
# 為何 USB 隨身碟在今天還很重要？

#KingstonIsWithYou

# 為何 USB 隨身碟在今天還很重要？

## 前言及內容

在今天這個數位化時代，全球有 60% 的企業資料儲存在雲端[1]，在此討論具有近 30 年歷史的儲存技術似乎有點奇怪。但自推出以來， USB 隨身碟這種儲存產品不斷變革。

USB 隨身碟不再只是連接硬碟、傳輸檔案和應用程式的工具。現今 USB 隨身碟的傳輸速度大幅提高，還是效能可靠且安全的可攜式儲存媒體。然而，雲端儲存解決方案的優點似乎大致一樣，USB 隨身碟還重要嗎？

在本電子書中，我們將探討 USB 隨身碟在雲端主導的環境中的定位。在業界頂尖專家的見解支持下，我們將探索當今組織運用 USB 隨身碟的方式，並思辨其在軟體型加密技術、獨立儲存環境和端點資料安全中所處的角色。


| 目錄 | 頁面 |
|---|---|
| 撰稿人 | 3 |
| USB 隨身碟的興起 | 4 |
| 滿足不斷演化的需求的可攜式儲存裝置 | 5-6 |
| 加密技術：硬體型加密 vs 軟體型加密 | 7-8 |
| 保護敏感資料的需求日益增長 | 9 |
| 保護敏感的財務資料 | 10 |
| 安全存取患者的健康資料 | 11 |
| USB 隨身碟在未來雲端儲存環境中的角色 | 12-13 |
| 摘要和關於 Kingston | 14 |


# 為何 USB 隨身碟在今天還很重要？

## 撰稿人

本電子書由三位業界 IT 及新興技術專家撰寫。

**Rafael Bloom**

Rafael Bloom 專精於高科技產品、行銷企劃以及業務開發等領域。他的諮詢業務聚焦於因應技術和法規改變所面臨的組織、產品和通訊相關挑戰。他的工作內容十分多元化，所涉及的專業知識包括設計、資料隱私和新興技術 (例如 AdTech、行動與 5G、人工智慧與機器學習) 的資訊治理和合規。

**Tomasz Surdyk**

Tomasz Surdyk 擁有超過 24 年的政府部門 IT 安全經驗，在資訊安全、個人資料和網路安全領域是舉足輕重的角色。他曾獲北約和歐盟的安全許可，並負責檢驗政府部門處理機密和個人資料的 ICT 系統和網路。近年來，他是一家專門提供安全解決方案公司的負責人，致力於提升業務資訊和個人資料的安全性。

**David Clarke**

David Clarke 被湯森路透公司 (Thompson Reuter) 評選為「英國社交媒體中最具影響力的 30 位風險管理、合規性與法遵科技方面思想領袖和思想家」中最具影響力的 10 位之一，同時名列 Kingston Technology 50 大全球專家名單。他過去數次擔任安全管理相關職位，例如全球 FTSE 100 公司的安全服務全球主管以及安全基礎設施主管。

# USB 隨身碟的興起

二十多年前第一個 USB (通用序列匯流排) 隨身碟問世，其廣泛的相容性打破了電腦領域的遊戲規則。USB 隨身碟自 2000 年 上市後開始迅速發展，大眾也廣泛使用各種裝置進行操作。USB 隨身碟資料傳輸速度越來越快，後來還有 USB 3.0 連接埠等強大的功能。

從那時起，行動資料儲存和安全技術有相當大的進步。我們將重點放在現今為不同儲存需求量身打造的各種 USB 隨身碟。從企業的角度來看，遠端和混和型工作量的增加、雲端服務使用和網路安全問題等正需要更有效的解決方案。此外，監管要求資料必須以合規方式進行儲存。這些壓力經常因「本地部署」及雲端運行的分散式複雜系統而加劇。

然後是結構化和非結構化資料量不斷增加的問題，例如文件、電子郵件、照片、影片和中繼資料等，這些都增加了企業不斷發展儲存需求的複雜性。

但如果雲端儲存能夠解決這些挑戰，那麼 USB 隨身碟在如今的商業環境中又有何重要性呢？

> 許多人認為 USB 隨身碟過時了，也不再重要，因為它們過去大多只是一次性、低效能、低安全性的裝置。- Rafael Bloom

# 滿足不斷演化的需求的可攜式儲存裝置

使用 USB 隨身碟作為可攜式儲存方式的時代已逐漸淡出，而使用具有額外資料防護和加密的高效能 USB 隨身碟，已成為個人資料安全的本地備份方式。這對於敏感資料的合規性很重要，例如人力資源記錄、醫療記錄、智慧財產 (IP) 防護以及所有個人身分資料 (PII) 等。此外，這種裝置具有快速資料傳輸、儲存、備份和安全功能，可用於：

- 需親自遞交的監管資訊
- 需在現場或非現場列印並遞交的法律和財務文件
- 勒索軟體可能構成威脅的任何潛在危險環境
- 傳輸到不允許網路存取的列印系統

加密 USB 供應商領導品牌 Kingston Technology 緊跟著不斷變化的需求，推出 Kingston IronKey™ S1000 等解決方案。這款頂尖的加密 USB 隨身碟符合最嚴格的標準，提供 XTS 模式 AES 256 位元加密，並擁有強大防竄改防護功能的獨立加密晶片，具備保護機密資料的能力。並且經 FIPS 140-2 Level 3 認證。這代表其加密硬體的有效性已被美國政府正式驗證，是需要加強資料防護方面的組織的理想選擇。

無論是雲端型或本地型資料，本硬體型加密 USB 隨身碟可提供中控式的安全裝置管理解決方案。無需軟體就能輕鬆使用的合規加密資料儲存裝置，還能節省 IT 寶貴的時間，提供專為快速且高效率部署所設計的解決方案。

# 滿足不斷演化的需求的可攜式儲存裝置

USB 隨身碟有備份和存檔功能，因此可以用於長期保護數位資產，並獨立於第三方雲端服務。儘管在雲端中能輕易處理大數據，但專有 IP 性質敏感，因此有必要將其儲存在加密且安全的 USB 隨身碟上，以此遠離網際網路，才能保障安全性。

此外，總有組織需要完全掌控其資料，這時就可以使用加密隨身碟。某些情況下，無法加密 HDD/SSD 上的儲存資料。使用外部加密 USB 隨身碟就能解決這個問題，例如 Kingston IronKey D300S。此 USB 隨身碟採用 XTS 模式 256 位元 AES 硬體加密，這是一種可加密 128 位元資料區塊的區塊加密模式。當需要對資料進行加密時，AES 會使用 XTS 加密模式，與以前的模式相比，能提供更好且更強大的資料防護。


> 在我看來，人們仍持續使用 USB 隨身碟，而且是資料安全不可或缺的一部分。此外，USB 隨身碟還用於裝置之間快速傳輸資訊，同時提供適當的儲存和防護功能。- Tomasz Surdyk

# 加密技術：硬體型加密 vs 軟體型加密

考慮資料加密的方式，其中硬體型加密比軟體型加密更容易管理，也更加安全。因為加密流程與主機系統的其餘部分是分離的，更難以攔截或加以破壞。中控設備級管理可透過區域網路、內部網路和網際網路連線管控隨身碟，適合搭配下列用途：

- 建立和執行個人且/或團體使用加密 USB 的策略
- 稽核檔案活動紀錄，能夠更妥善地追蹤組織資料的輸入和輸出
- 針對關鍵資料傳輸提供遠端內容備份
- 當 USB 遺失或損壞時遠端停用該裝置
- 忘記密碼時執行遠端密碼重置

以這種方式正確地管理授權隨身碟時，能將敏感資料被複製或分享的風險降到最低。此外，現今的硬體型加密 USB 隨身碟提供大量的額外安全性功能，有助於避免檔案和訊息被預期收件人以外的任何人存取或閱讀。

> 我認為硬體型加密優於軟體型加密。硬體型加密和軟體型加密方式在暴力攻擊下的脆弱程度差異很大。硬體型加密不容易被此類攻擊破壞。
> - Tomasz Surdyk

# 加密技術：硬體型加密 vs 軟體型加密

企業可能會因成本考量而選擇軟體型加密，但這有點短視近利。軟體型加密解決方案與其他程式共用主機設備的加密資源，故其安全性與電腦一樣程度，需要經常更新軟體，如果不加以維護，就容易受到攻擊。軟體型加密 USB 隨身碟可能會受到猜測密碼的無限暴力攻擊，其無法抵抗軟體字典攻擊，這是一種可在短時間內測試數百萬個字符組合的方式。

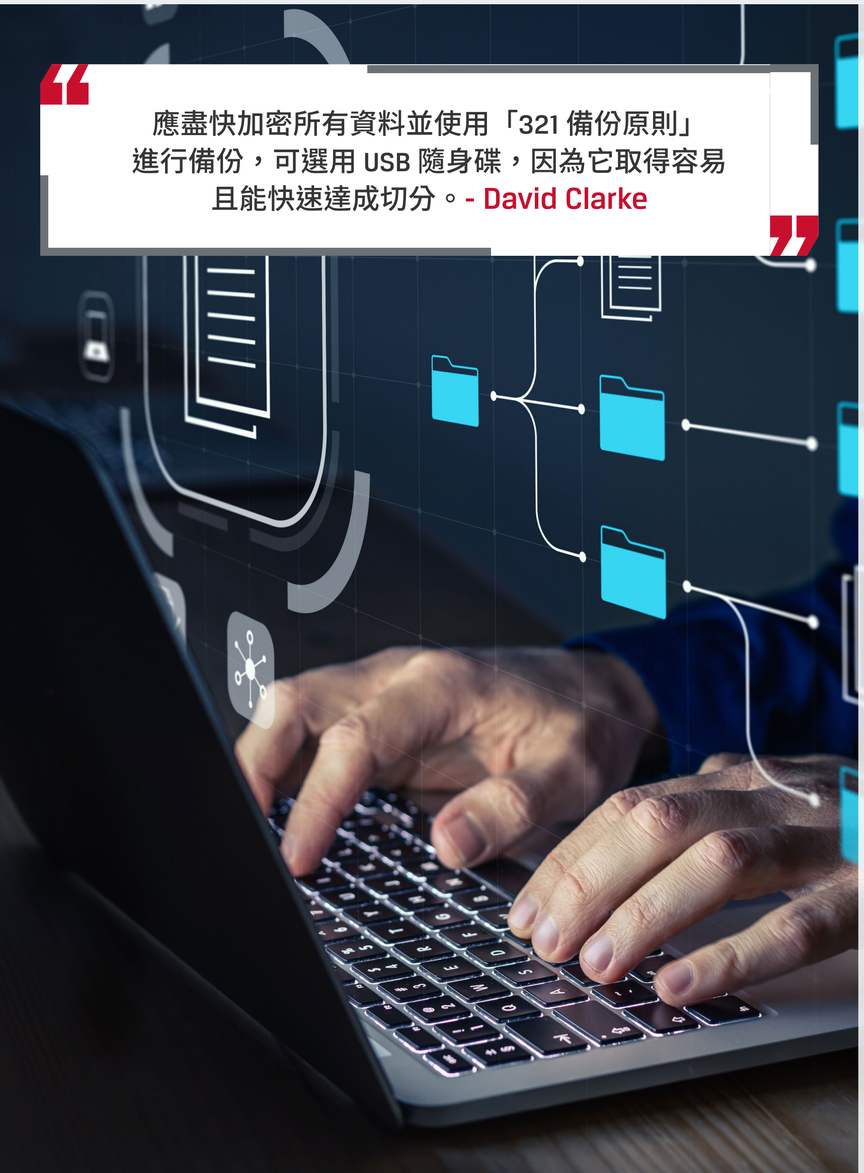
此外，軟體型加密也是一種可移除的加密方式。任何擁有軟體型加密隨身碟的員工都能複製資料、格式化 USB 隨身碟，並且移除加密功能。然後他們可以將資料檔案複製回隨身碟並加以使用，不用面臨在不同平台或作業系統上進行身分驗證這類的麻煩事。

如前述所提，硬體型加密則是將硬體加密及儲存資料等動作獨立於主機系統外進行。如果系統遭受破壞，這能確保有一層額外的防禦層。

尤其對於金融、醫療保健和政府單位而言，這點不容忽視。這是因為《健康保險流通與責任法案》(HIPAA) 和「支付卡產業資料安全標準」(PCI DSS) 對於敏感資訊加密通常有嚴格要求。

使用強大的硬體型加密裝置來遵守這些規定，終究有助於組織避免掉高額罰款、訴訟及可能嚴重損害商譽的風險。儘管硬體型加密隨身碟可能比 USB 隨身碟昂貴，但因違法所產生的訴訟成本和數小時的法律諮詢費用，就能輕鬆買入數百個加密隨身碟。

# 防護敏感資料的需求日益增長



> 應盡快加密所有資料並使用「321 備份原則」進行備份，可選用 USB 隨身碟，因為它取得容易且能快速達成切分。- David Clarke

每個組織都有義務確保其裝置具備足夠的安全功能，以保護敏感資料遺失或遭竊取。面對不斷增加的無數網路威脅，數位防護的完善度和使用者自身端點資料管理技能仍是需要探討的重要風險。內部威脅包括失去資料控管能力或 USB 儲存裝置、在安全環境外傳輸資料、使用未加密 USB 隨身碟以及共用密碼等行為，都可能是缺乏對終端使用者進行盡職調查所致。透過充分的培訓、教育和正確的 USB 隨身碟解決方案，這一切都能避免。

預先規劃和具良好實務演練的溝通架構也是應對潛在威脅的關鍵。今天所指的網路威脅是針對組織中的弱點。

開發加密 USB 計劃的最佳時機是在您實際需要之前，將加密 USB 隨身碟和策略整合到組織的整體安全性策略之中。如果組織沒有制定加密 USB 的計劃，也沒有指導方針，會讓人無所適從，且您的組織會面臨各種層面的風險，包括未遵守法規，例如《一般資料保護規範(GDPR) 第 32 條明確規定敏感資料需進行加密。

> 組織應具備一個明確的資料地圖，包括所有資料集的重要性和敏感度，規劃優先處理最重要的資料，例如實體移除與資料的連結，或停止使用這些資料來源。能快速隔離受影響的系統是箇中關鍵，而擁有一份經實務演練過的書面規劃也很重要。
> - Rafael Bloom

> 使用者處理敏感資料。如果沒處理好，責任會加重，並嚴重影響公司的形象和安全。應採用各種安全解決方案來保護敏感資料，如資料加密。
> - Tomasz Surdyk

# 保護敏感的財務資料

除了安全隱患之外，資料儲存和備份解決方案也必須遵守合規標準。有一些實務做法像管理和執行資料保留規劃，在垂直領域中很常見。至於其他實務做法，例如將企業資料移轉到雲端，這種處理方式則非常不同。

在許多垂直領域中，例如金融服務，已生效的法規會要求進行適當的強制資料管理。尤其是銀行產業一開始非常不願意使用第三方儲存和備份服務，至今仍有許多銀行堅持設置資料基礎設施。

金融機構還必須遵守日益增多的資料安全法規和標準，例如《沙賓法案》(SOX) 和《一般資料保護規範》(GDPR)。然而，隨著員工和承包商數量的增長，也會增加資料外洩和未遵守此類法律及規定授權實行的風險。

事實上，若員工無法保護其所攜帶的數位身分、可攜式工作裝置、客戶記錄和財務資料，合規性被破壞簡直易如反掌。這就是為何越來越多的組織轉而採用 Kingston IronKey 加密 USB 隨身碟等行動安全解決方案，無論員工將 USB 隨身碟帶到何處，都能保護數位身分和應用程式。

> 考量到整體趨勢轉向為更分散的 IT 和雲端基礎設施的純粹可擴展性時，很容易看出大多數產業和中小企業不再關心管理低溫機房。
> - Rafael Bloom

# 安全存取患者的健康資料

醫療保健是另一個資料安全性與以前相比更加重要的產業。患者資訊被竊取的風險更大，2021 年有 4567 萬則患者記錄外洩，是自 2015年以來最高[2]的數據。針對資料儲存和備份，患者資料是最重要且最全面的醫療資訊，能讓醫療保健提供者安全地治療病人。

這可能包括病史、測試、照片、放射檢測圖檔的患者電子健康記錄 (EHR)、薪資記錄、患者保險和應付款項在內的文件內容。隨著流動勞動力不斷增長，且全球醫療保健市場正值重大動盪和轉型，醫療保健提供者十分關心資料安全性也就不足為奇了。

> 隨著勒索軟體的成長，每個處理敏感資料的組織都必須考量在這種威脅下該如何運作。
> - Rafael Bloom

此外，未能預測風險並符合嚴格的要求，例如《健康保險流通與責任法案》(HIPAA)或《經濟與臨床健康資訊科技法案》(HITECH)，可能會導致代價高昂的醫療保健資訊外洩問題，進而動搖患者、合作夥伴和監管機構的信心。

借助 Kingston IronKey 加密系列 USB 隨身碟等解決方案，醫療保健組織可使用單一控制系統來控制幾個或數千個隨身碟和硬碟，確保執行密碼、應用程式使用和還原等設定政策。第一線工作人員可運用使用者友善解決方案，對更多患者提供支援，無需讓員工安裝驅動程式或其他軟體以安全地存取其儲存的資料。無論隨身碟身處何處，使用者和管理員都能輕易快速地鎖定資料。

# USB 隨身碟在未來雲端儲存環境中的角色

> 雲端資料儲存的現在與未來我仍舊認為實體上安全地保護資料，例如使用加密 USB 隨身碟，是最安全的作法。使用者無法完全掌控雲端中所發生的事情。但我們能掌控加密 USB 隨身碟中的資料，因為 USB 隨身碟由我們保護和存放。除了我們，沒有其他人能取得這些 USB 隨身碟。- Tomasz Surdyk

**既然 USB 隨身碟的優點顯而易見，那它們在未來雲端儲存中究竟扮演什麼角色呢？**

十年前，USB 隨身碟的需求量很龐大，它們是便利儲存和傳輸資料的主要工具。然而，隨著新形態混合工作模式和團隊分布逐漸分散的影響，雲端現在能快速簡易地存取許多裝置的資料。過去，隨身碟因傳輸檔案的獨特方便性而大受歡迎。但如今，雲端儲存服務提供了更便利的可攜性。

然而，雲端儲存目前仍存在許多限制。雲端儲存需要連接網路，這不僅影響備份及傳輸檔案的方式和時間，還造成更多安全隱患。當一家公司開始使用雲端時，不一定能控管資料從何存取。因此，使用個人或公共 Wi-Fi 連線來存取 VPN 這樣的簡單舉動，會帶來被駭客入侵的風險。而且，雲端服務對於威脅行為攻擊者而言非常具有吸引力，現今大多數惡意軟體（佔 61%）透過雲端應用程式進行攻擊[3]。

> 企業必須考量雲端服務無法使用時會發生的狀況、長期儲存的位置可能會有安全漏洞，以及資料必須完全掌握等。- David Clarke

# USB 隨身碟在未來雲端儲存環境中的角色


另一方面，USB 加密可以透過裝置的硬體或軟體完成。以硬體為中心的無軟體加密是提供保護並免於遭受網路攻擊最有效的方法。該解決方案十分有效且簡單，能防止資料洩漏，並能藉由終極安全性的資料防護，達到嚴格的合規標準，有助於組織安心管理威脅並降低風險。

因為它們是獨立的硬體型加密 USB 隨身碟，不需要主機電腦上的軟體元件。沒有軟體弱點，也能夠避免暴力密碼破解、探查以及記憶體雜湊攻擊的可能性。軟體型加密 USB 隨身碟還要面臨這種風險，任何使用者都能在任一電腦上將軟體型加密 USB 隨身碟格式化以停用加密功能，而且能以不受保護的方式使用隨身碟存取敏感資料。

硬體型加密 USB 隨身碟還提供了一種特殊的實體方式來保護資料安全。這種隨身碟允許使用者或管理員建立資訊存取標準，並能與現有本地端點的解決方案整合。當面臨雲端儲存無法執行或無法有效解決等問題時，這成為一種便捷且具成本效益的解決方案。另外，當需要將資料儲存到未連線網路的裝置中，例如私人連線或離線存取也適用。

> 根據資料對組織的日常實用程度，我們可以判斷資料是「熱資料」或是「冷資料」。當運作連續性和高效能對於組織或特定關鍵業務功能或流程更為重要時，將「冷資料」存放在雲端，並多加依賴存放在本地 USB 隨身碟中的「熱資料」，可能會更有效率。
>
> - Rafael Bloom

# 摘要

儘管我們無法預測未來的創新走向，但我們提供屢獲殊榮的 USB 隨身碟產品組合，能針對所有等級的行動資料防護需求提供更有彈性的加密解決方案。Kingston IronKey 系列產品是專為應對資料挑戰而設計，具字母和數字鍵盤的 USB 隨身碟，便於使用 PIN 碼防護；經 FIPS 140-2 Level 3 認證，具備最高等級的加密及防竄改防護；採用不影響安全性的 SuperSpeed USB 3.1 技術，且該系列的 USB 隨身碟提供強大且有效的資料傳輸和行動資料儲存解決方案。

我們值得信賴的專家團隊已經準備好支援您的資料儲存旅程。我們會協助您找到合適的儲存解決方案，以滿足您的所有需求。

無論您想建構加密 USB 規劃、確認最適合業務的 USB 隨身碟，還是建立並執行安全性策略，我們的專業能力可協助您保護機密資訊的安全，並遵守新法規。我們提供高度客製化服務，針對資料儲存的重點，致力於提供技術支援的產品，使您能夠跟上業界日新月異的變化。

## 關於 Kingston

Kingston 擁有 35 年的豐富經驗，具備識別和解決行動資料挑戰的知識，可輕鬆地讓您的員工安全地工作，而不會對您的組織造成任何負面影響。

#KingstonIsWithYou

1. Statista - https://www.statista.com/statistics/1062879/worldwide-cloud-storage-of-corporate-data
2. SC Magazine - https://www.scmagazine.com/analysis/breach/breaches-exposed-45-67m-patient-records-in-2021-largest-annual-total-since-2015
3. Infosecurity Magazine - https://www.infosecurity-magazine.com/blogs/cloud-services-top-of-mind-phishers