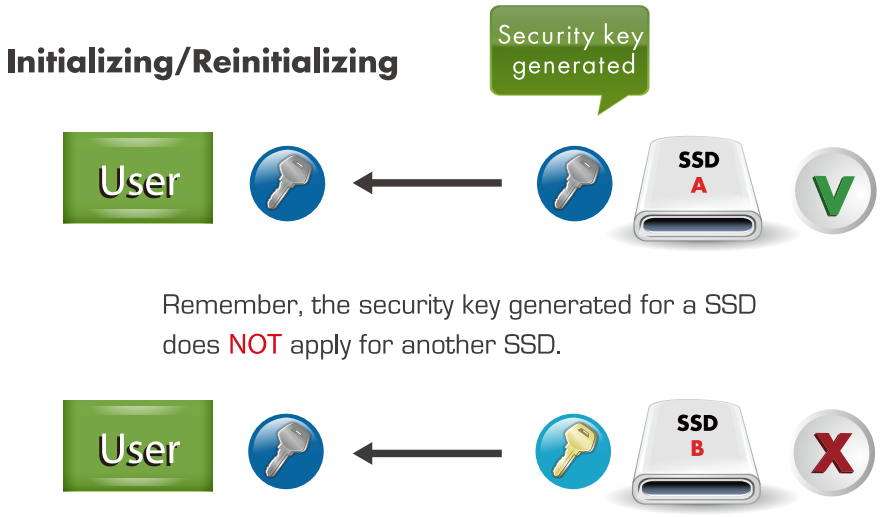
CoreProtector

The widespread adoption of SSDs over HDDs in mission critical applications may attract potential data theft. In order to reinforce data security, Apacer introduces the CoreProtector technology that integrates multiple layers of protection for your valuable data.

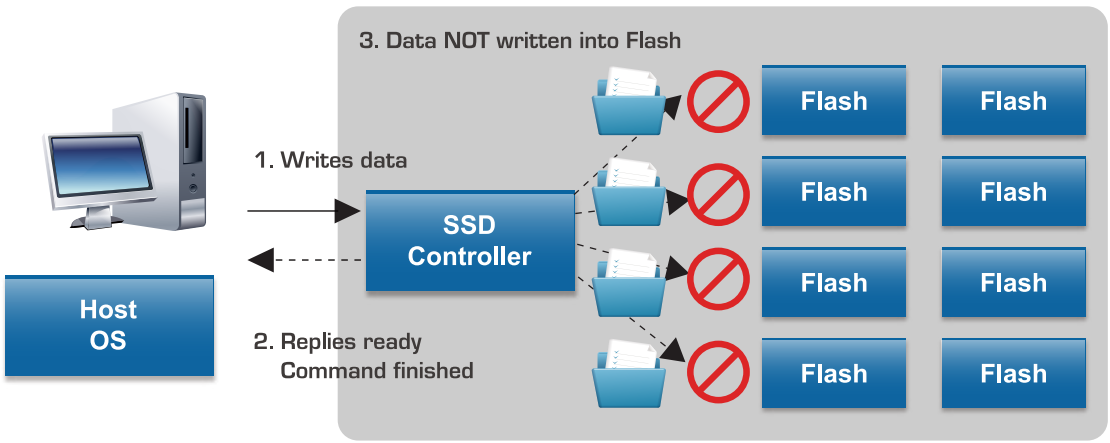
Class 1: Data Protect

Apacer SSDs come with a unique 512-byte Security Key when they leave the factory. The key is a activated whenever the host boots up. The host BIOS can retrieve the 512-byte key data and the host user can use it as password identifications for accessing certain application programs or booting up process. Failure to match the key will result in aborted operations.



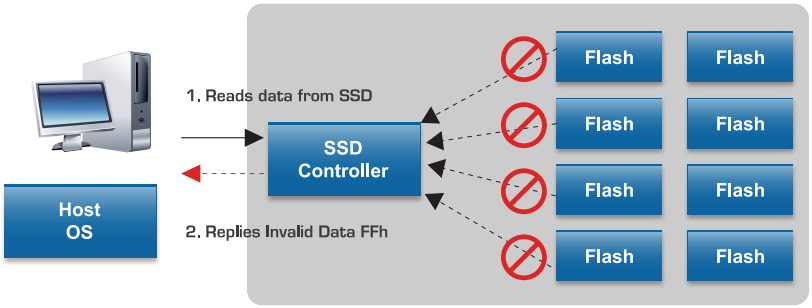
Class 2: Write Protect

Apacer implements the Virtual Write scheme that allows write commands to go through the flash controller and data temporarily stored. The OS can then function normally but since the whole process is virtual, no data has actually been written into the flash. When the host system is reset or rebooted, all the temporarily stored data will be lost and nowhere to be found in the system. Since the Virtual Write scheme runs at device level, it requires no software of driver installation and is independent from the host OS.



Class 3: Device Protect

Developed as a more comprehensive security solution, Device protect can be considered as Write protect scheme integrated with read protection that prevents unauthorized accesses to read files in the device. When enabled, the Device Protect scheme would allow read commands to go through flash controller, but no actual data in the device can be read during the whole process. Without the proper way to disable the protection, unauthorized read attempts would receive only invalid data, indicated as "FFh" or "00h"

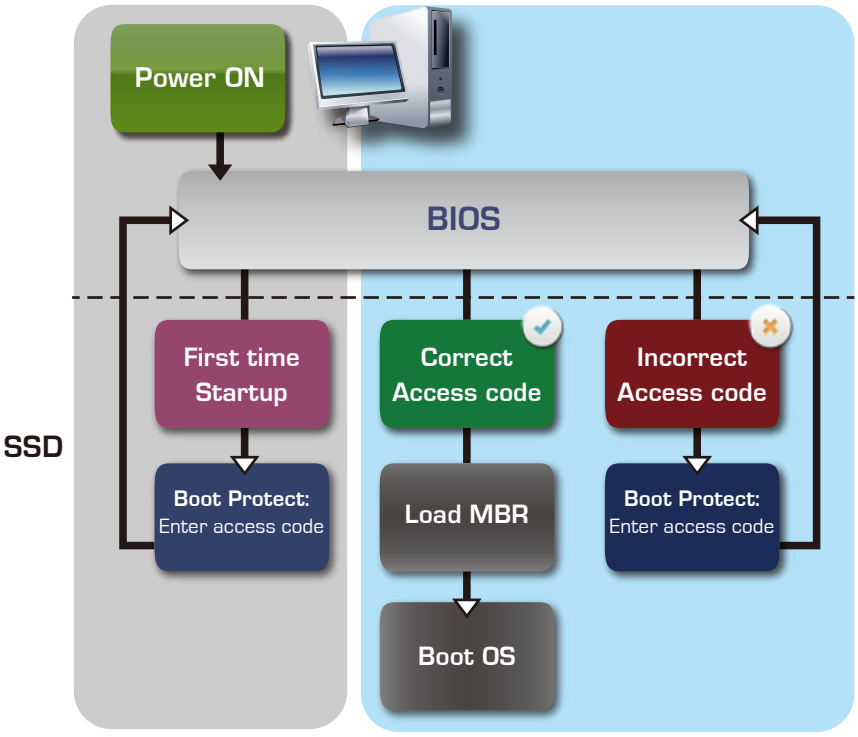


Class 4: Boot Protect

Boot Protect Technology is the ultimate security class of Apacer CoreProtector series that restricts the unauthorized from accessing the computer system. Users can set access code during the system booting process so that no one else would be able to access their operating system and SSDs without the correct access code.

Boot Protect technology is also ideally applicable for SSDs with multiple OS-run storage zones that are independent from one another. For instance, if a SSD is divided into two storage zones with OS installed in each, the host can decide which zone to access by entering the corresponding access code.

Boot Protect Process



Boot Protect Application