

賽門鐵克強化端點防護 推出最新版防止資料遺失解決方案

Data Loss Prevention 9.0 為迄今最重要的產品版本 協助企業對抗新威脅

全球領先的安全、儲存與系統管理解決方案廠商賽門鐵克 (Nasdaq: SYMC) 今(23)發表**資訊風險管理策略**產品之一 ——**Symantec Data Loss Prevention 9.0** 版，無論資訊於使用中或儲存的狀態，這套產品可加強企業組織對於機密資訊的搜尋、監控和保護能力。賽門鐵克藉由單一整合式介面保護結構化與非結構化資料，為企業提供全面性的防止資料遺失 (Data Loss Prevention, DLP)，範圍涵蓋端點、網路和儲存系統。

賽門鐵克透過持續的產品創新、對於客戶需求的回應，以及與賽門鐵克技術的互補整合，建立**賽門鐵克於 DLP 的業界領導地位**。Symantec Data Loss Prevention 新版本主要的創新部分包括：擴大對端點事件的涵蓋範圍、簡化端點 DLP 代理程式的管理以及增強資料搜尋的功能。

完整的端點事件涵蓋範圍

DLP 方案原先著重於阻止因員工疏失錯誤和業務流程遭到破壞時，所導致的機密資料暴露。然而，許多企業組織認為，惡意行為對機密資訊所造成的最大風險，是當員工處於行動狀態而未連線到公司網路的時候。為了防禦此種威脅，Symantec Data Loss Prevention 9.0 將資料遺失事件的涵蓋範圍擴大到自端點開始。賽門鐵克現在可防止員工在與公司網路中斷連線時，因使用筆記型電腦傳送電子郵件、網頁式電子郵件和即時訊息(Instant Message) 所造成的資料遺失。

Symantec Data Loss Prevention 的設計會阻止在端點上機密資訊的複製(copy)或貼上(paste) 動作，甚至防止此資料利用電子方式列印或傳真。這些新功能新增至賽門鐵克現有的控制中，可預防機密資料複製到 USB 裝置或 CD/DVD 光碟機。另外，憑藉賽門鐵克在**內容(content-aware)**偵測方面的專業知識，能辨識不論以何種封裝形態而存在的特定內容，對於成功的端點 DLP 防護也是十分關鍵。藉由全面的端點 DLP 事件涵蓋範圍，不論員工是否連接到公司網路，賽門鐵克都可提供不間斷的防止資料遺失功能。

端點 DLP：易於部署與管理

在整個企業組織部署新代理程式技術時，一個重要的成功因素便是解決方案是否能尋找到所有的端點，成功地部署代理程式，並依需求進行相關疑難排解。端點 DLP 的遞送(rollout)通常需先將技術部署至資訊風險較高的部門，然後再分階段遞送至企業組織的其餘單位。Symantec Data Loss Prevention 9.0 內建賽門鐵克完善的代理程式管理技術，可讓公司連續不斷地搜尋新的端點資產，自動部署代理程式及疑難排解端點代理程式所產生的問題，協助客戶簡化端點 DLP 的 部署與持續管理。Symantec Data Loss Prevention 同時也內建超過全球 22,000 多家公司使用且經過實證的賽門鐵克 Altiris 產品系列端點管理技術。

Esurance 資訊管理服務部的資深網路管理經理 David Aflak 表示：「賽門鐵克 DLP 解決方案的持續創新，讓我們能夠更容易且更有效地保護整個企業組織的資訊。以資料防護為重點的強化，例如，單一端點的管理主控台，讓我們更容易在整個企業組織中部署及管理」。

進階資料搜尋

除了增強的端點 DLP 防護以外，Symantec Data Loss Prevention 9.0 也加強了資料搜尋功能。企業客戶需要兩種內容搜尋模式，一種是傳統模式，會檢查內容儲存庫中的每個檔案是否違反政策，另一種是遵循模式 (compliance mode)，會快速匯總違反法規的伺服器 and 儲存庫。賽門鐵克在單一的解決方案中同時提供客戶兩種選項，目前尚未有其他產品能達成。

更快速的詳細目錄掃描(inventory scan)可協助企業快速找出包含機密資訊的資料儲存庫，讓企業更清楚資料風險與法規遵循的問題點。例如「遵循掃描(compliance scanning)」模式可大幅減少花在掃描的時間。同時企業組織也能評估儲存在 PST 檔案中機密資料的相關風險。最後，企業將可自動識別擁有機密資料權限的使用者，這對於清理散亂的機密檔案，以及實行可擴充的矯正程序管理是非常重要的。

智慧型產品整合

賽門鐵克管理平台 (之前稱為 Altiris 平台) 除了運用 Altiris 以簡化端點 DLP 代理程式管理以外，也可用於管理 Symantec Endpoint Protection 和 Symantec Backup Exec System Recovery 的代理程式 - 協助賽門鐵克客戶簡化遞送、協助自他牌產品移轉及保護端點組態。Symantec Data Loss Prevention 9.0 和 Symantec Brightmail Gateway 整合，讓客戶得以檢查入埠(inbound)和出埠(outbound)電子郵件中是否有惡意軟體、垃圾郵件以及資料遺失風險。此外，Symantec DLP 9.0 的設計也能夠掃描 Symantec Backup Exec System Recovery 所執行的階段式備份。

賽門鐵克防止資料遺失解決方案部門副總裁 Michael Wolfe 表示：「與 Symantec Management Platform、Brightmail Gateway 和 Backup Exec System Recovery 等賽門鐵克解決方案的智慧型整合，讓我們得以擴大防止資料遺失的界限，並超越客戶的期望。賽門鐵克將我們領先業界的互補技術與全球觸角結合，協助全球各地的用戶能安心地防止機密資訊遺失。」