

Software Encryption V Hardware Encryption



What is the difference between software and hardware-based encryption? Depending on the application you may be surprised by what is involved in securing your data.

HOSTING

Shares computer's resources to encrypt data with other programs on the computer – only as safe as your computer.

HOSTING

Uses a dedicated processor physically located on the encrypted drive.

PASSWORD

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

PASSWORD

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

UPDATES

Can require software updates.

UPDATES

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

DECRYPTION

Susceptible to brute force attacks, computer tries to limit the number of decryption attempts but hackers can access the computer's memory and reset the attempt counter.

DECRYPTION

Safeguard keys and critical security parameters within crypto-hardware.

AUTHENTICATION

Authentication uses host system resources.

AUTHENTICATION

Authentication takes place on the hardware.

PROTECTION

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

INSTALLATION

Operating system compatibility may vary.

INSTALLATION*

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

PROTECTION

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

FLEXIBILITY

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

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

So, in summary, whilst software-based encryption does have its advantages, it may not match its perception as being comprehensive. Whereas, hardware-based encryption offers a more robust solution. Want to know the best solution for securing your data? Use both. Together.

READ MORE ONLINE

kingston.com/solutions/data-security

* For USB's only - for SSD's we recommend using a SW encryption tool to activate the encryption function.

©2020 Kingston Technology Europe Co LLP and Kingston Digital Europe Co LLP, Kingston Court, Brooklands Close, Sunbury-on-Thames, Middlesex, TW16 7EP, England. Tel: +44 (0) 1932 738888 Fax: +44 (0) 1932 785469. All rights reserved. All trademarks and registered trademarks are the property of their respective owners.