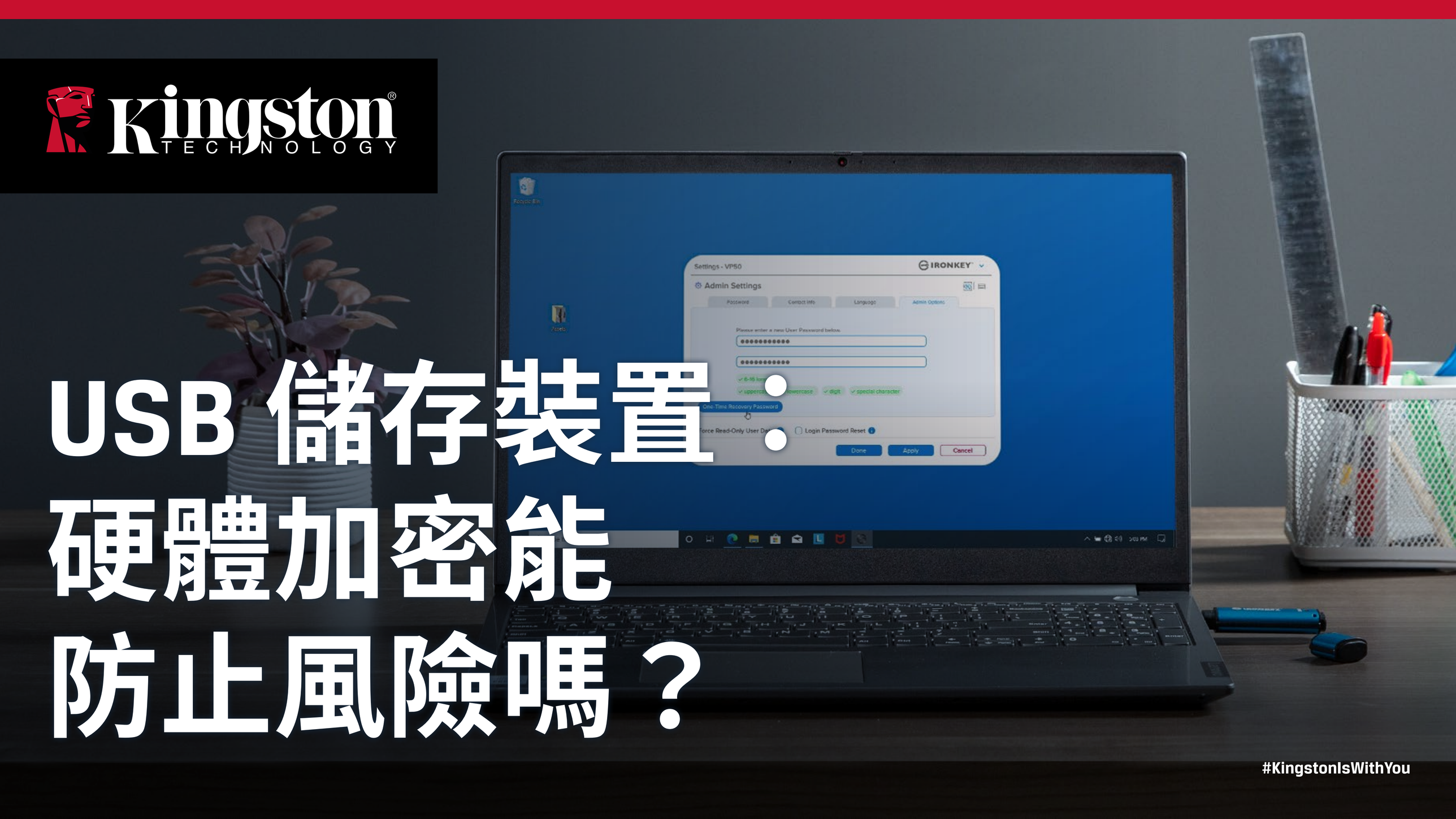
Kingston TECHNOLOGY

USB 儲存裝置：硬體加密能防止風險嗎？



#KingstonIsWithYou

USB 儲存裝置：硬體加密能防止風險嗎？

前言與目錄

現在的企業比以前更關心網路安全，但太多組織對於網路安全威脅一無所知且準備不足。根據 UpCity 指出，在美國只有 50% 的企業有制訂網路安全計畫；其中，有 32% 的企業並未在 COVID-19 疫情開始大流行、許多組織紛紛轉成遠端或混合工作型態後，進一步更新其網路安全計畫。網路攻擊的頻率只會越來越高，全球遭受勒索軟體攻擊的企業比例從 2020年的 37% 增加到 2021 年的 66%[1]。

不安全的網路可能對企業造成毀滅性的影響。除了網路攻擊的金錢損失之外，資料、安全和聲譽損失會造成企業不同層面的短期和長期負面影響。

造成網路安全威脅的常見裝置之一正是 USB 隨身碟。USB 隨身碟使用簡單，只要插入電腦即可，因此 USB 隨身碟在企業內無所不在。然而，就是這種簡便性使得 USB 隨身碟非常容易遭受攻擊。只要有一個隨身碟亂放或被偷，惡意攻擊者就有機會存取敏感資料。此時，加密功能可發揮作用確保 USB 隨身碟的使用安全，並可減少個人和企業的任何相關風險。在本電子書中，我們會回答以下問題：

- 為何加密 USB 隨身碟對於防止網路攻擊來說那麼重要？
- 組織會在哪個環節讓自身易受攻擊？
- 能做什麼準備來保護自己？

USB 儲存裝置：硬體加密能防止風險嗎？

撰稿人

本電子書由 IT 、新興技術領域的產業領導者以及我們的技術專家共同撰寫。

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」中的前十大影響者，同時名列 Kingston Technology 50 大全球專家名單。

Pasi Siukonen

Pasi Siukonen 帶領一支專業團隊，為 Kingston 產品的公關、行銷、現場銷售、技術支援與客戶服務等部門提供支援。他主要著眼於快閃記憶體與 SSD 產品線。

一般隨身碟和加密隨身碟之間的差異

一般未加密隨身碟非常易於取得和使用，但硬體加密能增加實體和數位等多層安全性，讓 USB 隨身碟更加安全。由於一般未加密隨身碟易於取得、低成本又方便攜帶，對使用者來說非常方便。然而，對於想竊取敏感資料、使用惡意軟體或勒索軟體入侵公司網路的惡意攻擊者，一般未加密隨身碟也大開方便之門。由於 USB 隨身碟為現今頻繁使用的產品，面臨網路攻擊的機會數不勝數。與一般隨身碟相關的主要風險有二：

- **勒索軟體攻擊**：藉由 USB 隨身碟，使用惡意軟體入侵公司網路，將其加密以綁架公司資訊和/或系統並勒索贖金。這些攻擊經常是由BadUSB 所引起，且已成為最惡名昭彰的惡意軟體類型。
- **資料失竊**：如果沒有妥善的安全措施，只要隨身碟丟失、失竊或無人看管，無論是客戶資料、原始程式碼，還是敏感的財務和績效資料，都會輕易地被存取。

BadUSB - 利用一般 USB 隨身碟無防護韌體的弱點，使用惡意軟體改寫程式，進行攻擊。此類惡意隨身碟非常普遍，網路犯罪份子易於取得，但大家對此的安全意識仍舊不足。因此，駭客攻擊簡直易如反掌，只要替換掉原本未加密隨身碟中的韌體，USB 隨身碟就能執行設定好的指令碼來攻擊防火牆。許多的網路攻擊是毫無戒心的內部人員所造成的，無論有意或無意。企業使用加密隨身碟來防範這些攻擊很重要，因為加密隨身碟受數位簽章韌體保護，可降低網路犯罪份子成功的機率。

> 與託管式 USB 隨身碟的成本相比，重建基礎設施的成本、贖金或其他敲詐費用可能相當高昂。
> - David Clarke

為何要使用 USB 加密隨身碟？

加密隨身碟是專門設計用於保護資料，以及保護隨身碟可能連結到的其他裝置。因此加密隨身碟是組織 IT 中的重要工具。隨著網路安全威脅升級，加密隨身碟的功能也越來越先進，如此一來才能領先那些想利用隨身碟漏洞的網路犯罪份子。正如您所見的 Kingston IronKey™ 硬體加密產品系列，多年來我們開發最強的 XTS 模式 AES 256 位元加密、堅固可防竄改的外殼、數位簽章韌體、虛擬鍵盤、短語及複雜密碼模式等，提供使用者真正的優質防護，以抵抗各種形式的攻擊。

由於許多企業對於網路風險的瞭解甚少，因此他們會選擇使用一般未加密的 USB 隨身碟，儘管這些隨身碟會帶來各種漏洞。其方便取得、低成本且運用軟體加密等特性，加上 USB 隨身碟使用欠缺企業審核流程，都是漏洞影響的一環。這類組織通常不具備遵守各種 IT 和網路安全標準的最佳操作政策或流程，例如 ISO27001、GDPR、SOC2 和 WISP 等國際標準。這代表只根據意見而非憑藉實證來評估風險，會使得許多組織容易遭受攻擊。

有些人可能會使用具備軟體加密工具的市售隨身碟，然而這只是表面上省錢，因為任何人都能利用網際網路上提供的免費或付費工具，來破解許多軟體加密隨身碟。如果使用者為了方便，或想在不受支援的作業系統平台上使用隨身碟，只需要簡單地將隨身碟格式化，就能將軟體加密從隨身碟中刪除。硬體加密 USB 隨身碟具有「隨時啟動且無法關閉」的加密功能，適合上述用途；並且具備防竄改、防破壞等設計，並使用數位簽章韌體來確保隨身碟的可靠性和完整性。限制密碼嘗試次數 (暴力攻擊法防護) 和虛擬鍵盤 (鍵盤和螢幕側錄防護) 是 IronKey VP50 等加密隨身碟的額外兩項功能，是業界最佳實務設計，能避免惡意攻擊者針對毫無戒心的使用者取得密碼。

如果 IronKey 隨身碟偵測到韌體遭到竄改，它會停用隨身碟並且使之無法啟動，藉此強化安全性。
- Pasi Siukonen

誰會有風險？

任何無法控管 USB 隨身碟的公司確實都曝露於風險之中，而且他們通常不清楚這些風險到底是什麼。而某些公司具備一些特性，使其面對網路攻擊時更脆弱且更具吸引力。

對於醫療保健和金融領域的公司而言，其資料對網路犯罪份子就更具吸引力，而且對公司及客戶的負面影響更大。2017 年，針對英國國民保健署的網路攻擊導致 19000 多個預約被取消，使其損失 9200 萬英鎊的產量，以及還原資料和系統的成本。受影響的患者不僅無法接受醫療保健服務，英國國民保健署對於事先收到的網路威脅警告沒有迅速及充分回應，也受到了嚴厲批評。所有組織都應該瞭解網路安全的最新情報，並且充分瞭解狀況。而處理敏感資料尤其是特殊類別資料的人員，應該對網路風險加倍警惕。

公司的營業額越高，惡意攻擊者能獲得的利益就越大，故公司面臨的網路威脅風險就越高。然而，這並不代表較小規模的組織就不需要擔心網路安全。當企業是較具有吸引力的攻擊目標時，這些企業通常也應具備應對網路威脅的資源和專門人員。然而，許多中小型企業並無專門的網路安全團隊，還可能破例不管控資深主管的 USB 隨身碟，特別容易造成毀滅性的後果。一些研究表明，中小型企業實際上更容易成為網路攻擊的目標。

高階主管的風險更大，因為這些人容易被追蹤，且通常在組織中擁有行政特權。換言之，網路控管 (例如 USB 隨身碟管理程序)並不適用於他們，因此他們容易淪為網路犯罪份子的目標。這就是「隨時啟動」加密隨身碟的優點，對網路安全的充分瞭解，並遵循最佳實務和流程，可大幅降低風險並防範攻擊。

> 近來有許多漏洞，都是惡意攻擊者利用內部人員所造成的，無論內部人員有意或無意。
> - David Clarke

誰會有風險？

> 組織應對網路安全威脅的準備不足。
> - David Clarke

供應鏈是組織的另一個潛在的脆弱點，針對供應鏈的攻擊相當常見。2013 年，美國零售商 Target 遭遇零售業史上最大的資料外洩事件之一，共有超過 4000 萬客戶的金融卡和信用卡資料外洩。就算 Target 本身非常注重網路安全，在受到攻擊前 6 個月才剛剛安裝好一個大規模網路安全系統，但攻擊者已滲透到 Target 的其中一個第三方供應商，藉此取得 Target 主要資料網路的存取權限。共計有 90 起針對 Target 的訴訟，因此 Target 損失了 6100 萬美元。雖然該公司對此次攻擊事件不負有直接責任，但其供應鏈網路安全的弱點足以造成財務和聲譽蒙受損失。

員工的變通辦法也可能是漏洞的來源。這些變通辦法可讓員工的日常工作更有效率，但往往會忽視基本的安全流程和最佳實務，例如密碼管理。英國國家網路安全中心 (National Cyber Security Centre，NCSC) 和美國網路安全暨基礎設施安全局 (Cybersecurity and Infrastructure Security Agency，CISA)的指引相當簡單，但對於不熟悉 IT 和網路安全的團隊而言，執行上特別困難。擁有一個專門的網路安全團隊固然有所幫助，但提供員工正確的工具，例如硬體加密 USB 隨身碟，可大幅降低員工使用變通辦法所帶來的風險。

> 現今的硬體加密 USB 隨身碟易於使用，且易於整合至現有的網路安全政策中。從各種介面 (圖形、鍵盤、觸控螢幕)，到廣泛的作業系統的支援，具備滿足每個組織需求的功能。 - Pasi Siukonen

組織要如何降低網路攻擊的風險？

從組織的角度來看，可以做很多準備來保護端點和資料。如果不具備治理、風險管理及合規性 (GRC) 原則，網路安全實務必然失敗，因此對企業來說最重要的是熟悉並遵循流程以保護自身。具備強大的端點安全軟體還能消除許多網路威脅，並在修補任何安全漏洞時盡可能快速因應。

> 對於風險管理而言，是否採用強制加密政策，和您選擇備份資料與否一樣重要，甚至可能更加重要。
> - Pasi Siukonen

但就個人角度而言，加密硬體可大幅降低網路安全威脅的漏洞。隨著遠端和混合工作型態的興起和熱潮，網路攻擊在去年更是增加許多；因此確保組織每個階層的員工都能安全地處理、傳輸和讀取公司資料，比以往更為重要。硬體加密 USB 隨身碟讓使用者保有隨身碟行動性和便利性的優點，同時也能大幅降低隨身碟的相關風險。一般隨身碟亂放或遭竊，可能造成資料、金錢和商譽損失，而硬體加密 USB 隨身碟則能保護敏感資料不受各種攻擊。網路犯罪份子持續開發新的攻擊方式，加密隨身碟也將繼續研發技術以應付這些新的挑戰。

總言之，應對網路攻擊的成本可說是相當高昂。事實上，組織層級若採用加密隨身碟，的確會涉及更多核准和設定流程；但長遠來看，無論是相對勒索的費用還是聲譽受損造成的收入損失，都能為公司省下大量費用。光是一次資料外洩所導致的法律費用，就遠高於硬體加密 USB 隨身碟的費用。

> Kingston 長期致力於提供絕佳的加密 USB 隨身碟解決方案，我們的產品組合可提供任何組織滿足其網路安全配置，包括產業標準的強制硬體加密、符合端點政策的設計和裝置管理功能等。
> - Pasi Siukonen

摘要

Kingston 持續著重於網路安全領域的發展，確保我們的 IronKey 加密隨身碟符合最新要求，並滿足各種規模組織的網路安全需求。在全球日漸關心網路安全議題的現在，我們相信如果有合適的工具和知識供組織使用，就能充分準備好迎接挑戰，同時保護組織本身、員工和消費者。

關於 Kingston

Kingston 擁有超過 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. https://www.techtarget.com/searchsecurity/news/252516423/Sophos-66-of-organizations-hit-by-ransomware-in-2021