

ThinkShield

Security Software Solutions

DRIVE ERASER. FOR ENTERPRISE. SIMPLE.

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

Powered by



Reduce Risk.
Increase Efficiency.
Be Sustainable.™

Smarter
technology
for all

Lenovo

MARKET-LEADING DATA SANITIZATION FOR HDDS/SSDS IN PCS, LAPTOPS, CHROMEBOOKS AND DRIVES

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

With ThinkShield Drive Eraser powered by Blancco, organizations have that market-leading method; scalable software providing essential protection by permanently erasing sensitive data from data centers, servers, HDDs and SSDs (including NVMe in desktops/laptops/Chromebooks), with IBR workflows enabling automated erasure even while devices are disconnected from networks.

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 NVMe (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
- ☑ Speed up erasure with automated processes and progress displays
- ☑ 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, integrated into Drive Eraser
- ☑ 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
- ☑ Generate post-processing labels per asset with Blancco Label Printer
- ☑ Helps improve your CSR / ESG standing

TECHNICAL SPECIFICATIONS

ERASURE		MINIMUM SYSTEM REQUIREMENTS	
<ul style="list-style-type: none"> 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 		<ul style="list-style-type: none"> 1 GB RAM memory in most cases (2 GB for PXE booting) Local erasure: <ul style="list-style-type: none"> 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): <ul style="list-style-type: none"> Ethernet NIC DHCP Server running on local network for PXE booting, remote erasure and report collection 	
USABILITY		REPORTING	
<ul style="list-style-type: none"> 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 		<ul style="list-style-type: none"> 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") 	
DEPLOYMENT	HARDWARE DETECTION & DIAGNOSTICS	CONFIGURABILITY & AUTOMATION	
<ul style="list-style-type: none"> Blancco Drive Eraser is platform independent Local control with HASP dongles, standalone images, or centralized control through the Blancco Management Portal 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) 	<ul style="list-style-type: none"> 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) 	<ul style="list-style-type: none"> 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 or Blancco Cloud; 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 	



TECHNICAL SPECIFICATIONS CONT.

HARDWARE SUPPORT	AUDITING	LANGUAGE SUPPORT
<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• English, German, Japanese, Chinese, Russian, French, Taiwanese, Italian and Portuguese, Slovak, Polish and Hungarian• Up to 20 different keyboard layouts supported

Ready for a demo?

Talk to your local Lenovo representative to see first hand how ThinkShield Drive Eraser increases data protection across the widest variety of drives and data storage scenarios.



Learn more at
cyber@Lenovo.com

Products and offers subject to availability. Lenovo reserves the right to alter product offerings and specifications, at any time, without notice. Lenovo makes every effort to ensure accuracy of all information but is not liable or responsible for any editorial, photographic or typographic errors. Images are for illustration purposes only. For full Lenovo product, service, and warranty specifications, visit www.lenovo.com. Lenovo and the Lenovo logo are trademarks or registered trademarks of Lenovo. Other company, product and service names may be trademarks or service marks of others.