The Issue of Data Persistence on Phones and Computers

www.WhiteCanyon.com | Sales@WhiteCanyon.com | 1 (801) 224-8900

OVERVIEW

Devices connected to your corporate network may contain data believed to have been deleted. Exposure of sensitive company data can put your security at risk. It can jeopardize the reputation of your business and risk your violating industry and federal regulations. These are just a few reasons to use hard drive wipe software to address data persistence, or remanence.

Deleting data in Windows/Linux/Apple operating systems doesn't guarantee it is gone forever. Remnants of information may still exist on hard drives in the form of zeros and ones. Leftover hidden files may exist, but wiping tools can overwrite data to ensure information is gone. This is a more effective method in cases of:

- Disk drives that have developed unusable tracks, which are inaccessible via traditional means of deleting data.
- Data stored in the cloud, such as within SaaS, IaaS, or PaaS systems, which unauthorized parties may be able to access.

WHAT IS DATA PERSISTENCE/REMANENCE?

Data remanence is when, even after you've deleted files or reformatted data storage devices, there are still residual bits of information left over. Fragments of information can be pieced together by advanced hacking methods, allowing cybercriminals to potentially retrieve sensitive data. File deletion, reformatting a storage medium, and storage media that allow for previously written information to be recovered do not fully protect your data.

Even if you lose your device or throw it in the trash, data remanence can expose sensitive company information.

WHY CAN'T DATA BE PERMANENTLY ERASED?

The process of erasing data can be complicated by many factors. Data persistence on a computer can be exacerbated by:

- **Inaccessible Storage**: Bad sectors on magnetic disks, reallocated tracks on hard disks, tapes with inter-record gaps, and relocated bad block tables on solid state drives cannot be overwritten in the same way as readily accessible data. Simple methods of overwriting data are often unsuccessful in these cases.

- **Advanced Storage:** As technology has gotten more sophisticated, the presence of data remnants has become more prevalent. A journaling file system writes data in multiple locations to protect data integrity. Data remnants may reside in locations outside typical file storage areas. Some storage media are designed to never overwrite data, particularly those with revision control. Anti-fragmentation features may also write file data to multiple locations, making full deletion next to impossible.
- **Media Type:** Methods such as degaussing only work on magnetic media, not optical media devices. You also can't purge a CD-R or DVD-R; information can be written only once but not erased (CD-RW and DVD-RW media may be overwritten). Flash-based solid-state drives store data and use algorithms that can be exploited, so data can be recovered even after being erased. This makes data remanence a problem.

Data persistence has even been observed with static random-access memory (SRAM) at room temperature, even though information storage is temporary and contingent on there being a power source. Dynamic random-access-memory (DRAM) chips must also have a power supply to retain data. Plus, they require contents to be refreshed to prevent data from fading away. However, this process can take several minutes at room temperature and up to a week if the medium is cooled with liquid nitrogen.

HOW DATA PERSISTENCE CAN HARM YOUR BUSINESS

Many forms of media are used in a modern business environment. Computers and servers may use different storage media, but you must also consider the mobile devices connected to your network and information and applications stored in the cloud. Data persistence on mobile and on company-owned devices can lead to harmful situations such as:

- **Security Breaches:** Data theft, whether by external hackers, internal staff, former employees, or due to the loss or theft of portable devices. Malicious programs can result in the loss or alteration of data, identity theft, and injection of spyware, viruses, trojans, and other damaging elements into your network.
- **Breach of Standards:** Standards such as NIST Special Publication 800-88; Army AR380-19, Information Systems Security; and Air Force AFSSI 8580, Remanence Security provide data security standards related to data persistence. If regulatory compliance requirements enforce the eradication of data, you must understand the required methods of validating the process to regulators or auditors.

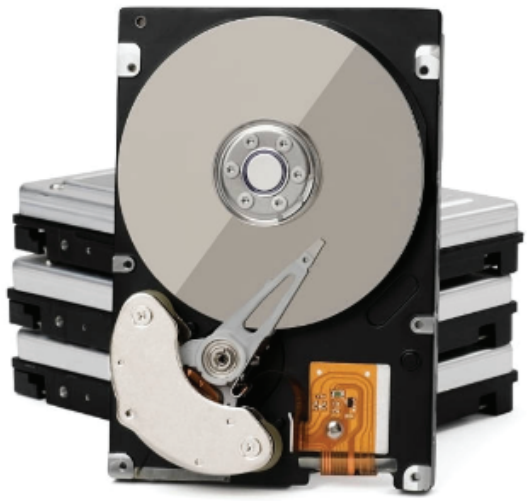
- **Uncertainty of Data:** There is no way to know whether an SaaS service you no longer use has written over your data or if data stored in the cloud can be destroyed in a logical sense. Finding all that data, alone, can be a challenge.

Data persistence can, therefore, lead to downtime, violation of regulations, operational problems, disruption of service to customers and clients, and damage to your company's and brand's reputation.

ELIMINATING REMNANT DATA

For on-premise resources, data destruction takes time and can be costly, depending on the method used. As you've seen here, it is important to eliminate remnant data. Here are some ways this can be achieved:

- **Clearing:** Removing sensitive data so they can't be retrieved using data recovery software or standard system procedures.
- **Purging:** Sanitizing of data before discarding old hard drives and other media, so data can't be reconstructed using known methods.
- **Destruction:** Physical destruction of the storage medium using techniques such as grinding, shredding, or incineration. Optical media may be delaminated or destroyed with electrical arcing or submersion in a polycarbonate solvent. Solid disks may be destroyed through vaporization or liquefaction.
- **Degaussing:** By using a degausser, the magnetic field of a storage medium can be removed or reduced, purging all data and rendering a hard disk inoperable. The disk may be used again if the magnetic pulse is weak, but stronger fields can destroy a hard drive's motor. Such degaussers approved by the U.S. government and military can do this.



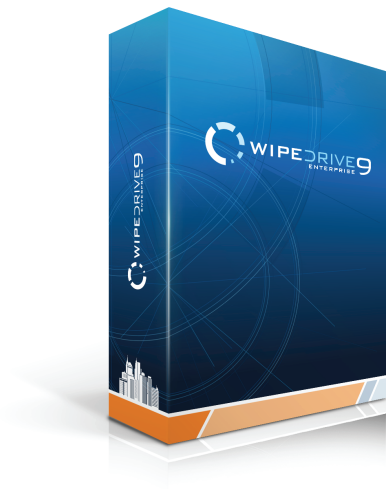
- **Encryption:** Data may be unrecoverable if it is encrypted, especially if the decryption key is overwritten. This is known as crypto-shredding. Whole disk and file-by-file encryption are possible methods. However, advanced methods may be used to acquire data, or someone may obtain a written copy of the decryption key.
- **Overwriting:** Overwriting is an extremely common and highly effective method of dealing with data persistence on computer and mobile storage. It has been conceptualized as a means of shredding, like that done with print media. A hard disk is often still writable after being cleared and not damaged by the overwriting process.

Overwriting Continued: A low-cost option, overwriting can target all or part of the storage medium. Overwriting software may be configured to target specific data or files, or even a storage device's partitions. The techniques vary from writing a pattern of all zeros, which prevents any previous data from being retrieved, to overwrite patterns that may be used over multiple passes. These address the risk of more advanced data recovery techniques.

Some downsides to overwriting include longer processing times for high-capacity drives, inaccessible areas of disks and, as was discovered in the mid-1990s, magnetic force microscopy may be used to recover overwritten data, although various experts have disputed its effectiveness.

PERMANENT ERASURE WITH HARD DRIVE WIPE SOFTWARE

WipeDrive Enterprise, from White Canyon Software, erases devices used by corporations and government entities, so sensitive data are gone, and it allows them to be used like new. The wipe software can be used with Workstations, Servers, iOS and Android devices that can present employers with security holes. Companies can properly erase them before reuse or permanent disposal.



The program doesn't only eliminate data remanence on mobile devices. It also generates audit reports to certify data have been wiped. Users can export these reports to different types of databases.

White Canyon Software provides data destruction software configured for enterprises and small businesses, as well as other software tools to deal with data remanence on computers and mobile devices. Learn more by calling 801-224-2952 and speak to a sales representative. Also, feel free to request a free trial of our hard drive wipe software today.