資料工作表

McAfee DLP Discover

識別及保護敏感資料

主要優點

識別資料外洩風險

- 掃描存放於所有可存取資源中的資訊
- 識別敏感資料的存放處所與內容擁有者
- 透過直覺式的介面來搜尋及檢視所有掃描的資料

建立原則與自訂報告

- 執行查詢並將結果轉換為保護規則
- 使用預建的法規遵循、公司管理及智慧財產原則
- 向相鄰的資訊安全性系統註冊敏感資訊

分類、分析及修補資料漏洞

- 利用多面向的分類機制來篩選及控制敏感資訊
- 為所有內容編列索引，並藉由查詢與挖掘來瞭解敏感資料
- 藉由註冊及產生特徵碼來保護文件與文件中的資訊，即便是遭到剽竊或調換時
- 當內容違反保護原則時傳送警示通知

存放在筆記型電腦、共用檔案伺服器、入口網站或文件管理系統中的資訊會使組織暴露在風險之中。數以 TB 或甚至 PB 計算的大量資訊都必須受到保護。但由於敏感資訊的標示參差不齊，這件事情做起來談何容易。除此之外，對大部分的組織而言，即便是已建置存取控制措施，他們仍無從得知或驗證敏感資料是否暴露在風險之中，抑或是找出資料擴散的地點。更糟的是，敏感資料所含的通常是比固定資料（如信用卡號碼或身分證字號）更難以定義的智慧財產 (IP) 資產。

預防敏感資料遺失

不論是來源碼、商業機密或策略性的業務計劃，IP 與其他資訊資產對於品牌、信譽及競爭優勢來說都是密不可分的要素。儘管保護資料傳輸是重要的工作，但是在發生不當存取或移動敏感資料前予以保護及瞭解其存放處所，才應該是您的第一道防線。

McAfee DLP Discover 能協助組織預防資料遺失。它不像舊式的解決方案需要您界定該保護的內容，反之，它能將顯而易見的資訊納入保護範圍內，並協助您尋找潛藏的資訊。

判斷應保護的資訊

爲了識別資訊與擴散風險，您可以設定 McAfee DLP Discover 以掃描特定的存放庫，然後找出應明確受到保護的資料。此外，McAfee DLP Discover 會爲所有編入的資料編制索引並透過直覺式的介面提供存取，使您得以快速搜尋潛在的敏感資料，瞭解內容的擁有者與存放處所。

定義保護原則

得知該保護的資訊後，McAfee DLP Discover 能協助正確地保護資訊。McAfee DLP Discover 提供直覺式且統一的原則建立、報告與管理方式，讓您能更有效地掌控資訊保護策略以保護儲存中的資料。McAfee DLP Discover 中原則、規則及分類的主要優點包括：

- 大量的內建原則提供簡單、立即可用的使用體驗
- 功能強大的規則建置引擎，不論是簡單的結構化資料 (信用卡、身分證字號) 或複雜的資訊 (智慧財產) 均適用
- 將搜尋結果分析轉換成保護規則，簡化規則的建立與驗證作業
- 與相鄰的資訊安全性媒介整合，維持一致的保護效力
- 排除公用文件與常用文字，避免這些良性的資訊產生事件

掃描網路中的違規情事

在定義原則後，您可以指示 McAfee DLP Discover 定期掃描網路資源中是否有違反原則的情事。彈性的排程選項可以用來執行持續、每日、每週或每月一次的掃描。

McAfee DLP Discover 能自動掃描所有可存取資源 (包括筆記型電腦、桌上型電腦、伺服器、文件存放庫、入口網站及檔案傳輸位置) 中是否有違規原則的情事。您可以根據 IP 位址、子網路、範圍或網路路徑來定義掃描群組。您也可以根據特定的參數來集中掃描作業的焦點，例如只掃描所有使用者的「我的文件」而不掃描系統資料夾、搜尋特定使用者擁有的檔案，或搜尋特定類型或大小的檔案。

規格

擷取與索引功能

- 為 McAfee DLP 4400 裝置中高達 80 TB 的資訊與 200 萬份文件編列索引

系統輸送量

- 高達 60 Mbps 的存放庫掃描能力

內容類型

支援超過 300 種內容類型的檔案分類，包括：

- Microsoft Office 文件
- 多媒體檔案
- 來源碼
- 設計檔案
- 封存檔
- 加密檔案
- 內建原則
- 智慧財產

支援的存放庫

- Common Internet File System (CIFS)/Server Message Block (SMB)
- 網路檔案系統 (NFS)
- HTTP/HTTPS
- FTP/FTPS
- Microsoft Sharepoint
- EMC Documentum
- 資料庫：Microsoft SQL、Oracle、DB2、MySQL Enterprise

文件註冊

您可以從任何存放庫註冊文件。已註冊之文件的特徵碼能用來在本機偵測敏感材料的擴散，或供其他 McAfee DLP 裝置之用。

報告

功能強大的事件分析引擎與搜尋結果檢視可讓您根據任兩個內容相關的樞紐點來自訂摘要檢視。提供清單與詳細資料檢視，以及能指出趨勢的摘要檢視。系統備有 20 個以上的可自訂預建報告與可自訂報告。

檢閱及修補違規

McAfee DLP Discover 透過整合的事件工作流程與案例管理，使機密資料不再擴散或降低擴散機會。如果 McAfee DLP Discover 發現違反防護政策的內容，它會產生事件並傳送通知。您可以將 McAfee DLP Discover 建立的事件新增至案例管理架構，此舉讓您得以從公司內的眾多組織中召集專家，針對違規情事採取動作。此外，風險儀表板不但能讓原則違規的狀態在安全人員面前一目了然，還能依據儲存中的資料或感興趣的參數產生報告。

擷取及分析儲存的資料

McAfee DLP Discover 除了能掃描網路資源以偵測原則違規之外，還能爲儲存在網路中的所有內容編制索引，讓您藉由查詢及挖掘資訊來瞭解敏感資料。McAfee DLP Discover 能讓您迅速瞭解敏感資料、資料的使用情況、資料的擁有者、資料的存放處所，以及資料擴散的地點。

複雜資料分類

McAfee DLP Discover 能讓您的組織保護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。藉由結合這些物件分類機制的輸入內容，McAfee DLP Discover 能建立高準度、多面向的分類措施來篩選及控制敏感資訊，以及執行搜尋來識別隱藏或未知的風險。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 控制卡	Intel RS2MB044 RAID 控制卡
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	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 Discover 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	1 個適用於 McAfee DLP Discover 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

39704ds_dlp_discover_1111