

Trading Data ROT for Increased Security, Compliance & Efficiency

Left unchecked, excess business data breeds needless storage costs, compliance concerns, and data security risks. Here's how to shed that load permanently and confidently—and increase business efficiency.

Unseen Data & Hidden Liability

The average enterprise stores 10 petabytes—or 10 million gigabytes—of data. Yet [landmark analysis from Veritas](#) shows that more than a third of it consists of stored-but-ignored files known as *ROT* data—and it costs businesses dearly in lost productivity, excess storage, compliance gaps, and heightened breach risk.

What is ROT?

ROT data can exist throughout your infrastructure: within desktops, mobile devices, data centers, and cloud servers. It includes:

- ① **Redundant**, or duplicate, files, including email attachments, intranet content, and excess backup data
- ① **Obsolete** files such as out-of-date documents or expired server session cookies
- ① **Trivial** data that has no business value, including large media files or personal employee files

Far from harmless, this glut of data slows operations while inflating cost and risk.

How ROT Hurts Business

- ① **Increased storage costs**—The annual cost of storing, securing, and administrating needless ROT files can cost tens of thousands of dollars per enterprise. Complex or distributed IT environments cost more.
- ① **Heightened risk of regulatory non-compliance**—Incorrect classification, data stored past its retention period, and inadequate security create fertile ground for non-compliance, particularly for sensitive data like financial, health, or personally identifiable information (PII).
- ① **Hidden data and risk**—Large sets of unstructured data obscure what data exists, where it's located, and who has access to it. Security and risk assessments on such data also take longer.
- ① **Increased data security risks**—Breach vulnerability increases as ROT files remain untouched and access permissions and file security policies become outdated.
- ① **Inefficient data discovery**—ROT complicates identifying, classifying, and analyzing information. This slows standard business operations, including responses to subject access and legal requests that can carry hefty financial penalties.
- ① **Opportunity costs**—The more data there is, the more resources it takes to deal with it. This cycle of inefficiency hinders agility and innovation by needlessly taking up staff time.

How to Rid Your Enterprise of ROT Data

So how do you get rid of ROT data, lower data breach risk, and cut costs from excess data storage? The following steps will help eradicate current excess data—and prevent future growth:

- ✔ **Initiate ROT data discovery**—Use a file analysis solution to locate non-business files, files that have been untouched for extended periods, duplicate copies, and other junk files.
- ✔ **Deduplicate your data**—Many data deduplication solutions scan for and replace duplicate data with a pointer to the main copy, creating a “single source of truth.”
- ✔ **Classify your data**—There are a host of solutions that can help here: Dedicated data discovery and classification solutions can identify files containing sensitive data like PII, protected health information (PHI), and payment card information (PCI). They also help categorize data as restricted, confidential, internal, or public. “Last accessed” timestamps indicate how relevant data is to the business. Real-time auditing solutions address ROT data associated with inactive user accounts. More comprehensive data security platforms discover, classify, tag, and score critical data, enabling faster decision making and data removal.
- ✔ **Remove post-retention data**—All data should be assigned a retention period. Once the retention period ends, expired data should be sanitized so it’s not a business liability. An electronic document management system (EDMS), used by lawyers, healthcare professionals, and others who must swiftly and reliably dispose of sensitive data, can automate finding data past its retention date.
- ✔ **Set up workflows to automatically archive and permanently erase files**—Policy-based data archiving and deletion within active environments frees up disk space, improves storage performance, and lowers costs. Needed data can be automatically archived on low-cost cloud or tape storage solutions, while the rest can be securely and permanently erased.
- ✔ **Repeat periodically**—Whichever solutions you choose to manage your redundant, obsolete, or trivial data, the process should be ongoing, formalized, and scheduled.

The Bottom Line

- ✔ Proper data discovery, classification, and erasure keeps you from paying to store unneeded, risk-heavy data.
- ✔ Blancco’s software-based data sanitization solutions, including Blancco File Eraser, Blancco LUN Eraser, and Blancco Virtual Machine Eraser, erase data throughout your enterprise IT infrastructure without any downtime.
- ✔ By harnessing Blancco solutions at data end-of-life, you can safely and permanently destroy data that’s no longer necessary for business or compliance purposes, recoup costs, lower your data risk, and redirect staff from managing unneeded data to moving your business forward.

Contact Blancco or your Blancco provider today to get started.

