

您怎麼落實資料外洩防護？



周世雄 2008/11/20 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/0,2000090425,20134302,00.htm>

資料外洩防護（DLP）是啥咪碗糕？

當我們拜訪新竹科學園區的公司、或軍方單位時，常常被要求不能攜帶照明手機，或者得在筆記型電腦的 USB 連接埠上貼上封條等，之所以會有這些防護機制，是因為重大資料外洩事件不斷發生，公司只好使出各種方式防護研發、業務、財務等機密文件。

不過，這與我現在要討論的 DLP 有何關聯性？事實上，無論是上述的「硬體式」防護，或者是我接下來要談論的「檔案管理(File Protection)、周邊管理(I/O Protection)、網路管理(LAN Protection)」，皆屬於 DLP 的範疇。

就我的觀察，截至今日，DLP 的技術發展雖然有不少的進展與突破，但仍不出以下三種類型：

第一，**檔案控管（File Protection）**：透過控管檔案本身避免資料外洩，如將機密文件加密。

第二，**周邊控管（I/O Protection）**：控管周邊硬體，這指限制或紀錄輸出入與儲存裝置等的使用狀況，以防範機密文件透過 USB 等周邊硬體外洩。

第三，**網路控管（Lan Protection）**：控管網路，透過限制、側錄，或記錄藉由網路傳佈的 email、MSN、Skype、http、ftp 等作業，防範機密文件透過網路而外洩。

這三者有何不同，且待我道來。

檔案控管（File Protection）的發展趨勢

當前的檔案控管模式有二，一種是僅能用來防護文件使用者外洩機密文件的「數位版權管理（Digital Rights Management，DRM）」機制，另外一種是可以同時防護文件作者與文件使用者的「即時讀寫加解密」機制。

1、數位版權管理

無論是前幾年較常被市場討論的數位版權管理（DRM）、或企業版的數位版權管理（Enterprise Digital Rights Management，E-DRM），皆起源於微軟在 2004 年大力炒作該議題（那些未引進台灣市場的外商產品先不看）。

微軟為炒做該市場，除針對終端應用軟體與伺服器作業系統推出相對應的產品，如 Office IRM（Information Rights Management）與 Windows RMS（Rights Management Services）等，鑑於協同工作日趨普及，微軟亦於其的企業入口網站產品上，整合上述的 DRM 產品，讓企業員工可以加密透過該企業入口網站上下載的文件。

DRM 的賣點是，即使企業員工不慎將受到 DRM 機制保護的機密文件轉給他人時，其亦無法開啟。

理由是，開啟該文件時，「必須連線到授權伺服器取得授權，才可以開啟文件」，基於此，企業無須擔心機密文件會因有心人士的不法手段而外洩。

不過，自微軟推出 RMS 以來，僅只有微軟的文書系統（Office System）架構在 RMS 上，其他應用軟體業者都未支援 RMS。

企業如欲將其他種應用軟體的文件整合至 DRM 機制中，代表該企業的資訊人員必須透過外掛程式將每一個應用軟體（每一個版本）及欲限制的功能整合至 DRM 機制中，其間過程相當費時費力，事實上，即使做得出來，也可能出現未控制到的安全漏洞。

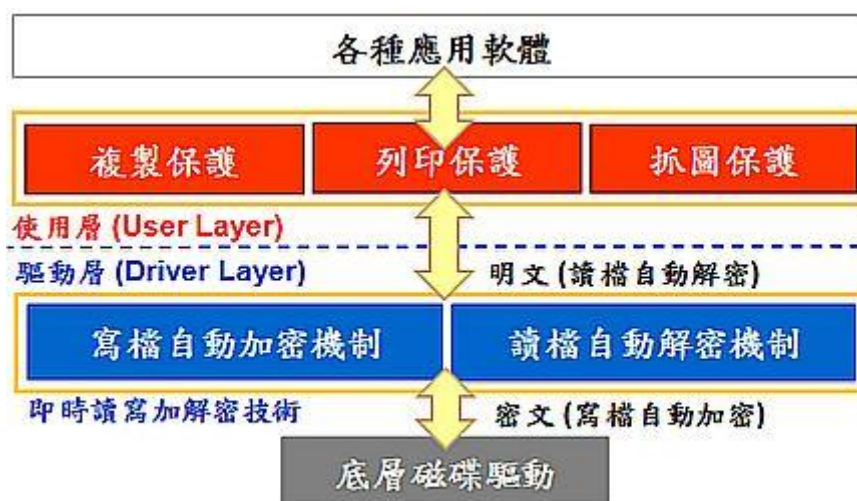
因此，我認為 DRM 僅適用於以 Microsoft Office 與 Arobat PDF 呈現的文件檔案。

另外值得一提的是，**DRM 技術防範的對象是文件檔案的使用者，而非作者**，如文件的作者可以將開啟的機密文件的畫面複製到 email 或其他檔案等，因此，需要一套可以防護作者外洩機密資料的防護工具，在這個狀況下，出現所謂的即時讀寫加解密產品。

2、即時讀寫加解密產品順勢崛起

由於 DRM 不適合保護 Microsoft Office 與 Arobat PDF 外的文件檔案，也無法防範文件作者盜取該資料，因此，標榜可在機密文件儲存時，自動進行加密、開啟時自動解密的「即時讀寫加解密」技術順勢崛起。

「即時讀寫加解密」技術的門檻很高，必須在驅動層（driver layer）設計 kernel-mode driver 程式，直接運行於 Windows 等作業系統的核心（kernel）中，接管檔案系統（見圖一）。



圖一：即時讀寫加解密產品的技術門檻極高。

「即時讀寫加解密」技術上的門檻之所以會這麼高，是為了要確保該機制不會造成用戶電腦不穩定，甚至毀損檔案等情況發生。

透過即時讀寫加解密產品，企業不需限制儲存裝置、輸入出裝置、網路、Email 與 MSN 等的使用功能，因為檔案在儲存時，即處於加密狀態，當然，即便該文件檔案外洩了，也無法開啟。

另外，有的即時讀寫加解密產品，會限制保護文件格式的數量，有的產品則無該問題；若企業採購的事後者，那意味著企業資訊人員可以透過「自行增加」等方式，保護「所有」應用軟體的文件檔案，不需額外花金錢與時間找原廠解決。

周邊控管 (I/O Protection) 的發展趨勢

當企業未採購可加解密機密文件的檔案控管產品時，可以透過圍堵周邊裝置的方式，確保內部機密文件是被妥善且安全的保護，不會透過周邊裝置外洩出去，這種作法，即是我所謂的周邊控管。

做法是，由中央控管所有終端電腦的儲存裝置，以及 **USB 隨身碟、外接硬碟、燒錄機、或印表機等輸出入裝置**，限制上述的周邊裝置是禁用、或僅可讀不可寫等狀態；此外，有些產品的作法是，當終端電腦使用者將資料複製到 **USB 隨身碟、或燒錄到光碟機時**，系統會自動進行資料加密等保護動作。

使用上述的周邊控管產品時，必須特別注意到，該產品是否可以圍堵到每一種儲存裝置、輸入出裝置，若答案為「非」，那些遭遺漏的周邊裝置即可能成為企業的安全隱憂。

事實上，我認為周邊控管產品是種違反人性的產品，試想，當企業員工因工作所需而得在硬碟空間嚴重不足的終端電腦上外接硬碟以維持作業時，上述的周邊控管產品卻加以阻撓，該名企業員工該怎麼辦？因此，**我認為所謂的周邊控管產品，只是 DLP 技術未成熟時的過渡產物**，當 DLP 技術日趨成熟，周邊控管產品必將慘遭市場淘汰。

網路控管（Lan Protection）的發展趨勢

網路控管產品與周邊控管產品的概念相似，是**透過側錄、監控、記錄，或限制藉由網路流通的未加密文件檔案的方式，落實資料外洩防護**。

常見的產品功能有二，一種是針對網路或郵件伺服器進行側錄等動作；另外一種做法是，事先分析機密文件的特徵，再限制機密文件可否透過網路、儲存裝置與輸出入裝置進行傳輸分享，或者是記錄存取該機密文件的使用者記錄等。

我個人認為，**網路控管產品僅適用於事後稽核，甚難即時防堵機密文件洩密**，不過，若是單純用在側錄、監控、記錄那些透過網路傳佈的資料一途，倒是一個不錯的產品。

本次，僅就我的所見所聞，與讀者分享我觀察到的 **DLP** 為何，下一次，我將進一步分享，成功導入 **DLP** 的關鍵因素，以及幾個常見的 **DLP** 迷思。

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。