Eurosoft
computer reliability solutions

ZeroData™ Windows® V1.6.1.0311

Eurosoft ZeroData™ Windows® permanently, safely and securely removes all of the data on storage devices, exceeding the data destruction levels specified by major organisations and Government bodies for PC reassignment, upgrades, refurbishment, ITAD, recycling and donation.

Increased storage of sensitive personal and commercial data along with the increase in reused or recycled IT equipment, has driven the need for permanent data erasure of hard drives and other storage devices – ZeroData Windows is fast and it's indispensable.

Awesome, Eurosoft only reminders…

Erases more drives than most…*regardless of drive type…legacy or UEFI*…from only one Windows-based application. First 12N Smart QR label. Even perform Purge erase on NVMe drives connected to iRST.

| ZeroData™ Windows® features	Benefits for You
New Command Switch option	No need for third party tools, it is now possible to include the contents of specific disk sectors to erasure logs and reports for inspection using / LDS switch option. E.G. by adding "/LDS1" the bootable fingerprint of the erased drive is added to the erasure logs and reports.
New Report Features	Save time, avoid errors, improve your audit trail. Automatically add both the erasure operator and supervisor names to PDF reports. Reports can be signed manually or automatically by including signature graphic files, automating the process of signing erasure reports.
Enhanced User Interface	See at a glance erasure status. When a drive is being erased the user interface colour is changes to yellow-orange. When completed, the colour will change to either green for to indicate the drive has been erased successfully or red if erasure failed.
Enhanced ATA and SCSI Sanitize	Improved compatibility of ATA and SCSI Sanitize command extends use of these erasure methods to a wider variety of ATA and SCSI storage devices.
Enhanced SCSI Format Unit and NVMe Format	Improved compatibility of SCSI Format Unit and NVMe Format extends use of these erasure methods to a wider variety of SCSI and NVMe storage devices.
Updated disk detection library	Added support for new disk models and new RAID card models.

Eurosoft
computer reliability solutions

Product Announcement
ZeroData™ Windows®
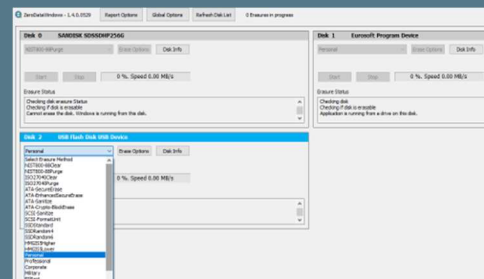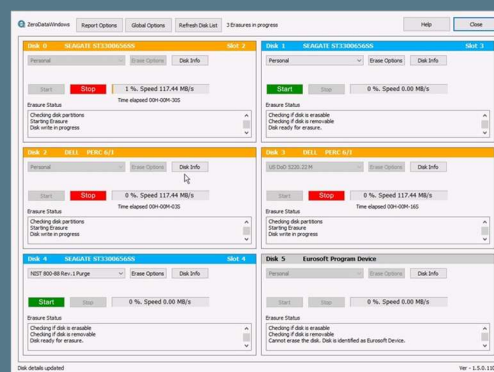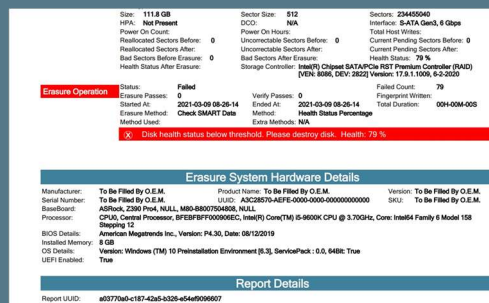
ZeroData™ Windows® Previous Release Highlights

Extra erasure options for NIST 800-88 Revision 1 and ISO/IEC 27040 Standards	ZeroData Windows already supports "optional erasure behaviour" described in NIST 800-88 Rev. 1 and ISO/IEC 27040:2015 standards by executing the command line switch "/nierem 0". Now with an additional zero overwrite pass applied to the disk if the erasure is carried out by a firmware command. This option gives the necessary means of ensuring complete data erasure even if the firmware command is not working as advertised by disk manufacturer.
BSI-GS and BSI-GSE erasure methods	Meet and exceed erasure guidelines set out by the **German Federal Office for Information Security (BSI)**. Offering more erasure methods, BSI-GS and BSI-GSE are based on BSI-TL03423, which outlines the requirements for erasure of classified documents from physical storage devices. Also extended to address NVMe SSD disks. BSI-GS and BSI-GSE are recognized as common erasure standards throughout the European Union and the rest of Europe.
Industry first – create **12N* Smart Labels conforming to ANSI/MH10 Standards**	ZeroData Windows Reporting Console prints RLA 12N QR Code Labels! Eurosoft as a member of Reverse Logistics Association and ZeroData Windows is the first data erasure solution that prints data erasure information according to 12N Smart QR code label standards, communicating erasure history across the reverse logistics supply chain. Stores detailed information with 4000 characters instead of 500 in a single label.
Label printing	ZeroData Windows Reporting Console prints disk labels that can be applied to surface of the disks or to surface of protective disk bags.
SSD optimization	Firmware methods are the preferred erasure methods for solid state disks, however these erasure methods cannot be executed every time. In cases where SSD disks are erased using regular overwrite methods, the erasure speeds for write operations may be low. Performing SSD Optimization before data erasing can have a positive effect on regular overwrite speeds, resulting in quicker drive erasure.
Command line drive health parameters	Added options to fail disks based on reported health percentage result based on the number of bad and weak sectors on the disk – hard drives and solid state drives. All drives' condition can be established to decide if a disk is worth erasing or not at the beginning of erasure operation and whether a disk can be safely reused after disk erasure operation or not.

Signed Erasure Reports

Print RLA 12N Labels

Yes, you need secure, permanent data erasure… Yes, you need to do it fast… Yes, you need secure reports of all data erasure… Do the products you use meet your demands? *Call us now* to discuss how you can save more money and time using ZeroData Windows. Or go to the website to try a package for yourself.

Conforming to **GDPR, government, military, NIST and ISO/IEC standards** you can trust ZeroData Windows to provide the proof you need of permanent erasure demanded by compliance standards worldwide.

1st place – Longest running PC diagnostic company – 40 years – with spectacular results from our **Microtopology** memory testing and the original 'self-boot' capability in 1986!

Eurosoft (UK) Ltd
Tel +44 (0)1202 297315
Fax: +44 (0)1202 558280
www.eurosoft-uk.com

Eurosoft (US) Inc.
Tel +1 (712) 255-7483
Fax: +1 (866) 615-9384
www.eurosoft-us.com

Microsoft Partner
Silver Independent Software Vendor (ISV)

Level 1 and II certified ASCLD/LAB International accredited forensic testing laboratory (ISO/IEC 17025:200).

Note: Windows PE v1.x contains a security feature that will cause end user's systems to reboot without prior notification to the end user after 24 hours of continuous use. Windows PE v2.x contains a security feature that will cause end user's systems to reboot without prior notification to the end user after 72 hours of continuous use.