



BorG 資料外洩防護新趨勢

把機密文件「顧條條」

資料外洩導致公司重大損失的案例在國內外屢見不鮮，這也讓今年資料外洩防護(DLP)相關議題從年初討論到年尾，市面上相關的產品更是琳琅滿目，卻讓企業不知該如何選擇。

許多人都有類似的經驗，當走進某些竹科大廠時，有照相功能的手機、USB不能攜入，警衛還會將筆記型電腦的USB埠給貼上封條，種種防護動作都是想要保護企業賴以維生的智慧資產。不過這種做法大多只能防止外部人士竊取內部機密，讓我們再來看看另一個案例。

相當火紅的線上遊戲「天堂3」原計在今年發行；不料在開發的過程中，該專案的負責人利用電子郵件、USB等方式將「天堂3」的程式代碼洩漏出去，並鼓動開發團隊一同離職另組新公司，並利用帶走的資料開發新的

遊戲，讓原公司損失了近10億臺幣。因此，防堵內賊、甚至是作者將資料外洩，是更重要的課題。

目前市面上有許多DLP解決方案，博格科技總經理周世雄將市面上DLP解決方案區分為三大類：週邊控管、網路控管，以及檔案控管。

DLP的分類

周世雄表示，所謂的週邊控管(I/O Protection)顧名思義就是要對企業內的週邊設備包括儲存設備、輸入/輸出裝置，採取管控、禁用措施；網路管控(LAN Protection)則是利用

設備進行網路監控與分析，或對機密文件存取動作進行監控。檔案控管作法主要是所謂數位版權管理(Digital Rights Management, DRM)，即針對文件的最源頭：檔案，來進行加密與保護。

對於專精於研究檔案控管市場多年的周世雄來說，週邊控管與網路控管做法都有其缺點。周世雄表示，週邊控管是屬於圍堵型的做法，必須犧牲電腦部分使用功能，算是一種「綁手綁腳」的方式，並且企圖改變使用者的使用習慣，例如對於某些儲存設備使用者僅有「只讀不寫」的權限，周世雄認

為，這種違背人性與使用者習慣的DLP產品，應該很快會被市場淘汰。

至於網路控管方式做法則有很多種，例如事先分析建立機密文件的特徵值，再限制機密文件可否傳輸分享，或是追蹤機密文件的存取紀錄等，但周世雄認為，這種做法比較適合做事後稽核，較難即時阻擋資料外洩。

從源頭做保護

周世雄解釋，DRM的做法是讓作者可以直接在應用軟體當中設定保護權限，或是將文件上傳至企業入口網站、檔案伺服器時，會自動進行加密保護措施。例如，微軟針對自家的應用程式、軟體在多年前即已推出微軟DRM平臺，因此使用者在Word、Excel、PowerPoint檔案中可以設定他人是否可以讀取、列印、複製等權限；Outlook則可以限制郵件不可轉寄。

但微軟的技術只能用在自家產品中，其他應用軟體廠商都未支援Windows RMS(Right Management Services)

授權伺服器。為因應市場需求，周世雄表示，博格科技多年前即研發出Acrobat Reader的PDF外掛程式，將PDF可以加入支援微軟的RMS，讓作者可以直接於該應用軟體中設定保護權限；不過，對於高科技製造商最重視的繪圖應用程式，如AutoCAD、Pro/E等，仍然無法受到保護與管控。

除此之外，DRM最大缺點是無法防範作者將機密資料外洩出去。周世雄表示，受到DRM保護的文件只有被授權者才能夠開啓文件，若只取得讀取權限的使用者，因為DRM技術已經將複製、列印、抓取畫面等功能取消，因此可以防範未授權使用者開啓/洩漏企業機密文件，但是卻無法防範「作者」將機密資料外洩出去，因為文件作者、程式設計者、繪圖者等仍然可以將文件內容複製到其他檔案，透過電子郵件、USB等將此資料傳送出去。就如同發生在韓國線上遊戲「天堂3」案例，無法阻止開發者將自己開發的資料洩漏出去。

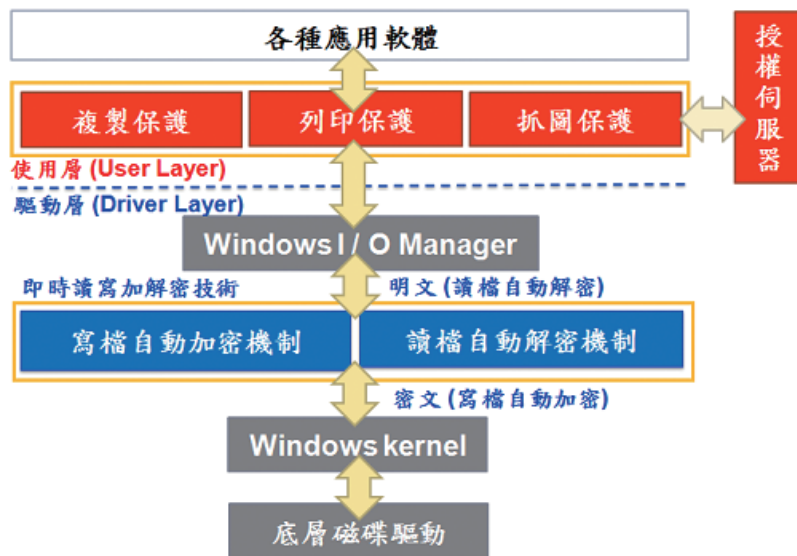
顧後卻無法瞻前

為了要防「作者」外洩機密資料，博格科技在今年8月推出了即時讀寫加解密技術。周世雄解釋此項技術可以在文件儲存時即自動加密保護，在有權限讀取的電腦中開啓，文件會自動解密。

周世雄表示，企業在採用即時讀寫加解密技術需要先設定哪些部門的哪些電腦當中的哪些應用程式需要列管，例如在設計部門中，各種繪圖軟體必須被列管，因此當設計者設計完成設計圖後，一儲存文件就自動加密，使用者若將文件寄至非同一群組的電腦中（也就是該電腦並無安裝特定的Client端軟體），仍然將無法開啓該檔案。

該技術也提供了「單向複製」的功能，經列管的文件內容只能複製到同類型的檔案文件中，無法複製至未經列管的檔案類型中，但是未經列管的檔案類型的文件內容則可以複製到經列管的檔案文件中。

周世雄強調，即時讀寫加解密技術支援所有檔案類型，包括文件、



博格科技的即時讀寫加解密技術。資料來源：博格科技

圖檔、影音檔等，也不用擔心保護機制會造成用戶的電腦不穩定或是檔案毀損問題，因為「該技術是寫在Windows驅動層(driver layer)的程式，直接運行於Windows等作業系統的核心(kernel)中，可以於檔案讀寫時自動進行文件加密和解密操作，因此可以保護所有在Windows作業系統中運行的應用軟體，並突破了文件損毀、電腦易當機等問題。」周世雄說。

但是目前博格科技所開發的即時讀寫加解密技術僅支援Windows，尚不支援Linux系統，周世雄坦言，畢竟Windows的市

場比較大，目前也尚無計畫要針對其他的作業系統進行相關技術的開發。

DLP導入成功的「三不」

周世雄表示，企業若想要成功導入DLP，讓機密資料能安穩地待在公司，首先就是DLP產品不能夠要求改變使用者習慣。因為大多數的人都是懶惰的，要試圖改變使用者的工作流程，就必須要有使用者會「忘記做」的準備，例如要使用者記得在傳送Word文件出去，必須要設保護動作，但如果使用者忘記了，資料就外洩出去了。

其次是不能犧牲電腦功

能，例如不能使用USB隨身碟，周世雄認為，這樣的做法對於大多數的行動工作者都相當不方便，違反人性，也容易導致使用者反彈，讓DLP產品無法落實與部署於企業當中。

最後是不要改變公司的管理制度。周世雄舉例，要導入DRM之前，文件必須先進行分級、也必須要先設定好部門權限、使用者權限等等流程，由於牽涉範圍過廣，往往讓DLP在導入之後，只有少數人在使用，對企業來說可謂勞民傷財又看不到導入後的實質成效。

周世雄表示，透過即時讀寫加解密技術可以讓員工在被保護的環境之下，正常閱讀、編輯文件，不需改變使用者的習慣，不需監視或封鎖網路，也不用阻擋週邊設備，更不用犧牲電腦使用功能。周世雄表示，這項技術是由國內4所大學：臺大、臺科大、長庚大學、東吳大學一同研發而成，國內許多製造業、IC設計業都對此技術有極大的興趣與需求，目前也將大力推廣此項技術。