blancco

WHITE PAPER

How to Securely Erase Different SSDs

Including NVMe, PCIe and More

by Greg Schulz

Who Should Read This?

This white paper is for IT data centers and cloud and managed service providers that have Fusion-io and other PCIe flash SSDs, such as NVMe SSDs, in their workstations, servers, storage systems or other appliances.

This white paper also applies to environments and applications that have government, industry or self-mandates for regulatory compliance and privacy.

Read this if you're looking to safely dispose of different types of SSD assets by selling them for reuse, scrap value or plan to re-deploy them for use in new or secondary application roles.

SSDs Offer:

- ✔ Higher performance (productivity) and lower response time latency vs. HDDs
- ✔ More activity (IOPS, TPS, Ie access) vs. HDDs
- ✔ Lower cost per I/O activity vs. HDDs
- ✔ Higher cost per raw capacity vs. HDDs
- ✔ More efficient, produce less heat vs. HDDs

Introduction

Flash-based memories, including NAND flash solid state drives (SSDs), are more difficult to deeply and permanently erase than magnetic hard disk drives (HDDs). Non-volatile memory express (NVMe)-based SSDs are a new type of flash-based memory that require new technologies to access and perform permanently wiped digital erasure. There are older generation flash-based SSDs, such as Fusion-io PCIe cards, that now need to be securely erased as part of disposition and decommissioning.

Secure digital erase technology protects your data and information while maximizing your investment in old and new SSDs.

In this white paper, we'll highlight issues, challenges and benefits of using Blancco's patented data erasure method along with specific Blancco LUN Eraser and Blancco Drive Eraser solutions, to securely wipe data from your SSDs. The biggest benefit? Verifiably and permanently wipe data from your SSDs so that they can be repositioned for use elsewhere or, prepared for safe secure certifiable disposition (scrap or sell).

Background

Deployment of SSDs in IT, cloud and managed service provider data centers has increased significantly over the past decade. This large installed base includes SSDs in workstations, compute servers, storage systems and appliances. The SSDs are used as persistent cache and I/O acceleration, as well as for storing data. SSDs are designed to store data with persistence, thus requiring a different secure erasure process and verification than HDDs.

SSDs exist in various packaging from PCIe Add-in-Cards (AiC), drive form factors, mini-cards (mSATA, SD and MicroSD) and USB Thumb drives. Workstations, Servers and storage systems access SSDs via interface protocols. Access interface protocols for SSDs include proprietary PCIe, SAS, AHCI/SATA, mSATA as well as new standard NVM Express (NVMe). NVMe uses PCIe AiC, U.2 (SFF 8639 drive form factor) and M.2 (Next Generation Form Factor-NGFF aka "gum stick" cards).

Many of the early generation of PCIe AiC SSDs, such as those from Fusion-io (now SanDisk), have reached or are nearing retirement from their primary deployment role. Given current challenges with secure data destruction, most of these devices are physically destroyed instead of being securely erased and repurposed for secondary use through resale or redeployment. Here are some of the data erasure issues and challenges for SSD and similar flash-based memories.

Issues and Challenges

NAND flash SSDs require a different erasure process than traditional magnetic media (HDDs). New digital erase process and professional software are needed to make sure all of the nooks and crannies are securely and permanently wiped. Storage devices based on flash memory require digital erasure to be done at deeper, lower levels, including in bad blocks. Newer SSDs, such as those using NVMe based access protocols, require new processes and complete erasure solutions.

Quick Facts About SSDs

- ✔ SSDs, such as Fusion-io, are getting older
- ✔ Older SSDs are still useful in new roles
- ✔ Digitally erase older SSDs for more value
- ✔ NVMe SSDs need new digital erasure processes
- ✔ Encryption does not replace digital erase for SSDs
- ✔ SSDs are more difficult to erase than HDDs

Many industries use SSDs for storing and processing sensitive data that is under compliance, regulatory or other mandates (governmental, industry or self-imposed). These mandates require secure erase, along with an audit trail, to prove the SSDs have been securely "wiped clean" before disposition – or redeployment.

From Issues to Solutions and Opportunities

Understanding the issues with NVMe accessed SSDs is your first step toward secure data destruction. The other part of the equation is knowing what to look for in a solution. Opportunities enabled by modern SSD digital erase solutions include redeployment of newer NVMe devices from their previous role into secondary less demanding scenarios. Some options include backup or data protection, reference and active-archive and other bulk storage needs.

Other SSDs that no longer have a practical use in your environment can be sold for reuse or scrap value after secure digital erasure. For example, older Fusion-io SSDs may have residual value for other organizations.

When choosing a modern SSD digital eraser solution, look for one that performs verified and complete data wiping. The process of permanently wiping includes accessing hidden data, bad blocks or other areas not accessible by general server-based utilities. It also means moving beyond tools that only clean the surface, or upper-level file systems, instead of going deeper below the logical or partition level. Other things to look for in a solution include support for older PCIe AiC SSDs, such as Fusion-io. And don't forget to include support of newer NVMe accessed SSDs.

Additional features and functions to look for in a data eraser solution include:

- Compliance with NIST and US DoD secure digital erasure standard such as 5220.22-M, among others
- Support for various NVM mediums (SLC, MLC, TLC, 3D &Vertical NAND flash)
- Available Low-level hardware command based erase, including hidden SSD data cells
- Ability to implement via an appliance if needed, or run directly on server where devices are installed
- Capability to provide concurrent deep erase of multiple SSDs at the same time on the same system
- Ability for devices to be safely redeployed internal or external, sold for use or scrap after erasure
- Support for both Linux and WinPEbased boot to run optimized processes for different needs
- Verification audit trails, reporting and notifications

Blancco Erasure Solutions

Blancco's secure data erasure solutions for LUNs, HDDs/SSDs in PC desktop computers, laptops, servers, x86 tablets and storage systems address all of the challenges, issues and criteria mentioned above. In addition,Blancco solutions enable opportunities for increasing efficiency across your organization with professional digital eraser tools that work with everything from older generation SSDs, such as Fusion-io, to new NVMe based devices.

Erasure as a service in larger data center decommissioning projects is growing in demand. Blancco software has undergone rigorous testing and certification to meet data center class requirements. Blancco also has professionals with the expertise to assist you with various aspects of planning and deployment, with advice tailored to your specific systems and environment.

Blancco Industry-Leading SSD Digital Eraser Solutions:

- ✔ Offer NIST 800-88 compatibility for both clear and purge level with verification
- ✔ Comply with particular sections of PCI DSS, HIPAA, SOX, ISO 27001 and EU General Data Protection Regulation
- ✔ Provide audit trail and documentation to verify full erasure of old and new SSD technologies
- ✔ Permanently wipe physical SSDs and virtual technologies (LUNs, Volumes, partitions)
- ✔ Provide increased ROI of expensive SSDs when they are safely repurposed or sold

Conclusion

Take the next step. Learn more about secure SSD erasure using Blancco File Eraser. Get your free strategy session and trial today to test SSD erasure in your data center(s).

About Blancco

Blancco Technology Group is the de facto standard in data erasure and mobile device diagnostics. The Blancco Data Eraser solutions provide thousands of organizations with an absolute line of defense against costly security breaches, as well as verification of regulatory compliance through a 100% tamper-proof audit trail. Our data erasure solutions have been tested, certified, approved and recommended by 18 governing bodies around the world. No other security firm can boast this level of compliance with the most rigorous requirements set by government agencies, legal authorities and independent testing laboratories.

The Blancco Mobile Diagnostics solutions enable mobile network operators, retailers and insurers to easily, quickly and accurately identify and resolve performance issues on their customers' mobile devices. As a result, mobile service providers can spend less time dealing with technical issues and, in turn, reduce the quantity of NTF returns, save on operational costs and increase customer satisfaction.

For more information, visit our website at www.blancco.com.

Contact Us

For Corporate Marketing, Please Contact:
Email: marketing@blancco.com

For Corporate Communications & PR, Please Contact:
Email: press@blancco.com