



OEM Tools: Data Wiping Issues And Weaknesses

Summary

Many SSD, NVMe and hard drive manufacturers provide OEM Tools for formatting, partitioning and secure erasure. Though many groups on the internet provide support for OEM Tools as an alternative to commercial data wipe solutions, this paper explains why OEM tools fail to be a practical replacement and addresses their major issues. v

OEM DRIVE TOOLS

OEM tools are designed to manage and erase a manufacturer's own drives. The OEM tools provide a list of functions, like format, partition and erase. Though each OEM tool is unique, most of the tools provide a cryptographic key removal and secure erasure of all the data on the drive. The erasure is secure if the manufacturer supports the ATA Secure Erase or Sanitize disk commands, which most do. Some manufacturer's OEM tools offer the option to revert a drive back to its original state, remove OPAL and eDrive protection, and even remove drive passwords.



OEM tools may seem like a viable alternative to data erasure software, but they have major weaknesses that cause them to be ineffective for the corporate and government environment. The major issue is the OEM tools are not certified by an outside party. The tools do not receive review, testing and verification that they erase data to any standard.

The OEM tools provide custom erasure patterns, but do not provide the specific NIST and DoD 5220.22M overwrite patterns. The OEM tools fail to provide verification of the erasure and on some drives, you must boot from the BIOS or recovery partition to start the deletion. Labor intensive and difficult to start, most OEM tools are not designed for high volume, high throughput wiping.

Audit reports are the most important part of any data erasure. The OEM tools do not provide logs of the erasures. Drives that have been erased with OEM tools must have reports manually created for proof of erasure.

OEM tools may be adequate for a typical home user that isn't concerned about their data being exposed but it is much too difficult, time intensive and lacks reporting.

OEM TOOL WEAKNESSES

- Requires specific OEM Tools for each drives
- Lacks Industry Standard Overwrite Patterns
- Non-Certified
- No Verification of Wipe
- Labor Intensive Process
- Difficult to Start
- Lacks Reporting and Documentation



WHY USE WIPEDRIVE ENTERPRISE DATA ERASURE SOLUTION?

WipeDrive Enterprise is a globally certified erasure tool and is designed to be cost effective, automated and reliable in any environment. If you want your data wiped securely and quickly, WipeDrive is the solution for you. Here are some additional benefits of WipeDrive Enterprise:

- WipeDrive Enterprise is automated and scalable across your organization.
- WipeDrive Enterprise certified by Common Criteria, NCSC and NATO. It is consistently tested by third-party tools to ensure compliance.
- WipeDrive Enterprise implements ATA commands to ensure SSD and NVMe drives are erased to government regulations.
- Audit reports are provided for each wipe. The reports are not locked in a console but are provided to the user in any manner they select.
- Integrates with your ERP system to ensure proven erasure of systems before they leave your facility.

OEM tools may seem to be a practical alternative to paid data erasure software but an in-depth analysis reveals they do not provide adequate protection, reporting, and are not compliant to industry standards. Corporate, global environments require highly developed wipe software tools that can meet an organization's requirements and provide high volume, high throughput wiping.

For more information, contact our Sales Team at [\(801\) 224-8900](tel:8012248900).