

## Benefits of Self-Encrypting Hard Drives

### Ease of Deployment & Speed

One of the major benefits to encrypting data using a trusted self-encrypting hard drive is speed and ease of deployment. When encrypting data using software encryption, an application running on your device actually does the encryption. This means your data has to be processed through the running of the software first before being stored on your device. This is typically a slow process—much slower than copying files straight to the device and not using software encryption. Since you actually have to run software to initiate this, your computer's resources can become tied down and your system performance will decrease. Mobile Armor's DriveArmor actually encrypts data using a special chip inside the device. Since a physical chip is what encrypts the data and not a piece of software, the result is faster encryption times as well as zero strain on your computer's resources. A key benefit of self-encrypting hard drives is that there is no wait on the initial background encryption.

In comparing Mobile Armor's DriveArmor (Hardware Encryption) with a typical Full Disk Encryption (FDE) Product, speed and performance are affected in the following ways:

|                         |   |
|-------------------------|---|
| <b>Preboot:</b>         | DriveArmor loads up to 1 minute quicker. It uses the latest Linux kernel so DriveArmor gains a speed advantage. DriveArmor also eliminate or lightens some unnecessary modules. |
| <b>Encryption:</b>      | The speed of encryption is dependent on the size of the drive. For example, a 250 GB drive would take DataArmor approximately 3.5 hrs. With DriveArmor, it is instant.          |
| <b>Boot to Windows:</b> | DriveArmor is quicker than FDE by approximately 30+ seconds.  |
| <b>Uninstall:</b>       | Is instant with DriveArmor while a FDE product must first decrypt the data. A 250 GB drive would provide DriveArmor approximately a 4 hr advantage.                             |

### Ease of Use & Performance

Software encryption applications require you to encrypt your data using the software itself. Usually you have to designate a spot on your flash drive just for encrypted data, which can often be a complex and confusing task to set up. Utilizing a trusted self-encrypting hard drive is significantly easier. Since the hardware on your device does the encrypting, all you have to do is essentially enter your password and use the device like a normal drive and the encryption will take place in the background. Data is always encrypted by the onboard encryption chip, from the very first second. After a quick DriveArmor activation, DriveArmor will instantly turn on the authentication and key management through the centralized Policy Server.

**The Benefits of Self Encrypting Hard Drives and Mobile Armor DriveArmor:**

**Ease of Deployment – Speed – Ease of Use – Performance**