LITE-ON Storage is now Solid State Storage Technology Corporation

Secure Erase and Sanitize: Securing Your Data

Data Erasure Overview

It’s important to have the ability to securely erase a drive. When decommissioning a device, whether for resale or recycling, there must be no data remnants present. A malicious agent could retrieve data from the drive and use it for various nefarious things, whether they are pulling passwords, privacy data, intellectual property, etc. It also simply makes sense not to leave data on a drive if in the future it is to be reused. Standards and techniques were developed to ensure this was case, first for hard disk drives (HDDs) and other Advanced Technology Attachment or ATA-based devices but later non-volatile media express (NVMe™) solid state drives (SSDs) as well. For this document, general terms will be utilized rather than the specific command strings in order to improve readability.

Secure Erase

Secure Erase, also known as Security Erase, was developed for ATA devices as part of the ATA Command Set (ACS), specifically for PATA and SATA HDDs. The goal was to have a method of completely wiping all data on the drive so that it could never be retrieved. This offered a strong level of security for when sensitive data had to be erased. Secure Erase later became available to SSDs but does not function in precisely the same way with those types of devices. This is because HDDs and SSDs operate differently, for example with SSDs requiring a flash translation layer (FTL) to map between physical and logical data locations.

Secure Erase with HDDs works by writing binary values, that is 0s and 1s, to the entirety of the drive, ensuring no recovery of the original data is possible. It’s important to contrast this to other types of erasures, such as a quick format in Windows or a low-level zeroing of the drive. A quick format is not secure and a low-level format only writes 0s to already-written areas. Security standards for intelligence groups will have specific requirements that differ from a secure erase, also, for example stipulating a set number of formats. Methods of overwriting with HDDs could take hours or even days when meeting these standards.

The Secure Erase function works different with SSDs, not least because there are both SATA and NVMe™

drives available. AHCI and NVMe™ are different protocols but can have overlapping functions, similar to trim (or TRIM) in ATA versus UNMAP in SCSI. Secure Erase for SSDs works by eliminating the mapping table on the drive. The mapping table acts as a table of contents or address book, pointing to data locations, stored as a form of metadata. Once data is removed from the mapping table the host or OS can notify the drive of these changes by engaging in a mass trim command. This essentially allows the drive to erase all the cells – flash must be erased before it can be rewritten – as the data contained within is no longer required.

While superficially secure, this does have some limitations. Secure Erase technically only deletes the mapping table and not the underlying blocks. SSDs again act differently than HDDs here because flash, once erased, effectively leaves no trace of prior data, assisted by the fact it's erased in blocks with a common voltage – the entire block is spiked to a high voltage. Technically speaking it could be possible to rebuild the mapping table or interrupt the Secure Erase process, plus there are challenges particularly with modern drives due to over-provisioned space and SLC caching. However, these devices tend to force the Secure Erase process to complete – even on power loss – and further the blocks are trimmed quickly.

Nevertheless, the Sanitize function was created to fully ensure that a drive is erased securely. Other elements of design, such as encryption, and variations of the Sanitize function also exist to assist in data erasure. The Sanitize command is also compatible with ATA, SCSI, and SAS (with also format) when supported by a device, allows for overwriting, block erasure, or a Crypto scramble. It's worth stating that modern drives may treat Secure Erase and Sanitize equivalently as controller firmware may send a block erase command regardless, so differentiation here is mostly academic.

Sanitize

The Sanitize command, or the Format NVM command for a namespace, as parts of the NVMe™ Specification for NVMe™ SSDs, were developed specifically to secure SSDs. It also erases the mapping table like Secure Erase but additionally erases written blocks. Although erasing blocks is a relatively slow process, the ability of modern drives to erase many or all at once for a sanitize means the command only takes a minute or two to process. Erasing in parallel is limited only by the power demands of the erase voltage.

Sanitize also requires the drive to complete the process once started, so it cannot be interrupted even in the case of power loss.

Secure Erase, for its part, is often a feature found in the BIOS/UEFI, in SSD toolboxes, and with bootable media like Parted Magic. Sanitize is also easily accessible in Linux with nvme-cli, that is the NVMe™ command line interface, as part of NVMe™ tools. Sanitize for ATA and SCSI can be achieved through hdparm. These tools allow for a block erase or discard which differ from fstrim which only discards unused blocks in the file system. An exception might be bad or damaged blocks which have failed an erase before being replaced by a spare. Generally speaking, the data from such blocks is already irretrievable.

This distinction is particularly important because a proper Sanitize will ensure all drive caches are deleted, preventing any sort of recovery. Sanitize also allows for a pattern overwrite, a type of shredding, although this tends not to be recommended on SSDs for two reasons: one, it reduces endurance and two, as mentioned above flash data is more challenging to forensically recover than data from a typical hard drive due to the technical structure. It should be mentioned that some data on the drive, that which is required for normal operation, will always remain.

Another element of SSDs, particularly modern and enterprise SSDs, is encryption. Self-Encrypting Drives (SEDs) can encrypt data through hardware on-the-fly, although this is not always completely secure. However, it allows a different type of Sanitize known as a Crypto Erase. The Crypto Erase simply discards the encryption key which makes it impossible to decrypt the data on the drive. This type of erase is extremely quick. Any sort of mapping or block discard can proceed afterwards for extra security. Current drives rely on 256-bit encryption via the Advanced Encryption Standard, or AES-256, and may be able to revert the drive to a Fresh Out-of-Box (FOB) state through physical security identification (PSID).

Modern SSDs also engage in scrambling and encryption internally for multiple reasons. For example, using the XOR command allows a more even distribution of 0s and 1s which reduces the error rate. This assists with data path protection, and XOR is also used for parity. Further, SSDs can actively encrypt the flash so that a bad actor cannot retrieve data from the drive if they happen to get access to the physical flash chips.

Crypto Erase can utilize the encryption hardware for a scramble function that can further obscure data following a block erase.

Standards and Other Considerations

There are several industry standards relevant to the secure wiping of data. The Department of Defense (DoD) in the United States has the DoD 5220.22-M data destruction standard, which notably is difficult to apply to flash media. This is especially true as it advocates for multiple overwrites. The DoD methods are therefore more of a guideline and specifically apply to HDDs and other forms of media, referring to the National Institute of Standards and Technology's (NIST) 800-88 for SSDs instead. This was revised in 2014 under SP800-88r1 (Revision 1) to better handle modern media.

The NIST 800-88 guidelines for media sanitization operate on a clear-purge-destroy approach to data sanitation. For example, with SSDs the clear protocol would include an overwrite or a Secure Erase. Purge would require a sanitize in the form of a block erase, a Crypto Erase scramble, or a normal Crypto Erase. Destroy would involve the actual physical destruction of the device. If this seems extreme, there are actually many patents for SSD self-destruction, particularly for use in the financial industry.

Related to this is the Trusted Computing Group (TCG) Opal specification which defines data encryption. Specifically, it is oriented at SEDs, and as such is tied to the Crypto Erase function. This uses AES-256 as mentioned but there are also software solutions that can be part of an overall security scheme.

Summary

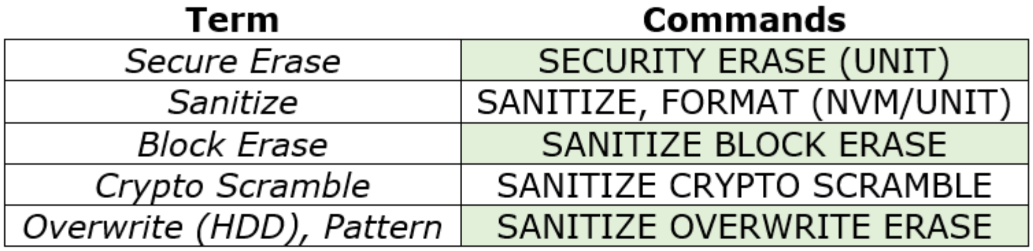
It is crucial in many industries to ensure that devices, once they are no longer needed or if they must be repurposed, are secured against the retrieval or recovery of critically sensitive data. Old standards and methods for HDDs proved insufficient for flash-based SSDs. Secure Erase provides a basic function or option for erasing any SSD and, if allowed to proceed normally, is sufficient for general data erase purposes.

However, Sanitize and its options are far more comprehensive, especially with NVMe™ drives.

Sanitize more appropriately works with SSDs which, with block-based flash media, have distinct technical properties. Typical mass overwriting is available if rarely advised due to the endurance hit, especially because cryptographic scrambling is a superior option particularly when followed up with a sanitize block erase. Ideally the mapping table is erased followed by a block discard, uninterruptible and capable of erasing the drive's cache as well. Overall guidelines like the revised 800-88 are beginning to catch up as the older DoD 5220.22-M is more applicable to HDDs.

Modern drives have multiple techniques available to reduce the chance of data recovery, including internal encryption which makes forensic efforts more difficult even with physical access. The very nature of flash makes it difficult to retrieve charge remnants – the source of data – due to a common block erasure but also the increasing sensitivity of data values within the flash cells. As cells hold more bits in a smaller space the voltage thresholds become narrower, a challenge for performance, endurance, and also data recovery.

Ultimately, it is in an organization's best interest not to rely on any one approach, but rather have a data chain of custody that ensures nothing is leaked. With regards to sanitation, this means engaging in best practices for SSDs – and preferably buying SSDs with advanced cryptographic features. Having a thorough protocol for sanitizing data devices should be a requirement even for less-sensitive data. Basic knowledge of how the devices work and how sanitize functions ensure a proper foundation for intelligent data handling.



Term	Commands
Secure Erase	SECURITY ERASE (UNIT)
Sanitize	SANITIZE, FORMAT (NVM/UNIT)
Block Erase	SANITIZE BLOCK ERASE
Crypto Scramble	SANITIZE CRYPTO SCRAMBLE
Overwrite (HDD), Pattern	SANITIZE OVERWRITE ERASE

*All product and company names may be trademarks or registered trademarks of their respective holders.

Our SSD Solutions

PCIe™ - Our ED1 Series is a powerful, high performance SSD made for edge storage applications. It comes in M.2 and U.2 form factors.

SATA - Our ER2 SSD Series delivers affordability and performance with superior random read/write speeds of up to 90,000/45,000 IOPS. It comes in M.2 and 2.5" form factors.

Please contact our Solid State Storage Technology Corp. expert for more information.

*Specifications and features are subject to change without prior notice. Images are samples only, not actual products.

Request Full Specs Sheets

ABOUT US

A subsidiary of KIOXIA Corporation, **Solid State Storage Technology Corporation** is a global leader in the design, development, and manufacturing of digital storage solutions. We offer a comprehensive lineup of high-performance customizable SSDs for the Enterprise, Industrial, and Business Client markets. With various form factors and interfaces, our SSD solutions help businesses simplify their storage infrastructures accelerating variable workloads, improving efficiency, and reducing total cost of ownership.

Learn more at www.ssstc.com