

# Blanco LUN Eraser

Eliminate the Risks of Residual Data on Enterprise Storage Systems

**Blanco LUN Eraser is purpose-built to meet the challenges of secure data erasure in active storage environments, supporting good data hygiene and regulatory compliance.**

As IT organizations work to protect their data from unauthorized access, their efforts toward complete security must not only protect the network perimeter, but also inside the data center. Warding off intrusion attempts is not enough in a world where security breaches are inevitable.

Eliminating residual information from enterprise systems plays a key role in data protection. Once sensitive data is no longer needed, it must be securely erased—not just deleted. 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. Blanco is the industry leader in data erasure, providing a range of software solutions engineered to target specific storage technologies.

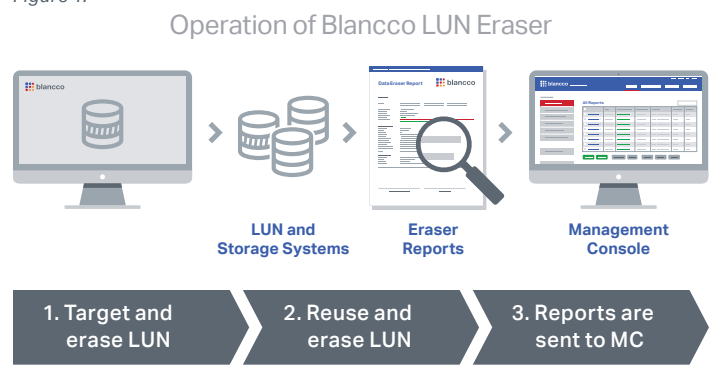
## Secure Data Erasure in Active Storage Systems

Applying data erasure algorithms on storage area networks and other active storage environments presents special challenges. Unlike a local drive on an individual PC or server, for example, a Logical Unit Number (LUN) may comprise a patchwork of storage locations that span multiple physical volumes. The storage system as a whole may also actively support other operational LUNs while the targeted LUN is being erased.

Blanco LUN Eraser is designed specifically for the needs of data erasure in active storage environments. Instead of simply deleting a LUN from the logical layer, Blanco LUN Eraser destroys the actual data on the underlying physical

storage, while still leaving the operating system intact and fully functional. The workflow is illustrated in Figure 1.

Figure 1.



The data erasure process starts with targeting one or more LUNs with Blanco LUN Eraser, directly from the command-line interface. While the targeted LUN is being erased and the associated data is being overwritten, all other LUNs on the same physical drives remain fully functional, with no downtime. After erasure is complete, the storage is immediately reusable, with the operating system intact and no recoverable data left over from the targeted LUN.

The environment generates certified erasure reports through the Blanco Management Console. These reports can support internal or external audits, including regulatory requirements such as Sarbanes-Oxley (SOX), the Payment Card Industry Data Security Standard (PCI DSS) and the Health Insurance Portability and Accountability Act (HIPAA).

### Enterprise-Ready Data Sanitization

Blanco LUN Eraser provides for secure erasure and reuse of storage resources without needing to take storage arrays offline. This capability is key to cost efficiency and avoiding impacts to data center productivity, particularly when doing business with regulated entities such as military, legal, healthcare and financial services customers. Blanco LUN Eraser also lets customers

automate data erasure, reducing dedicated resource requirements and avoiding human error.

Secure data erasure may be needed at various transition points, such as when a new user or application is assigned to a LUN, the end of data-retention periods or after disaster-recovery testing. All such cases should be governed by strict policies to protect sensitive information, backed by automated processes and a documented audit trail. Blanco LUN Eraser allows customers to enact those policies simply and dependably.

### Robust Reporting for Audit and Regulatory Support

When data erasure is complete, Blanco LUN Eraser generates an activity log and certified report to document that the data has been sanitized. Reports include a wide range of information by default, such as the LUN ID, port, network pat, and physical characteristics of the drive(s). Custom information fields can be added to meet organization-specific requirements.

### The Blanco Advantage: An Unparalleled Range of Certifications

Customers all over the world look to Blanco for the most rigorous assurances available of highest-confidence data erasure. Blanco solutions have been tested, certified, approved, and recommended by 15+ governing bodies globally. No other provider can offer its customers this level of compliance with worldwide regulations. View the entire list of certifications at [www.blanco.com/about-us/our-certifications/](http://www.blanco.com/about-us/our-certifications/).

The report can be in PDF form for easy viewing, as well as an XML file for machine-to-machine communication with governance, risk and compliance (GRC) or other reporting systems. It can be digitally signed using a secure certificate as an added level of assurance. In addition to being stored locally, reports can be uploaded to the Blanco Management Console, emailed, or sent by text message to a mobile device.

### Comprehensive, Flexible Operation

Blanco LUN Eraser can target one to 200 LUNs simultaneously, from any type of drive connected by IDE, SCSI, Fibre Channel or iSCSI. A range of operating systems are supported, including varieties of Windows, Linux, and UNIX, as well as storage hardware from leading equipment manufacturers. Operators can choose among popular erasure algorithms, for flexibility in meeting regulatory requirements.

LUNs can be targeted for deletion either from inside the network or by secure remote connection, without downtime or other interference with normal production. The command-line interface supports a broad range of features and configuration parameters, giving administrators outstanding flexibility and ease of use.

### Tailoring the Level of Automation

Blanco LUN Eraser lets each organization choose the level of automation appropriate for its needs. Different approaches can also be taken for various operations.

Blanco LUN Eraser securely erases data from active storage environments without downtime or other interruption to production systems. It provides robust, flexible operation and a certified audit trail, helping minimize risk in the event of a data breach while streamlining regulatory compliance.

Options for Levels of Automation in Blanco LUN Eraser Operation	
Manual	Administrator performs all tasks manually, including initiating erasure and saving/sending reports.
Semi-Automatic	Data erasure and sending reports is initiated automatically; report saving, hardware testing, and updating report fields is manual.
Automatic	Data erasure, hardware testing, updating report fields and sending reports are done automatically; saving reports is done manually.

For more information on Blanco LUN Eraser, visit [www.blanco.com/products/lun-eraser](http://www.blanco.com/products/lun-eraser).

To request a free trial of Blanco LUN Eraser, [click here](#).