Data Loss Prevention 功能一覽

全新功能，讓您更能安全地處理機密資料

產品型錄：防止資料外洩

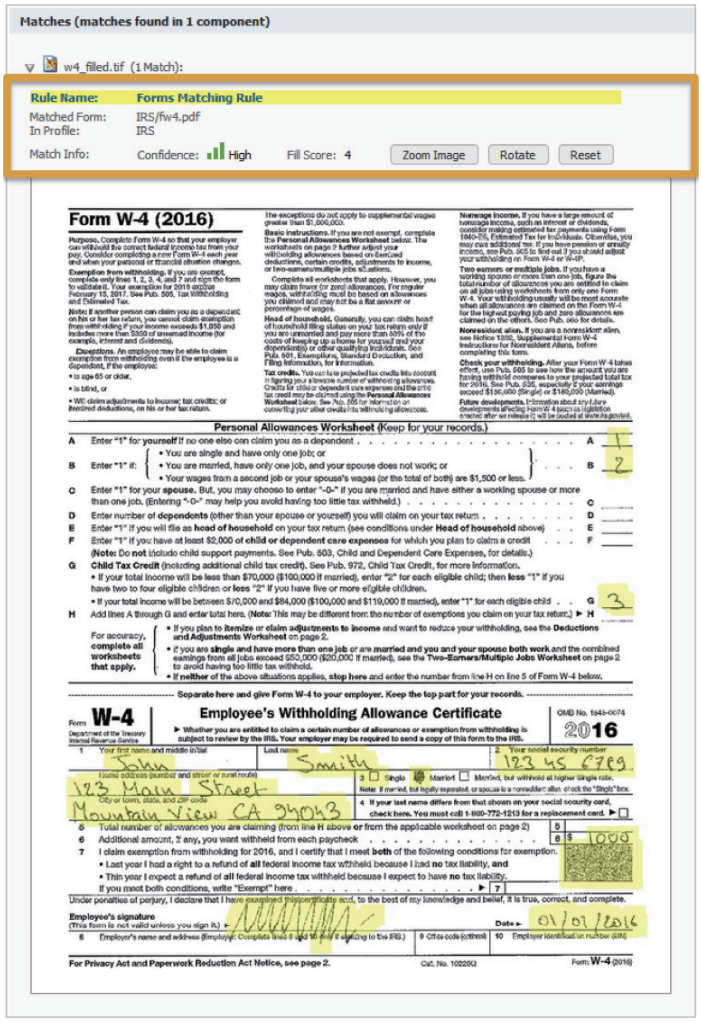
Symantec Data Loss Prevention 引進一系列全新的資訊防護功能，以領先業界的防止資料外洩技術為後盾，針對您的機密資料提供更優異的能見度與掌控度。

Data Loss Prevention 包含以下功能：

- **進階資料偵測** — 可在更多管道和文件類型中，擷取個人識別資訊和智慧財產
- **強化雲端搜尋** — 可針對 Box 中儲存和共用的敏感文件，增強檔案保護能力
- **更強大的端點監控** — 讓您使用 Mac 和 PC 的機密資料時，更能掌握自如
- **更清楚地瞭解加密通訊的情況** — 讓您發現並免除加密網頁流量產生的安全盲點

保護敏感表單

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。只要使用 Symantec **DLP Form Recognition**，即可保護手寫的影像資料和輸入的表單，例如退稅單、保險理賠單、就醫表單，或其他可能含有 PII 的表單。DLP Form Recognition 是一款全新的內容偵測技術，其中運用智慧型影像處理功能，可擷取及遏止經過掃描或拍攝等無法偵測到的表單外洩。



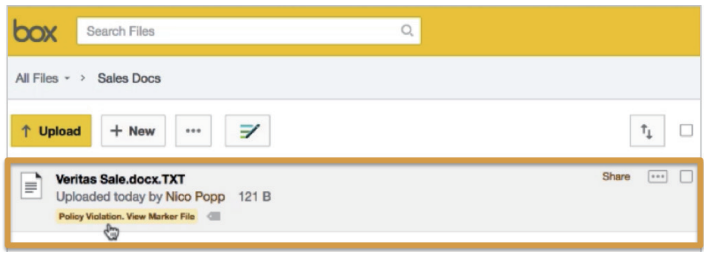
現在，DLP 使用者可輕鬆將 Form Recognition 附加到整個企業的單一授權；如此一來，您就能跨越一或多個偵測伺服器充分利用此產品，包括：Network Monitor、Network Prevent for Email、Network Prevent for Web、Network Discover 和 Network Protect 。

保護雲端中的機密資料

利用 Symantec DLP Endpoint Agent for Windows、DLP Cloud Storage 與 DLP Cloud Service for Email，員工即可隨心所欲安全地使用各種雲端應用程式工作，例如 Box、Gmail 和 Microsoft Office 365。

DLP Endpoint Agent for Windows 提供全新的監控和攔截功能，可讓檔案透過 Box Sync 和 Box for Office 應用程式上傳到 Box。使用者可上傳各式各樣的檔案到公司核准的 Box 帳戶，同時預防檔案透過 Box Sync 上傳到未核准的私人 Box 帳戶。

DLP Cloud Storage 能追蹤使用者在 Box 中儲存和共用的敏感資料，還能識別存有風險的行為，例如使用共用連結，讓未經授權的使用者具有開放的存取權限。一但使用者違反政策，DLP Cloud Storage 的全新「檔案隔離」功能會自動將暴露在風險中的檔案和資料夾移至 Box 中受保護的隔離資料夾，並在原本位置留下標記檔案，通知使用者檔案被隔離的情況。您不僅可以保護未受保護的檔案，還能將檔案標上記號，以便提醒使用者自行修正敏感檔案和資料夾。



DLP Cloud Service for Email 可有效監控和保護企業的電子郵件，無論是存放在傳統的內部部署電子郵件應用程式、公用或私有雲端電子郵件服務，還是兼具內部部署和雲端的混合式環境，全都固若金湯。這項雲端偵測服務，深度整合了 Gmail、Microsoft Office 365 Exchange Online 和目前的 Microsoft Exchange Server，可輕鬆銜接您現有的 DLP Enforce Server。

在端點上更安全地使用資料

無論連線與否，員工總是會面臨無數的危險。DLP Endpoint Agent for Mac OS 可讓您在各種狀況下保護資料，包括將資料下載至抽取式儲存裝置、在文件中進行複製和貼上，以及透過網頁傳送資料。為了讓您預防潛在的外洩風險，我們針對分享敏感資料的全新應用程式、檔案類型和員工常用的作業系統，提供進一步的支援服務。

- Mac OS 10.11
- Microsoft Office 2016 檔案類型
- Microsoft Outlook 2011 電子郵件用戶端
- Chrome、Firefox 和 Safari 瀏覽器 (透過 HTTP 和 HTTPS)
- 複製到網路共用資料
- 從剪貼簿貼上
- Skype 即時通訊用戶端

DLP Endpoint Agent for Windows 集結 Mac Agent 許多相同強大的功能，現在更針對以下應用程式和檔案類型的資料使用，新增防護功能，包括：

- Microsoft Office 2016 檔案類型
- Box for Office 和 Box Sync 應用程式
- Cisco Jabber 和商用 Skype 即時通訊用戶端

輕鬆管理不同環境中的各項政策

若要在將您的資料外洩政策移至不同的環境，例如從開發或測試環境移至到生產環境，將流程簡化與自動化，可讓您避免錯誤並節省寶貴時間。藉由政策匯入與匯出功能，您可以在 DLP Enforce Server 的執行個體之間輕鬆移轉各項政策。您可以先將政策匯出到含有完整政策詳細資料的檔案，包括政策群組和應變原則，然後毫無錯誤地匯入。

保護端點中的文件片段

員工會從不同檔案和應用程式的敏感文件中，剪下、複製並貼上資訊片段，但是當中有些可能未經核准且不安全，不適合員工使用。Symantec DLP 的「端點索引文件比對」功能，具備強大的資料比對能力，能輕鬆檢查文件片段，讓您可偵測原始形式及衍生形式的機密資料。「端點索引文件比對」功能，相當適合使用行動裝置或遠端作業的企業員工，進行處理非結構化資料的例行作業，也就是資料庫不支援的資訊。

更充分地掌握網路通訊

多數公司和客戶、合作夥伴及委外廠商的通訊，都是倚賴幾種主要的網路通訊協定，包括 HTTPS、HTTP 和 FTP。然而，員工透過加密和未加密的管道傳送機密資料時，無形就產生 IT 的盲點和漏洞。DLP 14.5 可讓您可針對 HTTPS、HTTP 和 FTP，取得進階的網頁監控和預防功能，方法是運用 DLP Network Prevent for Web，以及下列網路閘道和雲端代理伺服器的全新整合性：

- A10 Networks Application Delivery Controller、SSL Insight 和 Thunder Convergent Firewall
- Zscaler 網頁安全服務

更清楚地瞭解加密通訊的情況

全球有越來越多的網路流量受到加密，若是不能瞭解機密資料的情況，您的公司便會因為加密的通訊協定而外洩更多資料。DLP 可在您失去網路安全前，讓您檢查加密流量，重新取得掌控權。DLP 深度整合了首屈一指的 SSL 解密硬體裝置，可分析解密流量且預防機密資料遭到使用者發佈或傳送。DLP 14.5 可讓您取得網頁、電子郵件、FTP 和即時訊息通訊專用的全新 SSL 監控功能，並且整合 DLP Network Monitor 和下列 SSL 解密產品：

- Blue Coat SSL Visibility
- Palo Alto Networks Next Generation Firewall

關於賽門鐵克

賽門鐵克公司 (Symantec) 已於 2019/11 合併入博通 (BroadCom) 的企業安全部門，Symantec 是世界首屈一指的網路安全公司，無論資料位在何處，賽門鐵克皆可協助企業、政府和個人確保他們最重要資料的安全。全球各地的企業均利用賽門鐵克的策略性整合式解決方案，在端點、雲端和基防架防中有效地抵而最複雜的攻擊。賽門鐵克經營的安全防報網是全球防防最大的民間防報網路之一，防此能成想偵測最進防的威脅，進　提供完善的站護善更。
若想瞭解更t　資施，請提訪原廠網瞭 https://www.broadcom.com/solutions/integrated-cyber-defense