Blancco Drive Eraser

Permanent Data Sanitization for HDDs/ SSDs in PCs, Laptops and Servers

Why Blancco

Blancco is the industry standard in data erasure and mobile device diagnostics software. Blancco data erasure solutions provide thousands of organizations with the tools they need to add an additional layer of security to their endpoint security policies through secure erasure of IT assets. All erasures are verified and certified through a tamper-proof audit trail, and the product has the ability to erase to 25+ standards.

Blancco data erasure solutions have been tested, certified, approved and recommended by 15+ governing bodies and leading organizations around the world. No other data erasure software can boast this level of compliance with the rigorous requirements set by government agencies, legal authorities and independent testing laboratories.

Blancco Drive Eraser is a robust data sanitization solution for PC, laptop, server and storage environments.

The pressure on organizations to build and maintain robust security policies and safeguard their sensitive data continues to increase. With Blancco Drive Eraser, organizations can add an extra level of protection to their endpoint security policies by permanently erasing sensitive data from HDDs and SSDs, including NVMes, in desktop/laptop computers and servers. Our secure overwriting process sanitizes data on a wide variety of storage devices so you can safely resell, re-purpose or dispose of these assets at end-of-life.

Key Benefits

Secure, Certified & Patented* Overwriting Methods

- Guarantee your data has been erased from any drive, from HDDs to SSDs and NVMes, including self-encrypting drives

Flexible Deployments to Meet Your Specific Requirements

- Fully automate the erasure process or across on-premise or remote environments
- Select from variety of licensing options, such as local control with HASP dongles, standalone images—offline licensing via USB or centralized control through the Blancco Management Console or Blancco Cloud
- Deploy locally (CD, USB), via the network (PXE), preinstall (Windows, Linux), or via iLO, iDRAC, Cisco UCS, Intel AMT or install locally (appliance mode)
- Customize as many ISOs as you choose, with the ability to create different templates based on use cases, locations and business needs
- Leverage workflows to automate every step of your erasure process

Maximize IT Security Compliance

- Provide a tamper-proof audit trail for all assets with a digitally-signed Certificate of Erasure for every erasure instance

*Patent No 9286231

blancco

Technical Specifications

ERASURE

- Locally or remotely controlled data erasure via the Blancco Management Console
- 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 Console):
  - 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 Console
- 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”)

DEPLOYMENT

- Blancco Drive Eraser is platform independent
- Local control with HASP dongles, standalone images, or centralized control through the Blancco Management Console or Blancco Cloud
- Deploy locally (CD, USB), via the network (PXE), preinstall (Windows, Linux), or via iLO, iDRAC, Cisco UCS, Intel AMT or install locally (appliance mode)

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
- Hot swap capabilities

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 communicate back and forth with an Asset Management System or other existing system (“Two-Way Communication”) on asset and drive level
- Ability to execute customized workflows defined on the Blancco Management Console or Blancco Cloud; workflows can automate processing across all company assets

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
- 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 or ATA self-encrypting drives

AUDITING

- Verification algorithms to automatically check the overwritten patterns
- Hexviewer provides fast visual verification of the erasure for compliance
- 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, Chinese, Russian, French, Taiwanese, Italian and Portuguese, Slovak, Polish and Hungarian
- Up to 20 different keyboard layouts supported