KINGSTON IRONKEY™

硬體型與軟體型加密

了解主要差異，以及哪一個是更適合您需求的選擇。

在持續不斷的資料安全之戰中，硬體型加密和軟體型加密之間的差異，關鍵在於安全機制建置在何處，以及在實際使用環境中暴露於風險的程度。對於 USB 隨身碟與 SSD 固態硬碟而言，加密功能建置在何處，將決定資料受到保護的安全程度，以及它對周邊系統的依賴程度。

硬體型	與	軟體型
加密金鑰管理 加密金鑰由硬體內部產生，並安全儲存在隨身碟內。		**加密金鑰管理** 使用者密碼會直接作為加密金鑰，而金鑰可能存在於系統記憶體中。
暴力破解保護 透過限制嘗試次數來防禦暴力破解，超過嘗試次數限制後，隨身碟a會自動擦除資料，即便遺失或遭竊，也無法取得其中的敏感資料。		**暴力破解保護** 容易受到暴力破解攻擊，雖然電腦有嘗試限制解密次數，但駭客可存取系統記憶體並重設嘗試次數計數器。
是否需要安裝軟體或驅動程式 主機系統上無需安裝驅動程式或軟體。		**是否需要安裝軟體或驅動程式** 需要安裝軟體；驅動程式和作業系統相容性可能會有所不同。
加密資源 使用內建於儲存裝置中的專用加密處理器。		**加密資源** 使用主機電腦的 CPU 與系統資源加密和解密資料。.
對主機系統的依賴/暴露風險 安全機制隔離於裝置內部，即便連接至不受信任或已感染的電腦，資料仍可受到保護。		**對主機系統的依賴/暴露風險** 安全性依賴主機作業系統，若電腦感染了惡意軟體，安全風險較高。
加密狀態 根據設計，加密永遠為開啟狀態，無法移除或繞過。		**加密狀態** 可以啟用或停用加密，或因設定錯誤導致加密失效。
是否影響效能 加密作業改由硬體處理器負責，幾乎不影響效能。		**是否影響效能** 加密作業占用 CPU 資源，可能對效能產生負面影響。
靈活性 加密功能與特定 USB 隨身碟或 SSD 固態硬碟綁定。		**靈活性** 幾乎可在任何儲存媒體上進行。

軟體型加密提供靈活性，而硬體型加密可將安全機制隔離於裝置內部，降低暴露於系統層級風險的可能性。了解每種方法如何保護資料和控制存取的方式，有助於您根據工作流程與風險屬性，選擇最適合的安全防護等級。

www.kingston.com/ironkey