

McAfee 裝置到雲端 DLP

一致的資料保護

各種規模的公司普遍採用 Microsoft Office 365 等雲端式服務，賦予員工更大的使用彈性，使其能更輕鬆地存取核心商業應用程式。內部部署資料保護解決方案一般無法掌握 Office 365 等雲端服務中的資料，也無法控制雲端內的協同合作或共用作業。許多組織正紛紛考慮為雲端環境導入其他資料保護解決方案，但如此會使原則、報告和事件回應等機制分散而難以管理。這會推升營運開銷，且裝置、網路和雲端服務的資料保護措施不一致。

McAfee® 裝置到雲端 DLP 整合了下列兩項領先業界的技術，為端點、網路及雲端提供一致的資料保護：McAfee® Data Loss Prevention (McAfee DLP) 和 McAfee® MVISION Cloud。此整合可提供組織流暢且一致的資料保護體驗，大幅降低資料外洩風險，同時大幅提升營運效率。

分散的資料保護解決方案效率不佳

若要在雲端實作 DLP，以往常需在雲端重新建立您為內部部署環境所建立的 DLP 規則。內部部署 DLP 規則也缺乏雲端原生協同合作，或與雲端服務第三方共用的環境。這導致耗費過多時間複寫已為裝置和網路資料完成的工作，且可能強

制實施不同 DLP 引擎上不一致的原則。內部部署 DLP 無法掌握透過雲端協同合作或共用連結所造成的資料外洩。

輕鬆連結並同步內部部署 DLP 和雲端 DLP

透過 McAfee® ePolicy Orchestrator® (McAfee ePO™) 軟體，啟用裝置到雲端 DLP 可說是輕鬆無比。同時再搭配使用 MVISION Cloud 和 McAfee ePO 軟體，即可讓您以前所未有的速度，保護所有雲端服務的資料，並完整掌握雲端原生協同合作和共用情形。只要按一下，即可在一分鐘內輕鬆連結兩個解決方案¹。您在 McAfee ePO 軟體為裝置和網路建立的 DLP 規則會推送至 MVISION Cloud，在此，您可將其套用至

主要優勢

流暢整合

- 在 McAfee ePO 軟體中先將資料分類一次，之後便能針對裝置、網路和雲端環境使用適合的分類。
- 只要按一下，就能在一分鐘內輕鬆連結內部部署和雲端 DLP。

一致的資料外洩防護

- 多重環境一併適用共用原則和分類引擎。
- 同一變更不需在多個主控台中反覆執行。

針對所有事件管理與報告提供單一檢視

- 集中管理不同環境所發生的事件。
- 不需切換主控台即可檢視事件和報告。

與我們交流



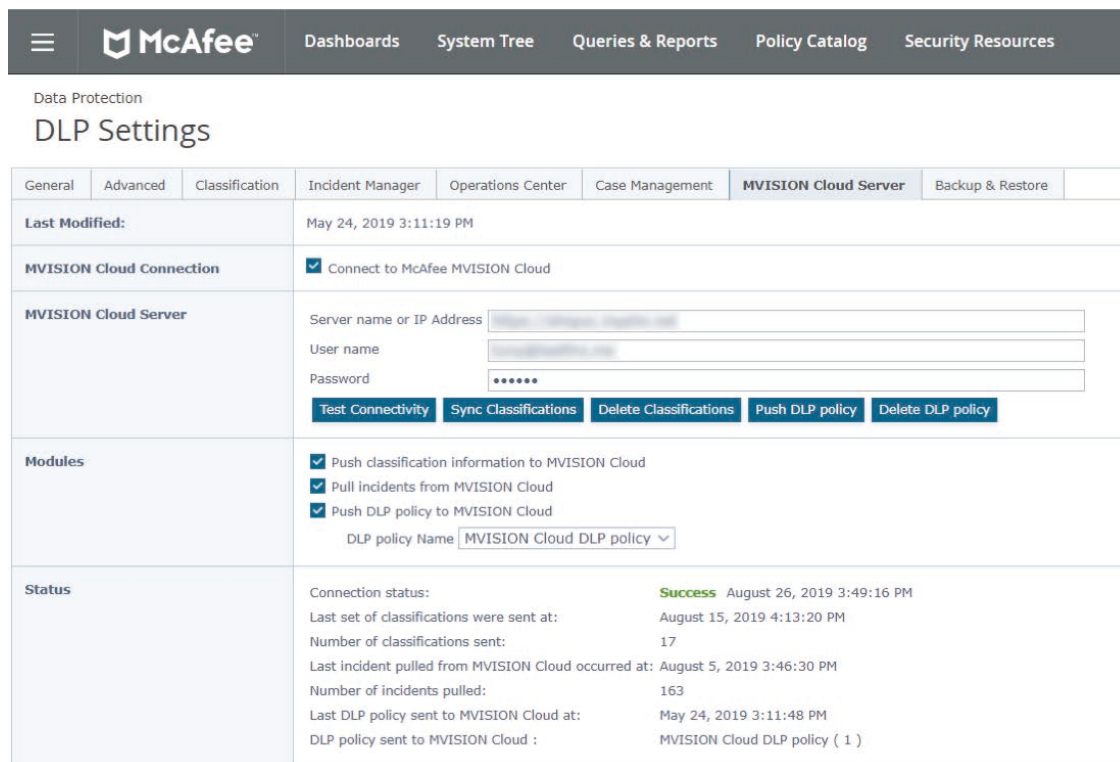
資料工作表

任何雲端服務和任何通過您網路的雲端原生流量。系統也會同步處理資料分類作業，確保端點和雲端的資料外洩防護同樣穩固。所有事件都會傳送至 McAfee ePO 軟體，從裝置到雲端都適用同一套 DLP 工作流程。

企業如何運用裝置到雲端 DLP 享有高營運效率

使用 McAfee ePO 軟體的客戶已運用此整合優勢，在雲端服務中輕鬆實施 DLP，並簡化營運作業。舉例來說，大型食品服務製造商要在端點和網路檔案共用作業中使用 McAfee DLP，就必須掌握其資料在雲端的位置，並研擬策略來保護資料。該組織先使用 McAfee® Web Gateway，透過分析其 Web 流量判斷熱門使用者目的地，以及公司資料在雲端的存放位置。結果此組織發現，絕大多數資料實際上集中於 Microsoft Office 365。

從內部部署來看，此公司對保護雲端資料的需求從未變動，但雲端的檔案共用和協同合作等環境差異衍生出新的挑戰。例如，此公司必須依需求掃描 Office 365 資料 (類似於內部部署掃描)，同時針對移入和移出 Office 365、專屬於雲端及不在網路掌控範圍之中的資料，強制實施 DLP 規則。以往該組織認為，雲端存取安全性中介 (CASB) 是滿足這些需求的最佳解決方案，並評估市面上多項產品。最後，該組織看上 MVISION Cloud 與 McAfee ePO 軟體的現有 DLP 規則緊密



The screenshot shows the McAfee ePO interface for DLP Settings. The top navigation bar includes 'Dashboards', 'System Tree', 'Queries & Reports', 'Policy Catalog', and 'Security Resources'. The main content area is titled 'Data Protection DLP Settings' and features a tabbed interface with 'MVISION Cloud Server' selected. The 'MVISION Cloud Connection' section has a checked checkbox for 'Connect to McAfee MVISION Cloud'. The 'MVISION Cloud Server' section contains input fields for 'Server name or IP Address', 'User name', and 'Password', along with buttons for 'Test Connectivity', 'Sync Classifications', 'Delete Classifications', 'Push DLP policy', and 'Delete DLP policy'. The 'Modules' section has three checked checkboxes: 'Push classification information to MVISION Cloud', 'Pull incidents from MVISION Cloud', and 'Push DLP policy to MVISION Cloud', with a dropdown for 'DLP policy Name' set to 'MVISION Cloud DLP policy'. The 'Status' section displays connection details, including a 'Success' status on August 26, 2019, and various metrics like 'Last set of classifications were sent at: August 15, 2019 4:13:20 PM' and 'Number of classifications sent: 17'.

圖 1. 在 McAfee ePO 軟體中將 DLP 原則同步至 MVISION Cloud。

整合，因而決定採用。安全性團隊從 McAfee ePO 軟體將內部部署資料分類推送至 MVISION Cloud，接著運用這些預先建立的分類撰寫 Office 365 原則。現在，該組織可在 McAfee

資料工作表

ePO 軟體中，集中管理資料分類、裝置和雲端的 DLP 事件，以及 McAfee Web Gateway 的 Web 流量報告。

「我們選擇 McAfee MVISION Cloud 作為 CASB，因為這能協助我們掌握資料去向、存取資料的使用者，並可輕鬆瞭解雲端服務相關風險。」

— 全球 IoT 製造商的資訊安全長

集中式事件管理及報告

透過 McAfee ePO 軟體，使用者可透過單一窗口管理所有 DLP 違規事件與報告，享有流暢而全面的使用體驗。無論 DLP 違規事件是源自企業裝置或雲端應用程式，使用者不必切換主控台，即可檢視事件及產生報告。這個集中式主控台也可讓您確實掌握不同環境中的敏感資料，有助於降低稽核和符合法規遵循要求的複雜程度。

摘要

隨著每天越來越多資料在雲端上建立及上傳至雲端，擁有一致的 DLP 原則，藉以保護企業端點、未受管理的裝置、網路或雲端應用程式的資料免於外洩，自然成為無比重要的課題。

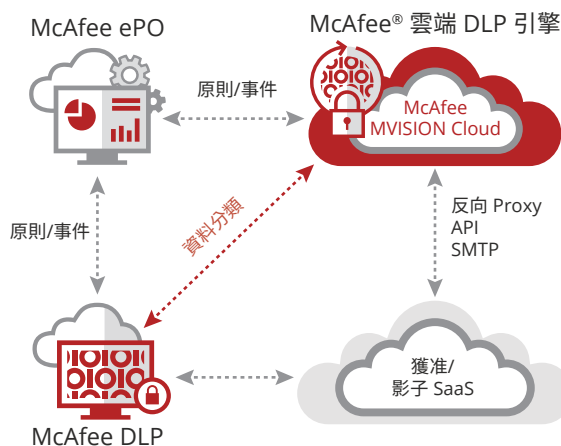


圖 2. McAfee 裝置到雲端 DLP 事件管理的一般架構。

McAfee 裝置到雲端 DLP 能為組織在多環境中提供流暢一致的資料保護體驗，提高營運效率節省時間，並有助於將資料外洩風險降至最低。

深入瞭解

如需詳細資訊，請造訪

mcafee.com/dataprotection



台灣
台北市信義區忠孝東路五段 68 號 29 樓
11065
電話：+886 2 8729 9222
www.mcafee.com/tw

McAfee 和 McAfee 標誌、ePolicy Orchestrator 與 McAfee ePO 是 McAfee, LLC 或其附設公司在美國及其他國家地區的商標或註冊商標。其他標誌與品牌可能為其各自擁有者的財產。Copyright © 2019 McAfee, LLC. 4352_0819
2019 年 8 月

1. 根據 McAfee 內部持續測試所獲得的結果。