



Software Encryption

VS

Hardware Encryption

HOSTING

Shares **computer's resources** to encrypt data with other programmes on the computer - only as safe as your computer.

Uses a **dedicated processor** physically located on the encrypted drive.

PASSWORD

Uses the **user's password** as the encryption key that scrambles data.

Processor contains a **random number generator** to generate an encryption key, which the user's password will unlock.

Can **require** software updates.

UPDATES

Increased performance by **off-loading encryption** from the host system.

DECRYPTION

Software encryption is vulnerable to hacking due to **weak protection against Brute Force attacks** using easily available online tools.

Safeguard keys and critical security parameters within **crypto-hardware**.

AUTHENTICATION

Authentication uses **host system resources**.

Authentication takes place **on the hardware encrypted drive**.

PROTECTION

Vulnerable to attacks and is only as secure as the host system.

Protection against the most common attacks, such as cold boot attacks, malicious code and brute force attacks.

INSTALLATION

Operating system **compatibility may vary**.

Does not require any type of software installation on the host PC.

Can be implemented on **all types of media**.

FLEXIBILITY

Encryption is **tied to a specific device**, so encryption is always on.

COST

Cost-effective in **small application** environments.

Cost-effective in **medium and larger application** environments, easily scalable.

Ask an Expert

Planning the right solution requires an understanding of your project's security goals. Let [Kingston's experts](#) guide you on how to best defend your sensitive data.