McAfee DLP Monitor

保護最敏感的資訊

主要優點

識別及保護敏感資訊

- 透過直覺式的搜尋引擎快速識別敏感資訊
- 實施鑑識分析以使現在與過去的風險事件相互關聯、偵測風險趨勢及識別威脅
- 立即建立規則以預防未來的行為

擷取所有網路流量並編制索引

- 篩選及控制敏感資訊以識別隱藏或未知的風險
- 為所有類型的內容編制索引，然後再進行查詢及挖掘以瞭解敏感資料及找出這些資料傳送的目標位置
- 監控內部檔案共用存取

建立及調整精密的規則

- 識別超過 300 種透過任何連接埠與應用程式傳送的獨特內容類型
- 跨越連接埠的限制將網路流量分類
- 能予以擴充以支援數十萬個同時連線

保護客戶與員工個人隱私資料（不論是身分證字號、信用卡號碼或其他個人資訊）是所有組織的責任。意外揭露資訊是發生資料遺失的首要原因。員工犯錯、遺失筆記型電腦及遺忘 USB 裝置等都是組織面臨到的主要安全性挑戰。連同如 Google Gmail、Yahoo! Mail、即時傳訊、Facebook 及其他等 Web 應用程式，這些都是代表資訊遺失的主要通訊管道。現在的組織需要能分析所有網際網路通訊及判斷資訊是否前往不當處所的高效能資料遺失防護解決方案。這些工作的進行都應避免使負荷業已過重的資訊安全團隊增加額外負擔。除了這些挑戰之外，法規遵循與智慧財產保護的重要性也不容小覷。

監控、追蹤傳輸中的資料並提出報告

不論業務類型為何，您都需要能識別透過任何應用程式、任何通訊協定、任何連接埠、及任何形式傳送之敏感資訊的可見性，同時還必須兼具高度的準確度。

有了 McAfee® Data Loss Prevention (DLP) Monitor 之後，您可以即時收集、追蹤在整個網路中傳輸的資料並提出報告，因此能瞭解有哪些資訊透過哪些方式在使用者與其他組織間流動。McAfee DLP Monitor 是一款高效能、以目標為導向的裝置，它特別能偵測出超過 300 種在任何連接埠或通訊協定上周遊的內容類型，因此能協助您揭露資料所面臨的威脅，以及採取動作來協助組織預防資料遺失。此外，McAfee DLP Monitor 還能透過一般使用者通知來教導使用者瞭解何謂資料遺失違規，以在不費吹灰之力的情況下改變行為。

即時掃描及分析資訊

McAfee DLP Monitor 能使用 SPAN 或 Tap 連接埠而整合至網路中，執行網路流量的即時掃描與分析。憑藉著超過 150 個範圍涵蓋法規遵循與智慧財產之合理使用方法的預建規則，McAfee DLP Monitor 能將文件的完整或部分內容（包括極小部分的抄襲）與全面的規則集進行比對。這可讓您偵測網路流量中的異常狀況，不論大小規模為何。

探索未曾考量過的風險

經由詳細地分類、索引及儲存所有網路流量（不僅只是符合即時規則的資訊），McAfee DLP Monitor 能讓您快速運用歷程資訊來瞭解哪些資料是敏感資料、資料的使用情況、資料的使用者及資料移動的目的地。此外，您還可以執行鉅細靡遺的調查與資訊歷程檢查，以偵測出先前未曾考量過的風險事件與資料揭露。搭配 McAfee DLP Discover 一同部署後，您亦可識別資料在網路中的儲存位置與資料的擁有者。

檢視事件報告以提供動作參考資訊

當 McAfee DLP Monitor 使用分類引擎來掃描、分析及分類流量後，它會將所有相關資訊存放在專屬的資料庫中。您可以使用直覺式的搜尋介面來檢視完整的報告以獲得所需的資訊（包括傳送者、目的地、傳送方式），因此可以判斷出外洩的資訊為何、從哪裡外洩，以及如何外洩。得知這些情報後，您可以套用一系列的動作來解決這些威脅，進而維護法規遵循及保護敏感資料。

規格

擷取與索引功能

- 為 McAfee DLP 4400 裝置中高達 80 TB 的資訊與 5000 萬份文件編列索引

系統輸送量

- 以高達 500 Mbps 的速度擷取內容（無取樣）
- 以高達 200 Mbps 的速度分類內容（無取樣）

網路整合

- 能使用 SPAN 連接埠或實際內連的網路 Tap（選用）以被動方式整合至網路中

內容類型

支援超過 300 種內容類型的檔案分類，包括：

- Office 文件
- 多媒體檔案
- P2P
- 來源碼
- 設計檔案
- 封存檔
- 加密檔案

支援的通訊協定

- 支援所有透過任何通訊協定或將 TCP 當做傳輸通訊協定之連接埠的傳輸。
- 包括 HTTP、SMTP、IMAP、POP3、FTP、Telnet、Rlogin、SSH、網頁郵件服務、Yahoo! Chat、AOL Chat、MSN Chat、ICY、RTSP、SOCKS、PCAnywhere、RDP、VNC、SMB、Citrix、Skype、IRC、LDAP、DASL、NTLM、Kazaa、BitTorrent、eDonkey、Gnutella、DirectConnect、MP2P、WinMX、Sherlock、eMule 等的通訊協定處理常式。

內建原則

提供多種適用於共同需求的內建原則與規則，包括法規遵循、智慧財產及合理使用方法等。您可以運用 McAfee 擷取資料庫來進行徹底的規則自訂化，以滿足業務的特定需求。

複雜資料分類

McAfee DLP Monitor 能讓您的組織掃描所有類型的敏感資料，不論是常見的固定格式資料，或是複雜且型態不一的智慧財產。藉由合併這些物件分類機制，McAfee DLP Monitor 能建置精準度高且詳細的分類引擎，並運用引擎來篩選敏感資訊及執行可識別隱藏或未知風險的搜尋。

物件分類機制包括：

- *多層式分類* - 涵蓋內容相關資訊與階層格式中的內容
- *文件註冊* - 包括資訊變更時的生物識別特徵碼
- *文法分析* - 偵測文字文件、試算表或來源碼等所有內容中的文法或語法
- *統計分析* - 追蹤特定文件或檔案中出現與特徵碼、文法或生物識別相符之項目的次數
- *檔案分類* - 跨越檔案或壓縮檔的副檔名限制，識別內容的類型

規格：McAfee DLP 4400 裝置

元件	說明
主機板	Intel Timber Creek System (S5520URR)
CPU	2 個 Intel X5660 12 M 快取，2.8 GHz（6 核心）
記憶體	24 GB P1333 DDR3 記憶體
RAID 控制器	Intel RS2MB044 RAID 控制器
電源供應器	2 個 760 W 熱交換電源供應器模組
硬碟機	12 個 Seagate Constellation ES 1T 7200 rpm 3 1/2" SATA 磁碟機
NIC 卡	3 個 Intel Dual Copper 1Gbps Ethernet I/O Module
DVD 光碟機	SATA DVD ROM
IPMI	Intel Remote Management Module 3 (AXXRMM3)
產品大小	2 機架單位 (2U)

規格：虛擬機器

McAfee DLP Monitor 可做爲於 VMware ESX 或 VMware ESXi 4.1 伺服器中運作的虛擬裝置。以下是執行虛擬裝置的硬體需求下限。

元件	需求
CPU	Intel 四核心
記憶體	8 GB RAM
硬碟	磁碟機 1：至少 128 GB（供 VM 軟體使用） 磁碟機 2：至少 640 GB（供 DLP 虛擬映像使用）
網路連接埠	3 個適用於 McAfee DLP Monitor 應用程式的連接埠
BIOS	啓用 VT 執行緒

McAfee
An Intel Company

邁克菲台北辦公室
台北市 104 南京東路三段132 號 4 樓 A2
886-2-2721-7766
www.mcafee.com/tw

39706ds_dlp_monitor_1111