Symantec Data Loss Prevention 解決方案

搜尋、監控並保護您敏感的公司資訊

產品型錄：**Data Loss Prevention**

在行動化雲端環境中保護您的資訊

確保企業敏感資訊的安全和遵循法規，絕非容易的事。然而在今日，您面對的是一系列全新的資料防護挑戰。由於越來越多的員工透過消費性雲端儲存服務分享檔案，並在自己的行動裝置上存取這些檔案，因此，敏感資訊已不在貴公司網路的安全防護範圍內。網路罪犯不斷想方設法擊潰傳統的安全措施，並竊取公司資訊，目標式網路攻擊也持續增加。當所有這些因素加總在一起時，管理與保護公司資訊並防止資訊外洩或遭竊，也變得益發困難。

那麼，您要如何在這樣充滿挑戰的環境中管理和保護資訊呢？面對日漸消失的安全邊界、層出不窮的目標式攻擊以及不斷演進的使用者習慣與期待，要如何應對才是完整又成功的資料防護策略？

Symantec Data Loss Prevention (簡稱 DLP) 透過回應當今雲端化與行動化現實狀況的全方位資訊保護方式，為這些問題提供了解答。利用 DLP，您就能達到以下目標：

- **搜尋**資料在雲端、行動裝置、網路、端點及儲存系統中存放的位置
- **監控**員工在登入企業網路及離線時如何使用資料
- **保護**資料免於外洩或遭竊，無論資料的儲存位置或使用方式，都能提供保護

賽門鐵克領先市場的方法和技術，能讓您的 DLP 功能擴展到雲端和行動裝置。並可將安全性和遵循政策延伸至您本身的網路之外。此外，它具備通過考驗的部署方法、直覺式的政策和資安事端管理工具，以及保護您遠離所有高風險管道的全方位涵蓋範圍，可提供您最低的整體持有成本。

利用具備內容感知的偵測功能搜尋更多資料

Symantec DLP 的基礎是一組無論資料正在儲存中、傳輸中或使用中，都能夠正確偵測企業中所有機密資料的進階技術。Symantec DLP 當中的偵測技術包括：

- **精確資料比對 (Exact Data Matching，簡稱 EDM)** 是透過比對結構化資料來源的方式來偵測內容，包含資料庫、目錄伺服器或其他結構化資料檔案。
- **索引式文件比對 (Indexed Document Matching，簡稱 IDM)** 運用比對方法來偵測儲存在非結構化資料 (包含 Microsoft Office 文件、PDF，以及像是 JPEG、CAD 設計圖和多媒體檔案等二進位檔案) 中的機密資料。IDM 也可偵測「衍生性」的內容，例如從來源文件複製到其他檔案的文字。
- **向量機器學習 (Vector Machine Learning，簡稱 VML)** 可保護具有罕見或難以描述之細微特徵的智慧財產，例如財務報表和原始程式碼。它能藉由對非結構化資料執行統計分析來偵測這類內容，並將它和相似的內容或文件加以比較。VML 與其他偵測技術不同之處在於，該技術不會要求您定位、描述或比對您需要保護的資料。

- **描述性內容比對 (Described Content Matching，簡稱 DCM)** 能針對特定關鍵字、規則運算式或模式以及檔案屬性尋找相符項目，藉此偵測內容。Symantec DLP 提供了 30 個立即可用的資料識別碼，也就是結合模式比對與內建情報以防止誤報的預先定義演算法。例如，「信用卡號」資料識別碼可偵測 16 個數字的模式，並使用「Luhn 檢查」加以驗證。
- **檔案類型偵測**可識別並偵測超過 330 種不同的檔案類型，例如電子郵件、圖形和封裝格式。您可以設定 Symantec DLP 來辨識幾乎任何一種自訂的檔案類型；它也可以讓您使用內容擷取應用程式開發介面 (Content Extraction API)，從特定檔案格式 (包括加密格式) 擷取內容。

搭配使用這些具內容感知能力的偵測技術，就能夠減少誤報、將 DLP 對使用者的影響降至最低，而且幾乎能尋找以任何檔案格式儲存在任何位置的機密資訊。

以一致的方式在整個環境中定義並強制執行政策

隨著資料遍及更廣大範圍的裝置和儲存環境，以一致的方式定義和強制執行政策的能力也變得至關緊要。Symantec DLP 具備整合式管理主控台 DLP Enforce Platform，以及業務情報報告工具 IT Analytics for DLP，讓您只需撰寫一次政策，就能在任何地點強制執行，大幅降低資訊風險。使用 **DLP Enforce 與 IT Analytics**，您就能夠：

- 使用**單一網頁式主控台**定義資料遺失政策、檢討和矯正資安事端，以及對所有端點、行動裝置、雲端服務和內部網路及儲存系統執行系統管理工作。
- 利用 **60 多種預先建置的政策範本**以及便利的**政策建置工具**，讓您的 DLP 解決方案能夠快速上線並持續運作。
- 利用穩健的**工作流程與矯正功能**，簡化並自動化資安事端應變流程。
- 利用可提供進階報告和突發性分析功能的**精密分析工具**，將**業務情報**套用至您的 DLP 工作中。其中包括擷取系統資料並歸納成多維立方體 (Multi-Dimensional Cube)，然後針對企業中不同的業務關係人建立相關報表、儀表板和計分卡的能力。

Symantec DLP 能夠協助您在多樣化的環境中尋找和監控所有機密資料。若再搭配 Enforce Platform，則更能確保您能夠運用一致性的政策並採取適當行動，以保護資訊安全無虞。

監控和保護您的雲端儲存和電子郵件

對於許多企業來說，將部署於內部的應用程式移至雲端，是提高彈性與降低成本的明智方式。但在充分利用雲端優勢的同時，該如何保有能見度以及對於公司敏感資訊的掌控度？**Symantec DLP for Cloud Storage 與 Cloud Prevent for Microsoft Office 365** 能藉由針對雲端儲存和電子郵件提供健全的搜尋、監控和保護功能，解決上述問題。

Symantec DLP for Cloud Storage 可進行安全協同合作，讓您深入瞭解使用者在 Box 上儲存和分享的所有公司檔案。它包含了功能強大的內容搜尋功能，可讓您輕鬆掃描 Box Business 與 Enterprise 帳戶，並瞭解敏感資料的儲存位置、使用方式和分享對象。Cloud Storage 甚至可透過在 Box 檔案上放置視覺化標籤，以及透過直覺式的線上入口網站「Symantec DLP 自助服務入口網站」啟用資安事端矯正，讓使用者自行矯正違反政策的情況。

Symantec DLP Cloud Prevent for Microsoft Office 365 與 Office 365: Exchange Online 緊密整合，讓您安心地將電子郵件移轉到雲端。您可以利用健全的內容監控和防護功能，獲得深入的能見度並控制使用者傳送的敏感電子郵件。利用 Cloud Prevent，您就能夠偵測敏感的公司資訊，並在適當時機採取適當的行動，例如通知使用者違反政策、將電子郵件重新導向至加密閘道以安全方式傳送，或是即時封鎖電子郵件，以防止重要資料外洩。

確保傳統端點上的資料安全無虞

雖然行動裝置和雲端儲存日漸普及，但端點仍然是公司機密資訊的主要儲存區。**無論使用者是否正在您的公司網路上或已離線，Symantec DLP Endpoint Discover 與 Endpoint Prevent** 都能讓您搜尋、監控和保護傳統桌面與虛擬桌面上的機密資料，進而可確保您的所有資訊安全無虞、受到妥善保護。

利用 Symantec DLP 高擴充性的單一代理程式，就能同時啟用 Endpoint Discover 與 Endpoint Prevent 模組。兩者搭配使用，您就能達到以下目標：

- **在 Windows 7、Windows 8、Windows 8.1 和 Mac OS X 電腦上，**針對各種事件執行本機掃描、偵測與即時監控。
- **監控筆記型電腦**與桌上型電腦正在下載、複製或傳輸的機密資料。包括：
  - **應用程式：**Outlook
  - **雲端儲存：**Box、Dropbox、Google Drive、Microsoft OneDrive
  - **電子郵件：**Outlook、Lotus Notes
  - **網路通訊協定：**HTTP/HTTPS、FTP
  - **抽取式儲存裝置：**USB、MTP、CF 和 SD 卡、eSATA、FireWire
  - **虛擬桌面：**Citrix、Microsoft Hyper-V、VMware
- **偵測到違反政策的情況時，**利用螢幕上的快顯視窗通知使用者或封鎖特定動作。
- 掃描筆記型電腦與桌上型電腦的本機磁碟，提供機密資料的完整清查，讓您能夠保護或重新安置已暴露的檔案。
- 使用多種掃描選項 (例如閒置掃描和差異掃描)，在高效能平行掃描數千個端點時，儘可能降低對於系統的影響。
- 部署可保護數十萬名端點使用者的高擴充性多層式架構。

將完整的資料防護功能擴充至您的行動裝置

自攜裝置 (BYOD) 使得工作與個人生活的界線日漸模糊。現今的使用者普遍期望能夠隨時使用任何連線類型從任何裝置存取敏感的公司資料。事實上，每 5 位員工中，就有 2 位承認他們曾下載工作用的檔案至個人手機和平板電腦上。Symantec DLP for Mobile 可為您提供面對此趨勢所需的能見度與掌控度，並為使用者提供彈性的行動存取方式，而且不會讓您的資訊處於風險之中。使用 Symantec DLP for Mobile，您就能達到以下目標：

- 將 DLP 監控和防護功能延伸到您的所有 iOS 與 Android 裝置，無論是誰擁有這些裝置。
- 利用進階的 Mobile Email Monitor 模組，在使用者透過 Microsoft Exchange ActiveSync 通訊協定將機密電子郵件下載至自己的 Android 與 iOS 裝置時予以偵測。這些監控功能都部署在您的網路出口點，並與反向 Web proxy 整合，提供流暢的行動電子郵件監控功能。
- 使用 Mobile Prevent 模組監控使用者的活動，並防止透過原生 iOS 郵件用戶端、瀏覽器和其他應用程式 (例如 Dropbox 與 Facebook) 傳輸機密資料。Mobile Prevent 可透過 3G 與 4G 行動通訊網路、Wi-Fi 網路和 iOS VPN On Demand 連線至您的企業網路。離埠行動流量會透過 VPN 路由傳送到您的 Web proxy、再傳送到 Mobile Prevent，而後者會分析資訊並自動修訂或封鎖機密資料。

尋找並保護難以捉摸的非結構化資料

非結構化資料正以每年 70% 的驚人速度增加，因此許多企業為了有效管理和保護資料而忙得焦頭爛額也是意料中事。將 Symantec DLP Network Discover、Network Protect、Data Insight 與 Data Insight 自助服務入口網站搭配使用，您就能夠控制所有非結構性資料不再受到粗心的員工或惡意攻擊者危害。

首先，Symantec DLP Network Discover 會掃描網路檔案共用、資料庫和其他企業資料儲存庫，以搜尋並找出機密資料。其中包括 Windows、Linux、AIX 和 Solaris 伺服器、Lotus Notes 與 SQL 資料庫以及 Microsoft Exchange 與 SharePoint 伺服器上的本機檔案系統。DLP Network Discover 可根據檔案的二進位特徵，辨識超過 330 種不同的檔案類型，包括自訂檔案類型。它也針對大型的分散式環境提供高速掃描功能，同時它還透過只掃描新增檔案或修改過的檔案，將效能最佳化。Network Discover 部署於您的公司 LAN 環境當中，且直接透過集中化的 Enforce 平台來溝通政策和資安事端資訊。

接著，Symantec DLP Network Protect 會在 Network Discover 之上增添健全的檔案防護功能。Network Protect 會自動清除並保護 Network Discover 偵測到的所有已暴露的檔案，並提供各種矯正選項，包括隔離或移動檔案、將檔案複製到隔離區，或是將政策加密和數位權限套用到特定檔案。Network Protect 甚至會在檔案的原始位置留下標記文字檔案，說明檔案遭隔離的原因，以便教育企業使用者關於違反政策的情況。

Symantec DLP 還包含 FlexResponse API Platform，讓您建置自訂檔案矯正動作。FlexResponse 可輕鬆地與賽門鐵克和第三方檔案安全解決方案立即進行整合，這些解決方案包括 Symantec File Share Encryption、Microsoft Rights Management Services、Liquid Machines、GigaTrust 及 Adobe LiveCycle。

最後，Symantec Data Insight 會從網路連接儲存 (Network Attached Storage，簡稱 NAS) 檔案伺服器、Windows 伺服器和 SharePoint 中，收集和分析使用者事件。這套資料管理解決方案是專為非結構化資料環境而設計，可針對資料擁有權、使用方式和存取控管提供豐富且可行的情報。Data Insight 也可與 Network Discover 整合，以搜尋機密檔案、識別資料擁有者、瞭解檔案權限和存取歷程記錄，並在發生異常的使用者活動時對您發出警示。利用 Symantec Data Insight，您就能夠瞭解您的環境中存在哪些資料、資料的使用方式、擁有者和存取者，也終於能夠對那些難以捉摸的「黑暗」資料照亮一線曙光。

Symantec Data Insight 也提供自助服務入口網站，讓資料擁有者能夠檢討和矯正網路檔案資安事端，也使得資安事端矯正工作流程的功能更有效率。藉由 Data Insight 自助服務入口網站，資料擁有者就會在發生違反政策的情況時自動收到電子郵件通知，並導向直覺式網頁入口網站，以矯正違規情事。IT 安全團隊也可以透過 Enforce Platform 的管理主控台，來檢閱和追蹤資安事端的活動。

將這四個基本的 DLP 模組搭配使用，幾乎就能夠搜尋、保護和管理所有儲存系統上的機密資料，讓您所有的非結構化資料安全無虞，無論資料成長速度有多快皆能應付自如。

監控和保護您傳輸中的資料

研究顯示，約有半數的員工會定期透過電子郵件將工作檔案寄送至個人的信箱，無怪乎電子郵件和網路會成為最常見的資料外洩管道。Symantec DLP Network Monitor、Network Prevent for Email 和 Network Prevent for Web 可藉由讓您監控各種網路通訊協定，並防止已授權或未經授權的網路使用者對機密資料做出不當處理，協助免除這個幾乎所有企業都會面臨的共通問題。

首先，Network Monitor 會偵測透過各種網路通訊協定傳送的機密資料，包括 SMTP、HTTP、FTP、IM、NNTP、自訂通訊埠特定的通訊協定，以及網際網路通訊協定版本 6 (IPv6)。它能夠在零封包損失的情況下，針對所有網路通訊執行深度內容檢測，不像其他的解決方案在尖峰負載期間進行封包取樣，而使您承擔誤報的高度風險。Network Monitor 部署於網路出口點，並且可與您的網路閥門或交換式連接埠分析器 (Switched Port Analyzer，簡稱 SPAN) 整合。

接著，Symantec DLP Network Prevent for Email 會檢測公司電子郵件是否有機密資料、通知使用者違反政策，以及將電子郵件封鎖或導向至機密閘道，以便安全地傳送。Network Prevent 也是部署在您的網路出口點，並與遵循 SMTP 的郵件傳輸代理程式 (Mail Transfer Agent，簡稱 MTA) 和雲端服務 (例如賽門鐵克電子郵件安全雲端服務) 整合。

最後，Symantec DLP Network Prevent for Web 可檢測透過 HTTP 和 HTTPS 傳送的傳出流量、通知使用者違反政策、以及封鎖或有條件地移除網頁貼文中的資料。正如同其他兩個模組，Network Prevent for Web 也是部署在您的網路出口點，並與遵循 ICAP 的 Web proxy 和雲端服務 (例如 Google Apps 及賽門鐵克網頁安全雲端服務) 整合。

現在就開始建置您的統一資訊防護解決方案

賽門鐵克已經準備就緒，可協助您將防止資料外洩功能延伸到雲端和所有高風險的資料外洩管道，無論資料在儲存中、傳輸中或使用中，都能讓您以更完整且有效的方式搜尋、監控和保護資訊。

歡迎造訪 Symantec.com/data-loss-prevention 瞭解更多資訊，並探索在目前行動雲端環境的資料外洩防護基礎上，採用統一方式的優點。

系統需求

Symantec DLP 包含了整合式管理平台、具內容感知能力的偵測伺服器與輕量型端點代理程式。它也提供各種彈性的部署選項，包括內部部署、混合雲端以及委外管理服務 (透過 Symantec DLP 專業化認證合作夥伴)。不同於其他防止資料外洩解決方案，賽門鐵克所提供的解決方案已經過證實，能夠在高度分散的環境中運作，且可擴充供數十萬個使用者和裝置使用。

DLP 伺服器

作業系統	Microsoft Windows Server 2008、2012 Red Hat Enterprise Linux VMware ESX 與 ESXi
處理器	2 個 3.0 GHz 處理器
記憶體	6 至 8 GB
儲存空間	140 GB
網路	1 個銅軸纜線或光纖 1GB/100MB 乙太網路網路介面卡
資料庫	Oracle 11g 標準版

DLP 端點代理程式

作業系統	Apple Mac OS X Microsoft Windows Microsoft Windows Server 2003、2008 Citrix XenApp 與 XenDesktop Microsoft Hyper-V VMware Workstation 與 View
記憶體	25 至 30 MB
儲存空間	70 至 80 MB

更多資訊

請造訪我們的網站

http://go.symantec.com/dlp

關於賽門鐵克

賽門鐵克保護全世界的資訊，也是安全、備份與可用性解決方案的全球領導廠商。我們創新的產品與服務能保護任何環境的人員與資訊，從最小的行動裝置到企業資料中心，乃至於雲端系統。我們在保護資料、身分與互動方面領先產業的專業能力，讓我們的客戶在連線世界中充滿信心。如需更多資訊，請造訪 www.symantec.com/zh/tw。

台灣賽門鐵克股份有限公司

地址：台北市信義路五段 7 號台北 101 大樓 13 樓 A 室
電話：(02) 8726-2000
傳真：(02) 8726-2199
www.symantec.com/zh/tw

21350666 07/15