Data Loss Prevention 14.6 有哪些新功能

新的功能可讓您更安全地使用敏感資訊

Symantec Data Loss Prevention 14.6 引進一系列全新的資訊防護功能，以領先業界的防止資料外洩技術為後盾，針對您的機密資料提供更優異的能見度與掌控度。內容包括：

- **擴充的雲端應用程式安全整合性** – 可讓您運用 Symantec Cloud Access Security Broker 與 Symantec Blue Coat Web Security Service，將 DLP 的涵蓋範圍延伸至雲端應用程式[1]。
- **更強大的端點監控功能** – 讓您針對 Mac 和 PC 電腦上所使用的敏感資料，獲得更高的掌控度，包含 Mac OS 10.12 與 Windows 10 周年更新。
- **擴展的資料搜尋範圍** – 讓您對 SharePoint 2016 中所儲存的敏感文件取得能見度。
- **改良的內容偵測功能** – 讓您偵測到更多類型的敏感資料，涵蓋更多文件類型，例如使用 Microsoft RMS 加密的檔案。
- **更簡單的系統管理** – 讓您更加輕鬆地管理規則、回應資安事端和部署我們的軟體。

保護雲端應用程式中的資料

安全性是採用雲端應用程式的企業所面臨的最大挑戰，尤其是 Office 365 和 之類的常見商用應用程式，其中儲存與共用了各種敏感的公司資料。運用 Symantec DLP，您可以讓員工自由又安全地在雲端中作業。

透過 Symantec DLP Cloud Service Connector (新的雲端式偵測服務，採用和我們就地部署軟體相同的先進技術)[2]、Symantec Cloud Access Security Broker 與 Symantec Blue Coat Web Security Service 之間的整合，[3]我們已將 DLP 的涵蓋範圍延伸到已核准和未核准的雲端應用程式。只要使用同一個管理主控台 (DLP Enforce)，您就可以針對超過 60 種雲端應用程式 (包括 Office 365、Box、Dropbox、Google Apps 或 Salesforce)，找出其中的資料漏洞。

1 - Symantec Cloud Access Security Broker 與 Symantec Blue Coat Web Security Service 為另售，需購買和 Symantec Data Loss Prevention 不同的授權。
2 - Symantec Data Loss Prevention Cloud Service Connector 以附加程式授權的形式另外銷售。
3 - Symantec Cloud Access Security Broker 與 Symantec Blue Coat Web Security Service 為另售，需購買和 Symantec Data Loss Prevention 不同的授權。

Symantec

在端點上更安全地使用資料

員工會遇到網路中和網路外的無數漏洞。運用 **DLP Endpoint Agent Mac OS 版本**，您就能保護在整個廣大範圍事件中使用的資料，包括下載至抽取式儲存裝置、在文件內複製和貼上，以及透過網際網路傳送。為協助您防止可能的資料外洩事件，我們新增了對最新平台與應用程式的支援：

- Mac OS 10.12
- Microsoft Outlook 2016
- 透過應用程式監控 (Application Monitoring) 功能，對應用程式進行更精細的監控

DLP Endpoint Agent Windows 版包含了 和我們 Mac Agent 相同的許多強大功能，現在還針對在這些平台和應用程式中所使用的資料，新增了保護的機制。

- Microsoft Windows 10 周年更新企業版
- Citrix 7.9 XenApp/XenDesktop
- Microsoft Edge
- 透過應用程式監控 (Application Monitoring) 功能，對應用程式進行更精細的監控

取得對 SharePoint 2016 資料的能見度

企業中的非結構化資料正在大幅增加，主要是來自於內部產生的文件，但很少有公司將重點放在管理和保護此類資料。運用 DLP Network Discover，您就可以得知最敏感資料的所在位置，並防止這些資料因為粗心大意的員工或惡意的攻擊者而外洩。利用高速掃描功能，DLP Network Discover 可以針對整個網路檔案共用區、資料庫和其他資料儲存庫 (現在也包括 Microsoft SharePoint 2016)，快速地找出儲存於這些地方的敏感資料。

找出儲存於任何位置的敏感資料

內容感知偵測技術幾乎能夠找出儲存於任何位置、具備任何檔案格式的敏感資料。Symantec DLP 採用了先進的描述、特徵比對和機器學習技術，能夠精確地偵測資料，不會讓誤報影響商務使用者，提供最完備的資料偵測功能。

在 DLP 14.6 中，我們已改良了內容偵測功能，可以針對更多類型的文件來偵測更多類型的資料：

- **Microsoft RMS 加密檔案：** 您現在可以針對由 Microsoft Rights Management Services (RMS) 所加密的檔案，偵測敏感的內容。
- **改良的規則運算式偵測功能：**DLP 偵測引擎能夠以更快速 (最高達 40 倍)、更穩定一致的效能，針對整個 DLP 端點代理程式和偵測伺服器來評估規則運算式。
- **更多內建的偵測智能：**DLP 14.6 針對新的歐盟一般資料保護規範 (European General Data Protection Regulation, GDPR)、美國《健康保險隱私及責任法案》 (HIPAA) 與 HITECH 提供了全新和更新的規則範本；DLP 14.6 也針對中國、法國、印度、日本、韓國、墨西哥、西班牙、瑞典和美國，提供了全新和更新的資料識別碼。

4 - Symantec Data Loss Prevention Form Recognition 是以附加程式的形式另外銷售。

保護表單文件

相較以往，企業更加仰賴掃描器和手機產生的影像文件，藉此將業務流程數位化。如此一來，企業便能輕鬆地與客戶及合作夥伴交換資訊；然而，這種方式卻也加深追蹤和控管敏感資料的難度，尤其是充滿個人識別資訊 (PII) 的掃描表單。

在 DLP 14.5 中推出的 Symantec DLP 表單辨識 (Form Recognition)[4] 功能，運用了智慧影像處理技術來辨識原本偵測不到的光柵影像格式敏感資料，例如掃描的影像，或用手打字或填寫的影像格式。使用 DLP 14.6，現在您即可針對能夠電子化填寫的 PDF 檔案，偵測其中的敏感資料。

更輕鬆地管理系統

在 DLP 14.6 中，使用者能夠更輕鬆地管理規則、回應資安事端，並且將我們的軟體和強化功能部署至 DLP Enforce Server 和主控台。

- **Windows Server 2016**：現在除了 Windows Server 2008 和 2012 以外，您還能再部署 DLP Enforce Server 和偵測伺服器 Windows Server 2016。
- **改良的規則管理功能**： DLP Policy List 頁面可篩選規則清單，以及套用大量操作動作，例如啟用/停用規則、匯出、下載和同時刪除多項規則等。
- **擴大存取事件變數**：系統管理員可存取更多事件欄位變數 (例如應用程式名稱、應用程式使用者)，進而在系統日誌 (syslog) 訊息和電子郵件通知中提供更具意義的背景文本。

關於賽門鐵克

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

12/16　零件編號 21366644