Our best-in-class secure data erasure tool gives you the advanced security features to protect the integrity of your data across all your devices. WipeDrive Enterprise 9 takes secure erasure to the next level with key improvements in security, efficiency and hardware support.

What is WipeDrive?

When a Windows or Linux system saves a file, it does two things: it creates an entry for the file in the Master File Table, which functions as a sort of 'table of contents' for the drive, and it saves the file data itself onto sectors of the hard drive. If a file is deleted using the Recycle Bin, the file is not actually removed. The file's entry in the Master File Table is deleted, but the data itself still remains intact on the hard drive. The space that it occupies is marked for use, letting the system know that the space is available for new files to be written to. Unless new data is written to the space held by the deleted file, the file still exists on the drive in its original state.

Any number of file recovery programs can easily look through the drive and find remnants of the file and put it back together, making it as if it was never deleted in the first place. The only way to truly delete a file is to overwrite it with other information.

The primary purpose of WipeDrive is to securely overwrite all data to make any type of data recovery impossible and document the process to comply with all applicable corporate and government regulations.

What are WipeDrive's Key Features?

UPDATED HARDWARE SUPPORT

WipeDrive now runs in both Linux and WinPE providing the best hardware support. With support for the latest NVMe SSD drives, WipeDrive 9 is ready for the next generation of drives. The world's first secure SSD wipe pattern which supports all SSD types regardless of manufacturer. WipeDrive 9 also supports the latest internally mounted M.2 drives.

SECURE REMOVAL OF HPA AND DCO

A host protected area (HPA), sometimes referred to as hidden protected area, is an area of a hard drive that is not normally visible to an operating system. A Device Configuration Overlay (DCO) is a hidden area on many of today's Hard Drives (HDDs and SSDs). Usually when information is stored in either the DCO or HPA, it is not accessible by the BIOS, OS, or the user.

As part of the wipe process WipeDrive securely removes and overwrites all data contained in HPAs and DCOs. WipeDrive also purges data when DCO's are locked.

SECURE ERASE OPTION

A modern hard drive comes with many spare sectors. When a sector is found to be bad by the firmware of a disk controller, the disk controller remaps the logical sector to a different physical sector.

The ANSI T-13 committee which oversees the Advanced Technology Attachment (ATA) interface

specification and the ANSI T-10 committee which governs the Small Computer System Interface (SCSI) specification have incorporated into their standards a command feature known as Secure Erase (SE). This command completely erases all remapped disk sectors (sectors that the drive no longer uses because of physical malfunctions).

WipeDrive uses the SE command as part of its NIST 800-88 REV 1 wipe process, to ensure the erasure of remapped sectors.

DETAILED AUDIT LOGGING

Documenting the secure data destruction process is a requirement for most Government agencies, companies involved in health care and the financial sector.

WipeDrive creates an audit log documenting every necessary detail to comply with all major regulations including DoD 5220.22-M, HIPAA, SOX, GDPR, Fiserv and others.

What are WipeDrive's Certifications?

WipeDrive is the only disk-wiping technology that meets NIAP's EAL 2+ Standard. WipeDrive has passed rigorous tests performed by Common Criteria on IT security and efficacy. WipeDrive recently passed the National Cyber Security Centre rigorous assessment standards.

LIST OF WIPEDRIVE CERTIFICATIONS

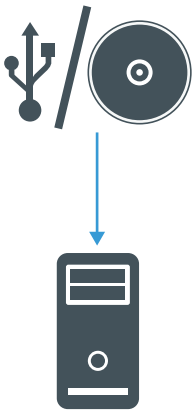
- NIAP EAL 2+
- NCSC (formerly CESG)
- NYCE Certifcation NMX-I-9126/02
- ADISA Certified for SSD
- US DoD 5220.22-M
- NIST 800-88 REV 1 Compliant
- Meets the Common Criteria Evaluation and Validation Scheme
- HIPAA
- FACTA standards
- Sarbanes-Oxley
- US Army AR380-19
- US Air Force System Security Instruction 5020
- US Navy Staff Office Publication P-5329-26
- US National Computer Security Center TG-025
- NATO NIAPC
- GB HMG Infosec Standard #5 Baseline
- GB HMG Infosec Standard #5 Enhanced
- German VSITR
- Australian Defense Signals Directorate ACSI-33(X0-PD)
- Australian Defense Signals Directorate ACSI-33(X1-P-PD)
- Canadian RCMP TSSIT OPS-II Standard Wipe
- CIS GOST P50739-95
- CSEC ITSG-06

Deployment Options

- All drives are wiped in accordance to NIST 800-88 REV 1 specification or any of WipeDrive's supported overwrite patterns. Customers may also create a custom pattern if needed.
- Software is run from a USB drive, CD or EXE Windows Install File.
- Multiple drives can be wiped simultaneously within a single device.
- Full audit trail compliant with all major data deletion standards (HIPAA, GDPR, Fiserv, SOX, DoD, GLB, etc.).

CD/USB

Wipe individual computers

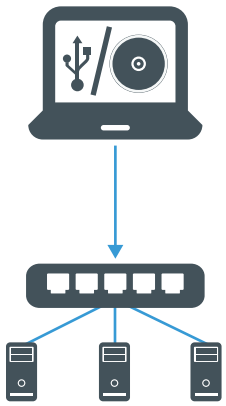


Process

- Program initiated via USB drive or CD.
- Selected storage drives are wiped according to selected or pre-configured settings.
- Audit log generated. Reports can be sent via email, stored on a network, saved to an attached drive, or stored in a database.

PXE NETWORK

Many at once at one location

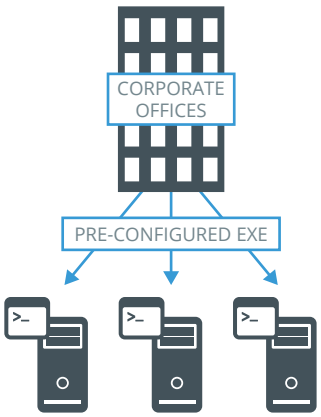


Process

- Program initiated on a PXE server via USB drive or CD.
- Computers booting into the PXE server automatically start the wiping process according to pre-configured settings. Hundreds of computers can be wiped at once.
- Audit log generated. Reports can be sent via email, stored on a network, saved to an attached drive, or stored in a database.

REMOTE WIPE

Many at a time, many locations



Process

- A pre-configured executable is sent from a centralized IT staff to any computer with administrative access.
- Remote computers start the wiping process without any local interaction.
- Audit log generated. Reports can be sent via email, stored on a network, saved to an attached drive, or stored in a database.

What are WipeDrive's System Requirements?

WIPE VIA CD OR USB

Running WipeDrive via USB or CD is normally a good choice when the number of computers to be wiped are small as the USB/CD must be inserted and booted on each system.

SYSTEM REQUIREMENTS

- All versions of Windows Vista, 7, OS/2, PC-based, 8, 8.1, and 10, Linux, Unix and Intel-based Mac systems.
- Any type of hard drive (IDE, SCSI, SATA, SSD).
- USB port (CD-ROM can also be used)
- 256 MB RAM

WIPE VIA PXE NETWORK

Running WipeDrive via PXE is normally a good choice when the number of computers to be wiped is large. Because the server controls the process, it is not necessary to attach monitors, mice or keyboards to workstations. The progress for each individual system is displayed on the server, the only requirement is that the boot priority for the system be set to 'Network Boot'.

Depending on the hardware used WipeDrive can support hundreds of systems simultaneously.

SYSTEM REQUIREMENTS

Computer designated to be the server (will not be wiped) with at least the following hardware:

- Pentium III-class processor or better
- 2 GB RAM
- USB port or CD-ROM drive
- Network card
- If using Cloud activation or logging outside the PXE network a second network card is required.

One or more machines, referred to as the 'clients', with at least the following hardware:

- Pentium-class processor or better
- 1 GB RAM
- Network card
- Network switches and cabling to configure all of the machines (server and clients) to be in the same network.

WIPE REMOTE COMPUTERS VIA .EXE

This method is best if your are wanting to securely wipe a computer not readily accessible. Using the WipeDrive application you can wipe a computer remotely one of two ways; through Remote Desktop Connection or through PsExec. This walkthrough will cover both. Before proceeding with this option please note the required criteria necessary for this to work.

REQUIRED FOR REMOTE DESKTOP CONNECTION

- Computer Name
- User
- User Password (a password MUST exist)

REQUIRED FOR PSEXEC

- PsExec: http://technet.microsoft.com/en-us/sysinternals/bb897553.aspx
- Grant permissions through Regedit (See PSExec setup page 10 of the Enterprise Manual)
- Computer Name
- User
- User Password (a password MUST exist)

WIPEDRIVE BOOT VIA .EXE

Running WipeDrive via EXE is normally a good choice when the number of computers to be wiped is large and the systems are spread over multiple locations.

The .EXE build is a scripted build of WipeDrive that can be run over a network on any system which you have administrative rights.

SYSTEM REQUIREMENTS

- Computer running Windows 98, NT, 2000, 2003, XP, Vista and 7. 8, 8.1 and 10
- 512 MB Free Hard Drive Space
- 1 GB RAM