Technical white paper

HP Secure Erase

Safely and effectively erase sensitive data from solid state drives

Table of contents

HP Secure Erase is a critical resource for IT administrators tasked with protecting sensitive data, and a key component of HP system security. HP Secure Erase makes it easy to sanitize local solid-state drives (SSDs) to industry standards before disposal or recycling.

Local storage sanitation—an important last step in the PC lifecycle

In an environment where sensitive user information is under attack at every stage of the system lifecycle, ensuring that data can be securely erased from a data storage device is paramount. Information can be vulnerable if left on a hard drive when a system is recycled or disposed of, or re-provisioned for another user. Properly sanitizing storage drives according to industry standards is a critical step in the PC lifecycle.

In addition to meeting industry standards for data erasure in standard magnetic hard disk drives (HDDs), HP has taken the additional step of developing HP Secure Erase—a standard feature in all HP business notebooks—that supports the methods outlined in the National Institute of Standards and Technology Special Publication 800-88. Secure Erase runs inside the drive hardware to overwrite data contained on the drive. Manufacturers of industry-standard SSDs approved for use in HP business notebook products have verified that running the Secure Erase command on their SSDs fully removes all user data so that it cannot be recovered.

Erasing SSDs vs. HDDs

On standard HDDs, data can be overwritten using a data-removal algorithm that writes multiple patterns on every sector, cluster, and bit of the hard drive. This process is documented in the Department of Defense (DOD) 5220.22-M Chapter 8 specification.[1] Tools that use this overwrite-based process are only effective on standard HDDs. Writing a predetermined data pattern to a NAND flash-based SSD does not result in an empty drive. Instead it results in a drive full of data that must be erased before new user data can be written, which massively shortens the service life.

Industry-standard disk sanitation

To securely erase all user data from an SSD and restore the drive to a fresh-out-of-box (FOB) performance state, the National Institute of Standards Technology (NIST) supports the "SECURITY ERASE UNIT" command that meets the minimum guideline for media sanitization of SSDs (NIST SP800- 88 Rev. 1).

HP Secure Erase relies on an ATA command called "Security Erase Unit" that is defined in the American National Standards Institute (ANSI) ATA and SCSI disk drive interface specification and meets NIST 800-88 Rev. 1 "Clear" guidelines. Instead of writing to the drive, the "Security Erase Unit" command causes the SSD to apply a voltage spike to all available NAND (flash memory) in unison, resetting every available block of space in one operation. This forces the drive to "forget" all stored data to the extent that it cannot be recovered by even the most advanced data recovery services. This process uses a single whole-program-erase cycle and is usually completed in less than two minutes. This time-to-sanitation represents a quantum leap ahead of similar processes for HDDs, which can typically take hours to securely eliminate user data.

What data is not erased?

After deploying HP Secure Erase on an SSD, all data in the user space is completely and irretrievably erased, and every block in the user space is ready to accept new host-written data, which moves the drive to its highest performance state (FOB). However, some data must be left in place, including data required for normal drive operation: SSD firmware copies that reside in the NAND, all SMART data, and retired NAND block mapping tables.

Conclusion

Writing or overwriting data to drive is the accepted practice of securely eliminating data from a HDD. However, in the case of NAND flash-based SSDs, overwriting is redundant, unnecessary, and a potentially insecure method of eliminating data. By using HP Secure Erase, users can ensure that SSD drives are completely sanitized and meet the minimum industry standards.

HP Secure Erase is easily enabled through the standard F10 BIOS setup process on most HP business PCs.

Learn more
hp.com/go/computersecurity

Notes

[1] Specification 5220.22-M no longer exists. The DoD has subsequently decided that secure information must be destroyed to remain secure. The NIST has restated in clear terms that a two-person rule (read human verification) shall be implemented but did not establish guidelines on the method of sanitization (it could be a single wipe with dual human verification, or a single destruction with the same).

Sign up for updates
hp.com/go/getupdated

Share with colleagues

4AA7-2608ENW, March 2018