DataLocker®
Simply Secure

EBOOK

DATA MANAGEMENT BEST PRACTICES: USING CRYPTOGRAPHIC ERASURE

TABLE OF CONTENTS

"DON'T LET YESTERDAY'S DATA DISRUPT YOUR ORGANIZATION'S FUTURE"

There are many ways to lose your data and cause a data breach, but what many don't know is how hard it can be to truly erase data and complete the data lifecycle, from creation to destruction. It can take significant effort to ensure that a storage drive is wiped clean and that the stored data is permanently gone. But fully eradicating data will ensure that it won't come back to haunt your organization in the future. It also means that you can stop some malware and ransomware attacks in their tracks. On the flip side, leaving data on discarded or reassigned storage drives can lead to big consequences.

InfoSecurity Magazine refers to poorly sanitized end-of-life hardware as a ticking time bomb[1]. This was exemplified by Rapid7 researcher Josh Frantz from 80 devices he purchased from a mix of thrift stores and resale shops. Only two devices were wiped properly, and three devices were encrypted.The recovered data included 214,019 images, 3,406 documents and 148,903 email messages[2]. In the wrong hands this recovered data could wreak havoc.

FULLY ERADICATING DATA WILL ENSURE THAT IT WON'T COME BACK TO HAUNT YOUR ORGANIZATION IN THE FUTURE.

Procedures for media sanitization are commonplace but the benefits of cryptographic erasure are sometimes overlooked, it also takes attention to detail to recognize that portable media introduces additional challenges with the portability and shared use. Portable media has shorter and repeated data lifecycles. While you can shred computer equipment as much as you shred paper, we will mainly focus this paper on the difference between software sanitization and cryptographic erasure.

SANITIZATION STANDARDS ABOUND

There are well over 30 different standards for media sanitization worldwide[3], chief among them is NIST 800:88. Securely wiping media is important for compliance standards such as HIPAA, GDPR, SOX, ISO 27000 and PCI. The actual active paragraphs, in terms of wiping, for most of these standards is listed here by the International Data Sanitization Consortium.

The word media is here used as a common term and applies to spinning hard drives (HDD) and solid-state drives (SSD) as well as portable media such as USB flash drives. Portable media is especially important as these devices often move around and proper media sanitization is crucial to avoid malware propagation and data breaches.

Getting rid of old or outdated information is not as simple as highlighting a file and sending it to the trash. Purging unwanted files is more complex than it appears on the surface.

FILE DELETION: BEHIND THE SCENES

Many parallels exist between the digital realm and its real-world counterpart. Take your standard set of documents. When you delete a file on a Windows-based hard drive, the file is sent to the Recycle Bin, where it sits until being emptied and removed from the system. Everything seems to check out as your hard drive properties reveal one less file and the added capacity gained in the removal process. In reality, this is more of a temporary illusion born out of convenience.

When you delete a file or format, you're actually only removing the link that makes it visible on your hard drive, which is stored in the file table. Operating systems are all about efficiency, so even deleting several gigabytes at a time is done fairly quickly. In the meantime, the data still exists, hidden in that pocket of space allocated to your total storage drive capacity, yet doesn't contribute to available free storage. Permanent data removal is a lengthier process equating to the time it takes to write those same files to your hard drive.

A regular USB drive truly hoards all data that you store on it, never removing anything until it absolutely has to. There is no acid-wash used when you push delete on a file or empty the trash can, not even when you quickly format a regular USB drive - all the data is still there. This leaves the standard USB drive with not only traces of what has been stored on it, but in many cases full copies.

WHEN YOU DELETE A FILE OR FORMAT, YOU'RE ACTUALLY ONLY REMOVING THE LINK THAT MAKES IT VISIBLE ON YOUR HARD DRIVE

Unfortunately, an operating system's tendency to prioritize performance can put sensitive data at risk. Those deleted files may not be visible on the surface but are easy to retrieve using free software available online, any motivated person can do it. This vulnerability is especially problematic when industry regulations are involved. Failure to properly dispose of social security numbers, credit card numbers, and other sensitive information could not only expose the owners of that data to fraud and identity theft, it could also result in severe compliance penalties.

The regular USB drive is the definition of a dirty disk, full of yesterday's and last year's files, and there are no systems that keep track of what has been stored on a regular USB drive during its entire lifespan so there is no telling what is really on a regular USB drive. Therefore, if lost or stolen the question is not only: Was there sensitive data on the device? But also: Was there at any point in time, sensitive data on the device?

Now let's venture out into the real world, where you've been tasked with getting rid of old files taking up space in the office. After gathering all the outdated paperwork, you toss the documents in the trash bin beside your desk and go about your day. Of course, anyone can retrieve those documents by simply fishing them out of the trash can.

SOFTWARE MEDIA SANITIZATION OF FLAT MEDIA

If a storage drive lacks the controller required to perform a true cryptographic erase, let's call it flat media, the only way to scrub it clean is to use software that specializes in media sanitization. For flat media you cannot reliably force encryption as the media will allow any data, clear text or cipher text to be stored on it. This means that the full media needs to be sanitized even if only a small part of it has been in use. Relying on native Windows features like a standard format, or deleting and emptying trash bin, would to be frank, setting yourself up for failure. It simply doesn't work and there are plenty of free tools like Recuva® that are available, filling just the purpose of recovering data that was "erased". As mentioned earlier, there are many different sanitization standards to adhere to but the basics of them are are:

- The full media needs to be overwritten.
- Then each byte of the media needs to read back to confirm that the process was successful.

There is of course often much more to software based media sanitization: sometimes 7 write passes are required to meet a certain standard and there are technical differences between flash based and spinning media.

As one can deduce quickly this will be a very time consuming and, if left to a regular user, error prone process. Which user will have the patience to wait for 3-4 hours[4] while the USB flash drive that they "need right now" is being sanitized. The time of the process will come down to the size of the drive and the read and write speeds of that drive. Thankfully for the everyday sanitizations that portable media requires there is a smarter way to go at media sanitization.

Screenshot: DBAN Hard drive erased and data clearing utility

INTRODUCING HARDWARE CRYPTOGRAPHIC ERASE

The gold standard of media sanitization is a correctly performed cryptographic erase performed in the storage controller as it enables powerful media sanitization policies. The main benefits are that it is:

- Fast, only takes milliseconds instead of hours.
- Reliable and guarantees 100% data sanitization each time.
- Enforced at the controller level, removing any chance of user error or judgment calls on when and how to encrypt.

What happens during a cryptographic erase, sometimes also referred to as a zeroize, is that the data encryption key is overwritten and confirmed to be overwritten, and then a new key is issued by the onboard random key generator. In more technical terms, the Data Encryption Key (DEK) for the encrypted Target Data (or the Key Encryption Key – KEK) is sanitized, making recovery of the decrypted Target Data infeasible.

What is left if someone would read back the drive sector by sector is full-strength cipher text, and if industry standards are followed it is regarded as unsalvageable. NIST describes it as:

> *CE [Cryptographic Erase], sanitization may be performed with high assurance much faster than with other sanitization techniques. The encryption itself acts to sanitize the data, subject to constraints identified in this guidelines document. Federal agencies must use FIPS 140 validated encryption modules in order to have assurance.*

CRYPTOGRAPHIC ERASURE BEST PRACTICES AND DATALOCKER

DataLocker K350, DL4 and Sentry ONE are all FIPS 140-2 level 3 certified and allow you to perform cryptographic erase that meets NIST 800:80 without connecting the storage partition to the host computer. The zeroization of the XTS-AES 256-bit encryption keys has been verified by independent NIST-accredited security labs. Using the battery-powered K350 you can zeroize without any additional equipment. This means that an operator can issue a cryptographic erase several times a day and thereby establish a strong parameter defense onto micro-segmented, air gapped, and OT networks.

Crypto erasure is quick and reliable using the DataLocker K350

HARDWARE CRYPTOGRAPHIC ERASE USE CASES

The best cases for using cryptographic erasure include:

- Carrying data onto network segmented or even micro-segmented computers (machines separated from the wired and wireless network), media must be sanitized on each use.
- Firmware upgrades for SCADA networks (including PLCs and RTUs), the target machines lack protection mechanisms so the media must be clean.
- Sanitizing media after storing sensitive or classified data in government to avoid data breaches.
- Reissuing a device between users on a regular basis and avoiding cross contamination of malware or sensitive data.

THE NEED FOR DATA LIFECYCLE SPEED: BEYOND R/W

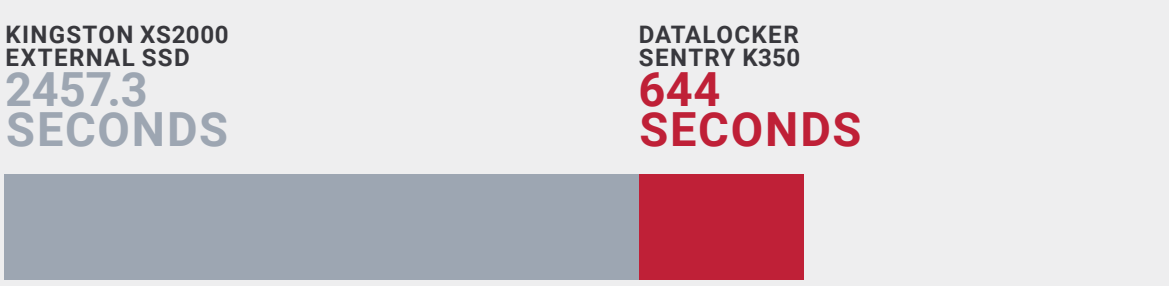
Speed benchmarks are a staple of portable media reviews. The focus is always on read and write speeds. But what happens when you instead compare the full data lifecycle speed of devices, one with FIPS 140-2 level hardware encryption (and crypto erase) and one without, our contestants as benchmarked by StorageReview:

KINGSTON XS2000 EXTERNAL SSD[5] - Arguably the world's fastest regular usb flash drive, in terms of R/W. It benchmarked 1,609MB/s read and 1,691MB/s write.

DATALOCKER SENTRY K350[6] - One of the world's most secure USB flash drives. Measured in at 124.3MB/s write and 235.6MB/s read.

The test case, write 50GB of data, read it back and then sanitize the media. Keep in mind that the XS2000 does not have any security measures in place for the stored data, so keep this a theoretical exercise.

Conclusion, purely looking at speed, in a lifecycle benchmark test the K350 is 400% faster than the world's fastest regular USB drive.



KINGSTON XS2000 EXTERNAL SSD:

Write 50GB, takes 29.6 seconds

Read 50GB, takes 31.1 seconds

Sanitize 1TB with the old DoD fast 3-pass standard[7]:

Takes 3 times 591.7 seconds (1775.1) and 621.5 seconds to verify with no overhead.

Total lifecycle time: 29.6 + 31.1 + 1775.1 + 621.5 = 2457.3 seconds, which is just over 40 minutes.

DATALOCKER SENTRY K350:

Write 50GB, takes 402 seconds

Read 50GB, takes 212 seconds

Crypto erase, enter command and apply, 30 seconds

Total lifecycle time: 402 + 212 + 30 = 644 seconds. Just over 10 minutes.

AUDITABLE CRYPTOGRAPHIC ERASE FOR COMPLIANCE

The SafeConsole central management software allows an administrator to issue a sanitize command which will be applied to the targeted device. A full auditable record will be available on the server once the command has been executed. This takes all the guesswork out of your portable media sanitization. Remember that keeping auditable records is part of most data management standards that impose media sanitization, case in point being HIPAA that states in § 164.306 Security standards: General rules section D: *Information system activity review (Required). Implement procedures to regularly review records of information system activity, such as audit logs, access reports and security incident tracking reports.*

To make sure your organization's data is kept safe, providing the users with secure USB drives is a good start. However, a central management solution will make sure that all risks of losing data are eliminated and provide powerful productivity tools.

With DataLocker Central Management platforms, achieve compliance for USB storage usage with full control, enforcing password policies, remote password resets, and audits protecting your data, your mobile workforce, and organization.

AUDIT

Get proof of compliance with a complete audit trail by user, including connections, login failures, resets, and loss reports.

INVENTORY

Monitor all your encrypted endpoints, including their location anywhere in the world.

CONTROL

Enforce policies such as file-type restrictions, password rules, or geographic boundaries.

MCAFEE ANTI-MALWARE

Protect data with a built-in anti-malware that scans/removes malware detected on the device and receives real-time reporting through central management.

AFFORDABLE

Total cost of ownership is less than a non-encrypted non-managed solution.

1 https://www.infosecurity-magazine.com/blogs/data-breaches-hardware-endoflife/

2 https://www.rapid7.com/blog/post/2019/03/19/buy-one-device-get-data-free-private-information-remains-on-donated-devices/

3 https://www.datasanitization.org/data-sanitization-regulations/

4 https://dban.org/help-center/ "With default options, a typical runtime on a typical disk is three or four hours, but performance varies greatly between drive and controller combinations."

5 https://www.storagereview.com/review/kingston-xs2000-review

6 https://www.storagereview.com/review/datalocker-sentry-k350-review

7 https://www.blancco.com/resources/blog-dod-5220-22-m-wiping-standard-method/
DoD 5220.22-M data sanitization method:
Pass 1: Overwrite all addressable locations with binary zeroes.
Pass 2: Overwrite all addressable locations with binary ones (the compliment of the above).
Pass 3: Overwrite all addressable locations with a random bit pattern
Verify the final overwrite pass.

DATALOCKER
+1 913-310-9088

sales@datalocker.com
To find your local DataLocker Reseller please visit
datalocker.com