

flash

機密資訊的終極保鑣—**Kingston** 加密隨身碟

**Kingston Flash** 產品經理 林文政





## 資料安全的日趨重要性

- 病毒駭客 - **Google**報告：每十個網站就有一個會自動下載木馬程式到訪客的電腦裡，藉以存取私密資料。
- 商業機密&客戶資料外流：**Fortune** 雜誌針對全美**100** 大企業所做的問卷調查，**70%**違反資安規定造成重要資料外洩的活動都是由內部人員所為。
- 個資法三讀通過：個資遭外洩 最高可求償**2億**

～2010/04/21自由時報



## 行動儲存裝置 – 個人使用便利 = 企業資安危機

- 員工使用便利
  - 可隨意攜帶檔案至辦公室外
  - 可自行使用非公司MIS提供之大容量隨身碟
  - 資料儲放在多樣移動裝置中，大大增加機密資料外洩的風險
- 使用非加密移動式儲存裝置普遍存在的資安漏洞
  - 缺乏完善的資料保護功能
  - 資安人員難以有效管理
- 資安危機個案
  - 2010/06/12 香港 - 九龍醫院護士學校的職員將大約300名學生的個人資料儲存在不具加密功能的隨身碟中，但因將隨身碟遺失在地鐵站，導致300名學生的個人資料外洩。





## 常見的資安防護方式

- 限制USB儲存裝置的使用
  - 缺點：不便於進行資料攜帶傳輸等動作
- 使用資安管理軟體
  - 缺點：需要較多人力、時間資源的投入  
只限於公司電腦、裝置使用
- 指紋碟.密碼碟
  - 缺點：安全層級較低，有被破解的風險
- 軟體加密
  - 缺點：加密處理時間較長  
需手動執行加密/解密，較易出現資安漏洞
- 硬體加密隨身碟
  - 自動執行加密/解密動作
  - 無須額外安裝其他軟體
  - 加密處理速度較快



**Win!**



# 什麼是加密？

- 加密技術是最常用的安全保密方法，利用特定的演算法把重要的資料變為亂碼（加密）傳送，到達目的地後再用相同或不同的演算法還原（解密）。
- 加密技術包括兩個元素：演算法 & 密鑰，演算法是將原始數據與一串數字（密鑰）結合，以進行編碼及解碼的步驟，產生不可理解的密文。
- 可通過適當的加密技術和管理機制來確保檔案傳輸的資訊通信安全

範例：

原始數據：我愛加密碟

密鑰：我-A 愛-B 加-C 密-D 碟-E

演算法：打亂排列順序53214

加密後：ECBAD

# Kingston 硬體加密碟 – 兼顧便利與安全的資安管理方式



- 終端使用者的操作便利性
  - 能安心地在外部環境中(資安網外)使用移動儲存裝置
  - 自動加密/解密
- 資安人員的管理便利性
  - 耐用、容易取得的儲存裝置
  - 快速簡單的安裝方式
  - 硬體加密技術
    - 不需管理者權限即可完成設定
    - 不需另外安裝任何軟體





# 硬體加密 vs. 軟體加密

## 硬體加密



原始檔案

- 自動執行加密動作
- 無須另外安裝其他軟體
- 加密處理較快



AES-256  
加密處理器

加密檔案

## 軟體加密

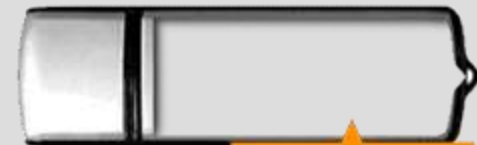


原始檔案

加密軟體

每台電腦都需要安裝  
加密軟體  
處理速度較慢

使用者用隨身碟傳輸檔案時  
可能會忘記啟用加密軟體



加密檔案?





## 入門款加密隨身碟 - DT Locker

產品線	最小讀寫速度	特色 / 優點	容量
DT Locker DTL/xGB	3 MB/s	<ul style="list-style-type: none"><li>• 256-bit AES 硬體加密技術</li><li>• 密碼保護</li><li>• 雙儲存空間: 公共區和加密區</li><li>• 無蓋旋轉設計</li><li>• 企業化商標服務Co-logo</li></ul>	4 ~ 16GB



\*何謂 AES ? Advanced Encryption Standard (AES) 為目前最安全的區塊加密法，為美國聯邦政府所採用的一種區塊加密標準。



## 進階版加密隨身碟 - DT Locker+

產品線	最小讀寫速度	特色 / 優點	容量
<b>DT Locker+</b> DTL+/xGB	3 MB/s	<ul style="list-style-type: none"><li>• 100% 256-bit AES 硬體加密</li><li>• 強化型密碼保護</li><li>• 無蓋旋轉設計</li><li>• 企業化商標服務Co-logo</li><li>• 支援Mac OS</li></ul>	4 ~ 32GB





## 高階版加密隨身碟 - DT Vault Privacy

產品線	最小讀寫速度	特色 / 優點	容量
<b>DT Vault Privacy</b>  <b>DTVP/xGB</b>	10MB/s or 66x	<ul style="list-style-type: none"><li>• <b>100% 256-bit AES</b> 硬體加密</li><li>• 強化型密碼保護</li><li>• 美國製造</li><li>• 防水金屬外殼</li><li>• 客製化</li><li>• 企業化商標服務Co-logo</li><li>• 支援Mac OS</li></ul>	2 ~ 32GB





## 極致版加密隨身碟 – DT 5000

產品線	最小讀寫速度	特色 / 優點	容量
<b>DT 5000</b> DT5000/XGB	5 MB/S	<ul style="list-style-type: none"><li>• 美國製造</li><li>• 採用SPYRUS技術</li><li>• 100% <b>256-bit AES</b> 硬體加密</li><li>• 防水金屬外殼</li><li>• 客製化</li><li>• 企業化商標服務Co-logo</li><li>• <b>FIPS 140-2第2級安全認證</b></li></ul>	2 ~ 16GB



\*何謂 FIPS 140-2認證？「聯邦資訊處理標準」  
美國聯邦政府規定，各單位採購密碼模組相關產品時，限採購通過FIPS 140-2驗證之產品

# 產品規格比較



	DT5000	DTVP	DT Locker+	DT Locker
	加密功能			
部份加密 (公用區 & 加密區)				✓
100% 全加密	✓	✓	✓	
密碼保護	加強型	加強型	加強型	基本型
FIPS 140-2認證	✓			
10次密碼輸入錯誤後，隨身碟會自動鎖住並格式化	✓	✓	✓	✓
	其他功能			
無蓋旋轉設計			✓	✓
防水設計	✓	✓		
讀寫速度(MB/s)	11/5	24/10	10/3	10/3
支援Mac	檔案傳輸	加密功能&檔案傳輸	加密功能&檔案傳輸	檔案傳輸
	產品定位			
目標市場	政府機關	企業/金融機構	中小企業/專業人士	一般消費者/商務人士

## 成功案例 – 會計師事務所&金融機構



- 背景：在業務上有保護客戶資料的需求，所以選擇了 Kingston 加密隨身碟作為其解決方案。
- 採用產品：DTL
- 客戶需求：
  - 密碼防護
  - 雙儲存空間 - 客製化存取空間
  - 硬體加密技術保護





## 成功案例 – 警察機關

- 背景：警察機關在尋求同時具備硬體加密及高速傳輸速度功能的隨身碟產品，Kingston DTVP 提供了最佳解決方案。
- 採用產品：DTVP
- 客戶需求：
  - 密碼保護
  - 完整硬體加密保護
  - 偵測到多次入侵動作後，磁碟即自動鎖住並重新格式化。







## 成功案例 – acer 奧委會專案

- 背景：為了保護奧運選手記錄資料的安全，acer 替奧委會尋找具備256-bit AES加密技術的加密隨身碟。
- 採用產品：DTVP
- 客戶需求：
  - 企業化商標服務 – 加入企業標誌以強化品牌識別
  - 密碼保護
  - 完整硬體加密保護



企業識別列印在隨身碟正反兩面

## 成功案例 – 政府機關



- 背景：為了嚴加保護機密的軍方資料，國防單位希望行動資料都能透過加密隨身碟來進行檔案傳輸，安全等級最高的 DTVP & DT5000 提供最佳解決方案。
- 採用產品：DTVP & DT5000
- 客戶需求：
  - FIPS(聯邦資料處理標準) 認證
  - 完整硬體AES技術加密保護
  - 高速資料傳輸
  - 防水 & 堅固外殼

