

Safely Decommission Servers Faster with Automated Data Erasure

If you run a data center, you're probably stretched for both budget and time. That can make it challenging to properly decommission servers, either at end-of-life or for re-provisioning. You need to ensure data is completely unrecoverable with secure [data sanitization](#) processes, while also addressing your resource constraints.

One option is to remove each local drive and physically destroy it, either in-house or using a third-party vendor. This approach is effective, but you may have concerns about the environmental impact. It also eliminates the ability to reuse or resell those assets. Additionally, if the drives have failed, you may be tempted to physically destroy them instead of returning them as part of the original lease contract—losing potential residual value. But there is another way.

Data erasure is an alternative to physical destruction that involves securely overwriting all sectors of the storage medium. This process sanitizes all data stored on the server so it can't be recovered, even with advanced forensics. Automation and other optimizations for large-scale data erasure can help make it as efficient as possible and reduce the impact on your internal resources.

Limited Automation in *Most* Data Erasure Software

Data erasure for servers typically involves manual, time-consuming processes. Technicians use specialized tools and equipment to access storage media in special-purpose boot environments and run erasure software. Software requirements will vary by organization, but should include:

- **Verification of successful erasure**, including a tamper-proof audit trail to [certify](#) data sanitization
- **Flexibility across media**, including conventional spinning hard disk drives (HDDs) and [solid state drives](#) (SSDs)
- **Choice of erasure methods**, including flexibility among specific [erasure standards](#) for regulatory compliance

Effective standards for data erasure contribute to overall [data hygiene](#) by ensuring that data is destroyed when it reaches the end of its retention date, is no longer necessary or isn't adding value to the business. This factor is essential in preventing unauthorized access, whether through a security breach or inadvertent disclosure.



Server-Based Erasure Streamlines Automation

A common approach to sanitizing data in large data centers involves technicians using a laptop that hosts a data erasure solution. The laptop is physically cabled to the server, and the server is network-booted into the erasure environment hosted on the laptop. Full erasure typically takes several hours and is dependent on the method you choose.

This scenario can be streamlined by connecting multiple servers to the laptop using a dedicated, unmanaged switch. While some erasure software supports erasing multiple servers at once, they typically must be individually cabled to the erasure console and booted one at a time, with technicians entering server-specific custom information for each one.

Erase on Loose Drives

A similar approach can be taken for loose drives that have been removed from their servers for decommissioning or repurposing. These drives are typically mounted in a purpose-built chassis or appliance.

While erasure can be done on multiple drives at once, this approach takes even more manual effort than server-based erasure. The drives need to be uninstalled from their servers, installed in the erasure chassis or appliance and then uninstalled after erasure is complete.

Harnessing the Benefits of Data Erasure Automation

Physically touching and individually booting hundreds or even thousands of servers in enterprise or terascale data centers is time and resource prohibitive. The key to increasing efficiency is more automation. Remote-controlled erasure allows you to:

- **Connect through the primary network** instead of with temporary server connections.
- **Enable simultaneous control** from the console outward to all servers.
- **Support erasure without console connectivity** after the process has been initiated.

Rather than cabling from the erasure console to each server, the process can be improved dramatically with erasure software that supports existing network infrastructure.

This simultaneous control allows you to distribute custom field information from the console to all servers without manual entry for each device.

Expanded automation allows data erasure to be set up and executed offline across multiple sites.



Increase Scalability Using Blanco Management Console & Blanco Drive Eraser

Blanco Management Console is designed specifically for highly automated data erasure, making server decommissioning more efficient. By connecting to and controlling the process on hundreds of servers at once, with minimal setup, the solution scales effectively to the largest data center environments.

It would be nearly impossible to run data erasure on hundreds of servers in a single night by connecting a cable to each one and booting it individually. Blanco Management Console overcomes those limitations, connecting through existing ToR switches and pushing the Blanco Drive Eraser client to each server.

You can then take control of all the servers from the Blanco Management Console interface. After verifying the correct target servers and drives are connected and choosing the preferred erasure standard, a single command can initiate erasure on all of them at once. The console allows you to monitor the progress of the erasure and collect extensive reports on the results after the process completes.

Streamlined Operations Support

Unlike many solutions, Blanco Management Console does not require continuous connection to the servers during data erasure. After one erasure job is initiated, a technician can disconnect the laptop or other system running the Blanco software and repeat the process in a different server room or at a different site, further increasing scalability. After each job is complete, the technician can return to each set of servers and easily download reports.

Operators with sufficient rights can view all data erasure licenses as well as create and manage all levels and types of user profiles. Blanco Management Console supports all Blanco data erasure products, so information from all those sources can be displayed in a unified interface, and reporting can be centrally managed for both internal and external stakeholders.

This hub for operations and compliance activities helps simplify and refine internal workflows, contributing to strong internal and external audit standards. Blanco solutions are certified by 18 governing bodies around the world, for compliance with regulatory frameworks such as PCI DSS, HIPAA, SOX and the EU GDPR.

Demonstrating Automation in Action

To show the potential of automated data erasure, Blanco provides real-world demonstrations in production environments. The following example is from a large, customer-owned data center.

- **Challenge:** Perform data sanitization on 856 servers, starting at close of business and finishing before the next morning. In all, the job included 5,117 HDDs with a capacity of one terabyte each.
- **Result:** Blanco Management Console and Blanco Drive Eraser completed the job in 10 hours, including two hours for setup and eight hours to run the actual erasure and collect reports certifying the results.
- **Benefit:** This demonstration shows that, using remote control from the central console interface, a single technician can complete work in a single night that would otherwise take several days, if not weeks.

Simple, Powerful, Scalable Server Decommissioning

Greater automation with Blanco Management Console makes life easier for data centers as they meet internal SLAs to decommission servers, either at end of life or prior to re-provisioning. These new approaches to automated data erasure offer dramatic workflow efficiencies, with environmental and budgetary advantages compared to physical destruction of decommissioned drives.

Because data erasure is completed on drives without leaving the security of the server room, data center operators reduce risk associated with transporting storage media that contains sensitive data and provide a tamper-proof audit trail that data sanitization has occurred. Guaranteeing that customer data has been destroyed beyond recovery safeguards your reputation and ensures compliance with today's toughest data privacy regulations.

Eliminating low-value tasks such as running temporary cables and booting hundreds of servers individually can make your data center more effective. In the face of growing resource limitations and larger amounts of data, these reduced requirements for a common day-to-day responsibility can pay dividends.

Contact us to learn how to start saving time and money with fast, efficient data center decommissioning.
[Get started with your free trial today.](#)