Blank is permanent

Inadequate forms of data destruction expose you to security risks and financial costs—learn how to avoid them.

Whether reformatting a drive, deleting files from an active environment, or even dragging files to the Recycle Bin, the information is still there. All these methods simply remove the pointers to the data without actually removing the data itself.

Dispel the myths around data deletion and reduce risk by permanently and completely erasing data from active storage environments.

Enterprises are drowning in data. In 2018, the estimated total globally was 33 zettabytes (ZB). Today, that figure is set to surpass 221 ZB by 2026.

A surprisingly small amount of this data is valuable. The Veritas Global Databerg report suggested that at least 85% of enterprise data is either dark (meaning it is collected but unused for other purposes, such as analytics) or redundant, obsolete, or trivial (ROT). More recently, 60% of respondents to Splunk's survey of over 1,300 IT decision makers confirmed that half or more of their organization's data is dark.

Organizations do not need or productively use lots of the information they store. This hoarding of unnecessary information creates security risks and financial costs. Each surplus file and log is a potential vulnerability, a financial anchor, and an energy drain on the environment.

Disciplined data sanitization solutions that permanently and irreversibly erase data can rectify this. However, many organizations still rely on what they think of as 'deletion.'

Deletion has a specific meaning, but it is also commonly used to describe formatting, wiping, factory resetting, and other options. One thing these processes share is that they may not fully erase files and folders. This failure could result in you not reducing your risk and not benefiting from the financial benefits of complete data erasure.

Blank is permanent because software-based erasure makes data completely and permanently unrecoverable. "Deleting" it may not.

Read on for your guide to the dangers of inadequate data destruction—and how to implement a better solution to your data dilemmas.

Erasing vs. Deleting: Are Your 'Deleted' Files Truly Gone?

With unnecessary data in active environments creating significant vulnerabilities and financial costs, organizations must have a plan of action for safeguarding sensitive, but no longer needed, files and folders.

When information is past any compulsory retention periods that may apply, or it no longer serves a business purpose, the best thing to do is to remove it completely. This reduces your data attack surface and the costs of storage. Getting rid of excess data also can be a requirement of data protection and data privacy regulations.

However, while there are a multitude of data destruction methods, including formatting, deletion, and wiping, many of them contain weaknesses that leave data behind and render data recoverable. This retained data puts organizations at greater breach risk, can incur greater liability in case of a breach, and can lead to financial penalties tied to regulatory noncompliance.

Whether reformatting a drive, deleting files from an active environment, or even dragging files to the Recycle Bin, the information is still there. All these methods simply remove the pointers to the data without actually removing the data itself.

Data Deletion Fails to Meet the Mark

Essentially, data deletion is merely hiding data, not removing it. Employees may be confused into believing that dragging individual files to their laptop or desktop Recycle Bin removes files permanently but that isn't the case.

There are good grounds for this confusion. In Microsoft's latest operating system, Windows 11, sending a file stored in OneDrive to the Recycle Bin prompts the user with the message that "Deleted files are removed everywhere," but this is accompanied by a smaller message that deleted files can be recovered for 93 days.

For locally stored files on a C: drive, deleted files go automatically to the Recycle Bin, and deletion notifications must be turned on manually. After this, Windows prompts the user with the following question: "Are you sure you want to move this file to the Recycle Bin?"

It's only when emptying the Recycle Bin that users now prompted with the question, "Are you sure you want to permanently delete this file?"

Given this assortment of information, employees may not understand exactly what the status of their data is. But at least this final question when emptying the Recycle Bin will permanently delete the file, right? Wrong.

This type of basic deletion only removes pointers to the data, not the data itself. It's the digital equivalent of removing a book's index without removing the pages.

The deletion described here is just one of the faulty data removal methods that are typically mentioned when people discuss deleting data. The following section sets out why formatting also creates similar risks.

Formatting Hard Drives Could Leave Your Enterprise Exposed to Data Breaches

Our Privacy for Sale research study, conducted in conjunction with Ontrack, outlines how Blancco IT staff in the U.S., Germany, Finland, and the U.K. purchased 159 SSDs and HDDs from a large online marketplace. These drives were analyzed by our partners at Ontrack using proprietary data recovery tools to see if any sensitive data remained.

We found that more than 40% of the second-hand hard drives contained data leftover from the previous user.

The leftover data included an array of office and employee emails, photos, and files, creating a risk of personal, financial, and reputational damage to individuals and their employers.

In addition, more than 15% of those drives contained sensitive information that could be dangerous in the hands of identity thieves or hackers.

"Out of the 159 drives analyzed, some type of data was found on 66 of them, with 25 of the drives containing PII such as photos, birth certificates, names, email addresses, and more."

Privacy for Sale: Data Security Risks in the Second-hand IT Asset Marketplace

Every seller we purchased drives from insisted that proper data sanitization methods had been performed. This demonstrates that sellers are attempting to permanently wipe data (and see the importance of this process). However, many are failing to use a fully effective solution.

For most devices analyzed, formatting was the data disposal method of choice. However, as the results show, this method is not always enough for complete and permanent data removal.

If these drives had come from a single organization (or from several) and ended up in the hands of bad actors, the result could have been a major data breach.

How could an organization have prevented this? In addition to the complete end-of-life erasure of assets such as drives and laptops, data sanitization should be continually applied to the active environments of data centers, cloud storage, and employee endpoints still active within the asset lifecycle.

Ongoing, active erasure ensures you're always up to date, reducing security threats to your data center and overall organization.

By overlapping data lifecycle management with the asset management lifecycle, enterprises can make IT equipment more secure in the case of loss or theft, for example. Proactively erasing data from active environments can be automated based on organizational policies.

Automated erasure policy specifications could include:

- Erasing files and folders older than a certain date
- Erasing files and folders older than a certain number of days
- Erasing files by file type (all .docx or .pdf files, for instance), potentially with date/day parameters
- Erasing temporary files
- Erasing the Recycle Bin
- Erasing free disk space
- Erasing slack space

The Enterprise Side of Erasing vs. Deleting Files & Folders

What happens to data when businesses unknowingly use inadequate data destruction methods to reduce surplus data?

They're not only left with a false sense of security, but massive amounts of data (like emails, confidential documents, and other sensitive information) that are at risk of being exposed and falling into the wrong hands.

Excess Data Storage Means Excess Data Breach & Regulatory Risk

In 2023, cyber-attacks and data breaches exposed more than eight billion data records according to IT Governance. Between January and June 2024, that figure reached over 35 billion. Cybersecurity incidents are rising fast.

Alongside breach risk, tougher data protection rules, such as Europe's General Data Protection Regulation (GDPR), the California Privacy Rights Act (CPRA), and the New Jersey Privacy Act (NJPA), mean that businesses can't afford to be lax with information management.

These regulations "are driving to the same storage limitation principle, which supports that organizations need to delete personal data when it's no longer necessary ." Again, in this context "delete" could mean a range of data destruction methods, not all of them equally effective.

Excess Data Storage Costs More

In addition, data storage costs and storage limitations are significant challenges for organizations.

Many don't realize how many "deleted" files are left behind on their single computer from inadequate data destruction alone. Run a simple recovery program on your PC and prepare to be shocked by the results—the choice between erasing vs. deleting becomes quite clear.

How to Ensure Your Enterprise Files Are Unrecoverable

How can businesses make it impossible for "deleted" files to be recovered? The answer is simple: securely erase files from active PCs, servers, LUNs, and even virtual machines.

Secure data erasure uses methods to overwrite files and folders according to an industry standard, then verifies that the erasure has taken place successfully.

In addition, for compliance purposes, verified data sanitization should be accompanied by a certificate of erasure noting exactly what was erased, when, by whom, and using what method.

This provides proof to auditors and industry regulators that you are abiding by specified retention and data protection best practices and requirements.

Data in active environments can also be erased automatically according to data management policies you set.

Mitigate Data Breach Risk with Permanent Data Destruction Methods

When choosing how to dispose of data, deleting files or formatting drives may seem easy and fast, but they come with a degree of risk.

Blank is permanent because software-based data erasure gets rid of data for good, ensuring it's impossible to recover files and that data cannot be leaked.

Take your data lifecycle management beyond temporary fixes; reduce the risk of data breaches with a permanent solution.