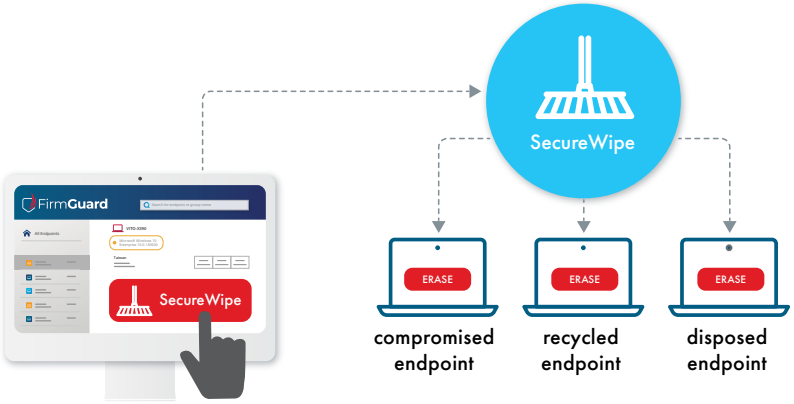
SOLUTION BRIEF

FirmGuard® SecureWipe

REMOTELY AND SECURELY ERASE ENDPOINT DRIVES (HDD/SSD)

What is SecureWipe?

SecureWipe is a FirmGuard feature that securely erases endpoint HDD, SSD, and other mass storage devices. It is triggered remotely from the FirmGuard Portal and forensically erases all data and partitions independent of the operating system (OS). A Certificate of Erasure (CoE) is also provided.



Benefits of SecureWipe

- Certificate of Erasure (CoE) provided for each wipe.
- Erase command is invoked remotely from a secure portal (no physical access to endpoint required).
- Wipe is performed at the UEFI firmware level, no dependence on operating system (OS).
- Multiple erase methods to choose from which support efficacy and/or compliance requirements.
- No specialized tools or utilities required.
- Selectively wipe specific drive(s) or individual partitions on a drive.

Supported Erase Methods

+ ATA and NVMe Secure Erase

Drive manufacturer provided method that is highly effective because the drive manufacturer understands the drive architecture better than anyone else.

+ Single Pass Zeros

Overwrites all data on the drive using a single pass of binary zeroes.

+ DoD 5220.22-M

US Department of Defense (DoD) developed method. Overwrites all data on the drive three times in succession with verification.

+ TCG Opal PSID Revert

Only works on TCG Opal compliant self-encrypted drives. Resets the cryptographic keys to factory default which effectively renders the drive unreadable.

+ Other Supported Methods Include:

- British HMG Infosec Standard 5, Enhanced
- CSE Canada ITSC-06
- German VSITR

phoenix technologies

SecureWipe

Use Cases

SecureWipe can be used for a variety of different scenarios or use cases.

- **Compromised endpoint** - If an endpoint has been lost or stolen, a FirmGuard adminstrator can immediately issue a wipe request and the next time the endpoint is detected the designated drive(s) will be securely erased.
- **Recycle an endpoint** - Before ownership of an endpoint is transferred, a FirmGuard administrator can easily and securely erase all previous data to ensure no information is compromised.
- **Endpoint disposal** - Before an endpoint is retired, a FirmGuard adminstrator can easily and securely erase all previous data to ensure that no information is compromised.

How Else Can an Endpoint be Wiped?

There are various other ways to erase the contents of an endpoint's hard drive, but almost all of them require physical access to the endpoint. In addition, many of them are cumbersome and require some level of technical sophistication.

OS File Delete - This is the worst because just deleting a file doesn't permanently erase it. The OS only removes a pointer to each file, leaving all the bits in place. The files are almost trivial to recover with software.

Software Utility - There are many programs (e.g., Parted Magic) to wipe a drive. They all however require physical access to the endpoint and often need technical expertise to, for example, setup a special boot disk.

UEFI BIOS Secure Wipe - This is a secure way because it doesn't rely on the OS and many OEMs provide a mechanism to enable this from a setup screen.

In some sense, this is exactly what SecureWipe does but with one major difference: ***no one has to be at the endpoint to execute the secure wipe.***

FirmGuard

Certificate of Erasure

This document is provided to ACME Corporation to certify that the Phoenix® SecureWipe™ program executed the erasure method(s) on the material(s) listed on the form below.

Data Erasure Performed By: FirmGuard SecureWipe
Endpoint Computer Name: DELL-LAT-3520-2
Endpoint Model: Latitude 3520
Time Issued: 08/14/2024 | 20:30 UTC
Time Acknowledged: 08/14/2024 | 20:30 UTC
Performed By: John Smith (johnsmith)

Drive	Erase Method	Serial Number	Size
HITACHI HTS725050A7E630	Single Pass Zeros	TF1500Y9GX9BTB	536.99 GB

SAMPLE

Any Certificate of Erasure provided via the FirmGuard® platform is subject to the Terms and Conditions, and other policies, of the FirmGuard® platform and the SecureWipe FirmGuard® module found at www.firmguard.com or successor website as of the date listed above ("Policies"). Phoenix Technologies does not make any representation or warranty of any kind regarding the completeness of any erasure or destruction beyond those explicitly recited in the Policies.

SecureWipe™ is designed to assist organizations in meeting compliance requirements related to data sanitization and protection, including but not limited to: ISO/IEC 27001, ISO/IEC 27002, NIST SP 800-53, NIST SP 800-88, NIST Cybersecurity Framework, GDPR, HIPAA Security Rule 45 CFR 164.310(d)(2), PCI DSS, DoD 5220.22-M, and FISMA. Users are responsible for ensuring full compliance with these standards.

phoenix technologies
2105 S. Bascom Avenue,
Suite 316 Campbell, CA 95008.3295

After each wipe, a Certificate of Erasure (CoE) is produced and stored in the portal to document the details of the wipe. A CoE can be crucial for compliance with data protection regulations like GDPR, HIPAA, or CMMC, as it serves as proof that sensitive data has been handled appropriately and securely destroyed. The CoE contains relevant information such as which specific endpoint and drive was erased, the erase method used, the administrator that performed the wipe and more.

SecureWipe helps maintain ISO and NIST compliance

SecureWipe helps FirmGuard customers, and their clients comply with a variety of industry standards. The list below provides a detailed breakdown of compliance with specific standards including individual clauses within the standard.

ISO 27001 Clause 8.2.3 (Management of Removable Media)	**SecureWipe** aids in managing and sanitizing removable media, reducing risks associated with data breaches.
ISO 27001 Clause 8.3.2 (Disposal of Media) **NIST SP 800-53 MP-6** (Media Sanitization)	**SecureWipe** ensures that all media is securely wiped to prevent data leakage upon disposal.
ISO 27001 Clause 15.1.2 (Dealing with Security Breaches)	**SecureWipe** is an essential tool for securely dealing with breaches involving data on discarded media.
ISO 27001 Clause 16.1.4 (Assessment of Information Security Incidents)	**SecureWipe** can be leveraged with mobile device management to remotely wipe systems that may have been stolen or compromised.
ISO 27001 Clause 18.1.3 (Protection of Records)	**SecureWipe** facilitates the secure deletion of records, complying with data protection regulations.
NIST SP 800-53 PE-16 (Delivery and Removal)	**SecureWipe** ensures secure removal of data from devices before delivery or disposal, aligning with NIST's physical security controls.
NIST SP 800-88 (Guidelines for Media Sanitization)	**SecureWipe** adheres to NIST guidelines for secure media sanitization by offering dozens of military grade forensic wiping algorithms.
NIST Cybersecurity Framework DE.AE-3 (Event Detection)	Ensure that data destruction events are properly detected and logged with **SecureWipe**.
NIST Cybersecurity Framework PR.IP-6 (Data Destruction)	**SecureWipe** exceeds NIST's recommendations for functionality that irreversibly destroys data.

Learn how FirmGuard can help you remotely secure, configure and update UEFI BIOS firmware. Book your 15 minute demo today.

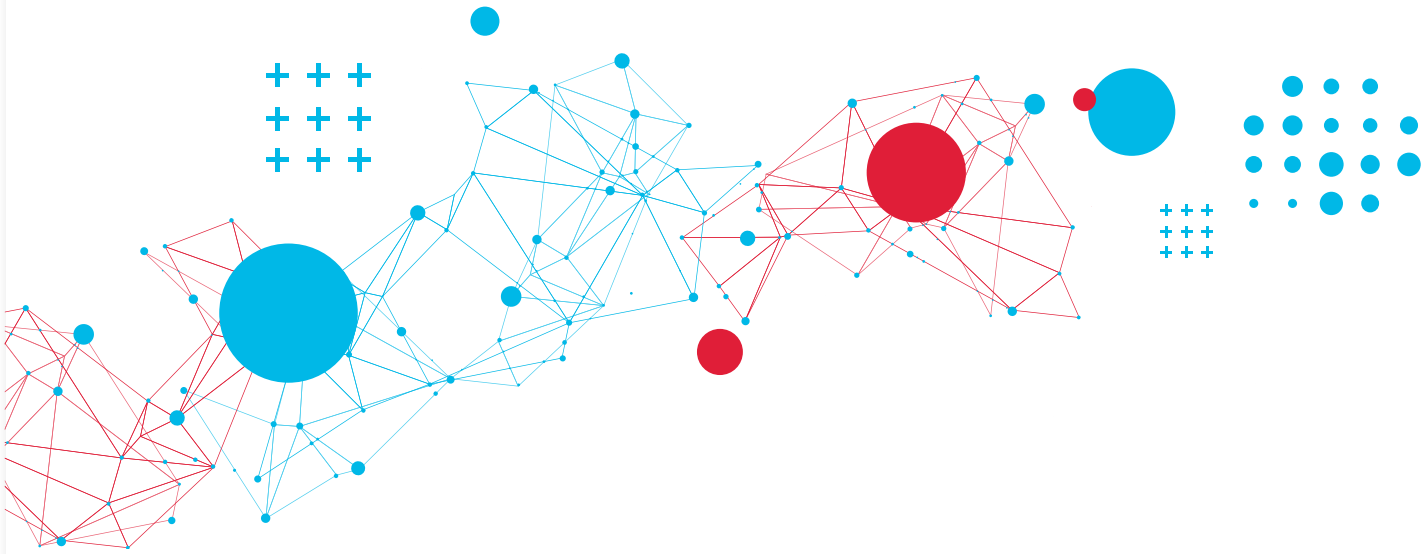
firmguard.com/demo

phoenix technologies

rev. 02.10.25

Comparison Chart

	Windows Reset	SecureWipe	Physical Destruction
NIST 800-88 Definition	**Clear**	**Purge**	**Destroy**
No Data Recoverable		✓	✓
Wipe Stolen Endpoint		✓	
Execute Wipe Remotely	✓	✓	
Certificate of Erasure/Destruction Provided		✓	✓
Low Cost	✓	✓	
Can Reuse Endpoint	✓	✓	
Endpoint Never Leaves Client Office	✓	✓	



Learn how FirmGuard can help you remotely secure, configure and update UEFI BIOS firmware. Book your 15 minute demo today.

firmguard.com/demo

phoenix technologies

rev. 02.10.25