

產品簡介

一覽

運用分層式閘道防護與政策控管，保護內部部署與私有雲的郵件架構，抵禦網路釣魚、勒索軟體、身分冒用與資料外洩等威脅。

商業效益

- 降低電子郵件攻擊風險
- 自主掌控電子郵件基礎架構與部署選擇
- 強化機敏通訊的治理與法規遵循
- 提升資安與郵件團隊的可視性與作業效率

主要功能

- 惡意程式與垃圾郵件防護
- 網路釣魚、身分冒用與商務電子郵件詐騙 (BEC) 防護
- 魚叉式網路釣魚與勒索軟體防護
- 目錄擷取攻擊與外寄垃圾郵件控管
- 內建資料外洩防護 (DLP)
- 完整稽核與郵件可視性

Messaging Gateway (郵件安全閘道)

因應當前威脅態勢的全方位電子郵件防護

概觀

電子郵件至今仍是入侵企業最快速的途徑之一，攻擊者也愈來愈常運用網路釣魚、勒索軟體與身分冒用手法，同時鎖定一般使用者與高階主管。許多組織雖然需要這個層級的防護，卻因法規、資料落地、架構或作業上的要求，必須將電子郵件系統維持在內部部署或私有雲端環境中。

Symantec® Messaging Gateway 專為自行管理電子郵件基礎架構的企業提供設備式(軟硬體整合或虛擬設備)防護，針對勒索軟體、魚叉式網路釣魚、商業電子郵件詐騙(BEC)、垃圾郵件及資料外洩，提供分層式的入埠與離埠安全防護。此方案整合多層偵測技術、進階內容過濾、內建資料保護與詳細稽核功能，並支援實體或虛擬設備架構，讓組織能在自有環境中擴充與管理。若有更進階的需求，Messaging Gateway 還可搭配 Symantec DLP for Email Security、內容加密與內容分析功能，使內部部署的電子郵件安全與更全面的資料保護及威脅偵測策略緊密整合。

為何需要超越基本的電子郵件防護

電子郵件依然是攻擊者接觸企業使用者最簡便的途徑。現今的攻擊活動常同時結合網路釣魚、勒索軟體、商務電子郵件詐騙與身分冒用等手法，不僅使用者難以辨識，基本的過濾機制也往往無法持續準確地攔截。許多企業雖然需要更強大的電子郵件安全防護，卻受限於法規遵循、資料主權、內部架構標準，或必須直接掌控郵件基礎架構等要求，而無法採用公有雲服務。

僅依賴基本的郵件伺服器控管或老舊的閘道防護機制，會在防禦、可視性與治理三個層面留下缺口。精密的攻擊手法能繞過靜態過濾機制，例如將連結或附件武器化，或藏身於看似合法的郵件中，以躲過簡單的信譽檢查。資安主管與郵件團隊需要分層式的控管機制，才能在郵件遞送前攔截威脅、落實外寄資料保護政策，並提供稽核與 SIEM 整合能力，使電子郵件安全與整體風險管理及法規遵循目標一致。

認識 Symantec Messaging Gateway

Symantec Messaging Gateway 提供超越基本過濾機制的分層式設備式防護，協助組織保障內部部署與私有雲環境中的電子郵件安全。此方案可防護進出郵件，抵禦惡意程式、垃圾郵件、網路釣魚、身分冒用、勒索軟體及其他郵件威脅，同時讓資安團隊能全面掌握郵件流量，並以政策進行控管。主要功能如下：

- **惡意程式與垃圾郵件防護：**結合多層偵測技術、信譽分析、啟發式分析與客戶專屬規則，在惡意附件、連結與大量廣告郵件送達使用者之前加以攔截，垃圾郵件攔截率超過 99%。

- **網路釣魚、身分冒用與商務電子郵件詐騙(BEC)防護：**結合 BEC 分析引擎與網域情資，並支援 DMARC、DKIM 與 SPF 驗證，偵測並攔截商務電子郵件詐騙、寄件人偽造與身分冒用等郵件。
- **魚叉式網路釣魚與勒索軟體防護：**透過 URL 信譽過濾機制攔截惡意連結，並在郵件遞送前，清除 Microsoft Office 與 PDF 附件中的零時差威脅，避免使用者遭受針對性勒索軟體攻擊。
- **目錄擷取攻擊與外寄垃圾郵件控管：**運用全球與本地寄件者信譽情資，攔截垃圾郵件與目錄擷取攻擊，並透過外寄流量控管，防止遭入侵的內部帳戶被用來大量發送垃圾郵件。
- **內建資料外洩防護：**運用內建字典、樣式與政策範本，靈活建立內容與法規遵循控管機制，並自動對傳輸中的郵件啟用 SMTP over TLS 加密。
- **詳細稽核與可視性：**透過單一網頁主控台，提供儀表板、可自訂報表、郵件追蹤與 SIEM 整合，協助監控威脅、調查事件，並落實法規遵循。

進階威脅檢測與資料保護模組

對於有更進階需求的組織，Messaging Gateway 可搭配附加模組，在不變更既有電子郵件架構的前提下，提升威脅偵測能力、擴大資料保護範圍，並強化加密功能。

- **適用複雜政策的進階DLP：**Symantec DLP for Email Security 可強化 Messaging Gateway 內建的郵件防護，提供更完整的政策控管、更彈性的工作流程，以及跨電子郵件、端點、網路、雲端、行動裝置與儲存環境的整合能力，進一步強化治理與法規遵循。
- **進階電子郵件加密服務：**Symantec PGP Gateway Email Encryption 新增依政策自動執行的推播式、提取式與透過式加密選項，協助組織保護機敏通訊、符合隱私與法規要求，同時免除自行管理金鑰或數位憑證的繁瑣。
- **進階威脅偵測與沙箱分析：**Symantec Content Analysis 提供多層檔案偵測功能，整合靜態分析、機器學習、防毒掃描與風險評分，並搭配內部部署或雲端沙箱引爆技術，找出可疑內容中的未知威脅與刻意規避偵測的威脅。

如需更多資訊，請造訪我們的網站：<https://www.savetime.com.tw/>

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政策性整合式解決方案，在端點、雲端和基礎架構中有效地抵禦最複雜的攻擊。賽門鐵克經營的安全情報網是全球規模最大的民間情報網路之一，因此能成功偵測最進階的威脅，進而提供完善的防護措施。

若想瞭解更多資訊，請造訪原廠網站 <https://www.broadcom.com/solutions/integrated-cyber-defense> 或

賽門鐵克解決方案專家：保安資訊有限公司的中文網站 <https://www.savetime.com.tw/> (好記：幫您節省時間，的公司，在台灣)

商業效益

- **降低電子郵件攻擊風險：**在進出郵件流程中加入分層式閘道防護，避免網路釣魚、勒索軟體、商務電子郵件詐騙與垃圾郵件演變成重大營運事件。資安團隊能在郵件傳送過程中提前預防，於威脅送達使用者之前加以攔截，阻斷常見的攻擊途徑。
- **掌控電子郵件基礎架構：**許多組織因法規遵循、資料落地或系統架構要求，必須將電子郵件安全維持在內部部署或私有雲環境。Messaging Gateway 採用由客戶自行管理的部署方式，提供企業級電子郵件防護，讓組織無須將郵件基礎架構遷移至公有雲服務。
- **強化機敏通訊的治理與法規遵循：**結合內建DLP、自動TLS加密，並可搭配進階DLP與內容加密模組，對機敏郵件執行一致的資料保護與加密政策，協助組織符合法規遵循、內部治理標準與稽核要求，同時確保機敏通訊的安全。
- **提升資安與郵件團隊的可視性與作業效率：**透過集中式政策控管、詳細稽核、內建與可自訂報表及SIEM整合，簡化管理作業。團隊能更快調查郵件活動、更有效掌握威脅趨勢，並在複雜環境中集中管理大規模的電子郵件防護部署。

為何選擇 Symantec 解決方案

Symantec 長期為大型、複雜的環境提供防護，這類環境中的電子郵件始終是主要的攻擊途徑，其中也包含必須將郵件基礎架構維持在內部部署或私有雲的企業。憑藉這些經驗，Messaging Gateway 提供超越基本過濾機制的分層式防護，可因應惡意程式、垃圾郵件、網路釣魚、身分冒用與商務電子郵件詐騙等威脅，並內建政策式資料保護，協助組織在掌控電子郵件安全架構的同時，降低電子郵件攻擊風險。

當需求持續成長時，組織可在 Messaging Gateway 之外，搭配 Symantec 進階 DLP、PGP 電子郵件加密與更完整的威脅偵測功能，並與更全面的端點、網頁及資料保護策略整合。憑藉 Symantec Integrated Cyber Defense Platform、全球支援服務與成熟的企業維運經驗，資安團隊能將內部部署與私有雲的電子郵件環境，納入整體安全架構，成為不可或缺的一環，而非各自獨立的單點解決方案。