

**Blank is  
best**

# Why drive and device destruction is flawed

**Examining the sustainability, efficiency, compliance, and security considerations business and IT leaders must act on.**

This guide evaluates the industry's most prevalent data sanitization approach, including its benefits and pitfalls, and considers the next generation: software-based data erasure.

# Blank is NextGen

**Here we are, living in an era where data feels as highly prized as gold bullion.**

**It empowers innovation, generates value, and differentiates the customer experience.**

**Seemingly, the more data we have, the more we can achieve.**

Yet on the flip side sits a harsh reality. Many organizations are actually drowning in data and will continue to do so, making it increasingly difficult to manage, filter for use and value, and retain appropriately for compliance.

IDC's Global DataSphere forecasts the amount of data that will be created on an annual basis. It predicts that over the next five years, data will grow at a compound annual growth rate (CAGR) of 21.2% to reach more than 221,000 exabytes (an exabyte is 1,000 petabytes) by 2026.

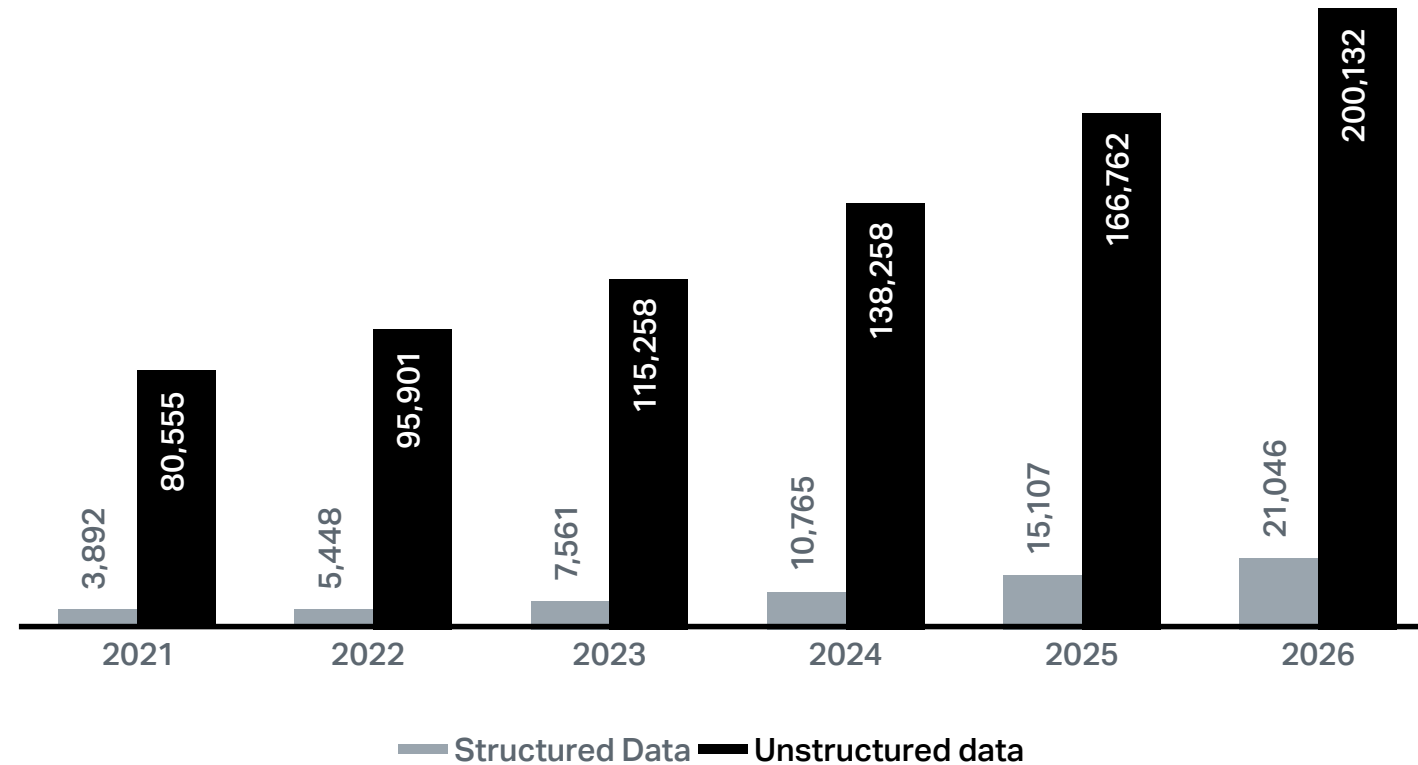


Figure 1: Worldwide Global DataSphere Data Forecast, 2021-2026 (Exabytes)<sup>1</sup>



As a rather startling example of the situation, the Veritas 2020 UK Databerg report found that 53% of data in organizations is dark—that is, with an undetermined business value. A further 28% of that data is redundant, outdated, or trivial (ROT).<sup>2</sup>

Also, where we use, store, and process data is always evolving. Changes in working practices, IT platforms, regulations, and the miniaturization of devices add to data management complexity.

For these reasons, as IT, compliance, and security professionals, or as those responsible for these functions, we must carefully consider how we deal with data, especially at the point we need to permanently get rid of it.

Are our data management policies fit for the times we live in?

Are our sanitization practices optimal from the perspectives of business efficiency, data security, regulatory compliance, and risk?

There's also overlap for the pressing question of environmental responsibility: Are today's data destruction methods sustainable from generation to generation, especially considering our current rate of data dependency and growth?

## What will you learn in 20 minutes?

- The largely unknown security shortfalls of the prevalent data sanitization method
- Impacts of physical destruction on your ESG (environmental, social, and governance) goals and global ecosystems
- The alternatives to current methods that provide more efficient business and improved compliance outcomes
- How some organizations are taking an active role in protecting data, their firms' reputations, and the environment



# Blank is **trusted**

**The default for many organizations when seeking to eliminate data for good is to destroy the devices upon which it lives: physical destruction.**

## **When is physical destruction ok?**

Indeed, there are certain circumstances where this approach is necessary: primarily, when the drive is so damaged that an erasure cannot be completed.

Yet often, physical destruction isn't limited to non-functional assets. Certain sectors, such as government, will mandate or produce firm guidance on preferred methods of data elimination. In many cases, they advocate for shredding, degaussing, or other forms of destruction that render devices unusable.

Physically destroying drives and devices can also "feel" like the most positive and hard-hitting action to take—it has visceral appeal, and it seems unfathomable that data could live on—though it can.

## **Avoidance isn't an option**

Keeping the device—and the data that exists on it—creates security breach vulnerabilities, causing business liability, compliance fails, and eye-watering fines. Avoidance of dealing with data is not, therefore, an option.

## **How shredded is safe?**

Whether or not your organization is happy with the data perpetuation risk that comes with shredding, degaussing, or other forms of IT asset destruction, another security problem arises through the process itself.

## **Chain of custody woes**

Whether implemented at your premises or offsite, the process of physical destruction eventually puts your data—and its security—in someone else's hands. Once your data has left your custody, it is effectively in the wild unless you implement stringent best practices.

You would think that was obvious, yet the IT industry is littered with examples where even the largest multinational organizations have had little oversight of the process. Devices have been found in public spaces with data still present and staggering fines have been imposed—all because an organization has made assumptions about the security of the destruction process that are simply not true.

What results is professional embarrassment, erosion of brand trust, financial loss, and a potential security nightmare for end customers if personally identifiable information is found and misused.

According to a Gartner® report,

**Robust, consistent and pervasive data sanitization must be a core C-level requirement for all IT organizations, in light of growing concerns about data privacy and security, leakage, and regulatory compliance.**

Gartner, Hype Cycle™ for Endpoint Security, 2023, Franz Hinner, Satarupa Patnaik, Eric Grenier, Nikul Patel, 1 August 2023.

Gartner and Hype Cycle are registered trademarks of Gartner, Inc. and/or its affiliates in the U.S. and internationally are used herein with permission.

All rights reserved.



### Spot the shredding security challenges

- 1. Processes:** best practice chain of custody principles must be consistently applied and verified.
- 2. Partners:** not all physical destruction parties within the ecosystem are concerned with data security.
- 3. Particles:** resultant particles can still contain data—a problem that is set to increase given the miniaturization of hardware and storage.

### Better way, better security

The far more secure route to permanent data elimination is via software-based erasure applied through a consistent, fully managed ongoing process.

Because erasure can happen at any time on any device, including SSDs, devices themselves need not be destroyed. Automation of the process also reduces the necessity for manual touch, eradicating the security issues that have typically come from the chain of custody concerns surrounding physical destruction.

This is how Blancco assures your devices and environments can be erased to 100% blank with total security.

#### Blancco:

- **25 years in business**
- **250 million erasures performed**
- **0 security breaches**

[Start your free data erasure trial](#)



# Blank is scalable

**As we have discussed in the Blank is trust section, while data continues to proliferate, its lifecycle management is a critical task for both the IT department and lines of business.**

It's an activity that must be urgently reviewed from an efficiency standpoint. This is particularly true with the increased adoption of IoT, AI, and the hybridization of cloud strategies. All of these are contributing to data escalation and putting an extra burden on enterprises to manage much more data, much more efficiently.

## **The physical destruction efficiency drain**

Since data first began its exponential growth, much has changed in the fields of data management and hardware architecture, making physical destruction an increasingly inefficient answer to data management and sanitization.

## **But where exactly do the problems lie?**

1. Physical destruction is slow to scale across geographies and types of technological environments
2. It's an inefficient use of IT asset management resources
3. Reporting is often sketchy and slow to produce, making auditing difficult
4. There is no way to customize workflows to ensure compliance
5. Upgrading drive destruction equipment can be expensive and cumbersome, making it more difficult to address changing policies quickly
6. Manual processes waste the IT team's skilled resources and IT budgets, as well as the planet's resources (more on this in our sustainability chapter)

In summary, as device estates expand to house exponentially growing data, managing data sanitization also becomes more complex, time consuming, and inefficient—not just on end-of-life devices, but also for end-of-life data that resides throughout enterprise networks.

The solution is to embed erasure into workflows that reach all areas of the IT estate from live environments to storage and decommissioned devices.





### Recommendation

Embed immediate data erasure into both data and device lifecycle processes, using software-based techniques. This saves time in the long run, keeps you on track with compliance, and adds a vital layer of security.

### Resolving the inefficiency conundrum

Integrated, automated data erasure throughout both data and asset lifecycles provides a final line of protection against data loss or breaches. It also enables timely data erasure at the point of disposal—whether that’s for one or thousands of devices that need to be retired, or for no-longer-needed active files.

However, in active networks, there’s no longer a need to store huge volumes of ROT data, kicking the can down the road before disposal. Instead, targeting files and folders through policy-based erasure automation cuts vulnerability and risk while boosting compliance—all with powerful immediacy.

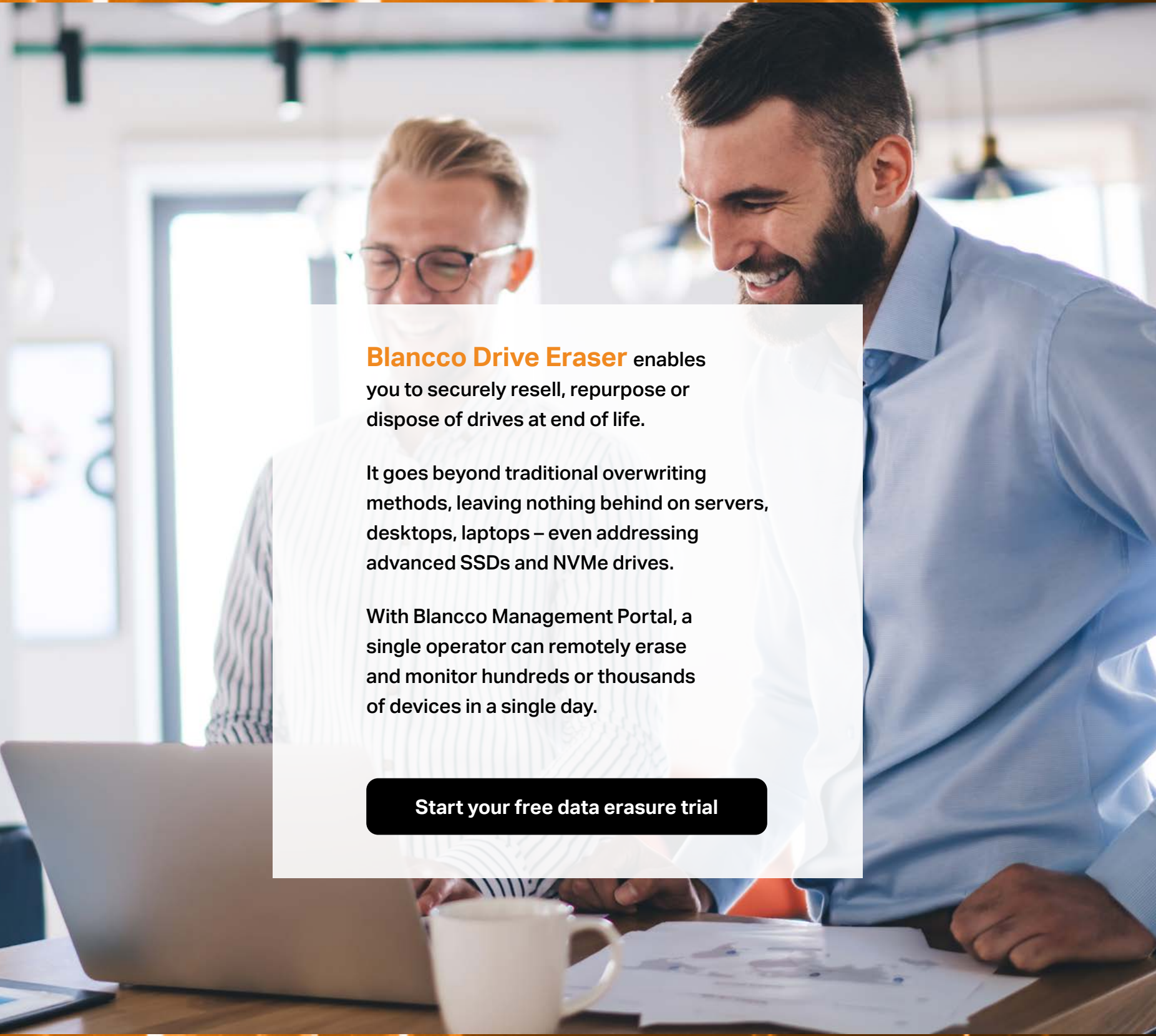
Doing so generates a more efficient “keep only what’s necessary” culture, leaving compliant end-of-life data disposal much less taxing to do, and greatly lowering the chance of keeping sensitive data too long.

For end-of-life data storage assets—whether within data centers or home offices—scalable, software-based erasure solutions make you a more efficient and secure IT organization. The business will benefit from extracting more value from IT assets over time as they are erased and recommissioned or resold. Not only is this a more efficient use of budget, it saves significant time by undertaking erasure in a planned, orderly, automated manner.



## Blancco benefits

- Scale to the needs of enterprises
- Reduce manual effort
- Improve efficiency and ensure reliable certified erasure against the broadest set of standards
- ITAM (IT asset management) and ITSM (IT service management) integration ensures sanitization is a key part of data and device lifecycle workflows
- Blancco integrates with the world's biggest technology and productivity platforms, such as ServiceNow
- **Real world: One Blancco tech customer erased 4,000 servers simultaneously<sup>3</sup>**
- **Another reduced labor processes for disposal by 80%<sup>4</sup>**



**Blancco Drive Eraser** enables you to securely resell, repurpose or dispose of drives at end of life.

It goes beyond traditional overwriting methods, leaving nothing behind on servers, desktops, laptops – even addressing advanced SSDs and NVMe drives.

With Blancco Management Portal, a single operator can remotely erase and monitor hundreds or thousands of devices in a single day.

[Start your free data erasure trial](#)

# Blank is certified

**The laws around data disposal and retention are so stringent that complying with industry and government regulations is ever more important.**

Huge fines continue to be issued as a result of non-compliance. For example, one global bank was embarrassed to find business-critical data left on devices after they had left the firm's buildings bound for physical destruction. This led to millions of dollars in fines, major reputational damage, and loss of customer trust.

## **The origin of the compliance challenge**

Many organizations do not truly understand the types of data they hold well enough to understand the best methods of sanitization: shredding and degaussing are all thought by many to be enough. They are not—not always.

## **Recommendation**

The best way to ensure compliance is by embedding it into data management lifecycles, right across the IT landscape. All responsible parties, from IT to legal to business risk, need to work closely together to create an automated, auditable, transparent, consistent erasure regime. Having to establish and maintain compliance is not an issue that IT should face alone.

By deploying a software-based data sanitization solution, such as Blancco data erasure, you will ease the compliance burden. We meet over 25 standards and guidelines that precisely track document erasure details approved by over 15 governing bodies. No

other data erasure software can boast this level of evaluation and certification against the rigorous requirements set by government agencies, legal authorities, and independent testing laboratories.

And with Blancco, not only is our software-based data sanitization solution certifiably proven to be effective and secure—your data erasures are certifiably checked, documented, and recorded for compliance.

Unlike so many other methods, our erasure solutions come with tamper-proof verification certificates that precisely track and document erasure details, all of which can be securely stored in a central repository for audit purposes.

**“The regulators know about Blancco, which saves us time and effort in explaining our decommissioning process. They respect Blancco, and we can show them the certificate of electronic erasure.”**

Global investment bank



**100% compliance with  
data sanitization standards.  
100% tamper-proof audit trail.**

**Start your free data erasure trial**

# Blank is green

## Physical destruction might be the prevailing method of data destruction, but it is not the ideal option for the environment.

In fact, it is more accurate to say that physical destruction is completely untenable from a sustainability point of view given that some 30 million tons of computers, smartphones, screens, and tablets are generated as e-waste every year.

The worst of it is that, according to the UN, only 20 percent of e-waste is recycled.<sup>5</sup>

- **61.3 million tons** of electronic waste (e-waste) will be discarded in 2023<sup>6</sup>
- **50.6 million** tons will go to landfill, be burned or illegally traded and treated in sub-standard ways<sup>7</sup>
- **50%** of all e-waste is computers, smartphones, screens, tablets, and TVs<sup>8</sup>
- **£7.9 billion/US\$10billion** of platinum, gold, and other precious metals are dumped every year within our electronic devices<sup>7</sup>

Simply put, as data volumes and types grow, we cannot simply continue our current hardware consumption and destruction cycles.

The trend in miniaturization of hardware is also making physical destruction—and the reclaim of valuable and harmful components—more complex and costly.

Is there a better way to get rid of data without having to destroy the hardware that houses it?

Yes, and with software-based erasure it is so easy to do. First, though, organizations must change their mindsets to focus on embracing the circular economy. Reuse, resell, or recommission must become a salient component of ESG strategies: Blancco can help with a better, more sustainably sensitive way to erase data for good.

## Data sanitization that's better for the planet

By updating your policies and adopting Blancco's software-based data erasure solutions, you can reduce budget constraints and erase any end-of-life data concerns from your organization. All while ensuring your original SSDs and other devices may be safely reused, returned to a lessor, or otherwise prevented from heading to landfill.

Blancco supports sustainability through:

- Secure device reuse
- IT asset circularity
- Diminished redundant, outdated, or trivial (ROT) data concerns
- E-waste reduction


One of the world's most innovative device and software manufacturers has  
erased >1million devices in the past 18 months and says the following of Blancco:

**Blancco gives us the confidence to resell drives and recoup the value from the materials without worrying about disclosing personal identifying information. We use Blancco to compare the known configuration (number of drives expected) with the results from Blancco to remove all dead media before reselling/recycling to ensure that we are meeting all compliance requirements.**



# Blank is progressive

As the issues of security, compliance, efficiency, and resource sustainability converge into a worldwide problem that can no longer be avoided, let's showcase some further benefits of the Blancco way as experienced by our customers.



**With Blancco, we are assured that no residual data remains in these devices before they are distributed to beneficiaries. Blancco gives us peace of mind that our data is secure and only present in authorized devices. All other devices that used to contain our data have been erased completely and that data cannot be recovered.**

Maria Angelica B. Rapadas, Chief Information Officer and Executive Director for Ayala



**Previously, all assets were shipped to engineers who then executed the more complicated erasure. Now, the end user can perform the sanitization on their own with Blancco, and then ship the asset directly to the recycling vendor. We avoid the extra \$25 shipping cost per asset and save at least 10% of time overall on erasure.**

American IT consultancy

**“Millions of students go without the tools to dream and achieve in the digital age. Instead of letting those very tools go into a landfill, LiteHaus International connects castoff equipment with the right second-phase owners. Secure erasure with Blancco is a critical part of our end-to-end solution.”**

Jack Growden, Founder and CEO, LiteHaus International

# Definition of terms

## Data sanitization

Blancco defines data sanitization as the process of deliberately, permanently and irreversibly removing or destroying the data stored on a memory device to make it unrecoverable—a definition in line with Gartner’s Hype Cycles.<sup>9</sup> A device that has been sanitized has no usable residual data, and even with the assistance of advanced forensic tools, the data will not ever be recovered.

There are three methods to achieve data sanitization: physical destruction, cryptographic erasure and data erasure.

## 1. Physical destruction

The process of shredding hard drives, smartphones, printer drives, laptops and other storage media into tiny pieces by large mechanical shredders. Other methods of physical destruction include incineration, melting, pulverization, and disintegration.

Degaussing is a form of physical destruction whereby data is exposed to the powerful magnetic field of a degausser and neutralized, rendering the data unrecoverable. Degaussing can only be achieved on hard disk drives (HDDs) and most tapes, but the drives or tapes cannot be re-used upon completion. Degaussing is not an effective method of data sanitization on solid-state drives (SSDs).

## 2. Cryptographic erasure

Alternatively known as Crypto Erase, cryptographic erasure is the process of using encryption software (either built-in or deployed) on the entire data storage device, and erasing the key used to decrypt the data. The encryption algorithm must be at a minimum of 128 bits. While the data remains on the storage device itself, by erasing the original key, the data is effectively impossible to decrypt. As a result, the data is rendered unrecoverable and is an appropriate method to achieve data sanitization.

In addition to data erasure, Blancco also offers cryptographic erasure.

## 3. Data erasure

This is the software-based method of securely overwriting data from any data storage device using zeros and ones onto all sectors of the device. By overwriting the data on the storage device, the data is rendered unrecoverable and achieves data sanitization.

Data erasure:

- Allows for selection of a specific standard, based on your industry and organization’s unique needs.
- Verifies the overwriting methodology has been successful and removed data across the entire device, or target data (if specifically called).
- Produces a tamper-proof certificate containing information that the erasure has been successful and written to all sectors of the device, along with data about the device and standard used.

\*All definitions provided courtesy of the International Data Sanitization Consortium.<sup>10</sup>



# Embrace the next generation of data erasure.

Let the future start today.

Start your free Blancco trial

© 2023 Blancco Technology Group. All rights reserved.

1. IDC white paper, sponsored by Dell Technologies and NVIDIA, High Data Growth and Modern Applications Drive New Storage Requirements in Digital Transformed Enterprises, July 2022, IDC Doc. #US49359722
2. <https://www.veritas.com/content/dam/Veritas/docs/reports/databerg-report-uk-2020.pdf>
3. <https://www.blancco.com/case-study/cs-top-technology-company-erases-4000-servers-simultaneously/>
4. <https://www.blancco.com/case-study/cs-sysmex-asia-pacific-achieves-data-protection-compliance-in-3-months/>
5. <https://www.unep.org/news-and-stories/press-release/un-report-time-seize-opportunity-tackle-challenge-e-waste>
6. <https://weee-forum.org/iewd-about/>
7. <https://www.weforum.org/reports/a-new-circular-vision-for-electronics-time-for-a-global-reboot>
8. <https://www.theguardian.com/environment/2020/jul/02/10bn-precious-metals-dumped-each-year-electronic-waste-un-toxic-e-waste-polluting>
9. <https://www.blancco.com/blog-data-sanitization-gartner-hype-cycle/>
- 10 . <https://www.datasanitization.org/data-sanitization-terminology/#::~:~:text=Data%20sanitization%20is%20the%20process,will%20not%20ever%20be%20recovered.>