

為何無法做到滴水不漏的資料外洩防護？



周世雄 2009/03/05 05:00:00

刊登於 ZDNet 名家專欄「漫談資料外洩防護趨勢」

<http://www.zdnet.com.tw/enterprise/column/jack/0,2000090425,20136352-1,00.htm>

根據美國資料竊盜資源中心（The Identity Theft Resource Center）於 2009/1/6 的統計報告：資料外洩的途徑，內部竊賊的比例達 15.7%、遭駭佔 13.9%、資料搬遷（旅行中資料遺失）佔 20.7%，而意外揭露則佔 14.4%。

也因此，市場上有許多協助企業解決上述問題的產品服務，經我分析，該類產品（即資料外洩防護產品）服務範疇不脫以下四種方式：

- 第一，**防範作者、使用者**：文件的作者、編輯者、使用者洩漏公司的機密資訊。
- 第二，**防範駭客**：駭客、木馬入侵竊取公司機密資訊。
- 第三，**防範設備遺失**：筆記本電腦、隨身碟等設備遺失，洩漏設備內的機密資訊。
- 第四，**防範離職員工**：離職員工帶走公司的重要資料，洩漏機密資訊。

其中，是以如何防堵內賊、甚至是作者以 Email、Web、MSN、隨身碟、列印、照相等方式外洩企業機密資料，最為重要。

資料外洩防護（DLP）產品導入失敗的三大原因

「安全」與「方便」是資料外洩防護（DLP）產品難以取捨的兩難，這也是為什麼某些公司導入「安全」但卻不「方便」的資料外洩防護產品後，因使用者反彈、怨聲不斷，被迫縮小使用規模：僅將該產品運用在少數部門。

上述案例多不勝枚舉，而這不禁讓我們開始懷疑資料外洩防護產品，究竟是適合企業內部廣泛使用？還是只能侷限於少數部門？

依照我的觀察，資料外洩防護（DLP）產品無法廣泛運用在企業內部，與以下三個因素有關：

1. **需要改變使用者的習慣**：如作者需手動設定權限，文件才受保護。
2. **需要犧牲電腦的使用功能**：限制儲存裝置、輸入出裝置、網路、Email、MSN 的使用功能，意味著使用者無法自由自在的透過 USB 隨身碟、MSN，如傳送檔案等。
3. **需要改變管理的制度**：需要先制定企業的權限政策、進行文件的分級，或需要整合到其他系統。



在「[您怎麼落實資料外洩防護?](#)」一文中，我已將 DLP 簡單區分成檔案控管 (File Protection)、周邊控管 (I/O Protection) 與網路控管 (Lan Protection) 等三大類，上述三類產品與導入失敗的 3 個原因有何關係？且待我分析比較如下。

壹、檔案控管 (File Protection)

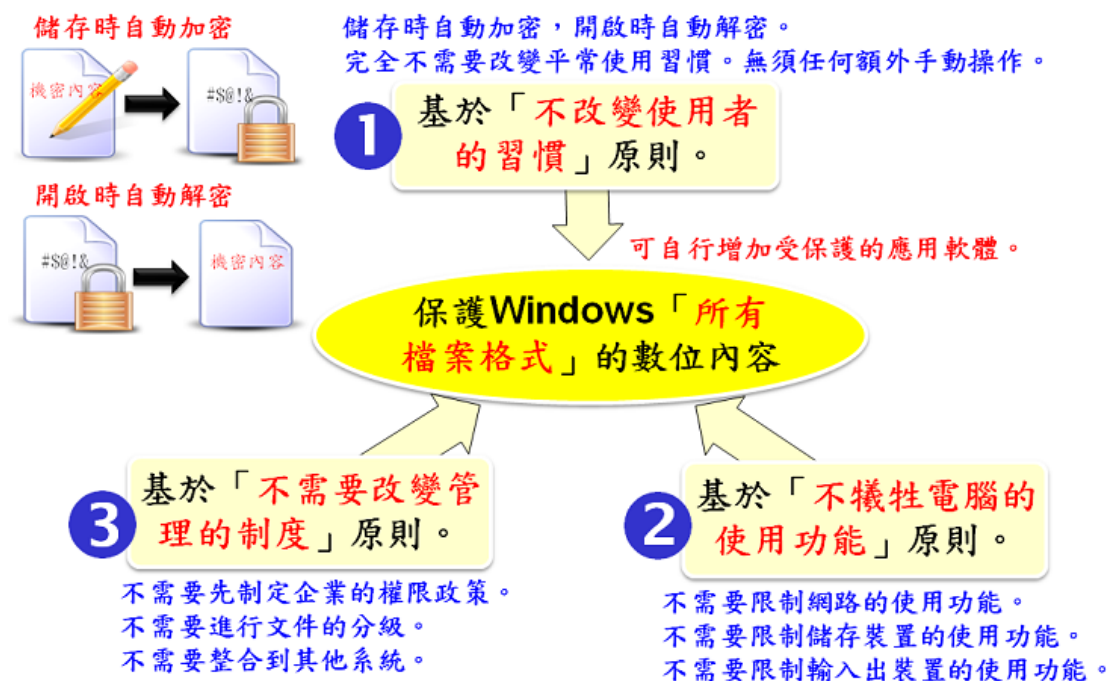
(一) 即時讀寫加解密

當企業使用的檔案控管產品是走「即時讀寫加解密」技術時，意味著員工在儲存與開啟檔案時，系統會自動為該檔案加解密，「不」需要改變使用者的習慣。

由於檔案本身已經加密保護了，所以「不」需要限制儲存裝置、輸入出裝置、網路、Email、MSN 的使用功能，自然的，「不」需要犧牲電腦的使用功能。

再者，也不需要先制定企業權限政策、不需要先進行文件的分級，甚至不需要整合到其他系統，即可佈署導入，所以，「不」需要改變管理的制度。

我個人認為，「即時讀寫加解密」技術的安全性較高，因為該技術不僅對使用者與作者都安全，還可以保護「所有」的檔案格式。



(二) 數位版權管理

至於「數位版權管理」(Digital Rights Management, DRM) 技術，因為需要作者手動設定權限，或多或少得稍稍改變使用者習慣，但若是以集中管理檔案的方式進行：上載到伺服器，即可做到自動加密，「不」需改變使用者的習慣。

而且，當檔案本身已經加密保護，即使外洩也無法開啟，所以「不」需要犧牲電腦的使用功能。

但是使用走「數位版權管理」技術的資料外洩防護產品，得先制定企業的權限政策、進行文件的分級，「需要」改變管理的制度。

在安全性方面，我認為，該技術雖對使用者安全，但對作者不安全。因為作者可將能開啟的檔案資料複製到其他檔案或 email。

另外，數位版權管理技術還有一個侷限，可保護的檔案格式「有限」，僅限於 Office 與 PDF 等。

貳、周邊控管 (I/O Protection)

周邊控管產品，需要限制使用儲存裝置、輸入出裝置等，不僅「需要」改變使用者的習慣，也「需要」犧牲電腦的某些功能。

就我的觀察，周邊控管產品雖然容易佈署導入，但也很容易造成使用者反彈、怨聲不斷。

而且，使用周邊控管產品的企業若沒有將每一種儲存裝置、輸入出裝置都圍堵起來，也會造成安全漏洞。

參、網路控管 (Lan Protection)

若要透過網路控管產品落實即時阻止洩密，定會限制某些網路功能，而這不僅意味著「需要」犧牲電腦的使用功能，也「需要」改變使用者的習慣。當然，若企業是將該類產品用做事後稽核而非即時阻止洩密：側錄產品，則沒有上述問題

另外，相對於可進行及時阻止外洩的網路控管產品，側錄產品除比較容易佈署導入，也不需要先制定相關的權限政策。

而且，跟周邊控管產品一樣，採用網路控管產品的企業若沒有管控到所有的網路功能，無異是開啟了企業安全漏洞。

結語

要導入一個能在企業內部被廣泛使用的資料外洩防護產品，除得考量「安全性」問題外，我認為該盡量避免使用可能得「改變使用者的習慣」與「犧牲電腦的使用功能」的產品，因為上述兩件事很容易造成使用者怨聲載道。

而「改變管理的制度」則是管理者不容易成功地導入的主要原因，因此必須基於「不改變使用者的習慣」、「不犧牲電腦的使用功能」、與「不需要改變管理的制度」的三個關鍵原則下，針對「所有檔案格式」的機密內容自動進行保護措施。

作者周世雄，現任職於「博格科技」公司總經理，從蘋果二號玩到 Web-based、.NET，有二十幾年電腦研發與行銷的工作經驗，歸納十年來數百家企業的 DLP、BPM 導入經驗與需求，逐步整理出有助於企業解決資料外洩防護與商業流程管理等問題的想法。