

## Hardware-Based Full Disk Encryption

Hardware-based encryption products overcome the two most significant barriers to widespread adoption of encryption technology — ease of use and system performance. Encryption built into the hard disk eliminates much of the setup and configuration complexity. Seagate's DriveTrust encryption drive technology isolates the encryption functions and stores the encryption keys in the hard drive itself, providing an added security benefit of blocking root kits and other malware from accessing keys and other sensitive information from the operating system. In addition, hardware encryption performance is very close to that of a non-encrypted drive with minimal impact on computing operations, far superior to software-based encryption.

### Advantages

1. **Full Disk Self-Encrypting** – The drive requires credentials to be supplied from a storage system to verify that the drive is being accessed by an authorized user before unlocking the drive. When unlocking the drive the data is encrypted before being written and decrypted before leaving the drive. (Figure 1)
2. **(Seagate) Drive Design Security** - Hackers can't benefit from knowing the intricate details of the drive's design and construction. **Reason:** The Encryption Key is not kept in the drive – only an encrypted version of the encryption key is kept in the drive. There are no clear text secrets anywhere on the drive, just a fingerprint (hash) of the password.
3. **Increase System Performance**
  - OS Agnostic meaning it has no knowledge of which OS is running and thus functions independently, allowing cross-platform support. The encryption function is transparent to the host, OS, DBs and applications increasing the security of the encryption key. **Reason:** The encryption key is passed directly from the storage system and NOT through a network and application server when unlocking the drive. Figure 2 (a) Performing encryption outside of the storage system increases complexity. (b) Automatic encryption in the drive simplifies key management for authentication (A Keys) and encrypts the (E Keys).
  - Encryption/Decryption will not decrease the performance or slow down the system. **Reason:** The encryption engine is in the controller ASIC and there is an encryption engine dedicated to each port on the drive.

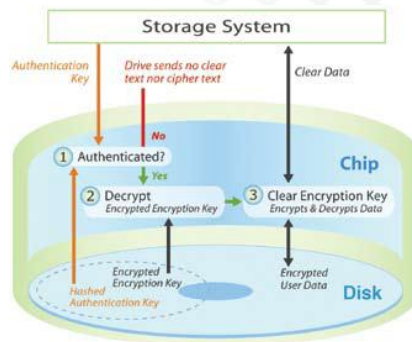


Figure 1

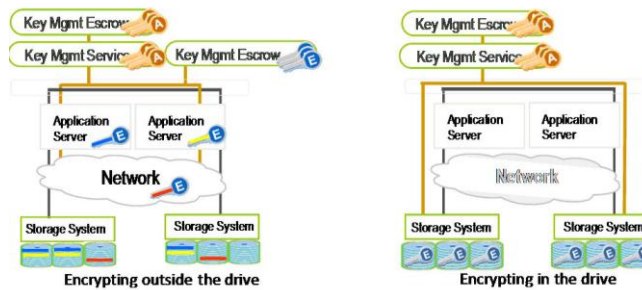


Figure 2

## Mobile Armor DriveArmor

Mobile Armor's DriveArmor™ incorporates the benefits of Hardware Encryption and couples it with the benefits and strengths of the **Mobile Armor Data Encryption & Device Management Suite**. DriveArmor provides centralized management of the Seagate drive from a single management console, a single management server and a single management agent. This allows IT professionals to manage security policies, enforce compliance and produce management reports across multiple hardware configurations and operating systems.

DriveArmor's technology fortifies the Seagate Momentus hard drives with remote management, strong authentication, and extensive auditing and reporting features. Unauthorized access to data on the hard drive is eliminated with DriveArmor's pre-boot authentication. This feature enforces policy-driven access control immediately when the drive powers up so that unauthorized users are disabled at pre-boot and cannot logon to the computer. DriveArmor stores user passwords in the drive memory so password signatures are totally inaccessible after computer shut down. This further safeguards data from being accessed by unauthorized users, enabling the complete protection of an organization's sensitive data at all times.