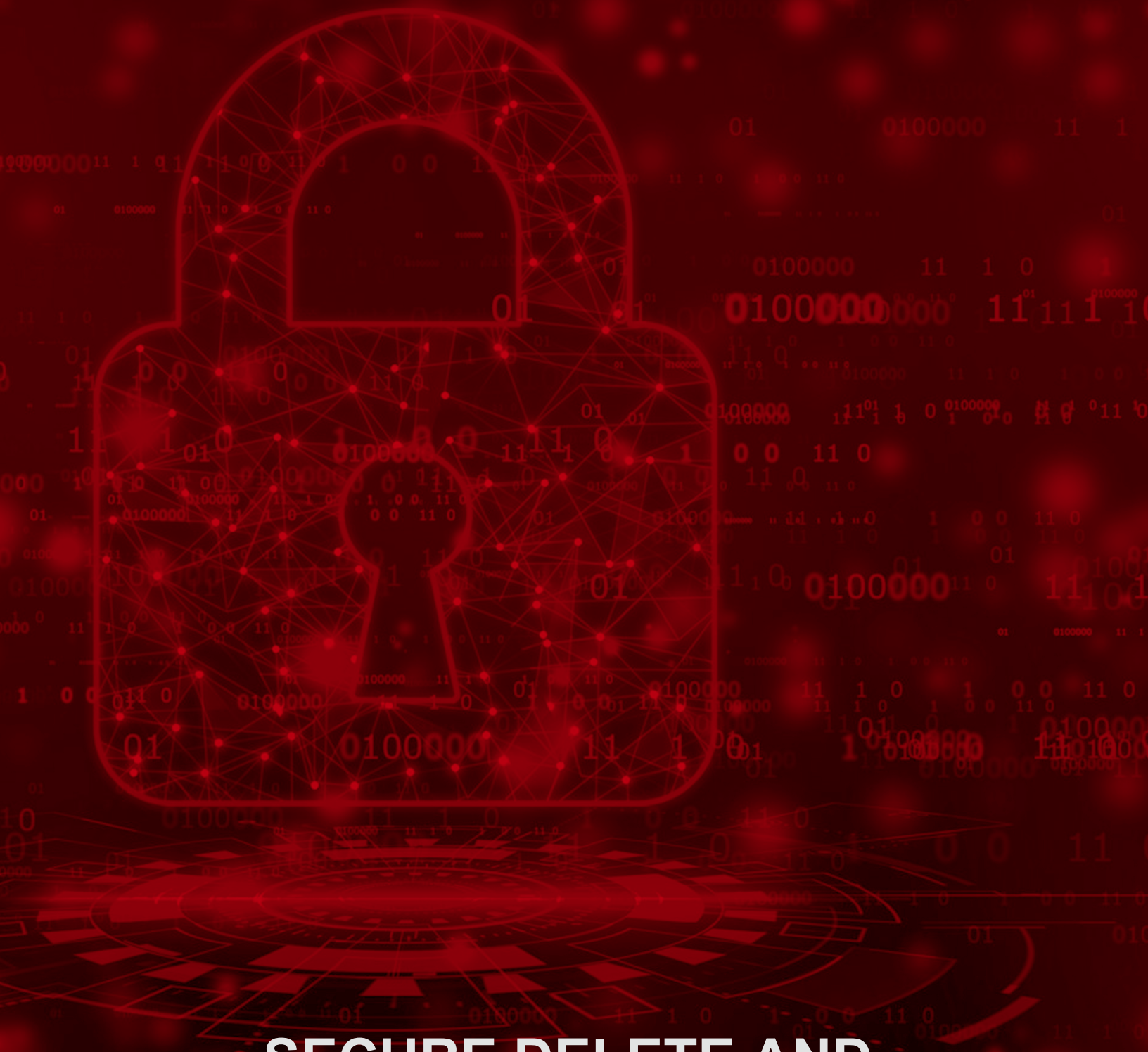
Delete Technology®



SECURE DELETE AND INFORMATION CERTIFICATE

IS THE DATA DELETE REALLY SECURE?

When it comes to safeguarding confidential information, organizations cannot afford to cut shortcuts. Complete destruction of data on data storage devices when it changes at the end of its useful life is essential to any corporate data protection strategy. For many organizations, this means shipping units through a shredder.

While this type of physical destruction is certainly valuable in any IT security policy, it is not always the best option. Yes, shredding most traditional drives will make data unrecoverable, but the destruction of newer technologies such as SSDs has been found to leave data in chunks of drives, creating the possibility of a data breach while the drive it is unusable.

Secure and certified data deletion has become a popular option for organizations that want to get rid of sensitive data records. Deleting data can add additional security to a physical destruction project. It can also be used as the only means of removing data from drives, mobile phones, removable media, and more.

But is erasing the data safe enough to replace physical destruction?

LIMITATIONS OF PHYSICAL DESTRUCTION

To explore the security credentials of software-based data deletion, we must first observe the limitations of physical destruction. Physical destruction has been strong industry support for the history of IT hardware, particularly for hard drives.

But it is not the only option, and often not the best option, for highly confidential data stored in the newest types of drives. SSDs and other IT assets can be physically destroyed using secure data protection.

brute force, but due to the increasingly dense way in which data is stored, the intact chips and the data they contain may remain in pieces of shredded hardware.

This vulnerability, plus unit replacement costs, can be costly for businesses.

It is also expensive for the environment. As the “green” movement gains momentum and global technology needs a rapid increase, there is concern about the rapid consumption of natural resources for new devices, as well as the large number of used devices (electronic waste) going to landfills. Given these two concerns about physical destruction, organizations are taking a closer look at its results and its role in sustainability, while maintaining strict standards.

Data Erase provides that security by overwriting data throughout the drive, including HPA / DCO areas and bad sectors, verifying that the data is unrecoverable, and providing tamper-proof documentation that the drives have been completely disinfected.

Additionally, respected data disinfection standards and industry leaders have validated data erasure as a safe end-of-life data protection option, either alone or in conjunction with the physical destruction of highly confidential data.

HOW DOES THE DATA ERASE WORK?

Software-based data erase overwrites the 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 require. Once this process is complete, the data on the device is completely unrecoverable by any forensic means, allowing the device to be reused if desired.

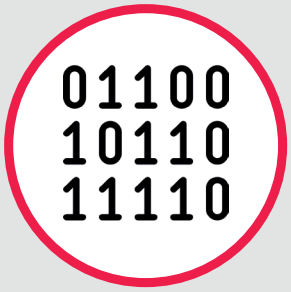
Data deletion achieves complete data disinfection as defined by the International Data Sanitation Consortium and Gartner.

A range of modern data governance compliance standards now includes data erasure as a preferred method of data disinfection. Although standards like DoD and NIST recommend different numbers of overwrite passes, they both validate that software-based overwriting is a safe way to delete data. Many companies use software-based data erasure to add an additional layer of security to their IT asset disposition process.

When the assets reach the end of their useful life, they can be completely disinfected by erasing the data before performing physical destruction, meaning that residual data from the shards cannot be recovered after the fact.

This added security enables organizations to go about their business with the comforting knowledge that they are protected against unauthorized access to data by dismantling assets.

And it's not just end-of-life IT assets that reap the benefits of software-based data deletion. Businesses can also erase data within active environments, securely and certifiably, without downtime. Compliance is key in any business that stores personally identifiable information. Many regulations, including GDPR and HIPAA, stipulate that companies must dispose of data in active environments once their retention date has passed.



Blancco is the industry leader in secure, software-based data erasure.

We offer a suite of erase solutions to completely disinfect any IT asset in active and end-of-life environments, creating a tamper-proof audit trail that demonstrates compliance with a range of global norms, standards, and guidelines.

Learn more about how data deletion can benefit your organization in our free whitepaper.

"Protection of business data: what what you need to know to protect corporate data throughout its life cycle. ”

"Data sanitization is the disciplined process of deliberately, permanently and irreversibly removing or destroying data stored on a memory device to make it unrecoverable."

"Gartner"