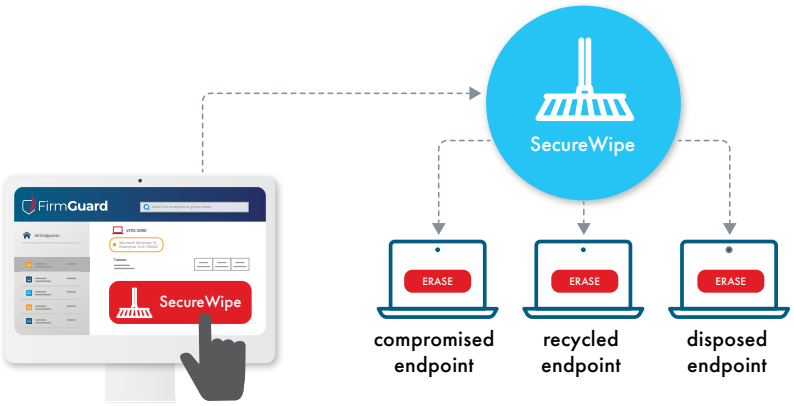
SOLUTION BRIEF

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).



Benefits of SecureWipe

- 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

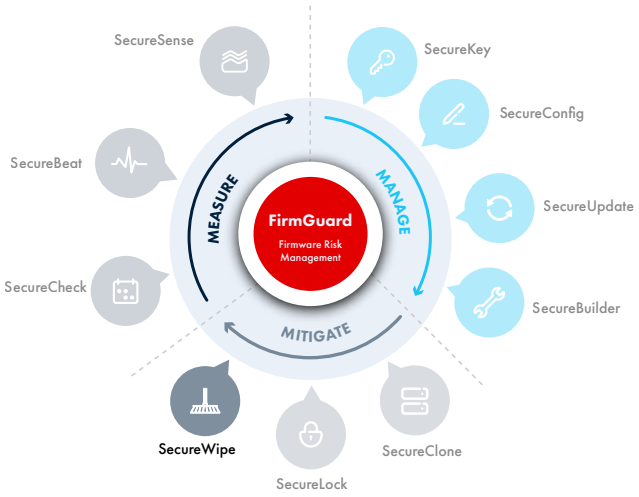
Only works on TCG Opal compliant self-encrypted drives. Resets the cryptographic keys to factory default which effectively renders the drive unreadable.

+ Other Supported Methods Include:

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

phoenix technologies

SecureWipe



Mitigate Features

SecureWipe is one of the key features in the FirmGuard mitigate suite. The other two mitigate features are SecureClone and SecureLock which backup endpoint data and temporarily disable the use of an endpoint, respectively.

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.***

For more details, please
contact your Phoenix representative
or email **firmguard@phoenix.com**.

phoenix technologies

rev. 01.02.24