產品型錄

Symantec Messaging Gateway 10.6

Symantec™ Messaging Gateway 利用單一平台提供內部部署的入埠與離埠訊息安全。攔截超過 99% 的垃圾郵件，誤報率低於百萬分之一，具備即時自動垃圾郵件防止與惡意軟體防止更新，可有效回應最新的訊息威脅。利用深入的報告功能，管理員便能將重心放在企業的整體安全措施上，重要高階主管與管理階層則可獲得他們所需的能見度。

Messaging Gateway 可作為虛擬或實體硬體裝置建置，讓您輕鬆擴充容量，即使垃圾郵件數量增加，也能流暢傳送訊息。

依據「IDC MarketScape：2016 年全球電子郵件安全廠商評估」資料指出，賽門鐵克為訊息安全市場整體營收最高的的領導廠商。

立即阻止進階威脅

Messaging Gateway 使用進階的多層式偵測技術和 Symantec Global Intelligence Network 提供的即時威脅情報，能夠立即阻止進階威脅。

多層式垃圾郵件與惡意軟體過濾	目標式攻擊防護	完整威脅情報	內容過濾與防止資料外洩
封鎖不當的電子郵件，避免傳送惡意連結與附件。	取得最佳防護，抵禦魚叉式網路釣魚、勒索軟體與 BEC 攻擊。	提供詳細的威脅分析與風險評分，以加快矯正的速度。	內容過濾，達到全面性入埠防護。避免公司機密資訊外洩。

圖 1 Symantec Messaging Gateway 使用進階的多層式偵測技術

Symantec

結合多層式偵測與完整威脅情報，透過強大的防護功能來抵禦魚叉式網路釣魚、企業電子郵件入侵 (BEC)、勒索軟體與其他進階威脅：

- 結合賽門鐵克全球與本地寄件者信譽資料庫和客戶專屬垃圾郵件規則，對垃圾郵件加以封鎖，攔截多達 90% 的不當電子郵件，使這些郵件無法進入您的網路。
- 利用進階的啟發式偵測技術來掃描電子郵件，並透過網域情報遏止網址綁架與身分詐騙，防堵魚叉式網路釣魚與 BEC。
- 移除 Microsoft Office® 和 PDF 附件中的零時差文件威脅，保護使用者免於勒索軟體之類的目標式攻擊。Messaging Gateway 可移除附件中可能的主動式惡意內容，並重建無毒的文件，再將文件附加到電子郵件內，然後寄給使用者。
- 利用以賽門鐵克全球資料庫為基礎的網址信譽過濾技術，抵禦電子郵件內的惡意連結。

保護電子郵件內的機密資料

Messaging Gateway 內建防止資料外洩與政策型加密控制，可封鎖、隔離或加密機密的電子郵件，避免資訊外洩。讓您減少花在控制電子郵件中分享敏感資料的時間，同時達成法規遵循與隱私權要求：

- 進階內容過濾控制可避免使用者收到不當的電子郵件，防止資料外洩技術可更輕鬆保護及控制機密資料。管理員可輕鬆建立有效且彈性的政策，透過利用特徵比對並識別出訊息或附件內真正的公司資料，藉此執行法規遵循規定，避免資料外洩。
- 政策導向的電子郵件加密可依照客戶指定的條件來評估訊息。假如需要加密，便將訊息寄送至 Symantec Content Encryption，這是一項可透過託管服務或在內部資料中心建置的附加功能。
- 與領先市場的 Symantec Data Loss Prevention 緊密整合，針對電子郵件內的敏感資訊提供監控與強制執行點。

管理訊息安全基礎架構，減少工作負荷

透過單一的網頁式主控台，提供包含威脅趨勢、攻擊統計資料與未遵循事件的整合檢視，簡化混合型 IPv6/IPv4 環境中多台 Messaging Gateway 硬體裝置的管理作業。Messaging Gateway 免除了使用多個主控台、不同政策以及不相容的記錄與報告程序帶來的複雜性，大幅降低訊息安全基礎架構的整體持有成本：

- 儀表板、摘要與詳細報告，包含 50 種可用內容或時間及排程產生自訂的預設報告，以找出威脅趨勢和潛在的法規遵循問題。
- 產生的系統日誌資料可匯出至第三方的安全資訊與事件管理工具，進行進一步的分析。
- 利用圖形式訊息稽核介面，快速判斷訊息的處理與傳送狀態，輕鬆進行訊息追蹤。
- 可自訂式政策定義，過濾電子報和其他行銷內容等不當電子郵件的傳送。

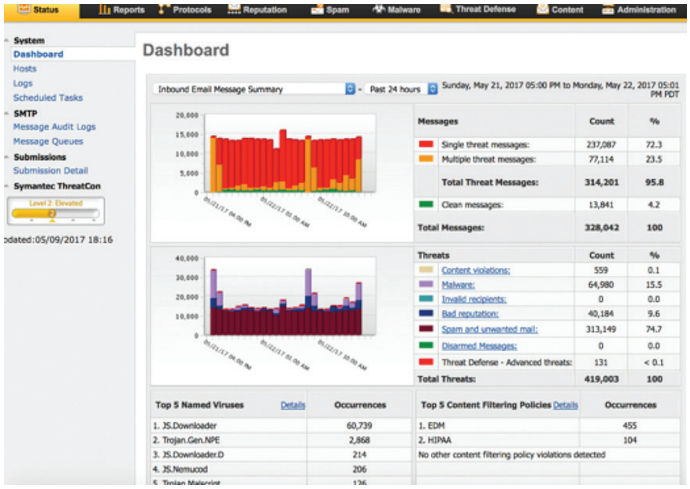

圖 2 Symantec Messaging Gateway 主控台

與 Symantec Content and Malware Analysis 整合

為了執行額外的進階威脅防護功能，Messaging Gateway 會將訊息內容卸載至 Symantec Content and Malware Analysis，以進行進一步的檢查，包括結合靜態、動態、信譽與 YARA 規則等分析技巧，提供可採取行動的情報。可彈性調適且可自訂式沙箱能提供全方位的惡意軟體揭露功能，迅速分析可疑的檔案與網址，與執行中的惡意軟體互動，以揭露其完整行為，同時找出零時差威脅與未知的惡意軟體。

系統需求

虛擬裝置選項 (相同的特色與功能)

- VMware ESXi™/VMware ESX®、VMware vSphere® 5.x、6.x
- Microsoft Hyper-V® 2008 或 2012

瀏覽器 (用於管理主控台)

- Microsoft Internet Explorer® 11.0 或更高版本
- Mozilla® Firefox® 45 或更高版本
- Google Chrome™ 55 或更高版本

	Symantec Messaging Gateway 8340	Symantec Messaging Gateway 8380
組織規模	中小企業	大型企業
一般建置	結合控制中心/掃描程式、專屬掃描程式或專屬控制中心	結合控制中心/掃描程式、專屬掃描程式或專屬控制中心
外型尺寸	1RU 機架安裝	1RU 機架安裝
電源供應器	單一	備援的熱抽換式自動切換通用電源供應器
處理器	1 x 四核心處理器	2 x 六核心處理器
硬碟/RAID	2 x 1 TB SAS RAID 1	6 x 300 GB Serial-attach SCSI (熱抽換式) RAID 10
NIC	Gigabit 乙太網路連接埠	Gigabit 乙太網路連接埠

Symantec Messaging Gateway 8300 系列硬體裝置

深入瞭解 **Symantec Messaging Gateway**。

深入瞭解 **Symantec Content and Malware Analysis**。

關於賽門鐵克

賽門鐵克公司 (NASDAQ：SYMC)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、雲端和基礎架構中有效地抵禦最複雜的攻擊。同樣地，全球各地超過 5,000 萬的人們和家庭社群，也仰賴賽門鐵克的諾頓產品和 LifeLock 產品套裝軟體來保護自身的居家數位生活及各種裝置。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 www.symantec.com.tw。

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.tw