blancco

Blancco Drive Eraser for ITAD

Market-leading Data Sanitization for HDDs/ SSDs in PCs, Laptops, Chromebooks, 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.

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.

View Our Certifications

Request Your Free Trial

Get Started Today

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

Organizations concerned with data security and compliance are feeling the pressure to build and maintain robust security policies, safeguard their sensitive data, and dispose of their assets responsibly.

With Blancco Drive Eraser, organizations can add an essential level of protection to endpoint security policies by permanently erasing sensitive data from HDDs and SSDs, including NVMes in desktop/laptop/Chromebook computers and servers.

Our secure overwriting process sanitizes data on a wide variety of storage devices, offering organizations the means for safe re-sale, re-purposing or disposal of data assets at end-of-life.

Key Benefits

- ☑ Guarantees your data has been erased from any drive, from HDDs to SSDs and NVMEs, including self-encrypting drives
- ☑ Receive a tamper-proof audit trail for all assets, with a digitally-signed Certificate of Erasure for each erasure instance
- ☑ Process loose drives and Chromebooks with ISO Image Installer, including a report viewer to track progress and specifically designed key diagnostics
- ☑ Increase efficiency and minimize manual processes with Intelligent Business Routing (IBR) workflows (including offline)
- ☑ Generate post-processing labels per asset with Blancco Label Printer
- ☑ Implement hardware tests to assist with diagnostics
- ☑ Full NIST compliance with support for NIST Purge and Clear, featuring full records of unsupported incidents for transparent auditing
- ☑ Support for internal drive erasure commands

blancco

Technical Specifications
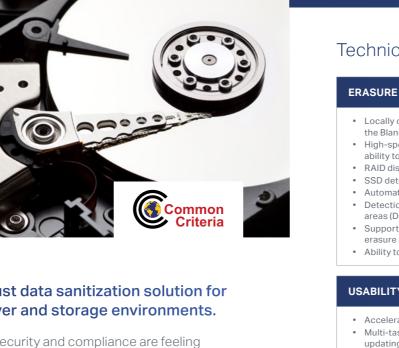
ERASURE	MINIMUM SYSTEM REQUIREMENTS
• Locally or remotely controlled data erasure via the Blancco Management Console • High-speed, simultaneous erasure of multiple drives, including the ability to customize drive batch sizes and drive speed thresholds • RAID dismantling and direct access to the underlying 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	• 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	REPORTING
• 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	• 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	HARDWARE DETECTION & DIAGNOSTICS	CONFIGURABILITY & AUTOMATION
• 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)	• 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)	• 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 external system (IBR workflows) on asset and drive level • Fine-tune erasure process (speed/time limit, configurable conditions, etc.) • Execute customized workflows defined on the Blancco Management Console or Blancco Cloud, locally or remotely; automate the processing across all company assets

HARDWARE SUPPORT	AUDITING	LANGUAGE 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, ATA and NVMe self-encrypting drives	• 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	• English, German, Japanese, Chinese, Russian, French, Taiwanese, Italian and Portuguese, Slovak, Polish and Hungarian • Up to 20 different keyboard layouts supported