KINGSTON IRONKEY™

Hardware vs Software Encryption

Understanding the key differences, and which is the better option for your needs.

In the ongoing battle for data security, the difference between hardware and software encryption comes down to where security lives and how exposed it is in real-world use. In USB drives and SSDs, where encryption is built determines how securely data is protected and how much it relies on the system around it.

HARDWARE	VS	SOFTWARE
Encryption key handling Encryption keys are generated internally by the hardware and stored securely within the drive.		**Encryption key handling** The user's password is used directly as the encryption key, and keys may reside in system memory.
Brute force attack protection Designed to protect against brute force attacks by limiting the number of attempts before the drive wipes itself preventing anyone from getting sensitive data if the drive is lost or stolen.		**Brute force attack protection** Susceptible to brute force attack, computer tries to limit the number of decryption attempts but hackers can access the computer's memory and reset the attempt counter.
Software or driver requirements No drivers or software installation required on the host system.		**Software or driver requirements** Requires software installation, drivers, and operating system compatibility may vary.
Encryption resources Uses a dedicated cryptographic processor built into the drive itself.		**Encryption resources** Uses the host computer's CPU and system resources to encrypt and decrypt data.
Host system dependency / exposure Security is isolated inside the device and remains protected even when connected to untrusted or infected computers.		**Host system dependency / exposure** Security depends on the host operating system and is more vulnerable if the computer is infected with malware.
Encryption status The encryption is always-on by design and cannot be removed or bypassed.		**Encryption status** The encryption can be enabled, disabled, or misconfigured.
Performance impact Minimal performance impact, as encryption is off loaded to the hardware processor.		**Performance impact** Can negatively affect performance because encryption shares CPU resources.
Flexibility Encryption is tied to the specific USB or SSD drive.		**Flexibility** Can be implemented on almost any storage media.

Software encryption offers flexibility, while hardware encryption keeps security isolated and less exposed to system-level risks. Understanding how each protects data and controls access helps you choose the right level of security for your workflows and risk profile.

www.kingston.com/ironkey

© 2026 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. All rights reserved. All trademarks and registered trademarks are the property of their respective owners.