blancco

Blancco Drive Eraser for Enterprise

Market-leading Data Sanitization for HDDs/ SSDs in PCs, Laptops, and Servers

Common Criteria

Why Blancco

Blancco Technology Group, a carbon-neutral supplier, provides organizations with secure, compliant, and automated solutions that accelerate the transition to the circular economy.

All erasures are verified and certified through a tamper-proof audit trail. With nearly 25 years of responding to customer needs and 35+ patented or patent-pending ideas, Blancco is the industry standard in data erasure and mobile lifecycle solutions. Our dedication to technological innovation empowers top-tier enterprises, IT asset disposition (ITAD) vendors, and mobile industry stakeholders to protect end-of-life data against unauthorized access, comply with data protection requirements, extend the useable life of IT assets, accelerate operations, and enhance the mobile customer experience.

View Our Certifications

Request Your Free Trial

Get Started Today

Blancco Drive Eraser is the premier data sanitization solution for PC, laptop, Chromebook and data center environments.

What is the best method to sanitize your IT asset portfolio?

Blancco Drive Eraser, our market-leading scalable erasure software, answers this question with its adherence to our four Value Pillars; a guarantee of Security, Efficiency, Compliance and Sustainability. Our scalable software provides essential protection by permanently erasing sensitive data from data centers, servers, HDDs and SSDs (including NVMes in desktops/laptops/ Chromebooks), with Intelligent Business Routing (IBR) workflows enabling automated erasure even while devices are disconnected from networks.

Blancco Drive Eraser works across the entire data lifecycle to provide enterprises with secure data sanitization, help proving regulatory compliance, and the means to re-sell, re-purpose or dispose of data assets at end-of-life as you see fit.

Key Benefits

- Guarantees data has been erased from any drive, from HDDs and self-encrypting drives to SSDs and NVMEs (complying with the IEEE standard and with SecureBoot support for increased security and efficiency)
- Receive a tamper-proof audit trail for all assets, with a digitally-signed Certificate of Erasure for each erasure instance and timestamps to monitor each step of the process
- Process loose drives and Chromebooks with ISO Image Installer, including a report viewer to track progress and specifically designed key diagnostics
- Minimize manual processes with IBR workflows
- Full NIST compliance with support for NIST Purge and Clear, featuring full records of unsupported incidents for transparent auditing
- Delete sensitive data from SSDs without compromising drive functionality with PSID revert
- Create custom erasure standards during overwrites to meet your unique standards

blancco

Technical Specifications

ERASURE

- Locally or remotely controlled data erasure via the Blancco Management Portal
- High-speed, simultaneous erasure of multiple drives, including the ability to customize drive batch sizes and drive speed thresholds
- RAID dismantling and direct access to the underlying physical drives
- SSD detection and secure erasure with Blancco´s patented SSD method
- Automated detection and unlocking of freeze locked drives
- Detection, notification and erasure of hidden areas (DCO, HPA) and remapped sectors
- Support for internal drive erasure commands, including cryptographic erasure and TCG feature set on self-encrypting drives
- Ability to reformat SATA and SAS drives after erasure

MINIMUM SYSTEM REQUIREMENTS

- 1 GB RAM memory in most cases (2 GB for PXE booting)
- Local erasure:
  - CD/DVD drive or USB port for booting the software
  - SVGA display and VESA compatible video card
  - USB port for saving reports
- Remote erasure (requires Blancco Management Portal):
  - Ethernet NIC
  - DHCP Server running on local network for PXE booting, remote erasure and report collection

USABILITY

- Accelerated NIST Purge erasure
- Multi-tasking to allow the hardware diagnostics and updating the report during the erasure time
- Screensaver displaying the erasure progress to monitor the process remotely
- Resume an erasure that has been interrupted without consuming extra licenses
- Dedicated interface for loose drive erasure
- Support for LAN and WLAN networks, including 802.1x authentication

REPORTING

- Digitally-signed Certificate of Erasure
- Choose between asset level or drive-level reports
- Save reports locally or send them through the network to the Blancco Management Portal
- Detailed reports enabled by enhanced hardware detection
- Extensive erasure information, including HDD details for seamless audit procedures
- User extendable report (with option to add “custom fields”)
- Reports Per Drive mode

DEPLOYMENT

- Blancco Drive Eraser is platform independent
- Local control with HASP dongles, standalone images, or centralized control through the Blancco Management Portal
- Deploy locally (CD, USB), via the network (PXE), preinstall (Windows, Linux), or via iLO, iDRAC, Cisco UCS, Intel AMT or install locally (appliance mode)
- NVME Over Farbic Support accessible through a network and shareable over multiple machines
- Blancco USB Creator (part of the Blancco Toolkit) incorporated as means to deploy Drive Eraser, allowing customers to create USB sticks (up to 10 at once)

HARDWARE DETECTION & DIAGNOSTICS

- 13+ hardware tests, including: RAM, CPU, Motherboard, Battery (current capacity & discharge), PC Speaker, Display, Pointing Devices, Keyboard, Optical Drive, Webcam, USB Ports, WiFi card, SMART Tests for drives, BIOS logo
- Hot swap capabilities
- Backwards compatibility with other Blancco products (BDECT, BMC, BUSBC)
- Release IP address at shutdown post-erasure, allowing address to be re-used for another layer of security

CONFIGURABILITY & AUTOMATION

- Customize erasure software to fit specific needs
- Customize input fields in erasure reports
- 4 levels of process automation: workflow, manual, semi-automatic, automatic
- Ability to execute customized workflows defined on the Blancco Management Portal; workflows can be executed locally or remotely and automate the processing across all company assets
- Configure/limit time erasures can take to maximize efficiency
- Ability to communicate back and forth with an Asset Management System or other external system

HARDWARE SUPPORT

- Erase data securely from PCs, laptops, servers and storage environments based in x86 and x86-64 architectures
- BIOS & UEFI machines including Intel-based Macs, Apple T2 and Secure Boot including support for expired functionalities
- IDE/ATA, SATA, SCSI, SAS, USB, Fibre Channel, FireWire hard disk drives of any size/blocksize
- SATA and SAS solid state drives of any size/blocksize
- eMMC drives of any size/blocksize
- NVMe drives of any size/blocksize
- SAS, SCSI, ATA and NVMe self-encrypting drives

AUDITING

- Verification algorithms to automatically check the overwritten patterns
- Hexviewer provides fast visual verification of the erasure for compliance
- Generate post-processing labels per asset with Blancco Label Printer
- Reports offer tamper-proof reporting and can include a customized digital signature
- Embed reports in the drives for a fast erasure audit
- Search and export reports via APIs

LANGUAGE SUPPORT

- English, German, Japanese (inc. written characters), Chinese, Russian, French, Taiwanese, Italian and Portuguese, Slovak, Polish, Korean (inc. written characters) and Hungarian
- Up to 20 different keyboard layouts supported

STANDARDS SUPPORTED

- 508 (US federal gov): provides accessibility to visually-disabled users with audio notifications and text-to-speech functions
- BSI-GSA (German gov): equivalent to NIST for German public sector / emergency services / military)
- 802.1X: network authentication standard