



CoreSecurity2 Delivers Next-level Security

Four layers of protection deliver truly deep security

Advantages:

- Disk erasure at varying levels of intensity, including NSA standard
- Disk destruction, for when even intense erasure is not enough
- Security key implementation
- Disk writing and reading protection
- Instant Keychange crypto erasure
- 256-bit encryption
- TCG Opal

Security Needs To Step Up

In today's information age driven by the ever-developing Internet, data is more vulnerable than ever to being retrieved and misused by unauthorized users. The loss or theft of data can lead to severe consequences. This is especially true in the fields of industry, healthcare and national defense, since their data is generally sensitive and confidential. In response to concerns over data breaches or leakage, Apacer has developed an innovative, comprehensive technology called CoreSecurity2 designed to strengthen data security through customized firmware and prevent data leakage, delivering higher reliability for storage devices.

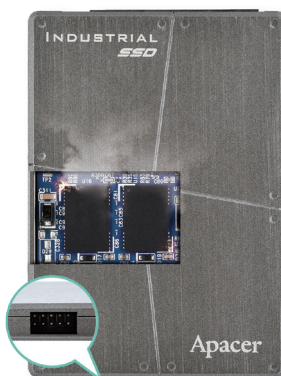
Four Levels Of Protection

CoreSecurity2 is a proprietary data protection technology built into Apacer's SSDs. It is crucial for mission-critical applications, where data erasure, drive sanitization, and reliability of storage are essential requirements. CoreSecurity2 combines four technologies driven by exclusive software commands to meet clients' demands for stronger data protection. The result is security that's truly DEEP.



Destroying

After activating the Destroy function, SSDs can no longer be used. This is most useful when an SSD is about to fall into the hands of bad actors such as unauthorized users or hackers. Activating the Destroy function destroys all data on the drive. Destroy commands can be sent via software or via a hardware trigger. The SSD destruction modes are divided into:



A single press on the hardware switch destroys the storage media thoroughly and completely

Physical Destruction

10100101110101011010
101011010100101011010
101001011010101011001
101011010100101011010
1010011101010111001
10101010101010101010
101001110101010101010
101011010100101011010
101001011101010110101
101001011101010110101
101011010100101011010
101001011010101011001
101011010100101011010

Firmware and all data wiped, rendering drive totally unusable

Digital Destruction

Erasing

CoreEraser technology provides a complete disk erasure solution that safely and completely erases all data on the hard disk, preventing the possibility of data being recovered. It is divided into three modes:

- Quick Erase, which can complete the erase operation in a very short time.
- Full Erase, with a more thorough erase function.
- Military Erase (MIL Erase), using military standard erasure techniques to overwrite the scrubbed data for even greater protection.

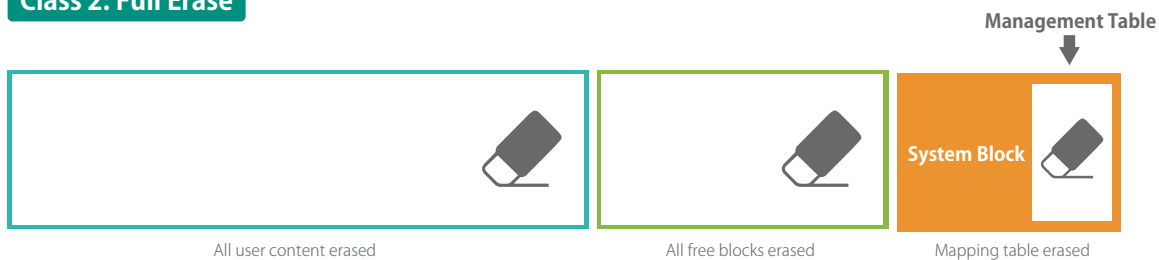
Drive Status Before Erasure



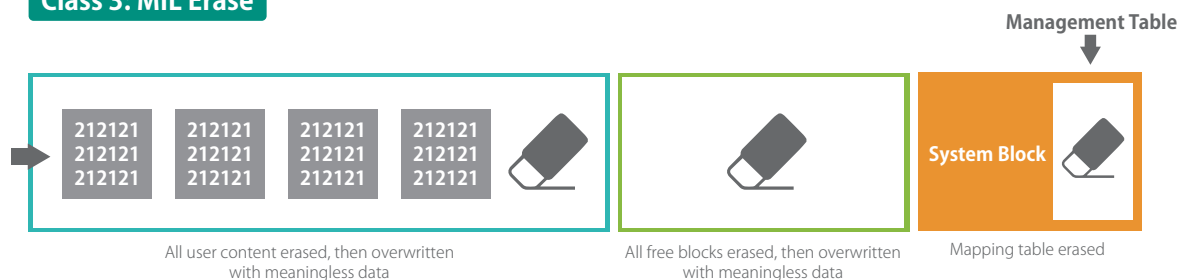
Class 1: Quick Erase



Class 2: Full Erase



Class 3: MIL Erase



Encrypting

Encryption technology implements the 256-bit AES standard into an SSD controller and complies with the TCG Opal 2.0 specification for providing complete data protection. An encryption key which is stored inside the SSD is required for data encryption and decryption. Apacer followed the TCG Opal 2.0 specification to create a software program called Opaque that can provide a higher level of SSD security functions, and the interface is shown below.

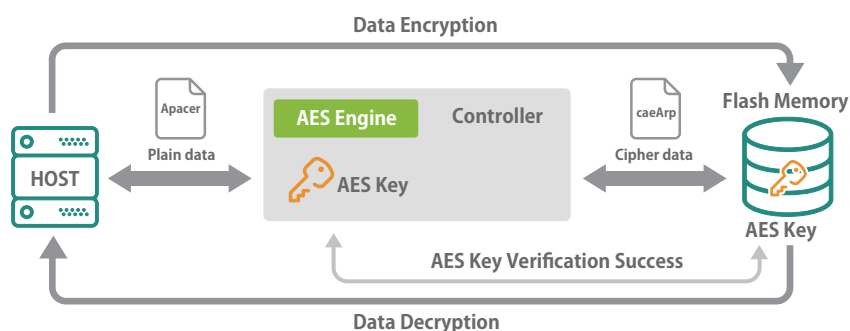
Opaque

The screenshot shows the Opaque software interface for Apacer SED Technology. The interface is dark-themed and includes the following elements:

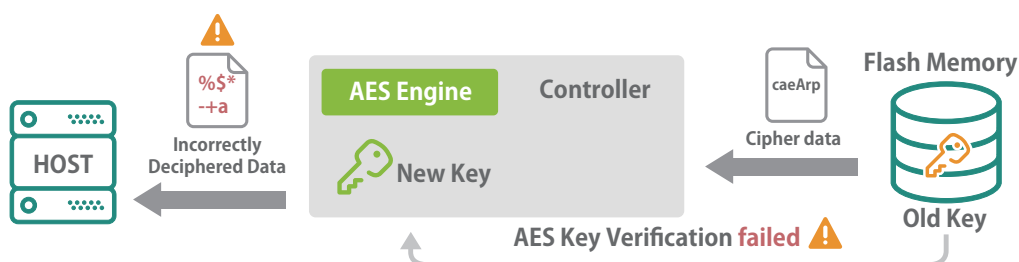
- Header:** "SED Technology Driven By TCG Opal" and "Apacer For Industrial".
- Disk Selection:** A dropdown menu showing "Disk 0" and "64GB SATA Flash Drive", with a "Refresh" button.
- Device Information:**
 - Model Name: 256G SATA Flash Driver
 - Serial Number: D01441700000012
 - Firmware Version: SFDM104B
 - MSID: 256G SATA
 - Total LBAs: 256G SATA
- Functionality Sections:**
 - Set Password:** Fields for Password, New Password, and a dropdown menu, with "Show" and "Confirm" buttons.
 - Pre-Boot Authentication:** Fields for authentication, with "Open File", "Load", and "Unload" buttons.
 - Set Locking Range:** Fields for Locking Range and LBAs Range, with "Set" and "Switch" buttons. The "Switch" section has "Enable" and "Disable" buttons.
 - Revert:** Fields for Password and a dropdown menu, with "Show" and "Enable" buttons.
- Show Information:** A section with "Locking Information" and "Query" buttons, and a text input field for "New Password".
- Right Sidebar:** Contains icons for help, close, and status.

The encryption technology is also adopted in Apacer's Instant Keychange™, and a user can quickly replace the original encryption key with a new one – essentially erasing the entire drive in less than one second.

Typical implementation of AES encryption/decryption



Data unreadable after execution of Instant Keychange command



Instant Keychange™

Instant Keychange Technology: For When Security is At Risk.

How long does it take to Sanitize a **2TB SSD**?

Erase 2 minutes

Instant Keychange 1 Sec

Time(Min)

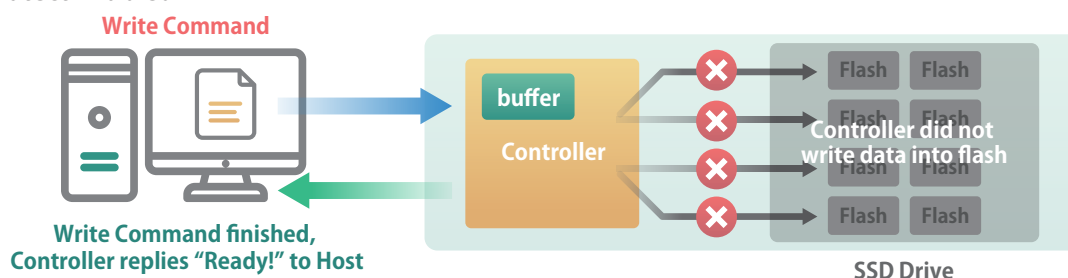
Protecting

Protecting unauthorized data from being tampered with or written to the hard drive is an excellent function to have. This solution can be activated through software or hardware settings and there is no need to install any extra software. It is divided into two modes:

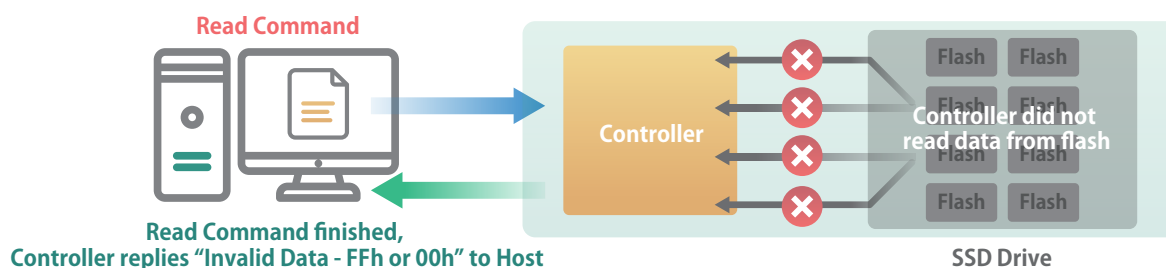
Write Protect: After enabling this function, the data will not be written into the NAND Flash, which prevents important data in the SSD from being overwritten or deleted by mistake. It is a read-only mode.

Device Protect: RAW formatting means that the data in the drive cannot be read, which can prevent users from tampering with any parameters on the SSD.

Write Protect Enabled



Device Protect Enabled



In this mode, the Write Protection shown above also applies.

Conclusion

Some of the world's leading technology companies have experienced embarrassing data breaches in the last decade or so. Many of those can be attributed to inadequate data security, and the breaches have led to both business losses and brand reputation damage. Once trust is lost, it's extremely hard to get back. Companies that are seeking a higher level of data security for SSDs now have an incomparable solution – Apacer's CoreSecurity2. It protects SSDs with a wide variety of form factors: contact your local Apacer representative today to learn more.



For more information, contact your Apacer representative

Taiwan (Headquarters)

Apacer Technology Inc.
Tel: +886-2-2267-8000
Fax: +886-2-2267-2261
Industrial@apacer.com

Japan

Apacer Technology Corp.
Tel: +81-3-5419-2668
Fax: +81-3-5419-0018
jpservices@apacer.com

U.S.A.

Apacer Memory America, Inc.
Tel: +1-408-518-8699
Fax: 1-510-249-9551
ssdsales@apacerus.com

Europe

Apacer Technology B.V.
Tel: +31-40-267-0000
Fax: +31-40-290-0686
sales@apacer.nl

India

Apacer Technologies Pvt. Ltd.
Tel: +91-80-41529061~3
Fax: +91-80-41700215
sales_india@apacer.com

China

Apacer Electronic(Shanghai) Co., Ltd.
Tel: +86-21-6228-9939
Industrial@apacer.com