Reparación del almacenamiento local: el último paso importante en el ciclo de vida de un computador

En entornos en los que la información confidencial del usuario está siendo atacada en todas las etapas del ciclo de vida del sistema, es fundamental asegurarse de que la información confidencial pueda borrarse de manera segura desde un dispositivo de almacenamiento de información. La información puede ser vulnerable si se deja en un disco duro mientras se recicla, se elimina el sistema o se cambia de usuario. El reparar de manera apropiada las unidades de almacenamiento conforme a los estándares de fábrica es un paso fundamental en el ciclo de vida de un computador.

Además de cumplir con los estándares de fábrica para borrar información en las unidades de disco duro (HDD) magnéticas, HP ha dado un paso extra al desarrollar HP Secure Erase, una característica común que viene en todos los notebooks empresariales HP, que respalda los métodos descritos en la publicación especial 800-88 del Instituto Nacional de Normas y Tecnología. HP Secure Erase se ejecuta dentro del hardware de la unidad para sobrescribir la información que se encuentra disponible en la unidad. Los fabricantes de unidades de estado sólido aprobadas para ser usadas en los notebooks empresariales de HP verificaron si al ejecutar el HP Secure Erase en la unidad de estado sólido se eliminaba por completo toda la información del usuario para que no pudiera ser recuperada.

Borrado de SSD vs. HDD

En las unidades de disco duro estándar se puede sobrescribir la información usando un algoritmo para eliminar información, que escriba múltiples patrones en cada sector, agrupación y bit del disco duro. Este proceso está documentado en el Departamento de Defensa de los Estados Unidos (DOD por sus siglas en inglés) 5220.22-M, capítulo 8.[1] Las herramientas que usan este proceso de sobrescritura solo son efectivas en unidades de disco duro estándar. Escribir un patrón de información predeterminado a un SSD con memoria flash NAND no resulta en una unidad vacía, sino en una unidad llena de información que tendrá que ser borrada antes de que el nuevo usuario pueda empezar a escribir su información, lo cual reduce enormemente la vida del servicio.

Recuperación del disco estándar
Para poder borrar de manera segura toda la información del usuario de la SSD y restaurar la unidad para que regrese a un estado de rendimiento como recién salido de la caja (FOB por sus siglas en inglés), el Instituto Nacional de Normas y Tecnología (NIST por sus siglas en inglés) soporta el comando de "UNIDAD DE BORRADO SEGURO" que cumple con las normas mínimas de reparación de medios de unidades de estado sólido (NIST SP800- 88 Rev. 1).

HP Secure Erase cuenta con un comando ATA llamado "Unidad de Borrado Seguro", que está definido en el ATA del Instituto Nacional Estadounidense de Normas (ANSI por sus siglas en inglés) y en la interfaz SCSI del disco duro y cumple con las normas "claras" NIST 800-88 Rev. 1. En vez de escribir en la unidad, el comando de "Unidad de Borrado Seguro" hace que la SSD aplique un pico al voltaje de todas las memorias disponibles NAND (memoria flash) simultáneamente, restaurando todos los bloques de espacio disponibles en una sola operación. Esto obliga a la unidad a "olvidar" toda la información almacenada a tal punto que no se pueda recuperar ni con los servicios de recuperación de información más avanzados. Este proceso usa un solo programa con un ciclo de borrado y por lo general finaliza en menos de dos minutos. Este tiempo de recuperación representa un gran salto hacia los procesos similares para las unidades de disco duro, que por lo general tarda horas en eliminar la información del usuario de manera segura.

¿Cuál es la información que no se borra?
Después de instalar HP Secure Erase en una SSD, toda la información del usuario se borra por completo e irreparablemente, y todos los bloques del espacio del usuario están listos para aceptar información nueva, lo que mueve la unidad a su estado de rendimiento más alto (FOB). Sin embargo, parte de la información debe dejarse en su lugar, incluyendo la información que se requiera para que la unidad opere de manera normal: copias del firmware de la SSD que se encuentran en la memoria NAND, toda la tecnología SMART y tablas de bloqueo de mapas de NAND retirados.

Conclusión

Escribir o sobrescribir información en la unidad se considera como la práctica aceptada para eliminar información de un HDD de manera segura. Sin embargo, en el caso de unidades de estado sólido de memoria NAND, la sobrescritura es redundante, innecesaria y un método posiblemente inseguro para eliminar información. Al usar HP Secure Erase, los usuarios pueden estar seguros de que las unidades de estado sólido están totalmente reparadas y que cumplen con las normas mínimas.

HP Secure Erase se puede instalar fácilmente a través del proceso de instalación F10 BIOS en la mayoría de los computadores empresariales HP.

Conoce más en
hp.com/lar/pcsecure

Notas

[1] La especificación 5220.22-M ya no existe. Por ende, el Departamento de Defensa de los Estados Unidos decidió que la información segura debe ser destruida para poder mantenerse a salvo. El NIST volvió a declarar de manera clara que la regla de dos personas (es decir, verificación humana) se debe implementar, pero no estableció las normas para el método de reparación (podría ser una simple eliminación con verificación humana doble o una sola destrucción con lo mismo).

Regístrate para recibir actualizaciones
hp.com/go/getupdated

Comparte con colegas

4AA7-2608SPL, septiembre de 2018