blancco

Is Data Erasure Really Secure?

When it comes to the safeguarding of sensitive information, organizations can't afford to cut corners. Completely destroying data on data storage devices when they reach end-of-life is essential for any corporate data protection strategy. For many organizations, this means sending drives through a shredder.

While this type of physical destruction is certainly valuable in any IT security policy, it's not always the best option.

Yes, shredding most traditional drives will render the data irrecoverable, but destroying newer technologies, such as SSDs, has been found to leave data on drive fragments, creating the possibility of a data breach while rendering the drive unusable.

Secure, certified data erasure has become a popular choice for organizations wanting to dispose of sensitive data records. Data erasure can add additional security to a physical destruction project. It can also be used as the sole means of removing data from drives, mobile phones, removable media and more.

But is data erasure secure enough to replace physical destruction?

Limitations of Physical Destruction

To explore the security credentials of software-based data erasure, we must first look at the limitations of physical destruction. Physical destruction has been an industry stalwart for the history of IT hardware, particularly for hard disk drives. But it's not the only, and often not the best, option for highly sensitive data stored on newer drive types.

SSDs and other IT assets can be physically destroyed with brute force, but because of the increasingly dense way data is stored, intact chips and the data they contain can remain on shards of shredded hardware. This vulnerability, plus drive replacement expenses, can be costly to business.

It's also costly to the environment. As the "green" movement gains momentum and global technology needs skyrocket, there's concern over the rapid consumption of natural resources for new devices, as well as the vast number of used devices (e-waste) going into landfills.

Given these two physical destruction concerns, organizations are taking a closer look at their bottom line and their role in sustainability while holding to strict standards of secure data protection.

Data erasure provides that security by overwriting data across the entire drive—including HPA/DCO areas and bad sectors—verifying that data is irrecoverable and providing tamper-proof documentation that drives have been thoroughly sanitized. What's more, respected data sanitization standards and industry leaders have validated data erasure as a secure data protection option at end-of-life, used either alone or in conjunction with physical destruction for highly confidential data.

How Does Data Erasure Work?

Software-based data erasure overwrites data on any storage device, replacing the original data with zeros and ones. All sectors of the device are completely overwritten, with the option to perform multiple overwrites where regulations dictate. Once this process is complete, the data on the device is completely unrecoverable by any forensic means, permitting reuse of the device if desired. Data erasure achieves complete data sanitization as defined by the International Data Sanitization Consortium and Gartner.

A range of modern-day standards of data governance compliance now include data erasure as a preferred method of data sanitization. Though standards such as DoD and NIST recommend different numbers of overwrite passes, both validate that software-based overwriting is a secure form of data disposal.

> "[D]ata sanitization is the disciplined process of deliberately, permanently, and irreversibly removing or destroying data stored on a memory device to make it unrecoverable."
> —Gartner

Many companies use software-based data erasure to add an additional layer of security to their IT asset disposition process. When assets reach end-of-life, they can be fully sanitized with data erasure before performing physical destruction, meaning no residual data can be recovered from fragments after the fact. This added security allows organizations to go about their business in the comforting knowledge that they are safeguarded against unauthorized data access when decommissioning assets.

And it's not just IT assets at end-of-life that reap the benefits of software-based data erasure. Businesses can also erase data within active environments—securely and certifiably—with no downtime. Compliance is key in any business that stores personally identifiable information. Many regulations, including GDPR and HIPAA, stipulate that businesses must dispose of data in active environments once it has passed its retention date.

Blancco is the industry leader in secure, software-based data erasure. We offer a suite of erasure solutions to fully sanitize any IT asset in active environments and at end-of-life, creating a tamper-proof audit trail that proves compliance with a range of global regulations, standards and guidelines.

Learn more about how data erasure can benefit your organization in our free white paper, "Enterprise Data Protection: What You Need to Know to Protect Corporate Data Throughout Its Lifecycle."

Then, test data erasure in your enterprise environment with a free Enterprise Trial.