Symantec by Broadcom

賽門鐵克DLP雲端電子郵件服務

Symantec DLP Cloud Service for Email

保護電子郵件免受現代威脅

解決方案簡介

快速一覽

賽門鐵克 DLP 雲端電子郵件服務 (Symantec DLP Cloud Service for Email) 讓組織能夠安全、無縫地將電子郵件移轉到雲端

主要優勢

- 全方位的威脅防護
- 持續政策強制
- 提供即時分析洞察
- 加速事件回應
- 快速部署

重要功能

- 整合多層次先進檢測技術
- Skeptic 掃描技術
- 傳輸中的內容感知資料外洩防護 (DLP)
- 無縫與雲端和 ESS 整合
- 統一管理主控台

雲端安全需要更強的保護來發揮優勢並轉化為其他相關優勢

Microsoft Office 365 和 Google Workspace 等雲端電子郵件系統具有得天獨厚的優勢，包括提升的敏捷度、更高的生產力和更低的成本。這些優勢為企業帶來了顯著的競爭優勢。然而，這無疑也讓安全風險變得更加嚴峻。雲端電子郵件平台內建的安全措施通常無法應對勒索軟體、商業電子郵件詐騙 (BEC) 和網路釣魚等進階威脅。傳統電子郵件安全解決方案也受限於分析不足和整合操作上的隔閡，難以滿足當今複雜威脅環境的要求，使企業面臨風險。

根據 2024 年 Verizon 資料外洩調查報告，電子郵件仍是網路犯罪份子的主要攻擊媒介，是傳播勒索軟體的主要手法，也是第二常見的資料外洩途徑。儘管雲端供應商已經提升其資料中心的安全性和可擴展性，但雲端電子郵件應用程式中的基礎安全功能不足以抵禦現代複雜的網路攻擊。為了充分發揮雲端技術的優勢，企業必須實施進階防護措施，以保護敏感資料並確保其抵禦不斷進化的威脅的能力。

Symantec DLP Cloud Service for Email 的簡介

Symantec® Email Security.cloud (ESS) 提供強大且全面的雲端電子郵件平台防護解決方案。它運用內建的防止資料外洩 (DLP) 和政策式加密控制來攔截、隔離或加密機密的電子郵件，增強合規性和隱私保護工作，這些功能使用 100 多個涵蓋關鍵字字典、一般運算式和 MIME 類型清單的預先定義清單，可識別並控制進出企業的機密電子郵件。與 Symantec DLP 整合可進一步能對整個環境內的機密資料（電子郵件、端點、網路、雲端、行動裝置以及存儲裝置) 進行搜尋、監控與提供企業級的保護。

Symantec DLP Cloud Service for Email 協助企業安全且流暢地將電子郵件遷移至雲端。這款從企業營運風險角度全面考量的解決方案超越了基本的合規性，不僅能夠保護敏感資訊免於意外或惡意內部人員的攻擊，還能攔截電子郵件中的威脅。該解決方案將業界領先的資料遺失防護和電子郵件安全功能整合到一個統一且易於部署的平台中，為 Microsoft Exchange Online 和 Gmail for Business 等領先的雲端電子郵件服務提供企業級合規性和安全控制。

專為電子郵件系統打造的資料外洩防護方案

防止資料遺失 (無論是意外、疏忽還是惡意造成的) 對於任何資訊安全計畫的成功非常重要。Symantec DLP Cloud Service for Email 可確保您不再擔心員工無意中洩露機密電子郵件，進而損害公司聲譽。此解決方案將全面的內容感知 DLP 功能擴展至 Office 365、Gmail 和 Exchange，掃描離埠電子郵件流量，尋找個人識別資訊 (PII) 和智慧財產權等敏感內容。

賽門鐵克電子郵件 DLP 雲端服務引進最先進的內容偵測功能來分析訊息內容和後設資料--metadata(data about data) 的脈絡：

- 精確資料比對 (EDM：Exact Data Matching)：透過指紋辨識或索引結構化資料可直接識別資料來源端 (例如：資料庫和目錄伺服器) 的機密資料，例如：「攔截所有洩漏客戶姓名及其相關的銀行帳號的行為」。
- 索引文件比對 (IDM：Indexed Document Matching)：運用「完整檔案比對」辨識非結構化資料 (包括 Microsoft Office 文件和 PDF 檔案，以及 JPEG、CAD 設計圖和多媒體檔案等二進位檔案) 中的機密資訊。
- 向量機器學習 (VML：Vector Machine Learning)：可自動學習來偵測難以形容的細微特徵與識別機密文件類型 (例如：財務文件與原始程式碼) 來保護智慧財產權。

因此，該解決方案能夠精確識別潛在的電子郵件資料外洩，並將誤報率降至最低，讓您能夠專注於真正的事件。

當偵測到敏感內容時，賽門鐵克 DLP 雲端電子郵件服務可提供即時保護。自動回應動作包括通知使用者、封鎖郵件或修改郵件以強制執行後續的加密或隔離。

最後，此解決方案的 Enforce Platform 是一個統一的管理控制台，可讓企業只需建立一次政策，即可在雲端、電子郵件、Web、端點和儲存管道上均強制執行該政策。您可以透過一個 Web 的主控台編寫 DLP 政策、資安事端矯正流程並執行系統管理，同時藉助直覺的政策建構器和 70 多個預建模板快速啟動並執行。此外，該平台還透過強大的工作流程和修復功能，簡化並自動化高流量環境中的事件回應。

抵禦來自電子郵件的攻擊

這個 DLP 雲端電子郵件服務為雲端電子郵件服務補強必要的安全性。該服務與賽門鐵克 ESS 技術無縫整合，可防禦目標式攻擊、魚叉式網路釣魚、進階的惡意程式、垃圾郵件及大量郵件。先進的反惡意軟體和反垃圾郵件功能可阻止電子郵件中的威脅入侵使用者信箱，而政策式加密控制則可保障與客戶和合作夥伴之間的敏感通訊安全。

賽門鐵克專利啟發式技術 Skeptic 的大亮點在於其強大的功能。Skeptic 會檢查多種電子郵件屬性以偵測異常，並利用前瞻性的啟發式演算法預測並消除潛在威脅。這個透過不斷學習的系統能夠主動、即時地防禦不斷演變的惡意內容。

保護傳送中的機密資料

賽門鐵克 DLP 雲端電子郵件服務將內容感知資料遺失防護功能擴展至 Microsoft Exchange Online 和 Gmail for Business。憑藉多重先進的偵測技術和內建的情報，該服務可對傳送中的資料進行準確、即時的監控和分析，最大限度地減少誤報和漏報，使企業能夠專注於實際事件。

自動回應動作 (例如：郵件攔截、重新導向和加密) 可即時防止關鍵資料洩漏。強大的事件補救選項包括可自訂的工作流程、電子郵件通知和一鍵回應，進而簡化事件管理。直觀的政策建構器、預建模板和行業特定的解決方案包簡化了政策編寫，使組織只需編寫一次政策，即可在雲端和本地郵件中一致地執行。

總結

賽門鐵克 DLP 雲端電子郵件服務 (Symantec DLP Cloud Service for Email) 為 Microsoft Office 365 和 Google Workspace 等雲端電子郵件平台的安全挑戰，提供全面的解決方案。雖然這些平台提供顯著的業務優勢，但其內建的防護功能往往無法真正有效抵禦勒索軟體、網路釣魚和商業電子郵件詐騙 (BEC) 等進階威脅。賽門鐵克解決方案透過強大的資料外洩防護、進階威脅偵測以及與賽門鐵克 ESS 技術的無縫整合，彌補這些不足。此解決方案具備 Skeptic 掃描、即時監控、直覺的政策編寫和自動化事件回應等工具，可確保主動防禦不斷演變的網路攻擊，同時最大限度地減少誤報。憑藉全球最大的民用情報網路和嚴格的服務等級協議 (SLA) 保障，賽門鐵克解決方案使企業能夠享受雲端電子郵件的優勢，而不必犧牲安全性。

保安資訊 SAVETIME INFORMATION SECURITY

保安資訊有限公司｜地址：台中市南屯區三和街 150 號

電話：0800-381500｜+886 4 23815000｜www.savetime.com.tw