

企業對資料外洩防護（DLP）的需求與解決方案

此文章由 [中華軟協](#) 發表於 2009 年 5 月 20 日 下午 18:35

作者：博格科技 周世雄 總經理

刊登於 中華民國資訊軟體協會 e 化部落 <http://eblog.cisanet.org.tw/post/20090520dlp.aspx>

歸納五年來近百家企業對於 DLP 的需求和導入實務經驗，與讀者分享從使用者、與管理者角度對 DLP 的需求與其解決方案，並以文件四個階段分析文件發佈前後的資料外洩防護措施，以及即時讀寫加解密和數位版權管理（DRM）產品的適合情境、防範對象、與防範方式。

使用者對 DLP 的需求與解決方案

資料外洩防護簡稱 DLP，為 Data Loss Prevention 或 Data Leakage Prevention 的縮寫。企業對於 DLP 的需求為何呢？其解決方案為何呢？

使用者、與管理者的需求是不同的，首先，讓我們先從使用者的需求來看，大部份的使用者都希望導入 DLP 後，不需要限制週邊硬體、網路的使用（因為會犧牲電腦的使用功能），也不需要改變使用者的操作習慣。

因此使用者的第一個需求為「不需要限制週邊硬體、網路的使用，不需要改變使用者的操作習慣」。

為達到「不需要限制週邊硬體、網路的使用」而仍然可以保護機密文件的需求，唯一的做法為「將機密文件本身加密」，就不怕會經由使用者電腦的週邊硬體（輸出入、與儲存裝置等）、或網路（Email、MSN、Skype、http、ftp 等）外洩機密文件。

若要達到「不需要改變使用者的操作習慣」需求，解決方案為於機密文件儲存時自動進行加密的動作，開啓時自動進行解密的動作，讓使用者不需要額外的操作，甚至感覺不到保護機制的存在。

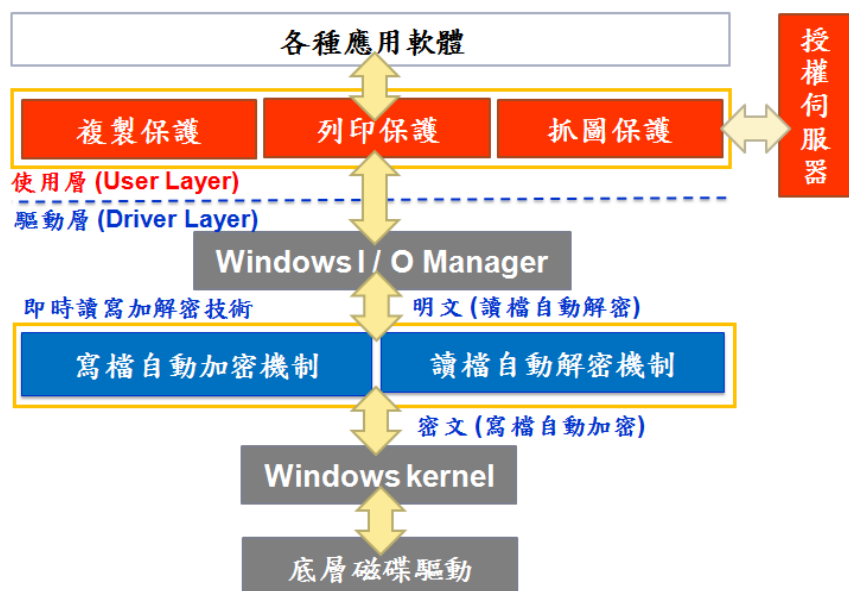
由於使用者期待可以保護許多的檔案格式，若採用外掛（plug-in）程式的做法，來控制應用軟體之選單、工具列按鈕、和快速鍵以限制複製、編輯、列印等功能，則需要於每一個應用軟體與每一個版本都提供一個外掛程式，工程十分浩大，因此我們放棄這個做法。

解決方案為採用「即時讀寫加解密」的技術，設計驅動層（Driver Layer）的 kernel-mode driver 程式，整個加密解密操作過程是自動完成的，無須任何額外手動操作。

「即時讀寫加解密」，直接運行於 Windows 作業系統的核心（kernel）中，接管檔案系統，自動識別什麼文件需要進行加密/解密操作，哪些不需要，將文件資料以密文形式儲存在硬碟機等儲存設備上，當需要讀寫該加密文件時，進行解密，使得系統在授權情況下可以即時地以明文形式讀該加密文件的資料。

所有的文件系統操作都是向 Windows I/O Manager 提出的，再由 Windows I/O Manager 將操作定位到具體某個文件系統來完成。

請參考下圖：



「寫檔自動加密機制」，當文件被儲存時，自動強制加密，最後存放在儲存設備上的文件是經過加密的。

「讀檔自動解密機制」，當文件被開啓閱讀、編輯時，使用者不須事先對文件進行解密，系統根據設定，自動對文件進行解密。

技術上最大的門檻，是必須解決快取記憶體問題，讓受控軟體在保護下運行，不會有明顯的延時，對讀寫文件的效率影響降到最低。利用「即時讀寫加解密」技術，不改變用戶的行為習慣，文件的資料得到安全地加密保護。而各種應用軟體又可以直接即時地以明文方式使用文件。儲存文件時自動轉成受保護的加密文件，包括將檔案儲存、匯出的所有副檔名之檔案，都是加密受保護的。

使用者的第二個需求為「**離線作業**」，即於平常操作時不需要連線到伺服器。

若加解密運作時，必須連線到伺服器，無法離線作業，對於業務人員等需時常外出人員非常不方便。

解決方案為伺服器只負責制定列管的應用軟體、電腦，而用戶端的使用者於儲存開啓文件時的自動加解密動作，都可以離線作業，不需連線到伺服器。

使用者的第三個需求為「**將機密文件給外部使用者，也有保護功能**」。

若給外部使用者的檔案，必須解密成原文，會造成防護上的漏洞。

解決方案為客戶、協力廠商等外部使用者可以完全地離線安裝與使用，不需要連線到公司的伺服器，鎖定特定電腦才可以開啓加密檔案，編輯後檔案仍受保護。

管理者對 DLP 的需求與解決方案

接著，若從管理者的角度來看的話，管理者則期望導入 DLP 時，第一個需求為「**不需要改變目前的管理制度，也不需要花很多時間維護**」。「**不需要改變目前的管理制度**」是讓企業能夠很夠快速導入資料外洩防護（DLP）的很好方法，為達到這個需求，需要做到的：

1. 不需要先制定複雜的企業權限政策。
2. 不需要預先進行文件的分級。

解決方案為將導入過程簡化到兩個步驟：

1. 列出列管的應用軟體、電腦，以及是否與別部門互通機密文件，於伺服器設定。
2. 由伺服器透過網路或離線安裝機制，發佈權限設定到用戶端。

如此一來，「**不需要改變目前的管理制度**」，於所有列管的電腦中，操作列管的應用軟體時，儲存時自動加密，開啓時自動解密，文件本身是加密檔案，只限於列管的電腦中使用，確保資料不會外洩。

對管理者而言，「**不需要花很多時間維護**」，除非權限設定有異動，否則不需要再花時間維護伺服器。

管理者的第二個需求為「**能夠保護的檔案格式不受限**」。

這個需求十分重要，因為企業內需要保護的檔案格式眾多，譬如 CAD/CAM 繪圖軟體可能高達十餘種，而且未來可能採用新的軟體或版本，期待能夠不受限於目前的幾種檔案格式，最好能夠保護所有應用軟體所產生的所有檔案格式文件。

解決方案為當新增加一種檔案格式或新版本的保護文件時，只要於伺服器設定，不需要更改用戶端已經安裝的軟體，可以自行增加，不需要找原廠額外處理。

如此一來，不需要擔憂未來無法採用新的應用軟體，而且當新增加一種檔案格式時，由於不需要更新用戶端的軟體，不需要花很多時間去更新公司每一台電腦的 DLP 軟體。

文件四個階段的資料外洩防護措施

接著，以文件的四個階段來說明文件發佈前後的資料外洩防護措施。

一個文件可能會歷經創作、傳送、分享、管理等四個階段，如下圖：



企業必須針對文件之創作、傳送、分享、管理等四個階段，進行不同的資料外洩防護的措施：

1. **發佈前**：資訊創作、資訊傳送階段為文件「發佈前」的階段，需要防止透過 Email、IM（即時訊息）、隨身碟等方式洩漏公司機密的資訊。
2. **發佈後**：資訊分享、資訊管理階段為文件「發佈後」的階段。於資訊分享階段，需要對檔案伺服器（File Server）、企業入口網站（Portal）、數位學習（E-learning）等資訊分享系統進行資料外洩的防護措施；於資訊管理階段，則必須對生命週期管理、文件管理、流程管理、專案管理、或現有管理系統等資訊管理系統進行資料外洩的防護措施。

讓我們從一個文件的發佈前、後階段，來分析那一個階段適合採用那一種的資料外洩防護（DLP）產品。

「發佈前」的資料外洩防護措施

對於不會放置於資訊分享、資訊管理系統的文件而言，「發佈前」文件的保全措施，以「防作者」為主；「即時讀寫加解密」產品適合於防範「發佈前」機密文件的安全。

爲什麼呢？

原因爲即時讀寫加解密產品，當作者創作文件儲存時，自動進行加密的保護措施，由於是基於「**不改變使用者的習慣**」，與「**不犧牲電腦的使用功能**」兩個原則，作者不會感到不方便，甚至感覺不到其存在，儲存時自動加密，開啓時自動解密，保護「發佈前」的文件安全，以防範內部人員或駭客非法入侵盜取機密文件，解決目前資料外洩防護產品的瓶頸，對「防作者」需求提供了技術上的突破。

「發佈後」的資料外洩防護措施

對於會放置於資訊分享、資訊管理系統的文件而言，「發佈後」文件的保全措施，以「**防一般使用者**」爲主，「**數位版權管理**」（DRM，爲 Digital Rights Management 之縮寫）產品適合於防範「發佈後」機密文件的安全。

爲什麼呢？

因爲 DRM 產品，可以只提供檢視的權限給一般使用者，以限制無法進行複製、編輯、列印、抓錄畫面的行爲，故開啓文件後，仍然受保護。若將加密文件外洩給別人，別人開啓時將因無法從授權伺服器取得使用者授權，而無法開啓，因此可以防範一般使用者盜取公司的機密文件。

防作者？防一般使用者？

企業要選購合適的資料外洩防護（DLP）產品，首先必須先認清是要「防作者」？還是要「防一般使用者」？

若要「防作者」，選擇即時讀寫加解密產品；若要「防一般使用者」，則建議選擇數位版權管理（DRM）產品。

結語

最後，將即時讀寫加解密、與數位版權管理（DRM）等兩種資料外洩防護（DLP）產品的適合情境、防範對象、與防範方式，歸納列表如下，供大家參考：

DLP產品	即時讀寫加解密產品	數位版權管理（DRM）產品
適合情境	保護「發佈前」的文件安全。 適用於保護程式設計、CAD/CAM繪圖軟體、Video/Audio檔案。	保護「發佈後」的文件安全。 適用於保護Microsoft Office、Acrobat PDF檔案。
防範對象	「防作者」洩漏機密文件。	「防一般使用者」洩漏機密文件。
防範方式	作者於讀寫時自動進行加解密的保護措施，儲存時自動加密，開啓時自動解密，符合「不改變使用者的習慣」，與「不犧牲電腦的使用功能」之兩個原則。	發佈給一般使用者時，作者可以直接於應用軟體當中設定保護權限，或將文件上載到企業入口網站、檔案伺服器時自動進行加密保護的保護措施。

作者小檔案

作者周世雄，現為博格科技總經理，從蘋果二號玩到 Web-based、.NET，將二十幾年電腦研發與行銷的工作經驗，以及十年來累積數百家企業的 DLP、BPM 導入經驗與需求，歸納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，以及產品。

榮獲經濟部【新創事業獎】、【創新研究獎】、【卓越 SBIR 產業貢獻獎】、台大創新育成中心【績優廠商獎】等政府獎項，以及 Microsoft【合作夥伴服務英雄獎】、【服務領導有方獎】、【Best IW Solution Partner Award】、【Windows Vista 應用軟體金像獎】、【Microsoft Office System 解決方案獎】等獎項，連絡 Email：JackChou@borg.com.tw