Blank is mission critical

Sanitize end-of-life data and assets consistently for the ultimate in data protection and security. Reduce risk and drive greater business value with a comprehensive plan to erase data, wherever it lives.

"The most devastating security failures often are the ones that we can't imagine — until they happen."

Maurice Uenuma
Stress-Testing Our Security Assumptions in a World of New & Novel Risks

Why It's Time for Data-centric Enterprises to Clean House

Many security and commercial failures share a root cause: they stem from false assumptions about the world. When the paradigm changes, those assumptions unravel.

For security professionals, the SolarWinds breach shattered the belief that verified updates were inherently secure. Commercially, Blockbuster's failure to recognize the potential of digital streaming led to bankruptcy.

It can be disastrous when basic assumptions go unexamined.

Rethinking data sanitization assumptions

"Data sanitization is a risk mitigation exercise rather than a serious security threat or an opportunity to create business value."

It's time to throw out the false assumption that data at the end of its life — whether it's on assets or in live environments — is neither a major risk nor an opportunity for creating value.

As our ongoing support for over 2,500 leading organizations worldwide shows, secure erasure is more than a check-box exercise in compliance. It is a strategic opportunity to develop robust systems that build trust, security, and value.

With data protection mandates, security challenges, technologies, and sustainability reporting all evolving, all organizations need strategies and solutions that evolve at the same pace — protecting data and providing new opportunities for growth and greater efficiency.

The solution is simple: if data is not needed for business or compliance purposes, eradicate it, wherever it's stored. Return end-of-life devices and unnecessarily occupied areas of live storage environments to a data-free state of "blank."

Blank is mission critical because it permanently and completely erases data so you can reduce risk, increase compliance, operate more efficiently, and hit sustainability goals.

The following pages are your guide to developing a scalable data sanitization strategy.

Common issues blocking secure end-of-life IT asset disposal

False assumptions about the need for data sanitization aside, there are a few additional reasons why your end-of-life data may not already be getting the treatment it critically needs.

- **A lack of consistent classification and sanitization.** Data classification involves sorting data by pre-defined characteristics (e.g., compliance, risk, privacy, and security) to organize and secure it efficiently. This makes it easier to sanitize the right data at the right time. But a lack of consistency in both classification and sanitization means redundant, obsolete, or trivial (ROT) data gets hoarded across the cloud, on-premises data centers, and individual assets. In fact, organizations often lack a complete picture of where their ROT data even is. The data "sphere" proposed by the International Data Corporation (IDC) is more of a data "splotch."

What is data sanitization anyway?

Data sanitization is the consistently applied, disciplined process of reliably and completely removing all data from a read/write medium so that it can no longer be read or recovered.

Sanitizing data to the highest level also involves erasing to a recognized standard, such as NIST SP 800-88 R1 or IEEE 2883-2022, automating the verification that erasure has taken place, and producing an audit-ready, tamper-resistant proof used for reporting and record-keeping.

- Even if you know which data or assets need sanitizing, you may not have **targeted solutions** for every job. For example, using an IT asset disposition (ITAD) vendor to dispose of end-of-life employee laptops can be effective, but it's less common for ITADs to erase LUNs on servers. For that, you could use a more efficient solution to target data in active environments.

- **Finally, many data destruction methods for end-of-life asset management are problematic.** Formatting, for example, may not completely erase confidential data and is unlikely to offer verification of erasure. Physical shredding or pulverizing may also fail to eradicate data beyond recovery or leave data-laden devices vulnerable during storage or transport. Plus, while post-destruction recycling can recover some useful elements, in many cases physical destruction consigns potentially useful equipment to become e-waste. Even when devices are successfully recycled, usable devices are still being destroyed, fueling the demand for yet more resource-intensive device manufacturing.

What's the most effective way to destroy data?

Software-based data erasure overwrites digitally stored information with random binary data according to a specified standard. It then verifies and certifies the erasure has been successful.

Secure data erasure can occur in both active and inactive environments across a variety of IT assets, as well as in data centers, and cloud environments.

What's needed is a holistic approach to end-of-life data management that eradicates data completely and permanently, wherever it lives.

Sanitization starts with identification

In live environments
As much as 85% of stored business data is 'dark' or ROT data.

On IT assets
One-third of enterprises use faulty IT asset sanitization methods.

If the data isn't there, it can't:

- be spilled, leaked, or breached.
- compromise data protection and privacy laws.
- run up storage costs.
- undermine your sustainability efforts.

Follow us as we set out how bad data sanitization assumptions are putting your organization at risk, and the benefits you'll receive from taking a consolidated approach.

Sanitize for data security

The data in your end-of-life assets and live environments present different security risks. But storing unnecessary data in both increases your attack surface.

In combination with other cybersecurity solutions, erasure should be the last line of defense guarding your data. Then, if hackers do gain access to corporate environments, or intercept erased devices, they either find less data or none at all.

Securing IT assets

Selling or redeploying end-of-life equipment can be a budget-conscious and sustainable choice. Yet many data destruction methods leave information behind. It's this perceived lack of security that leads some organizations to choose physical destruction.

When it comes to formatting or basic deletion, this is understandable. A Blancco research study found that over 15% of used drives still contained recoverable information after formatting.

But physical destruction is also not the secure solution many believe. The American National Security Agency (NSA) advocates shredding devices into 2mm pieces, which is about the thickness of a small coin. Yet, as data density increases, huge amounts of data can still be present on tiny fragments.

If physical destruction is unavoidable, software-based data sanitization should be used as an additional control prior to shredding. Completely erasing data onsite — prior to transporting assets for physical destruction — reduces the potential for data breaches by eliminating data before hardware is sent to other locations and handled by people outside your organization.

Securing live environments

Hoarding unnecessary information in data centers and live employee devices creates risk. The only way for data to be 100% completely secure is if it's no longer there.

That's not possible or desirable for all information, but it is essential for the 33% of data estimated to be redundant, obsolete, or trivial. Erasing unneeded files and folders, LUNs, virtual machines, and more, is key.

"The bank has reduced risk by improving its security posture and protections for personally identifiable information (PII) and other sensitive data. Standardized secure erasure methods apply data erasure best practices with highly repeatable, less manual processes that scale globally."

Case Study:
Financial Services Firm Unifies & Transforms Data Hygiene Practices with Secure Erasure

How to improve end-of-life data security

- Use hardware and software solutions to remotely or physically return end-of-life drives, laptops, and more, to a state of "blank" — where all data is sanitized beyond recovery.
- Go beyond the OS-level limitations of formatting, deletion, and non-verified wiping. Be sure that hidden areas, including host protected areas(HPA), device configuration overlays (DCO),and remapped sectors are blank.
- Secure and shorten your chain of custody by prioritizing data erasure at the point of decommissioning. Ensure any assets leaving your organization are comprehensively erased and documented beforehand.
- Use scripting and scheduling to automate the secure erasure of files, folders, and LUNs on active devices, servers, virtual machines, active storage, and hypervisor environments.
- Limit the hoarding of future ROT data by establishing sanitization rules. Centrally erase data without disrupting business operations.

Working with an ITAD vendor is one solution to processing decommissioned assets. Partner with an ITAD offering secure data erasure and a clear, secure, well-documented, and auditable trail for device disposal.

Experience secure data erasure first-hand.

Sign up for your free trial with Blancco.

Align data protection compliance to avoid penalties

While the European Union's General Data Protection Regulation (GDPR) may be the most high-profile data protection law, 80% of countries worldwide now have published or draft laws.

This evolving forest of legal requirements has changed the data landscape. Whether you're complying with data subject erasure requests or imposing retention limits, you need a strategic approach.

Compliant end-of-life IT asset disposal

Can common disposal methods compliantly process the IT equipment you decommission each year?

In many cases, no. Formatting and some forms of data wiping typically lack verification and certification, which results in no auditable proof of erasure. If you're asked to show how and when you comply with data erasure mandates, or if breach liability fines are tied to properly implemented data destruction practices, you need audit-worthy proof. Without it, you risk significant financial penalties.

Physical destruction can also lead to non-compliance, because in-person handling creates the risk of errors or insecure processing. Even if physical destruction is the final destination for end-of-life devices, erasure should happen at the point of decommissioning, before they are disconnected. This prevents data-laden drives from being lost or stolen along the disposition journey, such as when they are being stored, transported, or awaiting final destruction. For security and audit purposes, the processor should provide evidence of all erasures.

A compliant storage environment

Whether it's valuable or ROT, all information heightens data protection responsibilities.

Being able to verifiably sanitize your unstructured data in a granular way drives greater efficiency when complying with data subject requests for deletion. Proactive sanitization also reduces your attack surface by limiting the amount of data vulnerable to unauthorized access or accidental exposure.

How to improve data compliance

- Establish a detailed audit trail of assets and active storage erasures to help prove compliance with regulations such as GDPR.
- Develop a plan to address what happens when data reaches the end of its legal retention period. Automate data erasure processes to ensure nothing slips through the net.
- Use secure erasure to promptly destroy files, folders, and LUNs containing information on data subjects. Confirm compliance without having to destroy whole drives.
- To prevent regulated data spilling over to unauthorized users, thoroughly erase assets from more sensitive departments (e.g., human resources) before redeploying them to external users or less-protected areas (e.g., marketing) of your organization.
- Make sure you use solutions capable of eliminating data in line with new erasure standards such as IEEE 2883-2022 and the older but still important NIST 800-88. This will ensure continued compliance as drives evolve.

Compliance can be profitable.

Visit the Blancco Drive Eraser Value Assessment Tool to discover how!

"I'm a data protection officer and I make sure that the personal data of our clients are secure. Blancco simply closes the loop of the data lifecycle. That's why I really feel the need to include Blancco in our processes and governance."

DPO, large commercial bank

Streamline end-of-life data management

In large organizations, the management of both the data and IT asset lifecycles can be time-consuming and inefficient.

Get more value from your investments with a holistic approach.

End-of-life inefficiency

A continual cycle of purchasing and destroying massive numbers of laptops, mobiles, and other assets is costly and ineffective. The same goes for stockpiling used devices and allowing them to languish without maximizing their lifespans.

Nonetheless, **87% of global enterprises** admit not sanitizing assets as soon as they reach end-of-life, while 31% report taking more than a month to process devices. This extra time causes a greater loss of value and makes eventual reuse or resale less profitable.

Instead of procuring a continual stream of replacement assets, it may be possible to sanitize and redeploy existing equipment to less resource-intensive tasks.

Managing ROT data is costing you

The financial inefficiency of unnecessarily storing data is staggering.

Research from Veritas suggests that the average enterprise stores **10 petabytes (PB)** of data. If we accept that one-third of data is ROT, you could be holding on to (and paying to keep) around 7 billion pointless files.

While estimates vary, **research from 2023** suggested that enterprises should budget roughly $1 million to store 1PB of data for five years, either on-prem or in the cloud. Over the course of just one year then, enterprises storing 10PBs of data could be wasting over $600,000 on ROT data.

A major multinational technology company used Blancco's data center solution to erase **4,000 servers simultaneously overnight.** Blancco helped the company achieve its number one goal: NIST 800-88 compliance, with a tamper-proof Certificate of Erasure for every server.

How to streamline end-of-life erasure

- Maximize asset lifecycles and reduce purchasing by securely erasing devices at scale. Choose instead to refurbish, resell, or redeploy used hardware that has not yet reached the end of its useful life.
- Incorporate data erasure software seamlessly into IT asset management (ITAM) platforms like ServiceNow. Enable remote initiation of data erasure processes within the asset management system. For instance, make employee exits smoother by ensuring secure data erasure, device re-imaging, and direct handover to the next user—no need for devices to travel back and forth to a central office.
- Automate erasure schedules to streamline assets and active environments. This can range from periodically removing data from every laptop's Recycle Bin to automating erasure based on retention periods or inactivity.
- Use erasure hardware and software to decommission hundreds or even thousands of drives or servers simultaneously, preserving the uptime of your data operations.

Start your efficiency drive today.

Request your free trial. →

Boost sustainability

Data sanitization can help to reduce your greenhouse gas emissions and e-waste.

It's important to consider both data and devices here because the impacts of device churn and ROT data are so serious for the planet.

Asset destruction damages the environment

In cases where physical destruction is unavoidable, recycling can recover salvageable materials for reuse. Importantly, however, shredding, incinerating, or pulverizing equipment is often unnecessary and does not always result in effective recycling.

Less than a quarter (22.3%) of global e-waste is collected and recycled in line with international standards. The rest, much of which could have been sanitized and reused, falls into unregulated disposal and landfills.

When this happens, physical destruction increases greenhouse gas emissions, e-waste, and harmful chemicals in the air and groundwater.

ROT data raises emissions

The more data your organization stores, the more on-premises and cloud space it needs to house it. Both the storage and transmission of data generate a phenomenal amount of energy and emissions.

> "The Cloud now has a greater carbon footprint than the airline industry. A single data center can consume the equivalent electricity of 50,000 homes."
>
> **Steven Gonzalez Monserrate,**
> **The Staggering Ecological Impacts of Computation and the Cloud,**
> **The MIT Press Reader**

Regularly sanitizing ROT data from active storage environments means you can reduce costs, energy, and emissions.

> "[W]ith Blancco, you can properly wipe the devices and have a certificate of successful wiping. Now, for example, an R&D server can get reused in a production environment."
>
> **General account manager, IT services company**

How to reduce emissions with data sanitization

- The sustainable way to reduce asset-related emissions is to securely erase devices with certified software. This means they can then be refurbished for a second life (or more). They can be redeployed within your business or sold downstream rather than becoming landfill.
- Consider moving the sanitization process to your internal teams to limit the physical transportation of goods.
- Cut energy and emissions costs by regularly minimizing data.
- Reduce the emissions required for the manufacture of new hardware by securely reusing and redeploying existing tech.

Good for the environment is good for your bottom line too.

Discover how Blancco Drive Eraser saves you money by reducing physical destruction spending.

Blank brings it all together

Every organization has trigger events where end-of-life data and devices must be managed one way or another.

Projects as varied as employee offboarding, cloud migrations, and the end of leasing arrangements with equipment manufacturers, all raise questions about what you should do with your data.

Without a holistic strategy, these moments can become security vulnerabilities, compliance errors, efficiency drains, and sustainability roadblocks.

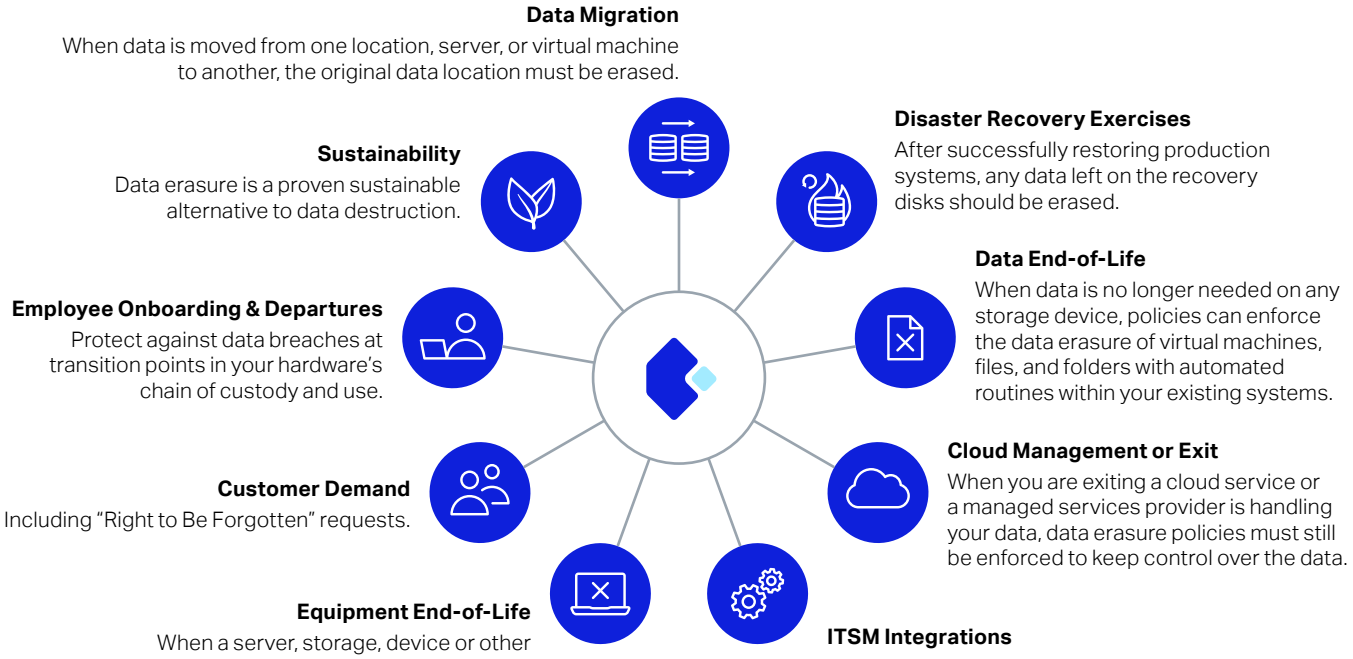
With a strategy, they can be opportunities to thrive.

Effective data sanitization intervenes at any point to return relevant devices and data to a state of blank, without damaging your organization. It's this wide-ranging approach that more and more enterprises are choosing in order to meet the demands of a rapidly growing data landscape.

To achieve more, make sure you have access to tools that can turn every end-of-life data decision to your advantage.

See how data sanitization can fit your organization.

Request your free Blancco trial.



The only data erasure company with end-to-end automation for sanitization, diagnostics, and reporting

Blancco Hardware Solutions
Secure, on-premise erasure of loose drives and drive enclosures within data centers or large IT facilities

Blancco Removable Media Eraser
Secure data erasure of removable flash media devices stored within smartphones, tablets, network routers and cameras

Blancco Mobile
Diagnostics and secure data erasure of smartphones and tablets

Blancco Drive Verifier
Secure drive erasure verification for PCs, laptops, and loose drives

Blancco Management Portal
Centralized data erasure reporting and management across your entire IT asset portfolio–on-premise or in the cloud

Blancco Driver Eraser
High speed, efficient secure data erasure of complex SSD and NVMe drives, including self-encrypting drives

Blancco Virtual Machine Eraser
Secure data erasure of complicated server and storage environments

Blancco File Eraser
Secure data erasure of files and folders on active PCs, laptops and servers

Blancco LUN Eraser
Secure data erasure of LUNs in an active storage environment, connected to both physical and virtual machines

Contact Us

For Corporate Marketing, please contact us at marketing@blancco.com