COMPARISON OF HARD DRIVE DATA PROTECTION METHODS

There are a number of methods available to protect data on a hard drive. *BIOS and operating system passwords* are frequently used, but they only provide very minimal security and can be readily removed by unskilled attackers without requiring sophisticated tools. *Hard drive password locking* is one of the most relied-upon security methods today. It is stronger than BIOS or operating system passwords, but this common protective measure can be easily defeated as well.

Software-based full drive encryption is significantly stronger than BIOS, operating system or hard drive password locking. Unfortunately, software-based encryption must run under the operating system and in the CPU, which can have an impact on the overall performance of the PC, as well as cause an exposure to the security methods used to safeguard the information on the PC itself. This means that there can be stealth processes running on the PC that can capture the encryption keys and even the non-encrypted data—which of course is not a very good scenario to have.

Hard drive-based security provides some of the best and strongest encryption solutions for personal computers. No sensitive data or keys are available to the CPU or to other applications running under the operating system. In addition to the security advantages, encryption done in the drive's hardware offers other attractive advantages. First, hard drive-based encryption has clear performance and reliability advantages. Second, because the encryption is integrated into the drive read/write function, it is transparent to the user. And finally, "factory" encryption significantly reduces the costs of acquisition, deployment and administration.

BIOS Password Very minimal protection	Available on nearly all PCs. Prevents the computer from fully booting unless the correct password is provided. Does not encrypt any data. Very easily thwarted, no special skills needed. For example, the hard drive can simply be moved to another device with the BIOS lock turned off.
Operating System Password Very minimal protection	Access to general OS functions is denied unless the correct password is given. Does not encrypt any data. Easily defeated by moving the hard drive to another computer. No special skills needed. Offers very minimal protection.
Hard Drive Password (using ATA) Minimal protection	Available on most notebooks and some desktops. Prevents the drive from retrieving data unless the correct password is provided. Does not encrypt any data. Easily defeated but requires specific skills or hiring someone with those skills. Stronger than BIOS or OS passwords but still weak protection and not suitable for data worth more than US$100.
Software-Based Full Drive Encryption Good protection	Add-on security product that modifies the hard drive drivers and encrypts all data as it is written to the drive. Requires correct password before the data is decrypted. Offers good protection but expensive to purchase and deploy, and impacts system performance which sometimes leads end users to turn it off. There is a potential for malware, trojans or rootkits to remotely turn off the software protection (the same as end users) without proper methods of protecting the software itself from attacks. Also worth noting, some software-based products require the encryption to be turned off whenever an operating system update must be installed—causing an administration burden and also risk of exposure.
Hard Drives Excellent protection	The hard drive contains built-in cryptographic hardware that encrypts all data as it is written to the drive. Requires the correct password to decrypt any data. Built into the computer so it's not an add-on, and totally transparent to the user. Does not impact performance. Extremely difficult to defeat when good passwords are used. Offers excellent protection.

Summary of the vulnerabilities of software encryption.

Comparison Categories	Hard Drive Encryption	Software Encryption
Key storage accessible to operating system (Open to attack)	No	Yes
Encryption process observable in memory (Open to snoop)	No	Yes
System performance negatively impacted by encryption process	No	Yes
User effort required to designate folder or files for encryption	No	Yes
Operating system upgrades more difficult than for a non-encrypted system	No	Yes