BRIEF
NOVEMBER 2016

IT@INTEL

Secure Erase for SSDs Helps Sanitize Data and Boost Efficiency

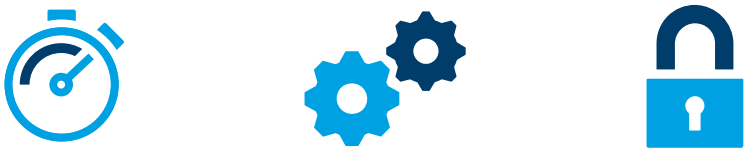
Executive Overview

Protecting data is one of Intel IT's most important duties to the enterprise. And the practice of protecting data includes not only data that is actively being used, but also data that needs to be erased when repurposing or disposing of PCs. Intel IT uses secure erase (see Figure 1) because it is the most effective way to sanitize data on an Intel® Solid State Drive (Intel® SSD). We have validated secure erase through internal testing and third-party testing and have approved its use in place of techniques traditionally used with hard disk drives (HDDs).

Our technicians wipe the data from approximately 20,000 SSDs every year.

Our technicians wipe the data from approximately 20,000 SSDs every year. Secure erase enables technicians to securely wipe a self-encrypting Intel SSD in just seconds. The legacy drive wipe processes involved a three-pass overwrite and could take hours (five or more hours for large drives) and required costly specialized software licenses and equipment. Because the secure erase process is simple and fast, wipe verification and technician training are also simplified. We believe the Intel® SSD Professional Family offers the best approach for storing and protecting corporate data and employees' personally identifiable information and that secure erase is the best method for protecting data when it is no longer needed.

Benefits of Secure Erase



Faster, More Secure Drive Wipes
Purge an SSD in a few seconds compared to more than an hour

Increased Operational Efficiency
Simplified process speeds wipe verification and helps eliminate human error

Better Data Security
Double purge of data using block and crypto erase

Figure 1. Secure erase of self-encrypting Intel® Solid State Drives is faster and more secure than legacy processes.

Robert Fugatt
Employee Computing Platforms
Business Operations Manager
Intel IT

Contents

Contributors

Joseph H. Babineaux, Jr.
Risk and Security Specialist, CISSP
Intel IT

Mark Bryan
Americas Region Client Services Manager
Intel IT

Doug DeVetter
Solutions Architect
Intel NVM Solutions Group

Acronyms

EOL	end-of-life
HDD	hard disk drive
SSD	solid state drive

Background

The data and intellectual property stored on Intel employees' laptops represent some of Intel's most important assets. Therefore Intel enforces well-defined information security policies that govern how data is managed. Historically Intel has adhered to a "no drive leaves Intel" policy. That is, any hard disk drive (HDD) or solid state drive (SSD) used at Intel could not be reused or resold outside Intel. This policy helped protect Intel's data from malicious attempts to extract data from old drives—thereby lessening the likelihood of accidental exposure of intellectual property or personally identifiable information and the associated potential financial loss.

Intel IT's device refresh process is designed to allow Intel employees to use the latest Intel® technologies, which in turn enables increased employee productivity and job satisfaction. We believe that investing in new, improved technologies is imperative to help us keep pace with ever-evolving business demands and remain on the cutting edge. Therefore we refresh employee laptops every two to four years. As part of the refresh process, the old PC is either repurposed internally or transitioned to end-of-life (EOL). In either case, all data on the drive must be removed (a process often referred to as data sanitization).

For repurposed drives, our legacy process involved several manual, time-consuming steps to wipe the drive. It typically took at least two, and sometimes five or more, hours. In addition, the process required software licenses and specialized equipment that cost several thousand dollars for each site. We had to replace the necessary cables often, and because the process involved multiple steps and considerable time, the opportunity for error was a concern. For example, a technician could be interrupted during the process so that the wipe was incomplete. This required us to add verification steps to mitigate possible errors.

We put EOL devices into a barrel and shipped them to our suppliers, who shredded and smelted them down to reclaim metals. Our rigorous disposal process tracked the device from disposal barrel to precious-metal reclamation facility to landfill.

All told, the drive wipe process was costly in time and effort—especially considering that we typically refresh about 20,000 PCs each year.

Our transition from HDDs to Intel® Solid State Drives (Intel® SSDs), and then more recently to self-encrypting Intel SSDs, has enabled a transformation of how we approach data sanitization. We are now using a new technology—secure erase—that allows us to effectively and quickly wipe an SSD—helping boost information security as well as operational efficiency.

Solution

Intel IT now uses secure erase when repurposing Intel SSDs internally. In addition, secure erase is now approved for external disposal or reuse of self-encrypting Intel SSDs, although our thorough reuse of drives, such as repurposing them for lab use, means we have not yet had a need for external disposal of SSDs. To date, we have deployed Intel SSDs to over 100,000 employees and continue to gradually phase out older SSDs and HDDs (for which we still use the legacy drive wipe process) through our refresh cycle. Eventually we anticipate secure erase will afford us the opportunity to donate used SSDs to community schools and other nonprofit organizations.

Secure Erase Meets Intel's Strict Information Security Guidelines

Intel's implementation of secure erase (Figure 2) purges all existing data (called a block erase) and generates a new media-encryption key (called a crypto erase) to help render even retired blocks of memory unreadable. Secure erase works with the entire Intel® SSD Professional Family. Block erase and crypto erase are two recommended purge methods for SSDs according to the National Institute of Standards and Technology* (NIST*) guideline[1] for data sanitization.

NIST rates secure erase on an SSD higher than software overwriting or any "clear" technology. In fact, secure erase is the highest level of security short of physically destroying the drive. In addition to our own internal testing, we contracted with a leading storage device testing company to further validate secure erase effectiveness. This company independently tested multiple Intel SSDs to verify that all usable data was removed from the device and no remnant data was accessible. After rigorous analysis, the company confirmed that our secure erase process accomplished these goals.

[1] csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_with-errata.pdf

Introducing Intel® Remote Secure Erase

Secure erase can be initiated on a SATA-connected solid state drive (SSD) as a secondary drive using the Intel® SSD Toolbox or the Intel® SSD Pro Administrator Tool.

Intel® Remote Secure Erase is another way to initiate secure erase. It can be performed from the IT management console, for the primary drive on local or remote PCs, with or without a functioning OS or management agent, making it easier for IT to manage data sanitization across the enterprise.

Intel IT is not yet using Intel Remote Secure Erase, but our validation of the secure erase drive wipe method has already set the stage for further evaluation.

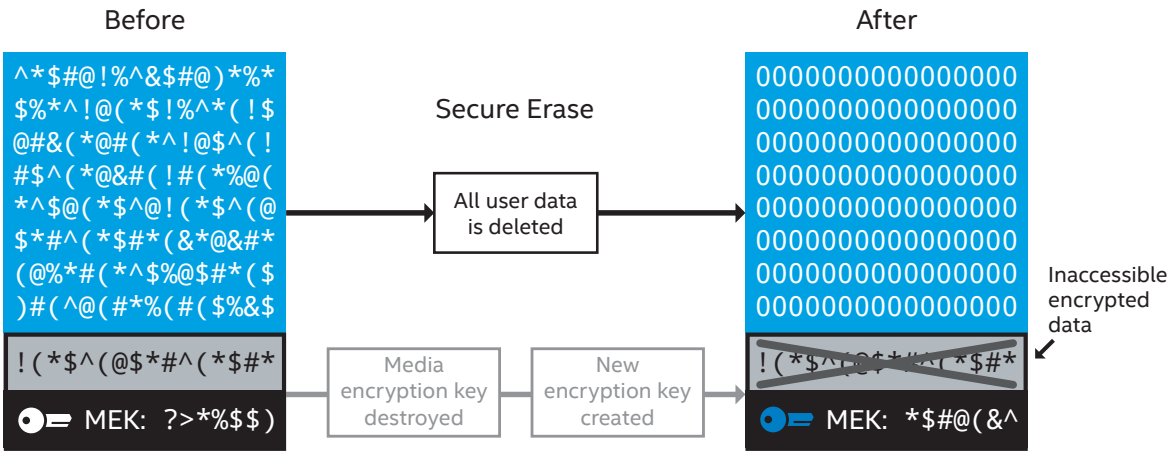


Figure 2. Secure erase is now the method of choice for Intel IT as we refresh and repurpose solid state drives for Intel's entire employee population.

Securely wipe an SSD in just seconds, compared to the legacy drive wipe process which took hours.

Secure Erase Offers Significant Enterprise Benefits

Secure erase has increased Intel IT's operational efficiency while heightening information security. Simply put, drive wipes are faster while possible human error is minimized.

Our technicians can now securely wipe an SSD in just seconds, compared to the legacy drive wipe process which took about two hours on average, and five or more hours for large drives. Using secure erase, we are convinced that no usable data remains on the drive. In addition, because the secure erase process is simple, wipe verification is much easier (and faster). The secure erase script automatically creates a log that tracks the secure erase operation for audit purposes.

These aspects of secure erase—better efficiency and enhanced security—enable the following additional enterprise benefits:

- Decreased operational cost.
- Reduced risk of data loss through simplified processes.
- Better capitalization of PCs as assets through more efficient reuse.
- A significant environmental benefit, because drives that we cannot reuse can be eventually repurposed outside Intel instead of being sent to a landfill.

Secure Erase Is Poised to Benefit the Larger Community

We intend to continue reusing as many SSDs as possible inside Intel; however, we anticipate that secure erase will ultimately result in our being able to repurpose drives outside of Intel as well. Intel is committed to being an active member of the communities in which we are located. Although we are currently reusing all our SSDs internally (thereby maximizing our hardware investment), the external reuse policy is already in place, and we hope that schools and other nonprofit organizations can soon benefit from receipt of SSDs securely wiped by secure erase.

Conclusion

Secure erase is an industry-approved method of securely wiping SSDs, already validated by Intel IT and by third-party testing. Our technicians use secure erase daily. We are confident that secure erase, combined with the Intel SSD Professional Family, is the most secure and efficient way to store and protect Intel's confidential information.

By enhancing both operational efficiency and information security, secure erase has transformed our approach to securely wiping SSDs when reusing devices or transitioning them to EOL. We can now securely wipe an SSD in seconds. Secure erase has even been approved for enabling SSDs to be eventually repurposed outside of Intel, such as donating drives to schools. There are hundreds of thousands of SSDs in use at Intel. Because protecting data is a top concern for Intel IT, and doing so as efficiently as possible just makes good business sense, secure erase is now an important component of our device refresh process.

For more information on Intel IT best practices, visit **intel.com/IT**.

Receive objective and personalized advice from unbiased professionals at **advisors.intel.com**. Fill out a simple form and one of our experienced experts will contact you within five business days.

IT@Intel

We connect IT professionals with their IT peers inside Intel. Our IT department solves some of today's most demanding and complex technology issues, and we want to share these lessons directly with our fellow IT professionals in an open peer-to-peer forum.

Our goal is simple: improve efficiency throughout the organization and enhance the business value of IT investments.

Follow us and join the conversation:

- Twitter
- #IntelIT
- LinkedIn
- IT Center Community

Visit us today at **intel.com/IT** or contact your local Intel representative if you would like to learn more.

Related Content

If you liked this paper, you may also be interested in these related stories:

- Intel® Solid State Drive Professional 1500 Series and Secure Erase paper
- The Full Mobile Deployment Benefits of Intel's Solid State Drives paper

Printed in USA Please Recycle 1116/JGLU/KC/PDF