Phoenix SecureWipe™

Datasheet

What is Phoenix SecureWipe?

Phoenix SecureWipe™ is a BIOS firmware product that securely erases SSD, HDD and other mass storage devices. It erases all data and partitions independent of the operating system and can be invoked locally via hotkey, or via remote control using OEM developed management solutions.

Why Use Phoenix SecureWipe?

- Protect sensitive data when recycling or disposing of a computing device
  - Consumers – identity theft, financial information, family photos
  - Enterprise – intellectual property and financial information
- Simple and easy to use without the need of any third party tools
  - No extra boot devices required to run specialized software
- Works on any x86 PC that uses Phoenix UEFI firmware
  - No dependencies on OS-specific software solutions
- Cost effective and built into the product before shipping to users
  - Resides in the firmware and cannot be accidentally removed by users

Selectable Erase Methods

- ATA and NVMe Secure Erase
- OPAL Password/PSID Revert
- US DoD 5220.22-M, [3 passes + verify]
- Single Pass Zeros, [1 pass]
- US Navy & Air Force, [3 passes + verify]
- British HMG Infosec Standard 5, Enhanced, [3 passes + verify]
- German VSITR, [7 passes]
- Russian GOST P50739-95 Level 1, [1 pass]
- Russian GOST P50739-95 Level 4, [1 pass]
- RCMP TSSIT OPS-II, [7 passes]
- CSE Canada ITSG-06 (Unclassified), [3 passes]

Packaging Options

- **Standalone:** run from UEFI Shell or a Utility Toolset with the default text-based Phoenix SecureWipe UI.
- **Integrated:** launched on-demand during POST via Hotkey, Boot Menu, or Setup.
- **Custom:** launched based on custom policies with a custom manufacturer-designed and branded UI.

Additional Features

- Binary distribution, easily integrates into UEFI firmware volumes, standard launch by UEFI drivers/application.
- Standard EDK II style code, compatible with both Phoenix and non-Phoenix EDK II UEFI firmware products.
- Block IO device support: FDD, HDD, SSD, NVMe, SD, eMMC, USB drives, SCSI drives (with UEFI OPROM), RAID (with UEFI OPROM).
- Works with other Phoenix products such as launching from HTTPs.
- Supports selective erasure of partitions exposed by the firmware, regardless of the underlying file system: UEFI GPT, NTFS, FAT32, etc.
- Includes EFI executable that can be launched from bootable media like other third party solutions.
- SDK wrapper provides customized interfaces.

What Makes Phoenix SecureWipe a Great Solution?

- Completely and securely erase the entire HDD/SSD
  - Built-in Windows/Linux OS features cannot erase the entire HDD/SSD
  - Phoenix SecureWipe™ built into the firmware has full access to the entire HDD/SSD
- Third party solutions to securely recycle computing devices are complicated and expensive With Phoenix SecureWipe™:
  - There is no need to download specialized tools and utilities
  - There is no need to be "technically savvy" or create special boot disks with complicated software
  - The erase utility can be invoked by a simple key press or a few mouse clicks
  - Enterprise requirements can be easily met using custom remote management solutions

Sample Uses

- Recycle consumer and enterprise PCs – a simple, easy and cost-effective method to securely wipe sensitive data before selling or disposal
- Upgrading to a new hard drive – copy the contents from an old hard drive to a new one and securely wipe the old hard drive before disposal
- Enterprise Management Services – using third party solutions, trigger a remote wipe of sensitive data if the device is lost or stolen

Want to learn more about Phoenix SecureWipe?

Send us an email at sales@phoenix.com

phoenix technologies