

WHITE PAPER

Safe, Secure, and Seamless

Hyperscale Data Center Solutions for
Confident Decommissioning

Contents

- Introduction 3**
- Hyperscale Data Centers: Big Power, Bigger Challenges 3**
- The Downsides of Destruction-Based Asset Dispositioning 4**
 - When Destruction Can't be Avoided 5
 - Comparing Three Hyperscaler IT Asset Disposition Workflows 6
 - Offsite Hyperscaler Dispositioning..... 7
 - Hybrid Hyperscaler Dispositioning..... 8
 - Integrated, Automated Erasure for Hyperscaler Operations..... 9
- Use Cases for Integrated, Automated Erasure 10**
 - Workflow Integration 10
 - Process Flow for Production Fallout Drives..... 11
- Active Erasure in Real-Time Environments 12**
 - Process for Secure File Erasure:..... 12
- Automated, Integrated Erasure's Benefits Across Four Pillars 13**
- Conclusion 13**
- About SK tes 14**
- About Blancco 14**

Introduction

For hyperscalers, everything is massive—from football field-sized data centers to intricate cooling systems and vast energy networks. Leading these facilities brings equally large risks: environmental impact, fines, and security threats. Their tech stacks support much of the 402.74 quintillion terabytes of data created daily, making them critical and high-profile parts of global infrastructure¹. When these assets reach the end of their life, decommissioning is carefully managed on-site to avoid disrupting operations. However, moving assets or performing physical destruction at external facilities can expose security gaps, cut productivity, and increase carbon footprints.

This whitepaper will explore how the decommissioning process can be integrated into workflows to make retiring assets a simple, transparent, and efficient task. Using hyperscaler datacenter solutions like those offered through SK tes and Blancco allows even the biggest organizations to scale decommissioning and streamline their entire IT asset lifecycle.

Hyperscale Data Centers: Big Power, Bigger Challenges

Hyperscalers face a big challenge when devices reach the end of their useful lives: deciding whether to erase or destroy them. Device erasure, a software-based method that permanently and completely removes data, and asset destruction, where the device is physically rendered unusable, are both complex processes. Each comes with its own difficulties, especially across four major priorities for hyperscalers: security, sustainability, efficiency, and compliance.



¹ Exploding Topics. How much data is generated per day? Retrieved October 4, 2024, from explodingtopics.com/blog/data-generated-per-day

Security	Sustainability	Efficiency	Compliance
- Retired assets from hyperscalers are prime targets for data theft. - Off-site erasure processes heighten the risk of losing control over sensitive data. - Inadequate data erasure exposes hyperscalers to severe security breaches, unauthorized access, and costly legal repercussions. One of the largest GDPR fines ever—\$60 million—was related to improperly decommissioning assets.²	- Off-site destruction contributes to e-waste and hampers sustainability efforts. - High profile companies are under increased pressure to reduce emissions. - Hyperscalers are major power consumers and those needs are only growing as AI programs become more prevalent. The International Energy Agency reports that data center emissions must be halved by 2030 to reach global net-zero goals by 2050.³	- Out of rack erasure involves physically removing drives for destruction, which is time-consuming and labor-intensive - Prolonged processing increases costs and resource consumption. - The ever-evolving complexity of storage technologies makes it more difficult to completely and permanently erase data. From 2025 to 2029, NAND flash storage density is projected to increase by 300%.⁴	- Hyperscalers must comply with complex global data protection laws. - Data breaches can lead to billion-dollar fines under regulations like GDPR. - Updating from NIST 800-88 to IEEE 2883* is crucial for stronger, modern data erasure standards but is challenging in large tech stacks. Almost 80% of the world's population is covered by some type of national data privacy law.⁵

* The National Institute of Standards and Technology (NIST) Special Publication 800-88 provides established guidelines for media sanitization, while the more recent Institute of Electrical and Electronics Engineers (IEEE) Standard 2883 introduces updated methods for secure data erasure and storage device destruction based on the latest technology

The Downsides of Destruction-Based Asset Dispositioning

The two broad ways to retire assets securely—sanitizing data or destroying the asset—both have their pros and cons. Data sanitization is typically considered superior as it allows the organization to recapture much of the residual value of the asset while overwriting or scrambling data at the binary level. However, hyperscalers with major security concerns may opt for a destruction-first approach.

² GDPR Register. (n.d.). Morgan Stanley fined \$60 million for failing to secure decommissioned hardware. Retrieved October 4, 2024, from gdprregister.eu/news/morgan-sanley-fined/

³ International Energy Agency. (n.d.). Data centres and data transmission networks. Retrieved October 4, 2024, from [iea.org/energy-system/buildings/data-centres-and-data-transmission-networks](https://www.iea.org/energy-system/buildings/data-centres-and-data-transmission-networks)

⁴ Clarke, C. (2024, August 5). IEEE's view of SSD and HDD technology roadmaps. Blocks and Files. Retrieved from blocksandfiles.com/2024/08/05/ieees-view-of-ssd-and-hdd-technology-roadmaps/

⁵ IAPP Staff. (n.d.). Identifying global privacy laws relevant to DPAs. International Association of Privacy Professionals. Retrieved October 4, 2024, from iapp.org/news/a/identifying-global-privacy-laws-relevant-dpas

This can include crushing, shredding, or incinerating the device to ensure it can never be reused. This comes with additional downsides beyond the general hyperscaler decommissioning challenges.

- **Security:** A destruction-only approach can leave a security gap between unprovisioning and final destruction. While hyperscalers generally sanitize drives in place before removal, relying solely on physical destruction can lead to vulnerabilities if drives are left idle or improperly tracked before being destroyed.
- **Compliance:** Manual destruction poses compliance challenges because it requires strict chain-of-custody processes. Without a verified serial number list and rescanning at each stage, errors like mis-scanned or missing serial numbers can lead to incomplete records. This is especially problematic after the drive has been shredded and workers must try and find disc serial numbers in piles of debris. Some agencies, like the U.S. National Security Agency, have strict requirements for destruction. For example, the NSA mandates that destroyed particles be no larger than 2 mm—about the thickness of a nickel—which can be hard to achieve with drives built for extreme environments.⁶ It also makes it near impossible to locate serial numbers if they were missed pre-shredding.
- **Sustainability:** Reuse is preferable not only to avoid landfills, but because manufacturing new devices creates the largest carbon footprint of the entire asset lifecycle. Extending device lifespans helps reduce this impact.
- **Efficiency:** The time spent managing and destroying assets diverts resources from an organization's core mission. Onsite destruction, especially for hyperscalers managing high volumes like 60,000 to 100,000 drives at a time, relies heavily on mobile shredders that require extensive maintenance from a skilled workforce. The high volume can cause significant wear on the equipment, increasing the risk of breakdowns and disrupting large decommissioning projects.
- **Value loss:** Industry experts recommend replacing servers every three to five years – but drives can retain value well throughout this period.⁷ That value can be recaptured through remarketing or donating. On the other hand, when devices are destroyed, that value is reduced to parts and pieces.

When Destruction Can't be Avoided

Sometimes, it only makes sense to destroy end-of-life assets due to their high security risk or complete obsolescence. However, even in this case, the approach should prioritize data erasure. When a drive is securely erased before destruction, the security gap is eliminated, ensuring sensitive data is no longer at risk.

For high-impact assets where physical destruction is required, wiping the storage media in-rack using a designated overwrite method and 100% verification—resulting in a report with storage media and parent serial numbers—ensures compliance and eliminates data exposure between the rack and destruction site.

Even for organizations that follow high standards, such as the NSA's requirement for 2 mm particle size, compliance becomes easier when devices don't need to be shredded to meet this standard (due to in-rack erasure). Larger fragments require less energy, making the process more sustainable and improving efficiency by reducing processing time.

⁶ National Security Agency. (2019, April 24). NSA evaluated products list for solid state disintegrators. Retrieved from nsa.gov/portals/75/documents/resources/everyone/media-destruction/NSAEPLSolidStateDisintegrators24April2019.pdf?ver=2019-05-15-155330-587

⁷ Dell Technologies. (n.d.). Why upgrade? Retrieved from i.dell.com/sites/csdocuments/Shared-Content_data-Sheets_Documents/en/DELL_Why_Upgrade_Incl_Link_to_Dell.pdf

Comparing Three Hyperscaler IT Asset Disposition Workflows

There are three primary methods that hyperscalers follow for their decommissioning process, whether they are destroying or planning to remarket assets:

1. **Offsite:** Most devices are transported to an offsite facility for dispositioning.
2. **Hybrid:** Some devices are addressed onsite while others are transported offsite.
3. **Integrated, automated:** Automated data erasure is integrated throughout the entire system, allowing for both incremental and bulk disposition.

Integrated, automated erasure embeds secure data removal directly into a hyperscalers automation framework, enabling seamless and efficient sanitization of devices. It offers benefits across all four pillars.

✓ **Security:**

Eliminates the gap between unprovisioning and sanitization, reducing the risk of data breaches.

✓ **Sustainability:**

Ensures proper sanitization, enabling responsible reuse or disposal of devices.

✓ **Efficiency:**

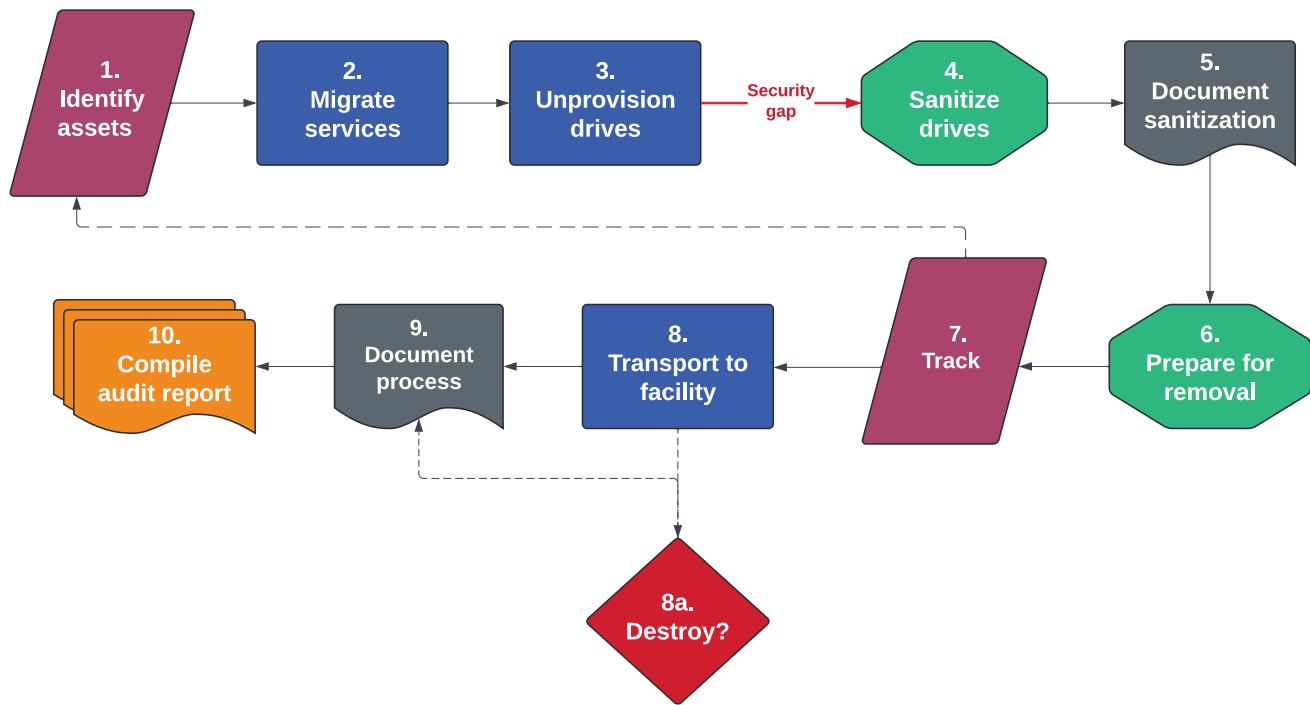
Streamlines the data erasure process, minimizing manual effort and human error.

✓ **Compliance:**

Automates adherence to data protection regulations, ensuring consistent legal compliance across all devices.



Offsite Hyperscaler Dispositioning

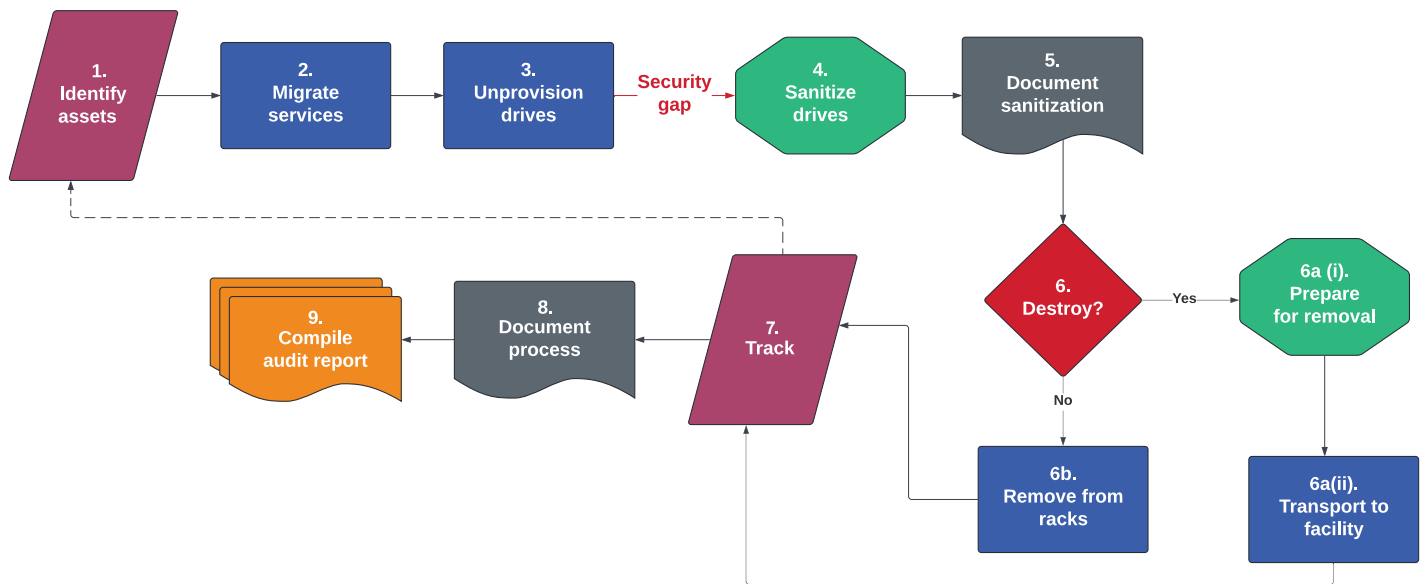


- 1. Identify assets:** Compile a list of drives to be decommissioned, tracking each asset with serial numbers for inventory management.
- 2. Migrate services:** Transfer active services from the drives to other resources within the fleet to maintain uninterrupted operations.
- 3. Unprovision drives:** Remove drives from production and delete encryption keys to prepare them for secure wiping. In some cases, drives may be left idle for a long period pending removal, leading to a security gap.
- 4. Sanitize drives onsite:** Erase drives in their racks using approved standards such as NIST or IEEE methods to ensure data is completely removed before physically taking out the drives for further handling or transport.
- 5. Verify and document sanitization:** Generate detailed sanitization certificates and verify each drive against the original serial number list.
- 6. Prepare for removal:** Physically remove sanitized drives, label them for tracking, and prepare for offsite transport.
- 7. Track and reconcile:** Cross-check drives against the initial asset list to ensure no devices were missed or incorrectly tracked.
- 8. Secure transport to facility:** Coordinate the secure transport of drives to an offsite facility for further handling or destruction.
 - a. Final destruction (if required):** Complete physical destruction of drives at the offsite facility using larger industrial shredders.
- 9. Document process:** Maintain a comprehensive record of all steps, including transport logs, certificates, and destruction records.
- 10. Generate compliance report:** Compile all documentation into a final report for compliance, audit, and client review.

The offsite process involves many steps and potential gaps where things can go wrong. As indicated by the red line, there is commonly a delay between asset unprovisioning and data sanitization, leading to security vulnerabilities.

To reduce these risks, hyperscale data centers are increasingly looking to minimize both offsite physical destruction and off-rack data erasure. The most effective solution is to implement integrated, in-rack erasure. By securing data before assets leave the rack, hyperscalers can close security gaps and improve overall data protection.

Hybrid Hyperscaler Dispositioning

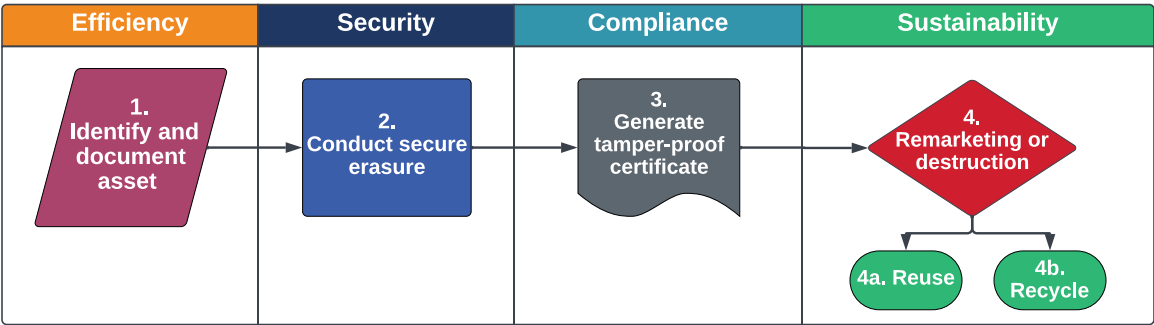


1. **Identify assets:** Create a detailed list of drives to be decommissioned, recording their serial numbers for tracking.
2. **Migrate services:** Transfer active services from the assets to other fleet-provided resources, ensuring no disruption.
3. **Unprovision drives:** Unprovision the assets by deleting encryption keys and preparing them for erasure. In some cases, drives may be left idle for a long period pending removal, leading to a security gap.
4. **Sanitize drives in rack:** Perform in-rack data erasure using open-source tools like nwipe or certified sanitization software, issuing sanitization certificates for each uniquely serialized drive.
5. **Verify sanitization:** Cross-check the sanitization certificates with the original asset list to ensure successful erasure.
6. **Decide on further processing:**
 - a. If physical destruction is required: (i) prepare devices for removal and (ii) transport to facility.
 - b. If no destruction is needed: Remove sanitized drives from racks and proceed with recycling or repurposing.
7. **Track and reconcile:** Maintain a clear chain of custody by verifying each asset against the initial list to prevent any discrepancies.
8. **Document the process:** Record all actions taken during sanitization and destruction for compliance and audit purposes.
9. **Generate final compliance report:** Compile sanitization certificates, destruction records, and audit logs into a comprehensive report.

The hybrid workflow offers some efficiency gains over one that involves manually pulling drives from their servers, but there are ways to enhance the dispositioning process further. This is where a third option comes in: integrated, automated erasure.

Integrated, Automated Erasure for Hyperscaler Operations

Integrated, automated erasure activates data sanitization directly in-rack when servers become idle or are no longer providing active services. By building erasure into existing workflows, hyperscalers can automatically sanitize data as soon as services are migrated or decommissioned—without waiting for a complete server batch. This approach enhances security, ensures compliance with strict data protection standards, and eliminates the risk of servers sitting idle with data.



1. **Identify and document asset:** Use integrated lifecycle management tools to identify assets based on service demand or when they become idle, ensuring full traceability and documentation.

2. **Conduct secure erasure:** The software automatically performs secure, permanent erasure based on predefined compliance standards as soon as the asset is no longer active.

3. **Generate tamper-proof certificate:** A tamper-proof certificate of erasure is generated, documenting detailed asset information, erasure type, and verification.
4. **Remarketing or destruction:** A ticket is automatically created, alerting the team to proceed with physical removal for repurposing or final destruction.

a. **Reuse:** Once securely erased, assets can be repurposed, reducing waste and costs associated with manufacturing new devices.

b. **Recycle:** If reuse isn't an option, the sanitized asset can be more efficiently broken down for recycling, minimizing energy consumption.

While hyperscalers efficiently scale resources as services demand, their decommissioning processes often fall short, with thousands of drives waiting for bulk disposition since incremental processes aren't practical. Integrated, automated erasure provides a scalable solution, allowing hyperscalers to manage this process flexibly—whether processing thousands of drives at once, individually, or in various other scenarios.

Use Cases for Integrated, Automated Erasure

There are three main use cases for automated, onsite erasure solutions. First, bulk decommissioning, where large numbers of drives are securely erased during standard hyperscaler decommissioning projects. Second, active erasure in real-time environments, which allows data to be erased immediately without disrupting ongoing operations. Third, ad hoc, small volume decommissioning, where hyperscalers can handle small-scale data removal independently without external support. These solutions give hyperscalers flexibility to manage data erasure based on their specific needs.

Automated, integrated erasure offers several key benefits in this scenario:

- **Mass scalability:** Erase tens of thousands of drives using an automated process that adapts to different drive types and erasure standards.
- **Built-in safeguards:** Ensure minor issues don't halt the entire process.
- **Improved efficiency:** Reduce—or even largely eliminate—time spent on manual erasure and destruction.
- **Flexibility:** Adapt to appropriate standards for a given asset.
- **Compliance:** Meet security and data sanitization standards automatically.
- **In-rack erasure:** Eliminate security risks by sanitizing drives before they are removed from their physical locations.

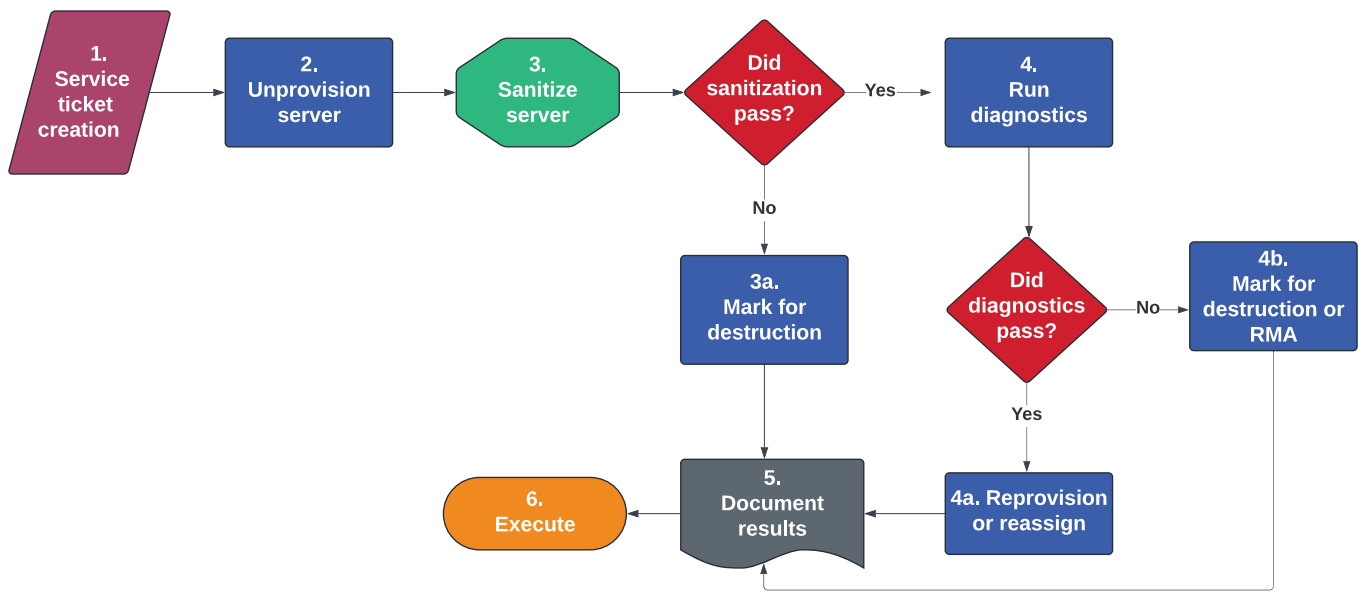
Efficiency Safeguards in Action

If a drive is damaged beyond functionality, traditional erasure methods may fail and disrupt the entire operation. With Blancco solutions incorporated into SK tes workflows, the system would generate an alert about the faulty drive while continuing to erase the remaining drives without interruption. This feature allows hyperscalers to address issues seamlessly, enabling them to clear large backlogs quickly and efficiently.

Workflow Integration

The return merchandise authorization process can be a major disruption for hyperscalers. When a device fails, it often leads to productivity delays, and managing the steps of locating, pulling, erasing, returning, and tracking the asset can be inefficient. However, with an integrated SK tes/Blancco solution, RMAs are streamlined.

Process Flow for Production Fallout Drives



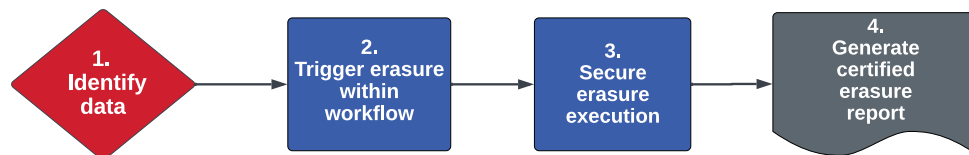
1. **Service ticket:** The process starts when a service ticket is created to locate, pull, and replace a failed server or disk. The ticket serves as the entry point for tracking and managing the process.
2. **Unprovision the server:** Automation pulls the server out of production mode and initiates the unprovision workflow. The server is rebooted to a diagnostic image to prepare it for testing and processing without manual intervention.
3. **Perform full server sanitization:** Perform a complete data sanitization of all disks to ensure no data remains before moving forward.
 - a. **If sanitization fails:** The server is marked for physical destruction to prevent data leakage.
4. **Run diagnostics:** After sanitization, diagnostics are performed on the server and its disks to verify health and performance attributes against predefined acceptance thresholds.
 - a. **If diagnostics pass:**
 - i. **Evaluate server's service life:** If the server is still within its expected service life, it is re-provisioned and returned to active use.
 - ii. **If the server is no longer needed for production:** Proceed with reassigning the server or designating it for spare use.
 - b. **If diagnostics fail:**
 - i. **Physical destruction or RMA:** Drives or components that fail diagnostics are sent for repair if they are recoverable. If they are beyond repair, they are immediately marked for destruction.
5. **Document sanitization and diagnostic results:** A report documenting the sanitization and diagnostic results is automatically uploaded to the portal for full traceability and compliance purposes.
6. **Execute removal or re-provisioning:**
 - a. **If successful:** The server, now sanitized and verified, can be repurposed, returned to the spare pool, or fully decommissioned based on business needs.
 - b. **If failed or processed multiple times:** Servers or components that have been processed through this workflow more than twice, or that fail any step, are designated for destruction instead of being re-circulated into the spare pool.

The process typically begins with a service ticket to locate, pull, and replace a failed disk. Once removed, the drive is placed in a secure location for a technician to retrieve and process. Automation can further enhance this by pulling servers out of production mode and running diagnostics on disks and servers as part of the decommissioning workflow. Drives that meet health and performance standards are returned to spare pools, while those that do not are processed for destruction or credit, ensuring a consistent, zero-touch workflow that maintains data security at every stage.

Active Erasure in Real-Time Environments

Hyperscalers face more than just complex asset decommissioning—they must also comply with stringent data privacy regulations like the EU's General Data Protection Regulation (GDPR) and other similar laws. Compliance with these regulations requires the secure handling and permanent removal of sensitive information when it is no longer legally required or when data subjects submit legally binding requests for deletion.

Blancco File Eraser helps organizations securely and permanently erase sensitive files, such as individual documents or folders. It overwrites data using advanced erasure algorithms, ensuring that information cannot be recovered, even with the most sophisticated forensic tools. This process includes the generation of a certified, tamper-proof report that meets compliance standards, making it easier for organizations to demonstrate adherence to data privacy laws.



Process for Secure File Erasure:

- 1. Identify data:** Begin by identifying files and folders that are no longer needed or are subject to deletion requests. This might include personal information or business-critical files stored within customer databases.
- 2. Trigger erasure within workflows:** Automatically initiate Blancco File Eraser at specific points in the data lifecycle (e.g., when data retention policies require deletion or when data is flagged for removal based on user requests).
- 3. Secure erasure execution:** Blancco File Eraser permanently overwrites the identified files and folders using advanced erasure methods. This ensures that the data is completely destroyed and cannot be reconstructed or recovered, supporting compliance with regulatory data sanitization requirements.
- 4. Generate certified erasure report:** After the secure erasure is complete, Blancco File Eraser generates a tamper-proof report that certifies the data has been fully removed. This report is essential for audit and compliance purposes, providing verifiable proof of secure data sanitization.

By integrating into existing workflows, Blancco File Eraser helps organizations enhance data security, enforce data retention policies, and ensure compliance with strict data privacy regulations.

Automated, Integrated Erasure's Benefits Across Four Pillars

SK tes and Blancco solutions enable hyperscalers to streamline workflows and automate the lifecycle management of data and assets. This integrated automation addresses key challenges in efficiency, security, sustainability, and compliance.

Security	Sustainability	Efficiency	Compliance
On-site, automated erasure reduces the risk of data exposure from "unplugged" assets. • Eliminates security gaps before asset removal • Reduces risk of data breaches • Minimizes attack surface • Prevents costly fines from mishandling	Automated erasure supports sustainability by enabling reuse, recycling, and minimizing e-waste. • Reduces carbon emissions • Extends asset lifespan • Lowers new device manufacturing needs • Minimizes e-waste through recycling	Automating the erasure process streamlines handling and reduces time, costs, and labor. • Creates zero-touch system • Prevents workflow disruptions • Handles bulk and incremental erasure • Automatically applies the correct erasure method	Integrated, in-rack erasure helps organizations meet global data protection regulations and evolving standards. • Supports compliance with GDPR, HIPAA, PCI-DSS • Aligns with IEEE 2883 and ISO 27040 guidelines • Reduces risk of non-compliance and penalties

Conclusion

Hyperscalers face significant challenges balancing security, efficiency, compliance, and sustainability when decommissioning assets. By leveraging SK tes and Blancco solutions, hyperscalers gain greater control over these activities. This strategy integrates automated data sanitization directly into workflows, strengthening data security and supporting compliance efforts. As a result, they can enhance operational efficiency, reduce costs, and advance their sustainability initiatives. It's a smart, strategic way to address the complex challenges they face today.

About SK tes

SK tes is a global leader in secure and sustainable technology lifecycle management services. Established in 2005, the company specializes in helping organizations responsibly transform and repurpose technology devices. With operations spanning over 40 facilities in more than 20 countries, SK tes processes more than 6.2 million assets annually.

By providing comprehensive solutions for technology deployment, decommissioning, and recycling, SK tes supports its clients in achieving both security and sustainability goals across their global operations.



About Blancco

Blancco Technology Group provides organizations with secure, compliant, and automated solutions that accelerate the transition to the circular economy. Each year, tens of millions of Blancco erasures allow top-tier organizations to protect end-of-life data against unauthorized access, safely redeploy data storage assets, and firmly comply with increased data protection and privacy requirements. Our precise device diagnostics help move used IT assets confidently into the circular economy, enabling enterprises, IT asset disposition vendors and recyclers, and mobile industry stakeholders to operate more sustainably.

Globally approved, recommended and certified by governing and industry bodies around the world, Blancco is the industry standard in data erasure and mobile lifecycle solutions. With 40+ patented or patent-pending ideas, we continue to grow the number of innovative solutions global companies can rely on to accelerate operations, secure their data, and grow their businesses.



For more information, visit sktes.com



Reduce Risk.
Increase Efficiency.
Be Sustainable.™